With the support of the Erasmus+ Programme of the European Union

EULIoT

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Факультет соціології і права

ЗБІРНИК МАТЕРІАЛІВ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ

ІНТЕРНЕТ РЕЧЕЙ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

05 травня 2023 року

КИЇВ
2023

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ:

Баранов О.А. - *доктор юридичних наук, професор, Керівник наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права» Національної академії правових наук України». Академічний лідер проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Головко О.М. - *кандидат юридичних наук, старший дослідник, старший викладач кафедри інтелектуальної власності та приватного права, КПІ ім. Ігоря Сікорського. Координатор проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Дубняк М.В. - *кандидат юридичних наук, старший викладач кафедри інформаційного, господарського та адміністративного права, КПІ ім. Ігоря Сікорського. Менеджер проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Видання рекомендоване до друку рішенням
Вченої ради факультету соціології і права
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
(протокол N 9 від 17.05.2023 року)

Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції: зб.матеріалів Міжнародної науково-практичної конференції (05.05.2023, м. Київ) : ел. збірник / Упоряд.: Баранов О.А., Головко О.М., Дубняк М.В. – Київ : КПІ ім. Ігоря Сікорського, 2023. – 296 с.

У конференції взяли участь провідні експерти та вчені наукових установ і навчальних закладів, викладачі закладів вищої освіти, представники правничих професій, а також молоді вчені та студенти.

Рекомендується науковцям, державним службовцям, підприємцям, правникам, викладачам, студентам та аспірантам, а також усім, хто цікавиться проблемами правового регулювання суспільних відносин у сфері застосування штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, хмарних технологій, великих даних та інших складових Інтернету речей (IoT), правовим забезпеченням цифрової трансформації, дослідженням національного законодавства та законодавства Європейського Союзу з питань забезпечення кібербезпеки, вільного обігу даних, захисту персональних даних.

Матеріали подано в авторській редакції.

Конференцію проведено в рамках реалізації міжнародного проекту у сфері освіти «Європейська інтеграція: законодавство та Інтернет речей» у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE (спільний проект КПІ ім. Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)».

Зміст

Програмні питання конференції

Секція 1. Проблеми правового регулювання суспільних відносин в сфері застосування штучного інтелекту, робототехніки, криптовалют, технологій блокчейн «хмарних» технологій, «великих даних» та інших складових Інтернету речей.

Секція 2. Правове забезпечення цифрової трансформації на основі впровадження технологій Інтернету речей у різних сферах діяльності: економіці, Індустрії 4.0, сільському господарстві, охороні здоров'я, комунальному господарстві (розумні міста, вулиці, будинки), транспорті (автономні автомобілі, розумні дороги, дрони тощо), управлінні державою, роздрібної торгівлі тощо.

Секція 3. Порівняльно-правові дослідження національного законодавства та законодавства Європейського Союзу з питань забезпечення кібербезпеки та вільного обігу даних, захисту персональних даних, застосування хмарних технологій та технологій блокчейну тощо.

Секція 4. Проблеми визначення юридичної відповідальності при застосуванні технологій Інтернету речей.

BRUSENTSEVA Irina

Prosecutor of the department of the Dnipropetrovsk Region Prosecutor's Office, Dnipro, Ukraine
ORCID: https://orcid.org/0009-0002-8238-2649
e-mail: law-dp@ukr.net

A DIGITAL STRATEGY FOR THE INVESTIGATIONOF THE INTERNET OF THINGS BREACHES

Abstract. The thesis raises issues related to the investigation of criminogenic events related to the use of the Internet of Things (IoT) because in this case, the evidence depends on the proper approach to gathering proof, namely IoT data. The implementation of traditional protocols is outdated, which complicates prosecution. In this regard, the author of this work proposes an investigation structure to solve the specified problem and to improve the analysis of IoT processing through the digital examination of data concentrated in IoT cloud computing infrastructures. Thus, the author emphasizes the lack of standardisation of evidence documentation in the context of IoT crime-alike usage and offers strategy research for IoT data investigation.

Keywords: digital forensics, IoT investigation, data transmission, evidence expertise.

Анотація. Дослідницька робота порушує проблеми належного рослідування криміногенних подій пов'язаних із застосуванням Інтернет Речей (IoT), тому що у такому разі доказування залежить від належного підходу у зборі доказів, а саме IoT даних. Впровадження традиційних протоколів є застарілим, що ускладнює прокурорське розслідування, тому пропонується удосконалити аналіз даних, що оброблюються IoT, шляхом цифрової експертизи даних зосереджених в інфраструктурах хмарних обчислень IoT. Окрім того, автор наголошує на відсутності стандартизації документування доказів в контексті злочинного використання IoT та пропонує цифрову стратегію для дослідження IoT даних слідством.
Ключові слова: цифрова експертиза, IoT розслідування, передача даних, дослідження доказів.

A. Problem

This new condition gives a rich arrangement of information sources; when utilized as a part of conjunction with each other, they can significantly illuminate a verifiable circumstance that may have happened with

practically zero solid human witness confirmation [3, p. 195]. Therefore, vendors usually dedicate sections to their products' privacy policies [2]. These policies cover data collection, data use, data storage, and the security of user data [ibid.]. On the other side, the implementation and adaptation of traditional security protocols solutions remain a challenge making it difficult to provide confidentiality of data transmission [7, p. 229]. This uncertainty could be defined as follows [5, p. 62]:

- ✓ Uncertainty in authentication stems from the incompleteness of information regarding the likelihood of whether the acceptance of an authentication request leads to an incident.
- ✓ Uncertainty in authorization stems from the incompleteness of data regarding the likelihood that an authorized action of a subject could lead to an incident.

Hence, considerable IoT appliances incorporate license concurrences which shield the business from litigation if the apparatus were to malfunction and force fatalities. Traditional prosecution offered a design reconstruction, semantic breakdown, and expert acquaintance practice correlated with a formal-timeline reconstruction and incident modelling. These approaches work well for traditional investigations based on web browsing or even executable binaries on computers [9, p. 13]. However, their proposed correlation methods are not

yet compatible with investigations based on IoT devices, particularly on digesting evidence sources such as firmware images and network packet captures [ibid.]. If negligence, by not following security best practices, is not a criminal offence, then organisations do not have an incentive to apply security by design, if menial and simple license agreements allow organisations to defer them from any liability then it would suggest that the lack of liability directive could have an impact on maintaining the longevity of an IoT device [7, p. 263]. The methods also do not yet classify IoT evidence sources based on internationally agreed standards (such as ISO27050e1:2019 and ISO30141:2018) despite having their own proposed ontology [9, p. 13]. Therefore, the prosecution of IoT data poses complexity around three issues [10, p. 6]:

1. The onboard data storage is not accessible via traditional digital forensics methods.
2. The cumulative dataset may exist in multiple locations.
3. Even if the data is acquired it may not be readable or accessible with existing tools.

B. Solution

Considering the above, many organisations attempt to include threat data feeds into their networks or systems without fully understanding how to deal with a daily flood of data filled with extraneous information across their

security systems [7, p. 49]. This emphasises the need for such security analysis to better secure such devices and protect users' privacy, and the need to provide independent kite-marking or similar to certify that the device has passed tests [2]. The possible framework analysis comprises seven phases, as follows [5, pp. 78-83]:

1. Readiness: This phase is concerned with understanding the architecture and technologies involved in deploying and maintaining a private cloud infrastructure such as data model, software/hardware components, network header, file format, programming syntax, and commands. As it is not realistic to expect any practitioner to be well-versed in every cloud computing technology and the underlying infrastructure (e.g. servers and client devices), a research or review of the documentation is essential to familiarise one with the potential approaches, tools or expertise required in the collecting and analysing of data, scoping the investigation boundaries, setting up the forensic workstation, or even refuting any defense that a piece of evidence was associated with the target cloud platform during a case trial;

2. Case Investigation Preparation: In this phase, the investigators prepare search warrants, with the assistance of the forensic practitioners. The latter also helps to gather information regarding the organisation-specific cloud deployment, determine the potential effects on an

investigation, and identify third-party service providers (if any) for cooperation;

3. Evidence Source Identification: In this phase, possible sources of evidence are identified and seized. The phase typically commences with the identification of client devices such as desktop computers, laptops, and mobile devices. During the second (or subsequent) iteration, the practitioner identifies the remote hardware (typically a cloud hosting server, peer node, etc.) that the client devices were connected to, based on the corresponding IP addresses, node identifications (IDs), computer names, and other relevant identifying information recovered from the client devices. The identity of the suspicious host could be validated by contacting the IP address owner (e.g. via the WHOIS query), seeking assistance from the Internet Service Provider (ISP), researching the IP address history (via the network traffic, Security Operation Centre logs, incident response archives, Internet search engines, etc.), and looking for clues in the data or log files;

4. Collection and Preservation of Evidence: In this phase, the evidence is collected and preserved. Once the file system is preserved, a forensic browser can be used to extract potential evidence from the working copy(ies), including cloud instances with an uncommon or proprietary format (bencode file, MySQL database, etc) for analysis using vendor-specific tools in latter phases (hence, preserve

and collect). In a situation when a physical acquisition is not possible, this phase commences with the logical acquisition (collection) of the visible data structures on the target system. As the structure of the data directory may vary it is recommended to fully copy the user's data directory. If the directory is huge and too complex to be copied in full, then the practitioners may copy directories matching keywords of interest (e.g. name of application, vendor, or specific components) provisioned during the Readiness phase;

5. Evidence Analysis and Reconstruction: In this phase, collected shreds of evidence are processed, analysed, and interpreted in a forensically sound manner. It is during this phase that the practitioners attempt to recover information useful for establishing connections between the suspect and the crime. The evidential data may potentially reveal the location(s) of the server or corresponding nodes, and subsequently lead to a second or more iterations of the process;

6. Presentation and Reporting: This phase involves the legal presentation of the collected evidential data in a court of law in a unified format;

7. Investigation Review and Lessons Learned: Finally, the practitioners review the investigative process, determine any problems that may need to be remediated, and document the lessons learned for future reference. The

learned lessons are great resources for the readiness phase of future investigations.

Finally, IoT operations are of significant prosecution interest among the software activities of IoT apparatuses. The research has shown, high-end IoT devices rely on cryptographic encryption to secure data both onboard and during transmission over networks. Respectively, the study proposes the feasibility to detect when IoT performs data encryption operations automatically. Sayakkara et al. [8, pp. S97-S99] provide an outline of the data acquisition process, data preprocessing, and classification into classes. Furthermore, prosecutors must interpret analysed IoT data in a meaningful way. For example, in the subject of heavy vehicle data, diagnostic software is typically penned by the original equipment manufacturers (OEMs) to interpret the data. While some OEMs offer additional data reporting tools, which can be valuable in reconstructing crashes, these programs lack certain safeguards necessary for ensuring dedicated prosecution. Therefore, according to Fagbola and Venter [6, p. 17] might be useful the concept of shadow IoT device digital forensic readiness because it is vital as a complementary approach to shadow Internet of Things forensics, investigation, and attack prevention. Thus, operatives need to be aware of these limitations and take them into account when analysing IoT. Accordingly,

the thesis proposes to look into data understanding triple implications [4, pp. 113-118]:

- ✓ Standards-Based Meaning: Most of the research presented in the literature so far has focused on comparing interpreted values to external instrumentation to verify the correctness of those values. Arguably, this is all that is necessary for an expert to establish the meaning of the data. There are, however, standards that help interpret data in engineering units as those specified in communications standards.
- ✓ Proprietary Meaning: Most new IoTs contain some event data recording capability. While it may be tempting to trust the interpretation of the OEM software, research has shown that the interpretation of the data may be an issue. Establishing and verifying the meaning of all data elements in digital records is a formidable task.
- ✓ Daily Engine Usage: Examining the digital record at the byte level and matching the hex data enables investigators to know what data were recorded and what data are calculated.

The identified above approaches in both framework standard phases and practical IoT data prosecution can conform to investigation direction and digital forensic improvement. Thus, Al-Dhaqm et al. [1, pp. 152492-152493] suggest a potential digital solution to address the identified gaps including:

- ✓ Subdomain-based metamodeling language: This can include attempts that aim to develop a formal language for the digital forensic domains using the metamodeling approach. It would, however, require initial metamodeling of the various subdomains that constitute the digital forensic domain.
- ✓ Domain-based ontology: like the metamodeling approach, the use of ontology and semantics have been explored as an approach to develop a standardized baseline for the domain. This approach can be used to reveal the degree of interdependencies among the various subdomains.
- ✓ Integrated framework for subdomains: studies have explored the potential of integrating diverse subdomain frameworks into a unified integrated framework. This logic can be adapted for the digital forensic domain. Investigation frameworks that can provide a reliable guide for developing a standard forensic process for the forensic domain remain a viable approach toward addressing some of the challenges.
- ✓ Harmonized integration process: Approaches that attempt to merge or harmonize processes from different subdomains present a potential to address the growing diversity of process models among the various subdomains. This can be further leveraged to develop a mechanism for a context-independent data collection

process. However, this approach can further integrate semantic logic. In essence, the process of developing a harmonized approach can rely on the semantics associated with the respective subdomain, to prevent redundancies.

- ✓ Structured representation of subdomain data: this is a major challenge within the digital forensic subdomain. Approaches that attempt to formalize data representation, and structured queries of potential digital artifacts evidence representation (in a context-independent manner) are a potential solution to data heterogeneity and the lack of a unified data format. Furthermore, the development of a structure representation is a required step toward forensic automation. Forensic automation has been considered a futuristic approach for digital forensics, which has the potential to reduce the dependency on human errors. Consequently, reduce investigation biases, enhance evidence reliability as well as reduce investigation time. Automation in this regard refers to the act of using machines to carry out some forensic processes with minimal or no human oversight. As a step towards developing a subdomain metamodel, for example, this study further proposes a metamodeling approach as a complementary process towards a generic digital forensic domain modelling.

C. Conclusion

The IoT presents many challenges to digital prosecution due to the complexity of the devices and the volume of data they produce. The traditional methods of exploration are not fully compatible with IoT devices, particularly when it comes to digesting evidence, but also lack of security by design creates a barrier to data privacy and security. To address these challenges, organisations need to include threat data feeds into their networks or systems to better secure IoT devices against data breaches.

A possible framework analysis incorporating seven phases to discourse IoT digital prosecution, including (i) readiness, (ii) case investigation preparation, (iii) evidence source identification, (iiii) collection and preservation of evidence, (iiiii) analysis, (iiiiii) reporting, and (iiiiiii) declaration of evidence. Comprehensively, prosecutors need to adapt to the unique challenges presented by IoT devices and continue to develop new methods to address them effectively.

REFERENCES:

1. Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K.-K. R., Al-Rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*, *9*, 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

2. Alharbi, R., & Aspinall, D. (2018). An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities. *IET Conference Proceedings*. https://doi.org/10.1049/cp.2018.0047
3. Banday, M. (2017). Enhancing the security of IOT in forensics. *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, 193–198. https://doi.org/10.1109/IC3TSN.2017.8284475
4. D'Anna, G. D. (2018). *Cybersecurity for commercial vehicles* (1st ed.). SAE International. https://doi.org/10.4271/R-464
5. Dehghantanha, A., & Choo, K.-K. R. (2019). *Handbook of Big Data and IoT Security* (A. Dehghantanha & K.-K. R. Choo, Eds.; 1st ed. 2019.). Springer International Publishing. https://doi.org/10.1007/978-3-030-10543-3
6. Fagbola, F. I., & Venter, H. S. (2022). Smart Digital Forensic Readiness Model for Shadow IoT Devices. *Applied Sciences*, *12*(2), 730–. https://doi.org/10.3390/app12020730
7. Montasari, R. (2021). *Digital forensic investigation of Internet of Things (IoT) devices* (R. Montasari, Ed.). Springer. https://doi.org/10.1007/978-3-030-60425-7
8. Sayakkara, A., Le-Khac, N.-A., & Scanlon, M. (2019). Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices. *Digital*

Investigation, *29*, S94–S103. https://doi.org/10.1016/j.diin.2019.04.012

9. Tok, Y. C., Wang, C., & Chattopadhyay, S. (2020). Stitcher: Correlating digital forensic evidence on internet-of-things devices. *Forensic Science International: Digital Investigation*, *35*, 301071–. https://doi.org/10.1016/j.fsidi.2020.301071
10. 10.Watson, S., & Dehghantanha, A. (2016). Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud & Security*, *2016*(6), 5–8. https://doi.org/10.1016/S1361-3723(15)30045-2

BULGAKOVA Valentyna A.

Pedagogue-Methodist of the Highest Category,
Supervisor of scientific manuscripts on history, sociology,
and law in Dnipropetrovsk Oblast', Gymnasium No. 91,
Kryvyi Rih, Ukraine
ORCID: https://orcid.org/0009-0009-6463-5228
e-mail: krotona24@gmail.com

A DIGITAL TRANSFORMATION OF EDUCATION TOWARDS EUROPEAN UNION IMPLEMENTATION OF THE INTERNET OF THINGS

Abstract. The digital transformation of education towards the European Union's implementation of the Internet of Things (IoT) presents a significant challenge for the educational process. This report highlights two important aspects of this theme: IoT interoperability across education and policy implementation of IoT for the learning process. The study indicates that the interaction between IoT platforms plays a crucial methodological role in facilitating communication among the participants of the educational process. Moreover, the IoT implementation program should focus not only on self-efficacy but also provide a clear plan for the IoT benefit by authorised participants of a particular

lesson especially during online learning. Therefore, the author suggests bearing these approaches into account to ensure successful IoT integration into education because it brings a positive impact on educational practice.
Keywords: IoT interoperability, smart campus, associative learning, integration platforms, logging data

Анотація. Цифрова трансформація у зв'язку з Європейським напрямком у впровадженні Інтернет Речей (IoT) є викликом для змін освітнього процесу. Тому дана стаття розглядає два важливі аспекти цієї теми: міжопераційність IoT для сумісності з викладанням і засвоєнням матеріалу відповідно, а також програма впровадження IoT в освіті. Дослідження показало, що взаємодія між платформами IoT має ключове методологічне значення обміну між учасниками навчального процесу. З іншої сторони програма впровадження IoT має бути зосереджена не лише на самоефективності, а й перебачати план використання IoT авторизованими учасниками того чи іншого уроку особливо під час онлайн-навчання. Отже, автор даної роботи пропонує врахувати вказані підходи до IoT, щоб забезпечити успішну інтеграцію IoT в освіту та мати позитивний вплив на навчальну практику.

Ключові слова: інтероперабільність IoT, розумний кампус, асоціативне навчання, інтеграційні платформи, авторизація

A. The IoT interoperability across education

The Internet of Things (IoT) is changing the way technology is used for the benefit of humans and the environment. Since the very beginning, IoT solutions were, and still are, mostly use-case-centric, resulting in the creation of various "IoT silos" [5, p. 119]. Every day the number of interconnected elements (objects) is increasing to provide information in real-time about the environment and its characteristics. Through the Digitising European Industry focus area, the EU prioritises ecosystem building, platform interoperability, technology integration, standardisation, and validation through large-scale pilots and experimentation facilities [3].

From an application perspective, the IoT and digital technologies are the key enablers for digital transformation in various sectors [ibid.]. Education is not distant from this EU course to heighten scholarly material and generate stimuli in educational activities. Interoperability can, of course, be "hard-wired," enabling total control over the whole process, and giving many possibilities for optimization [5, p. 119]. One of the changes is that objects go from being passive elements in educational

environments to becoming more active objects and more involved in supporting teaching [7, p. 202]. The role of technology should be to empower education and to create a motivational approach to educating young learners. For that reasoning, the learning methods are digital twofold adaptive: to comprehend the psyche of higher teaching learners toward scholastic IoT; to rev 'the shape of mind' adoption towards IoT discretions. The student-centric IoT applications should be developed in such a way that through connected and self-managed various IoT devices students are able to access, study, and propose academic concepts.

An alternative to proprietary platforms is FIWARE, the result of public-private collaboration that delivers tools and forms an innovation ecosystem for the creation of new applications and services on the Internet. Among the A16 Accelerator Programme that has been promoting the adoption of the FIWARE technical resources and assets, FI-ADOPT has distinguished its activity by focusing on certain areas where the development and impact of present and future solutions and digital services will be deeply determined by the integration of Open Source technologies: establishing and supporting continuous corporate and citizen’s learning and training; promoting and facilitating healthy behavioral dynamics and wellbeing shaping among the society and finally easing social and cultural integration

[4]. Furthermore, it is beneficial for enabling the applicable concept of smart campus because it ensures interoperability and the establishment of standard data models. Accordingly, an IoT-based smart campus includes objects like an IoT-based E-learning facility, IoT-based classroom, and laboratory, IoT-based sensors for sharing of notes, IoT-based sensors for mobile applications, and IoT-supported in-campus hotspots [6, p. 67]. Here, the "inter-silo" interoperability is of great importance, but achieving it across the IoT silos, or more generally, IoT platforms seems crucial for the future of the IoT [5, p. 119]. There, most likely, a “bridge” will have to be instantiated between the new platform and each of the already connected ones [ibid.].

B. The policy implementation of IoT for the learning process

The idea of connecting intelligent networks managed through the web and interaction with humans is in accordance with the evolution of e-learning, m-learning, and ubiquitous learning technology [Syakroni p. 3]. In order to develop IoT education adoption intention, implementation policy should hold self-efficacy because the feeling of inadequacy or insecurity (not being good enough) leads to students’ anxiety about their ability to handle digital products for online learning situations [9, p. 63].

Associative learning is one such beneficial theoretical concept to produce students understanding reasonably and involvement in the learning process via IoT real-time examples. Technologies such as augmented reality, 3D animation, and visual graphics, among others, can help in the implementation of IoT in learning. Similarly, the inclusion of animated activities to assemble and discover pleasantly generates healthy competition and knowledge sharing process. Ciolacu et al. [1] explored current approaches and proposed system architecture for IoT for Education 4.0 with real-time data from embedded sensors from smartphones, smartwatches, and the environment for data collection, storage, and AI analysis with data mining techniques.

Cost-effective network architecture is required at the school and universities level to deal with this data flow [6, p. 64]. It helps to connect, program, and control sensors for building an own IoT system [1]. The curriculum is delivered via an intelligent learning management system; it opens each unit based on student mastery of prior content [8, p. 36]. Rather than moving through age grades, students demonstrate competency over a body of knowledge at their own pace and associate with different learners at their school based on points of interest or association [ibid.] Besides, a real-time feedback system can be developed by the use of IoT technology which can help both students as

well as faculties in coordinating class flow [6, p. 71]. Hence, the thesis report supports the implementation of IoT education projects and learning on the next grounds:

- ✓ IoT provides an integration platform for devices that speak and communicate in ‘languages’ and intercommunicate in totally different ‘languages’ of its users;
- ✓ It allows the connection of open-source operating systems or embedded systems on microcontrollers, including sensor network nodes;
- ✓ IoT's data logging platform for connecting sensors in the cloud authorise connecting to networks such as databases, to the computational knowledge engine. Significantly, authorization policies are security policies, which specify what actions a user or role is allowed (positive authorizations or A+ policies) or not allowed (negative authorizations or A− policies) to perform on a set of target objects or resources (e.g, VM, Data) [12, p. 60];
- ✓ IoT solves education limitations in the areas: of wide geographical coverage, and real-time and independent access.

Therefore, the characteristics of the IoT capable of increasing interactivity and intelligent response between objects, are sufficient capital to contribute to the teaching

and learning process, especially in increasing interactivity between learning participants and learning objects, among fellow learning participants, and between learning objects [11, p. 4]. These consist of different modules such as radiofrequency, sensing, power management, and energy modules to collect and process data [10, p. 138]. The When attribute is used to specify the time in which the policy is applicable. Notable, Opara et al. [12, p. 62] offer optional attributes When, Where, Why, and How constraints, which confine the applicability of the policy. Hereinafter, the attribute Where is used to specify a constraint on the origin for a request to a cloud resource or the physical location(target) where data may be stored. The attribute Why specifies the reason for the access to the cloud resource, while the attribute How specifies the device used to access a cloud resource. Consequently, it is imperative to develop new tools for IoT management that tap into diverse inference, signal processing, communications, and networking techniques, by drawing from fields such as machine learning, optimization, and applied statistics [2, p. 779].

C. Conclusions

A. IoT interoperability in education is important for the growth and benefits of students. Interoperability across education can be achieved through the use of platforms

like FIWARE, which offers tools and innovation ecosystems. At the same time, a smart campus is a vision that can profit from interoperability and stock data bars. However, accomplishing interoperability across IoT outlets is crucial for the future of educational practice, and methodology may need to be created between unexplored and extant platforms. Therefore, cost-effective network architecture and a real-time feedback system would support IoT education projects.

B. The implementation of IoT in the learning process is advantageous for students and can be achieved through self-efficacy policies. Associative learning can aid in IoT performance. At the same time, a cost-effective grid architecture is required to deal with data flow, and a real-time feedback system is suggested for both students and lecturers. Authorization policies are significantly needed since they specify what actions or roles a student and lecturer are entitled or not to accomplish on a set of target objects or resources.

Accordingly to the above outcome, the author accentuates the advantages of IoT in education, including its integration platform for devices, open-source operating systems, and data logging platform models. This solution expands the possibilities beyond traditional teacher-student and student-student interactions, allowing for exchanges with objects. An architecture shall be defined that can be

used to structure educational scenarios and to facilitate the proposed models.

REFERENCES:

1. Ciolacu, M. I., Binder, L., & Popp, H. (2019). Enabling IoT in Education 4.0 with BioSensors from Wearables and Artificial Intelligence. *2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, 17–24. https://doi.org/10.1109/SIITME47687.2019.8990763
2. Chen, T., Barbarossa, S., Wang, X., Giannakis, G. B., & Zhang, Z.-L. (2019). Learning and Management for Internet of Things: Accounting for Adaptivity and Scalability. *Proceedings of the IEEE*, *107*(4), 778–796. https://doi.org/10.1109/JPROC.2019.2896243
3. European Commission (2022). Shaping Europe's digital future, Europe's Internet of Things Policy. Available online: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy
4. FIWARE (2016). FI-ADOPT: Enhancing Education, Heath & Social Integration through Technology. Available online: https://www.fiware.org/2016/05/19/fi-adopt-enhancing-education-heath-social-integration-through-technology/
5. Ganzha, M., Paprzycki, M., Pawłowski, W., Szmeja, P., & Wasielewska, K. (2017). Semantic interoperability in

the Internet of Things: An overview from the INTER-IoT perspective. *Journal of Network and Computer Applications*, *81*, 111–124. https://doi.org/10.1016/j.jnca.2016.08.00

6. Kumar Pani, S., & Pandey, M. (2021). Significance of IoT in the Education Domain. In *Internet of Things: Enabling Technologies, Security and Social Implications* (pp. 59–83). Springer Singapore Pte. Limited. https://doi.org/10.1007/978-981-15-8621-7_6
7. Rocha, Á., Correia, A. M., Adeli, H., Reis, L. P., & Mendonça Teixeira, M. (2016). IoT in Education: Integration of Objects with Virtual Academic Communities. In *New Advances in Information Systems and Technologies* (Vol. 444, pp. 201–212). Springer International Publishing AG. https://doi.org/10.1007/978-3-319-31232-3_19
8. Rodney, B. D. (2020). Understanding the paradigm shift in education in the twenty-first century: The role of technology and the Internet of Things. *Worldwide Hospitality and Tourism Themes*, *12*(1), 35–47. https://doi.org/10.1108/WHATT-10-2019-0068
9. Negm, E. (2023). Intention to use Internet of Things (IoT) in higher education online learning – the effect of technology readiness. *Higher Education, Skills and Work-Based Learning*, *13*(1), 53–65. https://doi.org/10.1108/HESWBL-05-2022-0121

10. 10.Singh, K. K., Singh, A., Cengiz, K., & Le, D.-N. (2020). Significance of Wireless Technology in Internet of Things (IoT). In *Machine Learning and Cognitive Computing for Mobile Communications and Wireless Networks* (pp. 131–154). John Wiley & Sons, Incorporated. https://doi.org/10.1002/9781119640554.ch6
11. Syakroni, A., Zamroni, Muali, C., Baharun, H., Sunarto, M. Z., Musthofa, B., & Wijaya, M. (2019). Motivation And Learning Outcomes Through The Internet Of Things; Learning In Pesantren. *Journal of Physics. Conference Series*, *1363*(1), 12084–. https://doi.org/10.1088/1742-6596/1363/1/012084
12. Yangui, S., Bouguettaya, A., Xue, X., Faci, N., Gaaloul, W., Yu, Q., Zhou, Z., Hernandez, N., & Nakagawa, E. Y. (2020). Representing Multicloud Security and Privacy Policies and Detecting Potential Problems. In *Service-Oriented Computing - ICSOC 2019 Workshops* (Vol. 12019, pp. 57–68). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-45989-5_5

BULGAKOVA Daria A.

Postdoc. in Tech. Law, Doctor of Laws, Ph.D. in International Law,
Lawyer, (Kryvyi Rih, UA)
ORCID: https://orcid.org/0000-0002-8640-3622
e-mail: dariabulgakova@yahoo.com

FORENSIC EXAMINATION OF THE INTERNET OF THINGS

Abstract. The report underlines the Internet of Things as a tool of crime that requires true-to-evidence forensic examination in proof of the merits during investigation. The author has discoursed affiliated methods and stressed the data aspects for the reliable process of Internet of Things evaluation and its further ground-based evidential outcome. Hence, the report calls to take a course for Internet of Things forensic legislation because formal forensic practice shall be contested.

Keywords: IoT crimes, proof of the merits, data accuracy and limitation, expertise

A. **The IoT is a crime tool**

The rapid application of the Internet of Things (IoT) in spheres of society's life has designated its types of equipment, and software products with criminality element. The IoT innovation with superhuman abilities could be engaged in cybercrimes, killing, plundering others' property, defaming reputations, creating ethical conflicts, and disintegrating various social structures. The IoT operations created by combining various anthropomorphic machines and communication perception systems with features of the human brain raise new possibilities for algorithms to be developed, allowing the prediction of the dispositions of an individual [12]. These advances in science and technology could convey IoT settings to the target with criminal intent. Hence, the negative traits of the evolution of progressive technology are IoT-based crimes, which divulges the joint discharge between technology and regulation, and retains the need to extend law. In this content, the IoT is questionable for the examination of illicit action when reacting and interacting with the environment.

Criminality with the use of IoT techniques shall be punished based on the analogy of traditional criminal law systems and charges, which have not yet challenged the application of forensic examination rules. As long as the case committed with the use of IoT is under investigation, the harm and victims of cybercrime are exposed. Hence, the

report stresses the increase of efficiency and quality of forensic examination regardless of IoT evaluation in proof of the merit procedure and substantiate the formulation of course on a IoT forensic law. It is, therefore, the report answers on the question: *Is a forensic examination of IoT (a crime tool) a reliable ground for proof on merit?* This mark is vital to improve the expertise in crime investigation operational activities and hearings regardless of evidence assessment, where typically experts' results are utilised in confirmation means that a particular IoT equipment and/or software products became the crime toll or served as a method for crime commitment.

B. Forensic examination methods for the IoT

The crime compelled by IoT is based on the layout loopholes of equipment and/or software products. It ought to be a ratio between ruling and justice in the countenance of IoT match and objective riff to enforce the global commitment of defending technology limitations because IoT supports criminalities. The breakdown of forensic examination conditions should not be delayed or absent from this knowledge. In this respect, the report is to conceive the theoretical, methodological, and practical floors of forensic IoT by devoting special knowledge in criminology and pose data-driven models oriented for the investigation and disclosure of IoT-based crimes.

Accordingly, the report states that the special knowledge of experts for IoT suspend module retains (but not limited to) interdisciplinary approach in the following scientific areas: automation, information systems, processes, electronics, engineering, communication, computing, programming. The generic subject of IoT expertise on facts, circumstances is essential for a criminal case and evaluation of its patterns, algorithmic processes, and data exchange. Therefore, the meaning of forensic examination of the IoT equipment and software products is given in this research work to be an independent type of forensic inquisition belonging to the class of computer-technical inspections, which is maintained out:

i. to identify and scan IoT functions for a potential crime;
ii. to determine the status of IoT as a crime tool;
iii. to access data contained on IoT with further comprehensive analysis.

Computer forensics can be considered as a sub-class of IoT digital forensics because the link is that both IoT devices (a set) and servers rely on the use of Operating Systems in addition to the user(s) that are also connected to IoT servers/devices depending on the adopted configuration [13, p. 11]. Thus, the investigation of IoT forensics for the achievement of mentioned above examination targets shall consist of three schemes: device-level forensics, network-

level forensics, and cloud-level forensics [1, p. 24]. In this regard, the report proposes the next examination check steps:

- ✓ a probe of IoT hardware and software;
- ✓ examination of IoT databases, networks, communication components;
- ✓ examination of peripheral IoT devices;
- ✓ assessment and design of forensic results.

When investigating IoT – a crime tool, it is needed to identify how particular IoT is used in crime. Identifying the difference between the intention of the developer and the result of IoT is important for investigators. Mainly, the experts should:

i. to accumulate and dissect the dataset, learning model, trained model, inference model, and IoT used model to commit a crime;

ii. to grasp the purpose of the IoT's user relevantly to the outcome of tech productivity.

Moreover, unlike traditional programming, IoT sets often result in unintended consequences, therefore, the relationship between input, output, and program in traditional programming and IoT are at the center of attention. Commonly, data and programs are processed on the computer to produce the output; otherwise, data and output are used to create a program in IoT. In particular, the parameters of IoT are often determined with some

randomness because many models use weights in the learning phase. Therefore, even if the same dataset and learning model is given, it may create programs with different parameters and outputs result. It means, it is hard to prove -whether IoT was used as a tool crime, how IoT was used, and how much damage IoT caused - because investigators would fail to reproduce the case.

C. The IoT in proof of the merits

The peculiarity of IoT forensics is its complexity. Generally, an IoT system uses various algorithms and libraries. Some rely on a mixture of application program interfaces for IoT efficiency. The fact that only definite expertise of the IoT system can be used for proving its merits, therefore, it is not relevant to collect all elements such as the training system, learning model, dataset, trained model, and inference system, due to the reliability respectively to the technical and legal targeted matters. Also, because perpetrators' behaviour leads to destroying traces of the crime, an expert focus shall have a scope up to the questionable structure and activity history of examined IoT and limited information for the research (which is good for precise and concrete expertise). On the other side, the framed collection of evidence makes it difficult for investigators to reproduce the crime scene. It is an important issue because reproducibility is one of the key

principles of digital forensics. Therefore, the report contests explicitly whether an expert's forensic examination about employing IoT for the crime is hold by the perpetrator to be criminally responsible for illegal actions. Hence, the report presents a look into two crucial aspects of IoT forensics:

- ✓ data accuracy of exanimated questions;
- ✓ data limitations in forensic expertise.

Data accuracy

The boost of IoT evidence submitted to digital forensic laboratories has been an issue due to the lack of experts to nail the weights. Cut-rate IoT quality examination can usher to inaccurate favourable or unfavourable effects and, thus, mistaken, potentially resulting in criminal accusations or convictions. For instance, to say, the National Registry of Exonerations reported that between 1989 and 2019 flawed forensic techniques contributed to almost one-quarter of wrongful convictions in the US [2]. For that kind of reasoning, both Article 5(4)(d) Convention 108+ [3] and Article 4(1)(d) Directive (EU) 2016/680 [4] affirm the canon of accuracy. Furthermore, since the algorithms allow users to encode the data before sending it to the cloud and decrypt it after returning to their own system [11, p. 1199], Shin et al. [8, p. S13] propose a forensic model to analyse the encrypted traffic with five methods such as echo dot, some Artificial Intelligence (AI) speakers, and in order to obtain artifacts

stored on the cloud. According to Smith [9] it is involved tracking messages and conversations accessed in investigations of an organised crime syndicate.

In other observations, the loftier the data intake's trustworthiness, - the better the investigative outputs of rationale. During the examination process, there may be a misinterpretation of codes, performance errors, use of inappropriate theories, and insufficient reference materials. Traditional forensic cannot explain the relationship between the calculus-type factors, or it is difficult to explain the choice of inductive calculus. Whether or not the mensuration factor type is appropriate, the enumeration process is like a black-box operation. Although expertise may produce outstanding results, determining the causal relationship of state of the IoT is necessary to understand the criminological outcome. It is essential to investigate operational reasons, and thus, to explain the rationality of the IoT finality.

In demand to confine which IoT objects should be given to the expert in each specific case, as well as how to select them for examination, it is advisable to get the recommendation of an expert (specialist) in the field of computer technology. For the expert shall be given the invention itself and, if necessary, a computer unit connecting IoT which shall be supplied in containers that make it impossible to access the data directly or connect the

system unit to the power network. Furthermore, to keep the data carriers in working condition, they shall be provided in separate packages. The expert shall be equipped with a medium of the software product or software code under investigation. However, extra problems may occur when determining whether IoT evidence complies with or violates applicable laws, for example, assessing non-discrimination or data protection rules in the process of forensic examination at large well-documented equivocal task [7, p. 538]. Given that, unlawfully obtained evidence is not necessarily inadmissible, assessing the weight such violations hold on the overall fairness of the trial may be particularly difficult for judges [ibid.].

Data limitation

The essential data, calculation methods, and value determinations derived from the IoT depend on input holder data. The decision-making process is not created by experts without grounds and covers infinitely variable laws, and legal facts, and supplies rationality through questioned data examination. To show that it is necessary to analyse the presented state of the IoT system with complex data, Jeong [5, pp. 184568-184569] illustrates an experiment conducted using an i7-8700 processor and an Nvidia GeForce 1070 Ti graphic card. There were trained several models to categorise binary files into Malware or Benign. If the

investigator had only collected only a portion of the dataset, it was trained models according to the size of the dataset. The 1,000 PE files for each category were used as a dataset. The 500 Malware files are collected from VirusShare, which is a publicly available repository. The 500 Benign files are collected from Software Informer, which is the most trustworthy source-provider of benign files, and from system directories created when Windows 10 is newly installed. The model was based on Convolutional Neural Network and a voting-based ensemble technique was used to improve the performance of the model. The study demonstrates the accuracy of the models with variations in the size of the dataset. To identify performance changes in the dataset, 60 percent of the dataset was randomly selected 10 times, and then experiment-trained models with the selected data. It is shown that there is a deviation in accuracy depending on the data selected for training. The experimental results establish that it is impractical with limited evidence.

Indeed, because IoT systems adopt transfer learning where pre-trained models are used as the starting point, obtaining origin data is becoming more challenging. Things like social media posts, text messages, CCTV images, digital photographs, and emails together can build up a picture of a crime like a jigsaw puzzle, but until now have been hugely time-consuming and difficult to piece together

[9]. The most impactful research can be considered domain-defining research that takes a broad view of IoT technology's future impact on the field of crime analytics using new models, new theories, and new data from deep learning and big data and that takes a forward-looking approach to formulating implications for law, law enforcement, legal systems, social surveillance, culture, and society [6, p. 13]. Therefore, those approaches to overcome the IoT complexity should be not neglected.

D. Finalisation

The author introduces challenges that digital forensics can encounter when investigating crimes committed with IoT-based tools and submit the defined open issue of forensic examination to investigate IoT-like crimes. The author describes foreseeable digital crime considering the dual-use nature of IoT. Because AI system is also developed on digital infrastructure including applicable equipment and software products are embedded within security threats.

Under the research, the results of the IoT expertise must be presented according to the term of data evaluation techniques in the form of a report with an objective and substantiated answers to the framed questions. According to the Yaacoub et al. [13, p. 10], legal evidence is based on identifying whether a given fact can be proven and backed

or not. Therefore, in the scenario when it is impossible to give a determination, the expert is obliged to draw up an explanatory note with the reasons for declining the examination. In this regard there is a forecast of possible reasons:

i. the unsuitability of IoT materials and their objects;
ii. the expert needs to be more qualified;
iii. modern technologies do not allow answering the task of examination.

Hence, if a forensic expert is required to report (or testify) in a legal proceeding regarding an algorithm's (IoT) decision, an easily available open-sourced and/or peer-reviewed procedure is likely to be understood and accepted [10, p. 5]. Otherwise, if an expert cannot rationalise the process, the result may hide a risk of legal fraud. Consequently, IoT forensics is conditional; therefore, the preceding shall be criminalised through specific legislation on IoT forensics.

REFERENCES:

1. Aljahdali, A., Aldissi, H., Banafee, S., Sobahi, S., & Nagro, W. (2021) IoT Forensic models analysis. *Revista Română de Informatică Și Automatică*, *31*(2), 21–34. https://doi.org/10.33436/v31i2y202102
2. Barrington, S., & Farid, H. (2023) A comparative analysis of human and AI performance in forensic estimation of physical attributes. *Scientific*

Reports, *13*(1), 4784–6. https://doi.org/10.1038/s41598-023-31821-3

3. Council of Europe (2018) Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+).
4. European Parliament and of the Council (2016) Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA *OJ L 119*, 89–131.
5. Jeong, D. (2020) Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access*, *8*, 184560–184574. https://doi.org/10.1109/ACCESS.2020.3029280
6. Oatley, Giles C. (2022) Themes in Data Mining, Big Data, and Crime Analytics. Wiley interdisciplinary reviews. Data mining and knowledge discovery 12.2: e1432–n/a. https://doi.org/10.1002/widm.1432

7. Quezada-Tavárez, Katherine, Plixavra Vogiatzoglou, and Sofie Royer (2021) Legal Challenges in Bringing AI Evidence to the Criminal Courtroom. *New Journal of European criminal law, 12(4),* 531–551. https://doi.org/10.1177/20322844211057019
8. Shin, Y., Kim, H., Kim, S., Yoo, D., Jo, W., & Shon, T. (2020) Certificate Injection-Based Encrypted Traffic Forensics in AI Speaker Ecosystem. *Forensic Science International: Digital Investigation*, *33*, 301010–. https://doi.org/10.1016/j.fsidi.2020.301010
9. Smith, P. (2018) WA Police bring in AI detectives: Exclusive. *The Australian Financial Review*.
10. 10.Solanke, A. A. (2022) Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic Science International: Digital Investigation*, *42*, 301403–. https://doi.org/10.1016/j.fsidi.2022.301403
11. 11. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys and Tutorials*, *22*(2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586
12. 12.Tortora, L., Meynen, G., Bijlsma, J., Tronci, E., Ferracuti, S., Forensische psychiatrie / psychologie,

Strafrecht en strafprocesrecht, & UCALL / Aansprakelijkheid en verantwoordelijkheid. (2020) Neuroprediction and A.I. in Forensic Psychiatry and Criminal Justice: A Neurolaw Perspective. *Frontiers in Psychology*, *11*, 220–220. https://doi.org/10.3389/fpsyg.2020.00220

13. 13.Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, *19*, 100544–. https://doi.org/10.1016/j.iot.2022.100544

DONG Qiao

student Faculty of Sociology and Law, National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

COMPARATIVE LEGAL STUDIES OF NATIONAL LEGISLATION AND LEGISLATION OF THE EUROPEAN UNION ON THE ISSUES OF PROTECTION OF PERSONAL DATA

With the development of information technology and the Internet, human society has entered the era of big data. Personal data urgently needs legal protection. At present,

the legislation on personal data protection in the world is divided into two major branches: the United States and the European Union. In the European Union, personal data protection has gone through a development process from privacy rights to personal data protection rights. The United States has not promulgated unified laws related to personal data protection. The personal data protection system has been gradually established through the expansion of privacy case law and the formulation of departmental written laws, especially for special departments with significant threats to personal data. By analyzing and comparing the advantages and disadvantages of the two protection systems, suggestions are made for Chinese legislation.

EU Legislation. In 1995, the European Union issued Directive 95, aimed at safeguarding the basic rights of natural persons in personal data processing and regulating the cross-border flow of personal data between member states. In 2000, the EU issued the EU Charter of Fundamental Rights, which explicitly stipulated in Article 8 that everyone has the right to protection of personal data, thus separating the right to personal data from the right to privacy and recognizing it as a separate fundamental human right.[1] The protection of personal data rights is raised to a constitutional level. In 2016, the European Parliament passed the General Data Protection Regulations (GDPR)[2], which on the one hand introduced many innovative

provisions for the protection of personal data rights, including the right to be forgotten and the right to carry data. On the other hand, it also had a huge impact on many enterprises outside the EU, such as Google US internet companies such as Facebook will be directly governed by EU data regulations.

The transformation of personal data protection by GDPR is mainly reflected in the following aspects: (1) strengthening the rights of data subjects. GDPR has more normative provisions for personal data rights. The rights of data subjects mainly include the right to know, access, correction, deletion, restriction of processing, portability, refusal, and anti automatic decision-making. The right to know of the data subject corresponds to the right to inform of the data controller. On the basis of Directive 95, GDPR provides more specific provisions on the content and implementation methods of the right to information of data subjects.GDPR provides for the first time the portability right, which can ensure that data subjects control personal data, with the aim of promoting the healthy circulation of data. Anti automatic decision-making power refers to the restriction on the data controller's automated processing, which affects the decision-making behavior of the data subject. (2) Clarify the obligations and responsibilities of data controllers and processors. Firstly, there is the principle of purpose limitation. The data controller must

collect and process personal data within a specific, clear, and legal scope of purpose, and the use of data processing is due to situations where other means cannot achieve the processing purpose. Secondly, safety guarantees and disclosure obligations. Data controllers and data processors should take technical and management measures to ensure that potential risks are addressed.[3] Furthermore, in terms of data impact assessment, data controllers should conduct risk assessments from the perspective of the nature, scope, background, and purpose of the processing when using new technologies to process data. They should anticipate the potential impact on the data subject in advance and consult with the data protection officer in advance. Finally, there is the industry code of conduct. The Code of Conduct is a standard set by the industry association organization where a certain category of data controllers or data processors operate to regulate data behavior within the industry. Although the provisions of the EU data regulations involve many aspects of personal data rights protection, overall they are mainly standardized around the main line of strengthening the control of personal data rights subjects over personal data, which directly reflects the EU's concept of treating personal data rights as a fundamental right.

Legislation in the United States. The decentralized personal data protection system in the United States is reflected in the public and non-public spheres, and the

objects of adjustment and constraint are correspondingly different.[4]

The legislative norms in the public domain mainly constrain the behavior of government agencies regarding personal data when exercising administrative power. The Privacy Act of 1974 is the most important regulation in the United States that protects privacy rights. This bill specifies the methods, scope, and openness of the federal government to collect citizen information, which is used to regulate the federal government's handling of personal information and alleviate conflicts between privacy rights and the use of personal information.

The non-public sector involves finance, consumers, drivers, health insurance, minors, and other aspects. As early as 1970, the United States introduced the Federal Fair Credit Reporting Act (FCRA), which is mainly used to regulate the collection and processing of personal information by credit reporting agencies. However, the scope of personal information allowed to be disclosed is relatively wide, resulting in insufficient protection of privacy rights. In 1974, Congress passed the Family Education Rights and Privacy Act, which protected parents' financial status, student recommendation letters, and grades. In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which protected

privacy rights including communication between emails, computers, or telephones, and pagers.

In addition to implementing decentralized legislation, the United States has also adopted an industry self-regulation model to address personal data protection issues in the private sector. The industry self-discipline model is mainly applied to industries and organizations not covered by individual legislation, hoping to achieve a balance between personal data protection and the economic development of related industries through self-restraint within the industry. To be precise, the self-regulation model of the US industry is not allowing the industry to manage itself, but is being promoted under government guidance. For example, companies such as Microsoft and IBM have initiated the establishment of a privacy certification agency, with the goal of supervising members to comply with industry established privacy rules and provide certification. Currently, the organization has provided certification for over 3000 websites. Therefore, the main operating mechanism of the industry self-discipline model is for autonomous institutions to set privacy standards and supervise members' implementation.

Enlightenment on Chinese Legislation

The EU's unified legislative model and the US's industry self-discipline oriented model have their own advantages. The EU is based on basic human rights and has

unified specialized legislation. Within the EU, laws such as GDPR have the characteristics of uniformity, systematization, and strict logic. The advantages are obvious, as they can strictly protect personal data, facilitate cross-border data circulation among countries within the EU, and improve data utilization. However, its excessive emphasis on human rights can lead to an increase in data circulation costs and weaken the transaction intention of data companies. At the same time, considering personal data rights as a fundamental human right has given them a high status in the EU legal system. Rights holders have strong autonomy over personal data and can proactively and conveniently safeguard their own rights. At the same time, establish an independent personal data protection agency and implement strict law enforcement measures, forcing all types of enterprises to fully understand relevant EU laws and regulations when conducting business activities within the EU, and carefully formulate corresponding privacy protection policies. The protected mode of personal data dominated by self-discipline in the US industry can well promote the development of the data market and give full play to the role of the economic market itself. Facing the increasingly frequent collection and processing of personal data in the information society, the US government not only hopes to create an environment conducive to cross-border trade and e-commerce, but also

to protect the privacy rights of individuals, so it strives to maintain dialogue with various industries, And adopt a way to encourage industry self-discipline to protect personal data and stimulate the creativity and innovation of enterprises. As a result, the protection of personal data in the US model is not as strong as the EU model, which adopts a unified legislative model and regards personal data rights as fundamental human rights.

So for China, when formulating the personal data protection law, we should not transfer any protected mode, but take its essence, discard its dross, absorb the advantages of foreign personal data protected mode, and design a personal data private law protected mode with Chinese characteristics in combination with China's basic national conditions and legal traditions.[5] The way in which Japan drew inspiration from foreign models in designing its personal data protection system is commendable: it adopts the EU's unified legislative model in form, but also absorbs some practices from the United States.

REFERENCES:

[1] CHEN Qian , ZHANG Zhi- cheng.Personal Sensitive Data Protection: EU Legislation and Reference.//Journal of Xiangtan University(Philosophy and Social Sciences),2018,5(3).

[2] Regulation(EU) 2016 /679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data , and repealing Directive 95 /46 /EC(General Data Protection Regulation [2016] OJ L119 /1 . 2016-04-27 .

[3] CAI Liyan,Dilemma and Breakthrough of the Rights Protection of Personal Data under Blockchain: A Case Study of GDPR//Journal of Beijing University of Aeronautics and Astronautics(Social Sciences Edition),2022,11(6).

[4] 项 焱,陈 曦:《大数据时代欧盟个人数据保护权初探》,华东理工大学学报（社会科学版），2019 年第 2 期。

[5] SHAOGuo song , HUANG Qi.Trends and Challenges of Global Convergence of Personal Data Protection.//JOURNAL OF SJTU(Philosophy and social science),2021,8(140)

DONG Qiao

student Faculty of Sociology and Law, National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

PROBLEMS OF DETERMINING LEGAL RESPONSIBILITY WHEN APPLYING INTERNET OF THINGS TECHNOLOGIES

The Internet of Things (IoT) has become a global technology that has transformed the way we interact with our environment. IoT devices have the potential to make our lives more convenient and efficient, but they also pose significant challenges when it comes to determining legal responsibility in cases of malfunctions, accidents, or data breaches. The complex supply chain and the lack of clear regulations and standards can make it challenging to identify who is responsible for IoT-related incidents. This can create legal ambiguity and uncertainty, making it difficult for victims to seek compensation and for companies to mitigate their risks. The legal obligations when applying IoT technologies include ensuring product safety, protecting user data, implementing adequate cybersecurity measures, respecting user privacy, and fulfilling contractual obligations. To address these

challenges, there is a need to establish clear legal frameworks and improve the transparency and traceability of IoT systems and devices. This would provide greater clarity and certainty for all stakeholders and help establish clear lines of responsibility for IoT-related incidents. By doing so, we can ensure that IoT technology continues to benefit society while also protecting the rights and interests of all stakeholder.

Introduction. The Internet of Things (IoT) has become an integral part of our daily lives. It is a network of interconnected physical devices, appliances, vehicles, and other objects that can collect and exchange data using the Internet. IoT technology has brought several benefits to society, including increased efficiency, convenience, and productivity (Nizetic et al., 2020). IoT technologies are considered to be one of the essential aspects of the fourth industrial revolution. However, it has also created new challenges for determining legal responsibility when things go wrong. This essay aims to explore the problems of determining legal responsibility when applying IoT technologies. The essay also suggests some possible solutions to these issues.

Legal Responsibilities of IoT. The IoT is based on various technologies which include sensors, NFC, RIFD, 3G, and 4G. These technologies perform the function of transferring massive amounts of sensitive information and

private data which leads to numerous ethical and legal challenges which must be addressed by individuals and organizations that provide and use these technologies (Azer & Abo Bakr, 2022). The legal responsibilities when applying IoT technologies can vary depending on the specific use case and the jurisdiction in which the technology is being used. However, there are some general legal responsibilities that apply to the use of IoT technologies which includes product liability, data protection, privacy, cybersecurity, and contractual obligations (Kirtley & Memmel, 2018).

IoT device manufacturers and suppliers have a legal responsibility to ensure that their products are safe and fit for their intended purpose. If a device causes harm or injury to a user or their property, the manufacturer or supplier may be held liable for any damages. Similarly, it is important to note that IoT devices collect and transmit large amounts of data, including personal data (Weber & Studer, 2016). Companies that use IoT technologies have a legal responsibility to protect this data and ensure that it is used in compliance with data protection regulations such as the “General Data Protection Regulation”. IoT devices are vulnerable to cyber-attacks, which can compromise the security and privacy of users' data. Companies that use IoT technologies have a legal responsibility to implement

adequate cybersecurity measures to protect their devices and the data they collect.

The data collected by IoT devices are often of a very sensitive nature which includes users' private information such as location data or health information. Therefore, respecting the privacy rights of users and ensuring that data collection and usage are in compliance with relevant privacy laws is the utmost responsibility of companies offering IoT services (Shahid et al., 2022). Additionally, companies using IoT technologies often have contractual obligations to their customers or partners, such as service level agreements or warranties which must be adhered to as they can be held liable if they fail to do so.

Difficulties in Determining Legal Responsibility. IoT has become a transformative technology that blends the digital and physical worlds, impacting various aspects of society. However, its universal and autonomous nature has created challenges in determining legal responsibility. The legal responsibilities for IoT include safety, security, privacy, governance, and contractual responsibility. These legal obligations are crucial for establishing trust in the technology and ensuring that stakeholders are held accountable for their actions (Singh et al., 2018). One of the primary challenges of determining legal responsibility in the IoT context is identifying who is responsible for a particular IoT system or device. IoT devices can be made

up of numerous interconnected components that may be manufactured and sold by different companies. This complex supply chain can make it challenging to determine who is responsible when something goes wrong (Flynn, 2021). For example, if a car accident occurs due to a malfunctioning sensor, it may not be immediately clear whether the fault lies with the manufacturer of the sensor, the car manufacturer, or the software developer who created the system.

IoT devices are often designed to be connected to the internet, which means they are vulnerable to hacking and cyberattacks. This vulnerability arises due to several factors, including the wide range of devices used in IoT, many of which have limited processing power and storage capabilities, and the use of default passwords and insecure communication protocols (Li & Liu, 2021). Additionally, the sheer number of devices involved in IoT networks means that securing every device in the network is a complex and challenging task. When an IoT device is hacked or compromised, it can be used as a launching point for attacks on other devices or systems. This means that hackers can use compromised IoT devices to launch distributed denial of service (DDoS) attacks, which flood target systems with traffic and disrupt their operations. Hackers can also use compromised IoT devices to gain access to sensitive information or to steal data (Snehi &

Bhandari, 2021). Determining who is responsible for securing IoT devices and ensuring they are not used for harm is a complex issue. In many cases, there are multiple parties involved, including manufacturers, software developers, and users. Each of these parties has a role to play in securing IoT devices, but the responsibility for doing so is often not well-defined. For example, IoT manufacturers may be responsible for developing secure hardware and software for their devices. However, they may not be responsible for updating the devices with security patches or for ensuring that users change default passwords. On the other hand, users may be responsible for securing their devices, but they may not have the technical knowledge or resources to do so effectively. Determining liability for damages resulting from a cyberattack involving compromised IoT devices is also challenging as it may be difficult to identify the source of the attack, which could involve multiple compromised devices from different manufacturers or users. Additionally, it may be challenging to determine whether a manufacturer or user was negligent in securing their devices, or whether the attack was the result of a sophisticated and targeted attack.

Another challenge is the lack of clear standards and regulations governing IoT technology. The IoT is still a relatively new and rapidly evolving technology, and there are few established legal frameworks for determining

responsibility in IoT-related incidents. This can create legal ambiguity and uncertainty, making it difficult for victims to seek compensation and for companies to mitigate their risks. Therefore, the absence of clear standards and regulations creates a significant risk of legal liability for IoT manufacturers, developers, and users. Without a clear legal framework to determine responsibility for security breaches or data theft, manufacturers, developers, and users may face legal liability (Singh et al., 2018). Moreover, the lack of clear standards and regulations also complicates the development of IoT technology. The absence of standardized protocols or formats can result in a fragmented IoT ecosystem with devices that are incompatible with each other. This can limit the usefulness and scalability of IoT technology. Several organizations are working to address the lack of clear standards and regulations in IoT technology. For instance, the “Institute of Electrical and Electronics Engineers (IEEE)” has developed a set of IoT standards, including IEEE 802.15.4, which specifies the physical and media access control (MAC) layer for low-rate wireless personal area networks (Gallegos Ramonet & Noguchi, 2022). Additionally, the “International Organization for Standardization (ISO)” has developed a set of IoT standards, including ISO/IEC 30141, which provides a framework for IoT system architecture.

Recent advancements in IoT technology have further complicated the issue of determining legal responsibility. One such development is the increasing use of artificial intelligence (AI) and machine learning (ML) in IoT devices. These technologies enable devices to learn from data and adapt to changing environments, making them more efficient and effective. However, they also raise questions about legal responsibility in the event of accidents or malfunctions. With AI and ML, IoT devices can learn and make decisions independently, without human intervention (Naik et al., 2022). Legal challenges occur where a device's decision-making processes cause harm to a person or property as in the case of a self-driving car where it may be difficult to determine whether the manufacturer of the car, the software developer, or the AI algorithm is responsible for any damages. Another challenge is the use of IoT devices in critical infrastructure, such as power grids, transportation systems, and healthcare facilities. The failure or malfunction of these devices can result in serious consequences, including loss of life, property damage, and financial losses. In such situations, the involvement of multiple parties makes it difficult to ascertain the ones legally responsible.

Recommendations

Some possible solutions for addressing the legal responsibility issues of IoT are (Tawalbeh et al., 2020):

- Standards and Regulations: Clear and comprehensive standards and regulations can help define legal responsibilities for IoT devices and systems. Governments and industry organizations can work together to develop and enforce these standards and regulations.
- Liability Insurance: Manufacturers, developers, and users can purchase liability insurance to protect themselves from legal claims arising from IoT-related incidents. Insurance providers can help define and enforce safety and security standards for IoT devices.
- Collaboration: Manufacturers, developers, and users can collaborate to establish best practices for IoT safety and security. Industry associations, academic institutions, and research organizations can also facilitate collaboration by providing resources and expertise.
- Education and Awareness: Education and awareness campaigns can help users understand the potential risks and legal responsibilities associated with IoT devices. These campaigns can also guide the security provision for IoT devices and protect personal data.
- Secure-by-Design: Manufacturers can adopt a "secure-by-design" approach, where security and privacy are integrated into the design and development of IoT devices from the outset. This can help ensure that

devices are more resilient to cyber-attacks and that user data is better protected.

- Risk Management: Companies that use IoT devices can develop and implement risk management plans that include measures to prevent, detect, and respond to security incidents. These plans can help identify legal responsibilities and ensure that appropriate measures are taken to mitigate risks.

Conclusion

Conclusively, there are various legal responsibilities of IoT, and it is often a challenge to determine who is legally responsible in case of data breaches and harm. The legal responsibilities of IoT include product liability, data protection, privacy, cybersecurity, and contractual obligations. However, the difficulties in determining legal responsibility arise from the complex supply chain, which can make it challenging to determine who is responsible when something goes wrong. Additionally, the vulnerability of IoT devices to hacking and cyberattacks makes it difficult to determine who is responsible for securing IoT devices and ensuring they are not used for harm. Moreover, the lack of clear standards and regulations governing IoT technology creates legal ambiguity and uncertainty, making it difficult for victims to seek compensation and for companies to mitigate their risks. A way forward is to establish clear legal frameworks to determine responsibility

for security breaches or data theft, protect sensitive user data, and ensure compliance with data protection regulations. Additionally, there is a need to collaborate among stakeholders to develop standardization and certification schemes to enhance the security and resilience of IoT devices.

REFERENCES:

[1] Azer, M., & Abo Bakr, A. (2022, May 31). *IoT Ethics Challenges and Legal Issues*.

[2] Flynn, S. (2021, August 24). *Product Liability in IoT: Who Is Responsible for Vulnerabilities?* Medium. https://theiotmagazine.com/product-liability-in-iot-who-is-responsible-for-vulnerabilities-847256b8eb96

[3] Gallegos Ramonet, A., & Noguchi, T. (2022). Performance Analysis of IEEE 802.15.4 Bootstrap Process. *Electronics*, *11*(24), Article 24. https://doi.org/10.3390/electronics11244090

[4] Kirtley, J., & Memmel, S. (2018). Rewriting the “Book of the Machine”: Regulatory and Liability Issues for the Internet of Things. *The Minnesota Journal of Law, Science & Technology*, *19*(2).

[5] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

[6] Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B. P., Chlosta, P., & Somani, B. K. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Frontiers in Surgery*, *9*. https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322

[7] Nizetic, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

[8] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*, *12*(4), Article 4. https://doi.org/10.3390/app12041927

[9] Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the IoT: Systems, Law, and Ways Forward. *Computer*, *51*, 54–65. https://doi.org/10.1109/MC.2018.3011052

[10] Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS

attacks. *Computer Science Review*, *40*, 100371. https://doi.org/10.1016/j.cosrev.2021.100371
[11] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10*(12), Article 12. https://doi.org/10.3390/app10124102
[12] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, *32*(5), 715–728. https://doi.org/10.1016/j.clsr.2016.07.002

GOLOVKO Olga
PhD in Law, senior researcher
senior lecturer, Department of Intellectual Property and Private Law
Faculty of Sociology and Law
Igor Sikorsky Kyiv Polytechnic Institute

EU LEGAL FRAMEWORKS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN SOCIAL ENTREPRENEURSHIP

AI technologies help to optimize the solution of current problems in society due to the rapid processing of large amounts of information and rapid decision-making that correspond to the current situation. Therefore, social

entrepreneurs are increasingly beginning to use these technologies to overcome social challenges and achieve a socially significant result.

Social entrepreneurship is entrepreneurial activity aimed at innovative, significant and positive change in society. While classical entrepreneurship is aimed at achieving financial profit, social entrepreneurs aim at achieving a certain social value.

The EU has a number of initiatives and policies dedicated specifically to social entrepreneurship. Among them, the following should be mentioned:

1) European Commission Social Business Initiative was launched in 2011 and aims to promote social entrepreneurship across the EU. It includes a number of measures to support social entrepreneurs, such as improving access to finance, providing training and mentoring, and raising awareness of social entrepreneurship.

2) The European Social Fund provides funding for initiatives aimed at improving employment opportunities, reducing poverty and promoting social integration. It can be used to support social entrepreneurship initiatives, including those related to the direct use of AI technologies [1].

3) The European Investment Fund provides financing and guarantees to small and medium-sized enterprises,

including social enterprises. This can help social enterprises access the funding they need to start and grow their businesses.

It is also worth to underline that the content of the Resolution of the European Parliament dated July 6, 2022 regarding the Report on the EU action plan for the social economy emphasizes the key role that new technologies and AI can play in job creation and the development and expansion of the social economy [2]. Particular attention is paid to the importance of expanding access to educational programs in digital skills and advanced technologies. In general, the adoption of this Resolution particularly emphasizes the promotion of the digital transition in the social economy (through taxation, public procurement and public assistance).

As we can see, we are talking about opportunities for social entrepreneurship, including the innovativeness of which is encouraged not only at the national level, but also at the pan-European level.

The European Commission has also launched the "Digital Social Innovation" initiative, which aims to support social entrepreneurs who use digital technologies to solve social problems [3].

The European Union's Horizon Europe research and innovation program focuses on AI for social good, which

aims to support research and innovation projects that use AI to solve social problems.

Among other European initiatives, it is worth mentioning AI4EU - a project financed by the European Commission and aimed at promoting the development and spread of AI in Europe. The project includes a number of initiatives to support the use of AI in various sectors, including social entrepreneurship.

In 2019, the European AI Alliance launched the AI for Social Good initiative to explore how artificial intelligence can be used to solve social and environmental problems.

In 2019, the European Commission issued Ethical Guidelines for Trusted Artificial Intelligence. These guidelines provide a framework for developing and deploying artificial intelligence in a transparent, accountable and socially responsible manner. The formation of a culture of using AI will make it possible to make these technologies, on the one hand, more accessible to the broad masses of the population, and on the other hand, create a clear and safe space for using AI.

Among the examples of the application of AI in social entrepreneurship, the following can be mentioned: Good-Loop is a social enterprise that uses AI technologies to create ethical advertising; EIDU is a social enterprise that uses educational technologies based on AI to provide access

to quality education for children from underprivileged communities; Enerbrain is a social enterprise that uses artificial intelligence technologies to optimize a building's energy consumption; Humanising Autonomy is a social enterprise that uses AI technologies to improve pedestrian safety. The platform uses AI algorithms to predict pedestrian behavior and warn drivers, helping to prevent accidents.

Thus, AI can help tackle societal challenges in a more innovative way. In addition, AI can help social enterprises scale their impact by automating repetitive tasks and providing data-driven insights that can inform decision-making. AI can also help social enterprises better understand and engage with their beneficiaries by analyzing data about their needs and preferences.

The trends definitely indicate that the application of AI technologies will become more and more massive and will contribute to overcoming various challenges facing humanity. From the point of view of a social entrepreneur, the use of these technologies has indisputable advantages. Lawmakers and lawyers are left to think through the rules of the game to overcome the risks and accompany the use of AI technologies.

The research was carried out within the framework of the implementation of the international project in the field of education "European Integration: legislation and the

IoT" ("European integration: legislation and the Internet of Things") within the direction of Jean Monnet "Module" of the "Erasmus+" program No. 620017-EPP-1-2020 -1-UA-EPPJMO-MODULE (joint project of Igor Sikorsky KPI, Erasmus+ Jean Monnet Foundation and the Executive Agency for Education, Audiovisual Activities and Culture with the support of the EU)". The European Commission's endorsement of this publication does not imply endorsement of the content, which reflects only the opinions of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein.

REFERENCES:

1. European Social Fund Plus. URL: https://ec.europa.eu/european-social-fund-plus/en (дата звернення: 17.04.2023).

2. European Parliament resolution of 6 July 2022 on the EU action plan for the social economy. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0288_EN.html (дата звернення: 25.04.2023).

3.Digital Social Innovation for Europe. URL: https://cordis.europa.eu/project/id/688192 (дата звернення: 25.04.2023).

NEKIT Kateryna
Dr. habil. in Law, Professor of Civil law department of the National university “Odesa Law Academy”, guest researcher at the Center of SME research and entrepreneurship of the University of Mannheim

EUROPEAN AND AMERICAN APPROACHES TO ENSURING SECURITY IN THE FIELD OF THE INTERNET OF THINGS

The number of devices connected to the Internet was 500 million in 2003, by 2010 their number had increased to 12.5 billion, and by 2025 the rollout of over 41 billion IoT devices is expected [1]. The permanent growth of the items, connected to the Internet, causes growth of concern about their security. With the aim to enable cybersecurity measures in the field of the Internet of Things, legislators in the US and EU are working on new acts. Thus, recently the EU Cybersecurity Act (2019) and the NIS Directive (2018) have been adopted in this area.

An important point of the EU Cybersecurity Act is that it defines an EU-wide cybersecurity certification framework. The European Cybersecurity Certification Framework should enable the issuance of cybersecurity certificates and statements of conformity for IoT products,

services, and processes. Initially, manufacturers and vendors will be able to have their products and services meet the EU cybersecurity pending standards voluntarily. However, the certification may eventually be compulsory.

It is stated, that the Cybersecurity Act provides a model that other non-EU countries and territories are following when crafting legislation, so getting prepared now will be a competitive advantage for the future [2].

The Directive on security of network and information systems (the NIS Directive) [3], in turn, provides legal measures to boost the overall level of cybersecurity in the EU by ensuring: Member States' preparedness, by requiring them to be appropriately equipped; cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States; a culture of security across sectors that are vital for the economy and society and that rely heavily on information and communication technologies, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure [2].

In the USA the main act regarding security in the field of the Internet of Things is the IoT Cybersecurity Improvement Act of 2020. The Act has a few primary components for strengthening IoT cybersecurity and the government’s critical technology infrastructure. First, the

National Institute of Standards and Technology (NIST) was tasked with developing security standards and guidelines for the appropriate use and management of all IoT devices owned or controlled by the federal government and connected to its information systems. This includes establishing minimum information security requirements for managing cybersecurity risks associated with these devices. In formulating these guidelines, NIST had to consider its current efforts regarding the security of IoT devices, as well as the "relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships" [4].

Thus, both, European and American legislators pointed out the necessity to standardize items, which can be elements of the Internet of Things. The discussion on standardization in the field of the Internet of Things has lasted for several years. Specialists in the field of IoT have actively discussed the need to coordinate the coexistence of various devices by introducing open certification of IoT products [5]. According to researchers, the introduction of certain standards in the field of the Internet of Things would also help to solve the problem of coordinating the coexistence of various components of the Internet of Things. Thus, it was noted that the proprietary and closed systems of the Internet of Things must give way to a more open space. A situation where there are many different non-

standardized devices is similar to a situation where, for example, each car manufacturer would use its own control system, one car would have a steering wheel, and another would have a joystick or control panel. Or if e-mail systems were incompatible, and the telephone could not be used to call numbers of other operators, and different brands of household appliances required different types of water or electricity connections. Likewise, in a closed or proprietary Internet of Things world where devices are not connected to each other, a homeowner will not be able to control lights, security, thermostat, locks, etc. from a central app or control panel. The need for standards for the Internet of Things was recognized several years ago. At that point, the Association for Standardization has developed a number of standards and protocols designed to help the development of connected systems [6]. Nowadays, these considerations were taken into account on the legislative level.

However, there's no national IoT cybersecurity regulatory framework nor a comprehensive set of standards in the US. At the same time, California was very progressive in this field. California legislature passed a new IoT security law in 2018 that became effective on 1 January 2020. This became the first IoT-specific security law in the USA. The law defines new security requirements for IoT devices connected directly or indirectly to the Internet with an IP or Bluetooth address. It requires that these devices

sold in California be fitted with “reasonable security features.” The security features should protect both the IoT device and the data it contains, in particular, if the device integrates a password, it must either be uniquely linked to that device or require the user to set their own password during the initial setup [2].

Thus, talking about European and American approaches to ensure security in the field of the Internet of Things, such legislative acts might be guides for Ukrainian legislator: the EU Cybersecurity Act, the NIS Directive (European level) as well as IoT Cybersecurity Improvement Act of 2020 (USA) and California IoT cybersecurity law. According to the last ones, the necessity of certification and standardization for the appropriate use and management of all IoT devices was recognized.

However, it should be mentioned that excessive government intervention in the regulation of relations in the field of the Internet of Things may hinder the development of technology. Considering that, to ensure information security in the field of the Internet of Things it is necessary, first of all, to apply self-regulation, which should be ensured through close cooperation between technology companies and civil society. This minimizes government intervention in this area, which will contribute to the rapid development of innovative technologies. However, according to the European as well as American approaches,

some common standards for the IoT devices should be implemented on the legislative level.

REFERENCES:

1. European commission. Europe's Internet of Things Policy. URL: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy
2. IoT Cybersecurity: regulating the Internet of Things. URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations
3. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *European Parliament and Council of Europe.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
4. Dunn G. New Federal Law for IoT Cybersecurity Requires the Development of Standards and Guidelines Throughout 2021. URL: https://www.gibsondunn.com/new-federal-law-for-iot-cybersecurity-requires-the-development-of-standards-and-guidelines-throughout-2021/#_ftn1
5. Виндерских Н. Опасность интернета вещей: зачем IoT рынку сертификация. *ain.ua.* URL: https://ain.ua/2017/09/01/opasnost-interneta-veshhej.
6. Некіт К.Г. Деякі правові проблеми Інтернету речей і напрями їх вирішення. *Часопис цивілістики*. 2018. №31. С. 54-58.

YENIN Maksym
Associate Professor of the Sociology Department,
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»,
yeninmaksym@gmail.com

DEVELOPMENT OF ARTIFICIAL INTELLIGENCE: CHALLENGES FOR THE LABOUR MARKET.

The emergence of ChatGPT in November 2022, thanks to the developments of the OpenAI company, became a worldwide sensation. The algorithm provides answers to complex questions in various languages, writes essays, articles, poems, songs and music, generates simple codes, provides financial analytics and more. The social consequences of the development of new technologies are assessed ambiguously in the expert environment. On the one hand, the processes of digitization, automation and robotization associated with the development of artificial intelligence contribute to the progressive development of production and the improvement of the quality of services in many areas, including education, health care, finance, transport, etc. On the other hand, analysts predict a reduction in jobs and an increase in unemployment, which

may lead to even greater social insecurity for employed people.

Fears that automation will cause mass unemployment have been known since the 19th century, when new machines and technologies were introduced in the textile industry. At the same time, from the very beginning of the industrial revolution, instead of professions that were displaced by machines, new ones appeared, and the average standard of living increased. However, at the post-industrial stage of development, humanity is in a situation where the imaginary linear determinism of previous trends may be false. Thus, in the past, machines competed with humans, as a rule, in brute physical strength, while in the intellectual sphere, humans maintained a huge advantage. After the automation of manual labour in agriculture and industry, new service professions emerged that required mental skills that only humans possess. However, today artificial intelligence is beginning to surpass humans not only in physical, but also in cognitive abilities, including the recognition of human emotions.

Artificial intelligence will indeed contribute to the creation of new professions, but they will require high qualifications, and therefore the question of mass employment remains open. During previous waves of automation, people were generally able to move from one monotonous and low-skilled job to another. In the industrial

society of the first half of the 20th century, a worker who became unemployed due to the mechanization of agriculture found work at a tractor factory. In the 1970s and 1980s, when the foundations of the post-industrial social order were laid, a worker from a tractor factory who was laid off due to downsizing was able to get a job (as an example) as a sales consultant in a supermarket. Such a change of professions was relatively painless because the transition from farm to factory or from factory to supermarket did not require extensive retraining. But in 2050, a taxi or truck driver who will be replaced by autonomous vehicles may have trouble getting a job in the field of programming virtual reality, creating games, or designing robots, because it requires specific knowledge and skills acquired through hard training over a long period of time.

Furthermore, no profession is immune to automation, as machine learning and jobs will continue to improve. A dismissed fifty-year-old taxi driver, at the cost of incredible efforts, can retrain to become a specialist in the maintenance and repair of robots that assemble, for example, smartphones, but it is possible that in ten years he will not have to retrain again, because this profession will be automated due to the emergence robots that can serve themselves independently.

Thus, despite the emergence of new professions, a whole class of people redundant for the labour market may arise. It is possible that the situation will worsen on two fronts at once - a high level of unemployment will be accompanied by a lack of qualified specialists. The challenges to the entire education system in such a unique historical situation are fundamental. If artificial intelligence can provide high-quality answers that exceed the abilities of most teachers in schools or professors in universities and academies, then traditional forms of learning and evaluating its success (preparation of essays, essays, writing answers on exams) may soon become obsolete and even to further strengthen the «imbalance of the labour market and the market of educational services in the context of the historical evolution of higher education» [1, p. 61]. In connection with the crisis phenomena in the higher education system, massive open online courses are already creating competition for universities: in the market of educational services, projects are becoming more and more in demand, with the help of which consumers have the opportunity to quickly obtain new qualifications and specific skills that can later be converted in income (for example, online programming courses, Internet marketing, creating mobile applications and online stores, etc.).

In many countries, the search for new educational solutions is being updated. In this regard, Japan, China and

Israel are indicative in this regard, where special attention is paid to the study of engineering technologies in school programs. In 2019, the Japanese government announced the introduction of mandatory learning of programming in elementary and middle school. In China, artificial intelligence courses are being introduced as a pilot project in some primary and secondary schools. In Israel, school students, in addition to standard subjects, listen to lectures about technologies, IT projects, their implementation possibilities and practical value. Students have the opportunity to learn how to program, create websites, and more. Such courses are designed to prepare young people for the labour market and increase the innovativeness of the country as a whole. The institution's administration involves successful start-ups, company managers and businessmen in the educational process. In schools there are technological laboratories with 3D printers, robots, smart boards, which makes it easier for young people to adapt to technological innovations. The governments of these countries pay special attention to professional technical education, allocating significant funds to the operation and growth of new educational professional institutions [2].

In order for people to adapt to rapidly changing technologies and social roles, lifelong learning, self-education and adaptability skills will be essential. Is it within the power of the majority of the population, even if

the political class makes higher education as accessible as possible for all social strata, promotes the development of post-materialistic motivation, as well as education and talent as the main sources of success for a modern individual? If, despite all these efforts, a large part of humanity becomes redundant and is pushed out of the labour market, the world awaits a highly polarized configuration of the social structure with a small creative group (elite), intelligent machines, and an uncreative and unproductive majority of people. We will have to explore new models of post-labour society, post-labour economy and post-labour politics, where work and employment will lose their central role in people's lives. How to keep people busy, organize their leisure time and social space? Studying and transferring to the level of technology ways of forming new life horizons, overcoming cultural and socio-psychological obstacles to life in a new society is a challenge for science and education. At present, ruling classes around the world are largely unresponsive to these future challenges, but sooner or later historical trends cannot be dismissed. A society divided by rigid borders into «us and them» produces great risks of its existence. We should not think how to beat artificial intelligence in intellectual abilities. When the car was invented, it did not mean that man had to learn to run faster than it. It is necessary to use new technologies to accelerate our own

development, as well as the progress of society as a whole. Neural networks prepare us for life in an elitist civilization in which all people must be able to think critically, be original and creative. This applies not only to professional life, but also to public life. But are we ready for it? One can observe, for example, the global trend of a crisis of democracy and a decline in the culture of discourse on important issues of the functioning and development of society in social media and networks - the place of rational arguments is taken by emotional urges, memes, stereotypes, fakes, etc. In this regard, Y. Habermas believes that digital (social) media (in the form in which they exist today) distort social reality and threaten the quality and depth of political discussions, democracy, civil society and open public space. With the advent of digital media, it seemed that they would contribute to the democratization of public space through egalitarian discussions, free communication in which each individual can be an «author», without the mandatory imposition of opinions by experts and journalists. However, parallel to the egalitarian potential, according to the scientist, there is an authoritarian tendency. Digital platforms for digital corporations (concerns) are primarily a business project, so instead of opinions and rational, qualitative, deep and reasoned positions and discussions of mature citizens, this space is saturated with superficial, manipulative ideological constructions capable

of evoking emotions and attracting the attention of the masses, users and new subscribers. Structured publicity is possible when citizens are ready to play the role of «author», but this requires intellectuals – teachers of discourses (debates), educated individuals with critical thinking who can teach rational discussion [3].

In my opinion, it is unlikely that artificial intelligence, which functions on the basis of algorithms, is capable of completely absorbing human freedom and replacing human thinking, which, being included in interaction with the surrounding world, has a greater potential for creativity, innovation. The human personality has intuition and an ethical component, which allows making not only logical, but also in accordance with situational contexts – moral and ethical choices that are not amenable to mechanical calculation. In the work «Existentialism is Humanism» written by J. P. Sartre in 1946, an example of a moral dilemma is given, which leaves space for human freedom. The young man does not know whether he should go to defend his homeland from the invaders or stay with his mother, for whom he is the only support. He hesitates between the values of direct service to a loved one and military work for a common cause. No written morality can give an answer here.

REFERENCES:

1. Кутуев П., Енин М., Костюченко С. Вызовы успешному трудоустройству молодежи в контексте идеологии университетского образования // Идеология и политика. 2019. №2 (13). С. 60–86.
2. Татомир І. Зайнятість та освітня політика в епоху штучного інтелекту й роботехніки // Демографія та соціальна економіка. 2019. №2. С. 178–193.
3. Jürgen Habermas. Ein neuer Strukturwandel der Öffentlichkeit und die deliberative Politik. URL: https://cutt.ly/G53LTqN

YUDINA Nataliya

Laureate of the President of Ukraine Prize for young scientists,
Ph.D. in Economics, Associate professor,
ORCID: 0000-0002-1730-9341,
Associate professor of the Department of Industrial Marketing
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
#Futurolog the Portal, http://futurolog.com.ua

TECHNOGENIC ECONOMY OF BIOMETRICS

The dynamics of the digital market of generated big data is growing during some years long. In 2023 its rate was near 40 % per year and will plan to reach 163 trillions gigabytes by 2025 [1]. This market is the most developing

in the worlds. This assumes that most representatives of business will implement different AI technologies into most their economic spheres as the tool for managing time and Big Data [2]. This way corresponds with future uncertainty and unpredictable consequences to all economic spheres and Humankind at all [3].

On the one hand banks have already started to implement the cybersecurity program of different types of their consumers' biometrics, in particular the voice samples (casts), palm prints. These technologies assume creating a unique biometric sample that provides additional protection for the consumer's bank account [4]. In accordance with the bank information this technology makes it possible for the bank consumers don't remember any other personal data to perform in operation in customer support (for example, account username, account numbers, passport numbers and so on). Such kind of the unique personal data base is creating and protected by banks. But on the other hand the similar unique personal data base of biometrics is creating by different social media which launch different trends on video. It turns into Big Data that are enough for the AI-algorithms to build a mathematical model that will be able to extrapolate it for the generation of some new content.

The neural networks are developing so rapidly and have already leant how to generate somebody's voice on the basis of its sample [5]. This clone, been made with the

neural network Synthesia and options Deepfake Call, managed to bypass the bank's security successfully. Microsoft has started to add OpenAI's chatbot technology to its common and popular applications [6]. It assumes that every user of these applications will turn into testers, teachers and "information raw material" which have been missing data for creating some particular mathematical model by AI. For example, some months ago the main feature of images, generated by AI, was an unnatural form of human's hands and fingers. It could be explained the fact that among selfies there hadn't been trends to post selfies of own hands and fingers in details. Therefore this information was missed for any extrapolations and generative images of human's hands by Generative AI (GAI).

The conjuncture of technological development has started to include unique human's biometrics. It is very important for Humankind to realize that every biometric information trend that appears in different social media will turn into the part of such kind of the collection and then Big Data processing by AI. For example, one of the current popular trends of TikTok assumes filming a human eye in details. If AI that processes personal biometrical information of particular persons starts to collaborate with GAI of social medias, the consequences of all these facts will be unpredictable for Humankind in the future and it

will make a person depend on technologies and be vulnerable of AI too much.

The biggest concern is the joining of three elements: big data of human's biometrics, Artificial Intelligence and the economic sphere. They will create an innovative technogenic economy of biometrics in the future, where humans may turn into just "information raw material" under the conditions of economic relations between different types of AI. This needs to implement different learning courses on cybersecurity and marketing en mass, because knowledge on cybersecurity can help to form the elementary technical guideline and marketing the moral concept and the future vision of the relationships between a humans and different types of AI, GAI, DMAI and so on.

REFERENCES:

1. Artificial Intelligence: in-depth market analysis. Market Insights report. Statista, April 2023, https://www.statista.com/study/50485/in-depth-report-artificial-intelligence/ .

2. Yudina, N. Time as Economic Value of Information Society. Scientific Challenges : Collection of Materials of the International Multidisciplinary Scientific and Practical Conference on the occasion of World Science Day for Peace and Development, Kyiv, November 29, 2019. / [compiler L. I. Yudina]. Kyiv, 2019. p. 111-113. URL : http://futurolog.com.ua/publish/16/zbirnyk.pdf#page=111.

3. Yudina, N. Business Forecasting of Marketing Activity Riskiness of Companies in Markets. *Economic Bulletin of National Technical University of Ukraine "Kyiv Polytechnic Institute"*. №17(2020). P. 372-383. URL : http://ev.fmm.kpi.ua/article/view/216380/
4. Protect yourself with voice biometric. Privatbank. https://privatbank.ua/voice-biometrics
5. Мачула А. Цифровий клон людини пройшов перевірку банку: деталі експерименту. 01.05.2023, https://psm7.com/uk/news/cifrovoj-klon-cheloveka-proshyol-proverku-banka-detali-eksperimenta.html .
6. Saini N. Microsoft may add OpenAI’s chatbot technology to Bing, Word. 08 Jan 2023, https://www.livemint.com/technology/tech-news/microsoft-may-add-openai-s-chatbot-technology-to-bing-word-11673176344504.html .

АНДРОЩУК Геннадій
канд. екон. наук, доцент,
головний науковий співробітник НДІ інтелектуальної власності НАПрН України

КОМПЛЕКСНЕ РЕГУЛЮВАННЯ ЦИФРОВИХ АКТИВІВ У ЄС

Сучасний етап економічного розвитку суспільства характеризується формуванням нової сфери економіки — цифрової, обумовленої збільшенням ролі цифрових технологій та електронно-інформаційних технічних засобів зв’язку в розвитку всіх головних галузей науки. Інтерес до цифрових активів і нових фінансових технологій зростає в Україні щороку. На сьогодні криптовалютою володіють понад 6 млн українців, а 2022 року, за даними аналітичної блокчейн-компанії Chainalysis, ми посіли третє місце за використанням крипти у світі, випереджаючи навіть США. [1, с.54] В червні 2022 року Україна набула статусу кандидата в члени Європейського Союзу (ЄС). Крім того, що набуття статусу дає можливі фінансові переваги, у вигляді певних фінансових програм, це вимагає також від України приведення законодавства до вимог ЄС.

Як регулюються операції з криптовалютою в ЄС? Криптовалюти є легальними в ЄС з певними особливостями в державах-членах. Оподаткування криптовалюти залежить від країни, де стягуються податок на прибуток, розмір якого варіюється від 0 до 50%.

У 2015 році Суд ЄС постановив, що обмін між традиційною валютою та криптовалютою або віртуальною валютою повинен бути звільнений від ПДВ, оскільки криптовалюта є послугою, а не товаром. 20 червня 2021 року Європейська комісія опублікувала пакет законодавчих пропозицій щодо регулювання переказів коштів і певних криптоактивів для захисту громадян ЄС і фінансової системи від відмивання грошей і фінансування тероризму. Законодавчий пакет включав перегляд Регламенту про перекази коштів 2015 року для відстеження переказів криптоактивів (Регламент 2015/847/EU), створюючи нову та більш узгоджену нормативну та інституційну базу протидії відмиванню коштів та фінансуванню тероризму в ЄС. Важлива віха для правил криптовалюти в ЄС була досягнута 5 жовтня 2022 року, коли Рада ЄС схвалила та опублікувала затверджений текст довгоочікуваного закону про ринки криптовалютних активів (Markets in Crypto Assets Regulation (далі – MiCA). MiCA розширює так зване Crypto Travel Rule, яке вже існує в

традиційних фінансах, на перекази криптоактивів. Це правило вимагає, щоб інформація про джерело активу та його бенефіціара передавалася разом із транзакцією та зберігалася з обох сторін передачі. Постачальники послуг криптоактивів (CASP) будуть зобов’язані надавати цю інформацію компетентним органам у разі проведення розслідування щодо відмивання грошей і фінансування тероризму.

Регламент про ринки криптоактивів (MiCA) – це регламент ЄС, який регулює випуск та надання послуг, пов'язаних із криптоактивами та стейблкоінами. Прийнятий 20 квітня 2023 року Європейським парламентом, **MiCA є першим і єдиним у своєму роді законодавством у світі та є прикладом для інших юрисдикцій**.

У жовтні 2022 року ЄС досягнув політичного консенсусу щодо регулювання ринків криптоактивів (MiCA). Наразі його ратифіковано Європейським парламентом і, таким чином, стає першою нормативно-правовою базою для криптоактивів у світі. MiCA охоплює емітентів та постачальників послуг з метою захисту споживачів та інвесторів, забезпечення фінансової стабільності та підтримки інновацій. Регламент, який набуде чинності в період з середини 2024 року до початку 2025 року, позиціонує Європу як привабливий регіон на ринку криптовалют.

«MiCA – це новаторський законодавчий документ із погляду регулювання криптовалютних ринків. Це, безперечно, робить Європейський Союз світовим лідером. Ми також повинні бути добре обізнані, що криптовалютні ринки є мультиюрисдикційними. Регуляторні зусилля, аналогічні до MiCA в інших юрисдикціях, сприятимуть створенню безпечної, надійної та необхідної екосистеми для ринків криптоактивів у всьому світі», — пояснює Марія Хосе Ескрібано, член групи цифрового регулювання BBVA. [2]

Що регулює MiCA? MiCA визначає криптоактив як «цифрове уявлення вартості або прав, які можуть передаватися та зберігатися в електронному вигляді з використанням технології розподіленого реєстру або аналогічної технології». У Регламенті проводиться різницю між «криптовалютами», з одного боку, і «токенами», з іншого. MiCA також встановлює вимоги до емітентів криптоактивів та постачальників послуг криптоактивів (CASP). Емітенти криптоактивів повинні надавати повну та прозору інформацію про криптоактиви, які вони випускають, та дотримуватись правил розкриття інформації та прозорості. Постачальники послуг криптоактивів повинні бути зареєстровані, застосовувати заходи безпеки та відповідати вимогам щодо боротьби з відмиванням

грошей. Класифікація криптоактивів. MiCA забезпечує нормативно-правову базу цифрових активів, використовують технологію децентралізованого реєстру (DLT). Основні криптоактиви, що покриваються MiCA:

1. Токени, прив'язані до активів (ART), тип криптоактиву, призначений для підтримки стабільної вартості за рахунок посилання на вартість кількох фіатних валют, що є законним платіжним засобом, одного або кількох товарів або одного чи кількох криптоактивів, або поєднання таких активів. До цієї категорії входять усі криптоактиви, які не кваліфікуються як «токени електронних грошей», які мають підтримувати стабільну вартість, посилаючись на вартість фіатної валюти, яка є законним платіжним засобом. Прикладом цього є Digix (DGX), забезпечений еквівалентною кількістю фізичного золота, що зберігається у безпечному сховищі.

2. Жетони електронних грошей (EMT), які мають підтримувати стабільну вартість, посилаючись на вартість фіатної валюти, яка є законним платіжним засобом. Різниця між ART та EMT полягає у конфігурації базового активу, який підтримує ціну. ART використовують безготівкові активи чи кошик валют, тоді як EMT використовують єдину валюту, що наближає їх до концепції електронних грошей.

3. Криптоактиви, які не вважаються ART або EMT, такі як «службові токени», які призначені для надання цифрового доступу до товару чи послуги, доступних у DLT, і приймаються лише емітентом цього токена. На відміну від токенів безпеки вони не вважаються фінансовим інструментом відповідно до законодавства про цінні папери багатьох країн.

Криптоактиви, що не покриваються MiCA. MiCa виключає нові парадигми, такі як індустрія DeFi (децентралізовані фінанси) та незамінні токени (NFT). Згідно з визначенням, наданим Європейським центральним банком, DeFi — це новий спосіб надання фінансових послуг, який обходиться без традиційних централізованих посередників і натомість покладається на автоматизовані протоколи.

"MiCA залишає за рамками кілька компонентів світу цифрових активів", - пояснила Марія Хосе Ескрібано. *«DeFi — це один з них, а також незамінні токени, токени безпеки і навіть фінансування криптоактивів. Всі ці змінні або вже мають своє регулювання відповідно до їхньої природи, як у випадку з сек'юріті-токенами, або мають такі специфічні особливості, що законодавцям необхідно провести подальший аналіз для налаштування нормативно-правової бази, яка відповідним чином враховує ризики»*, — зазначила вона . У будь-якому випадку, *«MiCA,*

безперечно, є кроком вперед до надійного захисту прав споживачів при мінімізації ризиків, які ці ринки можуть становити для фінансової стабільності», - констатувала вона. [2]

З іншого боку, невзаємозамінні токени - це унікальні та неподільні токени, які є твором цифрового мистецтва, відео, твіт або будь-який інший унікальний об'єкт. На відміну від криптовалют, які взаємозамінні або обмінюються на інші рівноцінні криптовалюти, NFT є неповторними та підтримуються унікальними активами. Цифрові валюти центральних банків (CBDC) також виходять за межі MiCA. **Яке значення має MiCA?** Експерти із цифрового регулювання BBVA пояснюють, що MiCA забезпечить нормативну визначеність та надійніший захист споживачів на ринку криптовалют, підтримуючи при цьому інновації. Для досягнення цієї мети MiCA створює механізми, які гарантують, що стабільні монети дійсно стабільні, вимагають підвищеної прозорості на ринку і не дозволяють гравцям створювати надмірний ризик, забезпечуючи при цьому справжній захист активів, які перебувають під вартою. MiCA також прагне пом'якшити вплив криптовалют на довкілля. Деякий майнінг криптовалюти — процес перевірки транзакцій та додавання нових одиниць до блокчейну — потребує потужного обладнання, що споживає велику кількість

енергії, яка може бути отримана з викопного палива, такого як вугілля. Промисловість також потребує значного обсягу комп'ютерних компонентів та виробляє електронні відходи. MiCA розроблений як будівельний блок ширших зусиль з регулювання, які включають такі ініціативи, як Закон про цифрову операційну стійкість (DORA), пілотний режим DLT та Положення про переказ коштів (TFR). DORA встановлює стандарти для розробки та підтримки заходів безпеки в організаціях фінансового сектору та третіх осіб, які надають супутні послуги, такі як хмарні обчислення та аналіз даних. Пілотний режим DLT спрямований на впровадження пілотних ринкових інфраструктур для випуску, торгівлі та розрахунку токенів безпеки з використанням технології DLT, а також змінює визначення фінансового інструменту відповідно до Директиви MiFID II, щоб включити інструменти, засновані на технології DLT. Нарешті, Регламент про переказ коштів (TFR) застосовується до переказів криптоактивів та забезпечує фінансову прозорість під час обміну криптоактивами. [2,3].

MiCA: переваги та недоліки. **[4]** MiCA спрямований на захист споживачів та інвесторів, а також на створення прозорості та стабільності в індустрії. Експерти зазначають, що MiCA підвищить інвестиційну привабливість регіону. Єдиний підхід до

регулювання цифрових активів спростить взаємодію профільних компаній з регуляторами та знизить адміністративні витрати. Серед основних переваг експерти виділяють такі: спрощення експансії на ринку. підвищення довіри до індустрії, можливість працювати у всіх країнах ЄС, маючи ліцензію однієї з них. Однак при цьому зазначається, що нові правила будуть більш сприятливими для великих гравців, а невеликі проєкти, стартапи можуть зіткнутися зі збільшенням витрат та навіть можуть покинути ринок. Окрім того, виникає загроза зарегульованості крипто галузі.

Україні потрібна термінова легалізація віртуальних активів, що дасть поштовх для створення нового сектору економіки та сприятиме додатковим податковим надходженням до бюджету. Зараз законодавці завершують підготовку оновленого законопроєкту про віртуальні активи, який, ймовірно, буде ухвалений наприкінці року. Регулювання в Україні, що розповсюдиться і на криптогалузь, буде побудоване на європейських нормах MiCA, Нове законодавство детальніше описуватиме профільні поняття про цифрові активи й закладе основні принципи оподаткування в галузях, дотичних, зокрема, до криптовалют. Проте це остаточно не вирішить ключових проблем індустрії, що опинилася в сірій зоні і фактично не може функціонувати в Україні

через неформальні обмеження з боку банків. По-перше, Європа лише в липні ухвалить остаточну редакцію MiCA. По-друге, українському парламенту необхідно впровадити відповідні зміни до Податкового кодексу, а це може затягнути процес.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Геннадій Андрощук Патентування крипто валютних і блокчейн-технологій: стан, тенденції, проблеми регулювання. // Теорія і практика інтелектуальної власності 12/2023.- С53-63.

2.EU Markets in Cryptoassets (MiCA) Regulation: What is it and why does it matter? URL: https://www.bbva.com/en/innovation/eu-markets-in-cryptoassets-mica-regulation-what-is-it-and-why-does-it-matter/

3.EU lawmakers approve world’s first comprehensive framework for crypto regulation. URL: https://www.cnbc.com/2023/04/20/eu-lawmakers-approve-worlds-first-comprehensive-crypto-regulation.html

4.Як прийняття MiCA вплине на криптоіндустрію ЄС та України: думки експертів. URL: https://fintechinsider.com.ua/yak-pryjnyattya-mica-vplyne-na-kryptoindustriyu-yes-ta-ukrayiny-dumky-ekspertiv/

БАЛАЧІНА Єлизавета
студентка, Дніпровський національний
університет імені Олеся Гончара
ДЖУР Ольга
к.т.н., Дніпровський національний
університет імені Олеся Гончара

КРИПТОВАЛЮТА: ОСОБЛИВОСТІ ЕКОНОМІЧНОГО ТА ПРАВОВОГО УПРАВЛІННЯ

Криптовалюта є різновидом електронних грошей, насамперед цифрових та віртуальних. Одиниця валюти є монета, яка захищена від підробки. Вона є зашифрованою інформацією, скопіювати яку неможливо. Криптовалюта емітується в мережі та не пов'язана зі звичайною валютою чи державною валютною системою [4].

Вперше термін «криптовалюта» стали використовувати після появи платіжної системи «Біткоїн», розробленої в 2009 р. До 01.07.2013 р. програмне забезпечення практично всіх криптовалют базувалося на відкритому вихідному коді системи «Біткоїн». У липні 2013 р. з'явилися нові платформи, які підтримують різну інфраструктуру – біржову торгівлю, магазини та інше. До таких криптоплатформ відносяться: BitShares, Mastercoin, NXT та інші

платформи На сьогоднішній день будь-який бажаючий може не тільки отримувати криптовалюту, але й створювати свою [3, с. 152].

У більшості країн існує законодавство про випуск та обіг електронних грошей. Йдеться насамперед про Директиву Європейського парламенту та Ради ЄС від 16 вересня 2009 р. 2009/110/ЄС про допуск до діяльності організацій електронних грошей та її здійснення, а також про пруденційний нагляд за цими організаціями, про зміну Директив 2005/60/ЄС та 2006/48/ЄС та про скасування Директиви 2000/46/ЄС [1, с. 68].

Ще у 2012 р. Європейський центральний банк визначав віртуальну валюту як «тип нерегульованих цифрових грошей, який випускається і зазвичай контролюється їхніми розробниками, використовується та приймається серед членів певної віртуальної спільноти». ЄЦБ класифікує біткоін як децентралізовану віртуальну валюту, воліючи використовувати термін «віртуальна валюта», а не «цифрова» чи «крипто». Поки що це була перша спроба визначитися з предметом регулювання [3, с. 153].

У 2015 р. Європейський Центробанк проаналізував ризики та визначив юридичний та економічний характер криптовалюту. На його думку, віртуальна валюта не є грошима чи валютою з

юридичної точки зору. З економічної точки зору криптовалюти не повністю відповідають усім трьом функцій грошей як обміну, збереження цінності та способу обліку. Але криптовалюта може виконувати функцію засобу обміну чи одиниці обліку.

Однак через їх високу волатильність її не можна назвати засобом для заощадження. Вона, скоріше, є «договірними грошима». Це «угода між покупцем та продавцем, щоб прийняти цю віртуальну валюту як платіжний засіб». У результаті ЄЦБ уточнив розуміння криптовалюти, а саме: *«віртуальна валюта – це цифрове уявлення вартості, не випущене центральним банком або кредитною установою, яке в деяких випадках може використовуватись як альтернатива грошам*» [2].

Сьогодні визначення статусу криптовалют є важливим для обговорення питання, до чого належить регулювання цього явища – до компетенції ЄС, держав-членів ЄС або спільної компетенції. Це передбачає застосування положень *acquis* ЄС або національного законодавства держав-членів ЄС, або обох. Щоб знайти відповідь на це питання, слід звернутися до статей 2-6 Римського договору про функціонування ЄС 1957 року, згідно з якими:

- до виключної компетенції ЄС входить грошова політика в зоні євро, якщо криптовалюту визнають як гроші або електронні гроші.
- до спільної компетенції ЄС та держав-членів відносяться питання внутрішнього ринку та захисту прав споживачів, а також технологічного розвитку [2].

Законопроект «Про віртуальні валюти» № 3637 від 11.06.2020 р. був зареєстрований у Верховній Раді України, після чого проходив процедуру розгляду у профільних комітетах, вносився на доопрацювання та повертався для подальшого розгляду [5]. Нарешті, 02.12.2020 року було прийнято рішення про прийняття законопроекту за основу у першому читанні, а 08.09.2021 року - прийнято його в цілому. Проте, хоча закон було підписано Головою Верховної Ради та направлено на підпис Президенту 21.09.2022 року, гарант Конституції відмовився підписувати його та повернув до лав Верховної Ради зі своїми пропозиціями 05.10.2021 року. Після п'яти місяців проходження процедур розгляду та погоджень з пропозиціями Президента, закон був підписаний Головою Верховної Ради та направлений на підпис Президенту 11.03.2022 року, і нарешті 15.03.2022 року став офіційно прийнятим законом.

Законопроект №7150 зі змінами до Податкового кодексу України був зареєстрований в Верховній Раді України 13.03.2022 року [6]. Застосування санкцій, передбачених статтею 23, може бути обмежене до впровадження Державного реєстру постачальників послуг, пов’язаних з оборотом віртуальних активів, якщо це зазначено у пункті 2 Розділу VI Прикінцевих та перехідних положень. Законодавство України про віртуальні активи, як визначено в статті 3 Закону 2074, складається з Конституції України, міжнародних договорів, які були підтверджені Верховною Радою України, Цивільного кодексу України, цього Закону, Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та інших законів, а також нормативно-правових актів, які були прийняті на їх виконання.

Запуск легального ринку віртуальних активів допоможе Україні вийти на провідне місце у світовій цифровій економіці, використовуючи свій потужний потенціал. Цей законопроект дозволить українським блокчейн-компаніям легалізувати свої бізнес-процеси та офіційно працювати з банківською системою. Крім того, громадяни, які заробляють на операціях з віртуальними активами, також матимуть можливість

користуватися цим ринком, що допоможе уникнути юридичних ризиків та приверне увагу міжнародних криптокомпаній і залучить іноземні інвестиції в нову прогресивну галузь [3, с. 155-156].

Після впровадження нормативного регулювання на криптовалютному ринку, міжнародні компанії матимуть можливість законно реєструвати блокчейн-бізнес в Україні. Крім того, запропонований законопроект вносить зміни до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом». Відповідно до цих змін, після створення центрального органу виконавчої влади, що впроваджує політику у сфері обігу віртуальних активів, функції державного фінансового моніторингу в галузі обігу віртуальних активів передаються до нього від Міністерства цифрової трансформації. Україна враховує позитивний міжнародний досвід законодавчого регулювання обігу віртуальних активів у різних країнах світу та оцінює потенційні та реальні ризики [2].

Україні надзвичайно важливо прийняти законопроект «Про віртуальні активи» [9], який передбачає комплексне регулювання відносин, пов'язаних зі створенням, випуском та обігом віртуальних активів. Це сприятиме забезпеченню відкритості та прозорості в угодах, що укладаються на

ринку віртуальних активів, а також допоможе запобігти зловживанням з боку недобросовісних учасників. З набуттям чинності цим законом, власники віртуальних активів, зокрема криптовалют, зможуть отримати ряд переваг, оскільки законодавче регулювання забезпечить захист їхніх статків у віртуальних активах в разі непередбачуваних ситуацій.

Отже, питання щодо правового статусу криптовалюти обговорюється як у світі в цілому, так і в ЄС, і вимагає спільних дій. Згідно поточної позиції багатьох держав-членів та ЄС в цілому, регулювання цього правового явища є спільною компетенцією. Однією з підстав для такого висновку є п. 10 преамбули до Директиви ЄС №2018/843, який було згадано раніше, де проведено розмежування між віртуальними валютами, грошима та електронними грошима [2].

Для України в сучасних умовах актуальним є схвалення законопроекту “Про віртуальні активи” [5], проект якого передбачає комплексне регулювання відносин, що виникають з приводу створення, випуску та обігу віртуальних активів. Реалізація запропонованих положень сприятиме забезпеченню відкритості та прозорості угод, які укладаються на ринку віртуальних активів, та запобіганню зловживанням на цьому ринку з боку недобросовісних учасників. З набуттям чинності цим законом власники віртуальних активів, й зокрема

криптовалют, отримають низку переваг. Завдяки тому, що з’явиться законодавче регулювання цієї сфери, вони, як мінімум, зможуть захистити свої статки у віртуальних активах, якщо щось трапиться.

Крім того, будуть вирішені питання щодо розбудови інфраструктури ринку віртуальних активів, забезпечення його відкритості та ефективності. Метою прийняття цього акту є: впорядкування нормативно-правового регулювання для ринку віртуальних активів, його учасників; визначення правового статусу віртуальних активів як об'єктів цивільних прав; впорядкування цивільно-правових відносин між фізичними та юридичними особами, які виникають в процесі використання віртуальних активів; визначення правового статусу учасників ринку та користувачів у сфері віртуальних активів; встановлення основних засад та принципів державної політики у сфері віртуальних активів; державне регулювання та контроль на ринку віртуальних активів.

Такі види попиту на криптовалюту, як спекулятивно-інвесторський, переказ криптовалюти на інший рахунок без комісії (або менше 0,1%) завжди будуть потребувати особливо ретельного виду контролю із боку держави. Потребує обережного використання та контролю заходи по купівлі товару за криптовалюту, оскільки цей вид операцій може

призвести до втрати власності на майно і не може бути застосований на підприємствах оборонного сектору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Волосович С.В. Віртуальна валюта: глобалізаційні виклики і перспективи розвитку. Економіка України. 2016. № 4. С.68–87.

2. Горохов А. Криптовалюта в Україні: усі «за» та «проти». URL: http://eizvestia.com/uk/finance-ukr/full/210-kriptovalyuta-v-ukraini-usi-za-i-proti

3. Логойда В.М. Перспективи врегулювання правового статусу криптовалюти в Україні. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. № 63. С.152- 157.

4. Мамзуренко О. Регулювання цифрових активів: досягнення України за 2019 рік та ситуація у світі. Nachasi. URL: https://nachasi.com/2019/12/26/regulyvanna-cyfrovyh-aktyviv/

5. Про віртуальні активи. Закон України, № 2074-IX від 17.02.2022. URL: https://zakon. rada.gov.ua/go/2074-20

6. Офіційний сайт Верховної Ради України. Проект Закону Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами. № 7150 від 13.03.2022. URL: https://itd.rada.gov.ua/ billInfo/Bills/Card/39211

7. Офіційний сайт платформи Ліга:Закон. Цивільний кодекс України. №435-IV від 16.01.2003. URL: https://ips.ligazakon.net/document/T030435.
8. Левенець О. Що таке криптовалюта і як вона працює. Creditznatok UA. URL: https:// creditznatok.com.ua/ua/article/lichnye-finansy/ chto-takoe-kriptovalyuta-i-kak-ona-rabotaet/

БЕЖЕВЕЦЬ Алла

старший викладач, кафедри інформаційного,
господарського та адміністративного права,
КПІ ім. Ігоря Сікорського

ЕЛЕКТРОННІ ГРОШІ ЯК ЕЛЕМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

Незважаючи на такий складний для України час – життя в умовах повномасштабного вторгнення – в країні продовжуються еволюційні зміни законодавства, спрямовані на євроінтеграцію та цифровізацію усіх сфер. І хоча деякі зміни не можна назвати нагальними, проте вони відбулися, і це доволі амбітний крок на шляху цифрової трансформації суспільства.

Йтиметься про електронні гроші. 12 січня 2023 року Закон України «Про платіжні послуги» (далі –

Закон) отримав нову редакцію, яка вразила своєю сміливістю як надавачів, так і отримувачів платіжних послуг. Цей закон не був несподіванкою і пройшов тривалий шлях від закладення його підвалин Постановою Правління Національного банку України від 25.06.2008 №178 (втратила чинність у 2011 році), тобто з підзаконного рівня. Наразі потреба у законодавчому врегулюванні цього питання знайшла своє втілення у зазначеному вище акті.

Пропонуємо розглянути деякі новели, що відтепер легалізовано в Україні. Так, відповідно до ст. 3 нової редакції закону грошові кошти (кошти) існують в Україні у готівковій (формі грошових знаків) та безготівковій (формі записів на рахунках) формах. Грошові кошти (кошти) для цілей цього Закону включають також електронні гроші та цифрові гроші у випадках, передбачених цим Законом. Отже, з огляду на зазначене, а також враховуючи, що згідно преамбули Закону слова "грошові кошти" замінено словом "кошти", а електронні гаманці користувачів прирівнюються до банківських рахунків, виходячі зі змісту Закону України «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг» [2], доцільно зробити висновок про урівняння грошових коштів, електронних грошей та цифрових грошей. І хоча

електронні гроші можна вважати еквівалентом реальних грошей не в усіх випадках, а лише прямо передбачених Законом, це дозволить проводити повсякденні, рутинні розрахунки, наприклад, за комунальні послуги або сплату податків, оплачувати товари, роботи або послуги за допомогою не тільки «звичайних» грошей.

Цифрові гроші – це електронна форма грошової одиниці України, емітентом якої є Національний банк України [1]. Іншими словами, це цифрова гривня і випускає її виключно НБУ. Згідно інформації, що міститься на офіційному сайті НБУ, е-гривня покликана доповнити готівкову та безготівкову форми гривні, виконуючи усі функції грошей [3].

Електронні гроші та цифрові гроші існують лише в безготівковій формі [1]. При цьому не слід ототожнювати електронні гроші та безготівку. Хоча за ідентифікацією (реєстрацією в фіскальному органі) та способом використання (оплата товарів, робіт, послуг, отримання готівки) безготівковий рахунок і електронний гаманець схожі, але в той же час мають і багато відмінних ознак. Серед основних, на нашу думку, слід зазначити наступні:

- Електронні гроші зберігаються в електронному гаманці, який по суті є програмним застосунком, що встановлюється на електронний пристрій -

телефон або комп'ютер. Безготівковий рахунок відкривається шляхом внесення готівки на рахунок в фінансовій установі.

- Для безготівкових рахунків законодавством не встановлено лімітів поповнення або витрат, в той час, як для електронних гаманців такі ліміти передбачено.
- На відміну від поповнення електронного гаманця, існує багато зручних способів поповнення рахунку (внесення готівки, переказ через банкомат, термінал для поповнення тощо).
- Безготівкові кошти можна отримати/надати в кредит, а для електронних грошей кредитування не передбачено.

Проводячи дослідження, вважаємо за необхідне порівняти електронні гроші та криптовалюту. На превеликий жаль власників та адептів Bitcoin, Ethereum, Litecoin та іншої кріпти, які, вірогідно, сподівалися на легалізацію крипторинку, доцільно зауважити, що криптовалюта хоча і відноситься до різновидів цифрової валюти, проте має інше походження та регулювання ніж електронні гроші, а тому до сфери Закону не відноситься. Станом на сьогоднішній день ринок криптовалюти все ще залишається поза увагою законодавця.

Враховуючи наведене вище, підставно відзначити, що національне законодавство продовжує свій рух на шляху до цифровізації найважливіших сфер життя. Ці кроки стають більш помітними та корисними для пересічного українця, адже легалізуються речі, які спрощують життя і роблять його більш зручним. А людиноцентриський підхід має стати визначальним в провадженні політики та подальшої реалізації стратегії цифровізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1) Про платіжні послуги. Закон України від 30.06.2021. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text
2) Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг. Закон України від 12.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2888-20#n607
3) Про е-гривню – цифрові гроші Національного банку. Офіційний сайт НБУ. URL: https://bank.gov.ua/ua/payments/e-hryvnia

ВАРИНСЬКИЙ Владислав

кандидат політичних наук, доцент,
доцент кафедри філософії
Національного університету
«Одеська морська академія»

ОГЛЯД ОСНОВНИХ ЗАГРОЗ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАМІЩЕННІ РОБОЧИХ МІСЦЬ

Однією з основних проблем, пов'язаних з використанням штучного інтелекту (далі – ШІ) ШІ є можливість зміщення робочих місць. Використання штучного інтелекту в сфері виробництва даватиме підвищення продуктивності, краще планування і керування часом і, зрештою, до більш швидкого досягнення цілей. Допомога штучного інтелекту може знизити робоче навантаження та рівень стресу, дозволяючи людини зосередитися на інших важливих аспектах вашого життя. У міру того, як машини стануть інтелектуальнішими, цілком імовірно, що вони замінять людей у багатьох галузях.

Занепокоєння полягає в тому, що в міру того, як машини стають інтелектуальнішими та здібнішими, вони можуть замінити людей у багатьох галузях. Це

може призвести до масового переміщення робочих місць, оскільки машини можуть виконувати завдання більш ефективно, точно і з меншими витратами, ніж люди. Вплив зміщення робочих місць може мати далекосяжні наслідки, включаючи безробіття, втрату доходу та допомоги, а також економічну нестабільність. Це особливо турбує галузі, які вже мають труднощі, а також працівників, зайнятих на робочих місцях, які легко автоматизувати. Для вирішення цієї проблеми важливо розглянути політику та стратегії, які можуть пом'якшити наслідки усунення робочих місць, такі як програми підвищення кваліфікації та перекваліфікації для працівників, інвестиції в нові галузі та технології та створення мереж соціального захисту для постраждалих осіб та спільнот.

Умовно, небезпеки заміщення робочих місць штучним інтелектом можна згрупувати наступним чином:

1. Безробіття. Використання штучного інтелекту може призвести до звільнення людей, які раніше виконували ці роботи. Це може призвести до безробіття у не лише у виробничій сфері, а в менеджменті, і, звичайно, провокуватиме дуже чутливі соціальні проблеми. І це – не просто «роботи» і скорочення робочих місць низько кваліфікованих «конвеєрних» робітників, це – зовсім інший рівень

втрати персоналу з освітою робочих місць: страждатимуть домогосподарства, зазнаватиме освітня сфера.

Наприклад, розвиток автономних транспортних з ШІ може призвести до скорочення робочих місць водіїв та груп (екіпажів) працівників транспортних компаній. Це – реактивні прошарки. Відповідно, слід очікувати страйків, навіть, на стадії підходів до такого впровадження. Якщо ж виходити з п. 1, то штучний інтелект зможе заміщувати, якнайменше, диспетчерські, логістичні служби, тощо.

2. Втручання в «чутливі» для соціуму сфери. Наприклад, фінансова, медична та юридична сфери. Використання алгоритмів ШІ для аналізу даних та прийняття рішень може призвести до скорочення робочих місць у фінансових установах, а в медичній сфері не лише це, а й поступового відходу від медичної етики. Юридична же сера, і, зокрема, правосуддя, де суддя приймає рішень н власне переконання, в цілому, є однією з найбільш уразливих «тонких матерій», де об'єктивована «позиція» ШІ не може враховувати всіх емоційних відтінків суб'єктивної сторони вчинюваного, тобто – реально оцінювати людськими вимірами характер і ступінь вини обвинуваченого.

2. Нерівність – порушення людського принципу рівності. Хоча ШІ і може утворювати нові робочі місця,

зокрема, в системі самого керування штучним інтелектом, загрози принципу рівності, як гарантія прав людини, також можуть серйозно зазнавати. Зокрема, використання ШІ в сферах створення робочих місць та найму може призвести до збільшення розриву між тими, хто має доступ до нових технологій, і тими, то доступу до них не має.

3. Значущість помилок. ШІ може помилятися, і його помилки можуть призводити до серйозних наслідків. Невелика помилка ШІ, який керує літаком чи судном, можуть стати причиною трагедії. Зокрема, такі помилки можуть відбутися, навіть, у разі порушення енергоресурсу ШІ, внаслідок чого недостатня обробки інформації при розпізнаванні висоти хвиль, чи їх відтінку, можуть дати первинно некоректні дані для кута повороту судна.

Дуже яскравим з точки зору можливості помилок ШІ при використання його в правосудді.

З точки зору можливості та ергономічності, дійсно, штучний інтелект може бути використаний у правосудді для автоматизації та оптимізації процесів, таких як аналіз доказів, передбачення рішень, автоматизація рутинних процесів, оптимізація часу, запобігання помилкам. Однак, необхідно враховувати, що використання ШІ може викликати етичні питання в тандемах: прозорість і конфіденційність / захист даних,

прозорість і індивідуальний підхід, індивідуалізація покарання і загальна практика, доцільність і гуманність, і т. д.

Навіть, при першому погляді можна говорити про загрози при делегуванні здійснення правосуддя штучному інтелекту – помилки пов'язані з вірогідністю несправедливості, а також із нестачею прозорості та відкритості процесу:

- по-перше, ШІ може припускатися помилок у прийнятті рішень, особливо якщо він заснований на неповних або неточних даних. Це може призвести до несправедливих рішень та порушення прав людини;

- по-друге, використання ШІ може призвести до нестачі прозорості та відкритості процесу. Якщо алгоритми ШІ не є зрозумілими та доступними для громадськості, то це може призвести до недовіри до системи правосуддя та погіршення її легітимності;

- по-третє, використання ШІ може призвести до посилення дискримінації та нерівності. Якщо алгоритми ШІ ґрунтуються на стереотипах та упередженнях, то це може призвести до несправедливих рішень та порушення прав людини.

Спектр загроз некерованого, у тому числі експериментального використання ШІ, навіть, на рівні заміщення робочих місць охопити неможливо. І жодна футурологічна практика не зможе передбачити, що саме

можна дозволити ШІ робити, адже макі можливості охоплюватимуть досі швидко величезний спектр діяльності людей.

Натомість, рішеннями правових політик на рівні світу, і на рівні держав, можна визначити і унеможливити для впровадження ШІ певні сфери, зокрема, щодо заміщення персоналу. Таке регулювання допустимості використання ШІ може бути побудоване за принципом: «ШІ можна впроваджувати/використовувати лише там, де не заборонено». Але заборони мають бути рішучими і суворими, і знаття таких заборон може відбутися лише тоді, коли використання ШІ доведе свою оптимальну безпеку і сувору відповідність принципам робототехніки – через десятки років його використання в інших, дозволених сферах.

ВАСЬКО Владислав
аспірант, ДНУ ІІБП НАПрН України

УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ В БЛОКЧЕЙНІ: ОГЛЯД ПРАВОВИХ ПРОБЛЕМ

Швидкі темпи розвитку технологій 4-ої промислової революції (інтернету речей, машино-машинних комунікації, робототехніки, великих даних, блокчейну та штучного інтелекту) в останні роки призвели не тільки до масштабних трансформацій традиційних галузей економіки, а й до значних змін у суспільстві в цілому. Оскільки ці технології продовжують розвиватися і набувають все більшого поширення, вони також створюють унікальні правові виклики, які потребують ретельного вивчення.

Блокчейн – це технологія децентралізованого розподіленого реєстру, що забезпечує безпеку і надійність збереження даних. Іншими словами, це тип бази даних, яка складається з так званих блоків, котрі пов'язані і захищені за допомогою криптографії. Кожен блок містить позначку часу і криптографічний хеш попереднього блоку, створюючи ланцюжок, який неможливо змінити без зміни наступних блоків [1]. Це робить дані, що зберігаються в блокчейні, незмінними і

прозорими, оскільки всі учасники мережі мають до них доступ і можуть перевірити їхню автентичність без необхідності залучення центральних органів або посередників.

Незважаючи на те, що децентралізований і незмінний характер блокчейну може надати унікальні переваги для більшості сучасних бізнес-моделей та покращити низку державних послуг, котрі надаються органами публічної влади, він також створює комплексні правові проблеми його застосування.

Один з головних ризиків використання цієї технології полягає в неможливості повного контролю та/або зупинення роботи мережі блокчейн, оскільки вона підтримується безліччю не пов'язаних між собою комп'ютерів. Транзакції в блокчейні підтверджуються вузлами, що гарантує, що жоден суб'єкт не може змінити записану в ньому інформацію без консенсусу з мережею [1]. Це створює проблеми визначення юридичної відповідальності учасників блокчейн-середовища у разі неналежного його функціонування, оскільки кожен вузол мережі має свій власний вклад у валідацію транзакцій та збереження інформації в блокчейні [2]. Тобто, у разі виникнення проблем в роботі блокчейну розподіл ризиків і визначення ступені вини є дуже складним процесом, котрий вимагає аналізу діяльності всіх учасників системи.

Крім того, слід зазначити, що блокчейн може працювати в різних юрисдикціях і географічних кордонах. Це в свою чергу також породжує ряд правових проблем, оскільки у такому децентралізованому середовищі складно визначити застосовне право до відносин, які виникають між учасниками системи. У зв'язку з цим у різних країнах можуть діяти різні правила, закони та підзаконні НПА, які можуть суперечити один одному. Відсутність централізованого органу, який би регулював і керував технологією, може створювати невизначеність, а суперечки можуть виникати через різне тлумачення законів і нормативних актів.

Тому задля вирішення вищезазначених проблем вкрай важливо подолати анонімність учасників блокчейну, що надасть змогу встановлювати місцеперебування сторін, відстежувати транзакції та визначити, хто нестиме відповідальність за ті чи інші дії в мережі. Однак важливо зазначити, що місцезнаходження вузла не обов'язково збігається з місцезнаходженням фізичної або юридичної особи, яка здійснює транзакцію [3]. Саме тут виникає питання автентифікації особи віддаленої сторони. Для забезпечення безпеки і легітимності транзакцій вкрай важливо мати надійну систему перевірки осіб, яка до

того ж може забезпечувати необхідний рівень довіри між сторонами та мінімізувати випадки шахрайства.

У цьому аспекті необхідно розуміти, що цифрова ідентифікація складається з інформації про особу, що зберігається і передається різним користувачам. Зазвичай методи цифрової ідентифікації включають два етапи: автентифікацію та верифікацію особи. Автентифікація особи – це процес перевірки ідентичності фізичної чи юридичної особи, як правило, за допомогою облікових даних, таких як імена користувачів, паролі або біометричні дані. Після перевірки автентичності особа реєструється в системі і може використовувати свій обліковий запис для здійснення транзакцій. Підтвердження особи відбувається під час кожної транзакції і передбачає використання даних зареєстрованої особи. Це може включати використання цифрових підписів або інших форм ідентифікації для нерозривного зв'язку особи з транзакцією [4].

Таким чином, у разі здійснення транзакцій у мережі, в ній будуть зберігатись два ключові елементи: ідентифікаційні дані закріплені за особою, та ідентифікаційні дані закріплені за транзакцією, яка здійснюється. Перший елемент ідентифікує сторони і, отже, безпосередньо впливає на можливість здійснення правочинів. Другий – це масив інформації про

транзакції (наприклад, вид, час виконання, місце здійснення тощо), які здійснює користувач. Отже, ми приходимо до розуміння того, що ідентичність є фундаментальним елементом, який пов'язує інформацію про вчинені учасниками блокчейн-мережі дії (включаючи транзакції) з конкретними фізичними чи юридичними особами та визначенням місця їх фактичного перебування.

Тому, для впровадження системи управління ризиками у блокчейні необхідно його доповнити ідентифікатором, який зможе не тільки посприяти в забезпеченні більшої безпеки, але й гарантувати захист прав та інтересів учасників мережі. На сьогодні існує два основних підходи до реалізації цієї системи [5].

1.Позамережеве управління ідентифікацією – це система, в якій інформація про особу зберігається поза блокчейном, але пов'язана з ним за допомогою криптографічних механізмів. У цій системі особиста інформація користувачів зберігається в захищеній, зашифрованій базі даних, яка не є загальнодоступною. Коли користувачеві потрібно підтвердити свою особу, він надає криптографічний доказ, який пов'язаний з його ідентифікаційною інформацією в позамережевій базі даних.

Перевагою позамережевого управління ідентифікацією є висока масштабованість та

ефективність, оскільки ідентифікаційна інформація не зберігається в самому блокчейні. Ця система також має потенціал для збереження конфіденційності, оскільки персональна інформація зберігається в захищеній базі даних, а не у відкритому доступі в блокчейні.

Однак управління ідентифікацією поза ланцюжком також може бути менш прозорим, ніж управління ідентифікацією в ланцюжку, оскільки інформація про особу не є безпосередньо доступною в блокчейні. Крім того, можуть виникнути проблеми з безпекою позамережевої бази даних, оскільки вона не так добре захищена, як сам блокчейн.

2.Внутрішньомережеве управління ідентифікацією відноситься до системи, в якій інформація про особу зберігається безпосередньо в блокчейні. Це означає, що персональні дані користувачів записується у вигляді транзакцій у розподілене середовище. Ці транзакції є незмінними і захищеними від підробки, але до них може отримати доступ і перевірити будь-хто, хто має доступ до блокчейну.

Перевагою управління ідентифікацією в мережі блокчейн є високий рівень безпеки. Крім того, застосування цієї технології може зменшити потребу в посередниках і сторонніх службах верифікації, що

призведе до більшої ефективності та матиме суттєвий економічний ефект.

Хоча децентралізований і прозорий характер блокчейну може запропонувати значні переваги для управління ідентифікацією, він також викликає питання, що стосуються захисту даних і конфіденційності. Оскільки системи ідентифікації на основі блокчейну записують дані незмінно і публічно, існує ризик того, що персональні дані можуть бути розкриті або використані не за призначенням, якщо управління в блокчейн-середовищі щодо них здійснюється неналежним чином. Це особливо актуально в світлі Загального регламенту ЄС про захист даних (GDPR), який встановлює суворі вимоги до збору, обробки та зберігання особистої інформації [6].

Щоб відповідати GDPR та іншим законам про захист даних, системи ідентифікації на основі блокчейну повинні гарантувати, що персональні дані збираються і обробляються з відповідної згоди, зашифровуються, якщо це необхідно, і доступні тільки уповноваженим особам. Крім того, особи повинні мати право на доступ, виправлення та видалення своїх персональних даних, що є дуже складним завданням у децентралізованому середовищі блокчейну [6].

Ще однією правовою проблемою, пов'язаною з управлінням ідентифікацією на основі блокчейну, є

відсутність стандартизації в галузі. Наразі не існує загальновизнаних стандартів для таких систем, що може створити невизначеність щодо дотримання ними правових та регуляторних норм. Але робота в цьому напрямку вже ведеться, так Європейська система суверенної ідентичності (ESSIF), яка є частиною Європейської інфраструктури блокчейн-сервісів (EBSI) працює над створенням стандартів для децентралізованих систем ідентифікації для надання транскордонних державних послуг на території ЄС з використанням технології блокчейн [7].

Отже, як централізований, так і децентралізований підходи до управління ідентифікаційними даними мають свої плюси і мінуси, і рішення про те, який з них використовувати, буде залежати від конкретного контексту та вимог системи. Хоча рішення на основі блокчейну мають низку переваг над централізованими середовищами, їхнє впровадження та використання може бути обмеженим доти, доки вони не розв’яжуть проблему конфіденційності персональних даних та будуть більш широко визнані та прийняті державними регуляторними органами. У свою чергу вирішення проблеми ідентифікації учасників блокчейн-мережі допоможе розв’язати інші правові проблеми застосування цієї технології. Але в цьому сенсі також

необхідно враховувати особливості децентралізованих мереж, адже за своєю природою більшість публічних блокчейнів є вже саморегулюючими середовищами. Тому описані нами проблеми і їх часткове вирішення будуть стосуватись більшою мірою контрольованих (закритих) блокчейн-систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Hayes A. Blockchain Facts: What Is It, How It Works, and How It Can Be Used. URL: https://bit.ly/3VyoeCW

2.Васько В.А. Проблема визначення змісту юридичної відповідальності валідаторів блокчейн-транзакцій. Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали II всеукр. наук.-практ. конф., Київ, 25 грудня 2022 р. / наук. керівник конф. О. А. Баранов ; упор.: В. М. Фурашев, С. О. Дорогих, М. В. Дубняк. – Київ-Одеса, 2022. – С.82-86

3.Brooke B. What Are Blockchain Nodes and How Do They Work?. URL: https://bit.ly/41ZGoQm

4.Verification and authentication: What's the difference and what's the latest? URL: https://bit.ly/42gFxuA

5.Blockchain Identity Management: Complete Guide 2023. URL: https://bit.ly/3LTPLeH.

6.Blockchain and GDPR (General Data Protection Regulation). URL: https://bit.ly/3Vu6lFm

7.ESSIF - European Self Sovereign Identity Framework. URL: https://bit.ly/412OCpB

ВОРОНЬКО Марина
студентка, КПІ ім. Ігоря Сікорського

СВОБОДА ПАНОРАМИ: ОГЛЯД УКРАЇНСЬКОГО ЗАКОНОДАВСТВА

Свобода панорами є винятком із загального авторського права. Відповідно до тлумачення авторів Занопопроєкту №1677 (про який нижче піде мова): Свобода панорами – це можливість фотографувати, знімати на відео, замальовувати та іншим способом фіксувати зовнішній вигляд тих захищених авторськими правами об’єктів, які знаходяться у відкритих для вільного відвідування місцях або видимі з таких місць, тобто будівель, пам’ятників, мостів, інтер’єрів станцій метро і т. д. Також свобода панорами передбачає відсутність будь-яких обмежень з боку авторів творів на виготовлення, розповсюдження і публічну демонстрацію подібних зображень [3]. У законодавстві України найбільш наближеним до розуміння свободи панорами є п.10 ч.2 ст.22 Закону України “Про авторське право і суміжні права”, відповідно до якого, без дозволу суб’єктів авторського права і безоплатно, але із зазначенням імені автора і джерела запозичення, допускається створення зображень творів архітектури та образотворчого

мистецтва, що постійно розташовані у доступних для громадськості місцях, та подальше використання таких об’єктів, за умови, що такі дії не мають самостійного економічного значення [1]. Як бачимо, в даному випадку йде мова про свободу панорами без дозволу на використання з комерційною метою.

Метою свободи панорами є, по-перше, задоволення культурних потреби громадян щодо доступу до творів мистецтва, які мають публічний характер. По-друге, це забезпечення піднесення сфери туристичної літератури, наповнення освітніх і наукових ресурсів візуальним контентом, пришвидшення розвитку художньої фотографії і кіно. В першу чергу це стосується творів архітектури і мистецтва, щодо яких ще не припинило дію авторське право (тобто не пройшло 70 років після смерті автора твору). Це, наприклад, комплекс післявоєнної забудови центру Києва, будівля Верховної Ради України, майже всі пам’ятники Тарасові Шевченку, всі пам’ятники, присвячені Незалежності України, загиблим у Голодоморі та Другій світовій війні [3]. Окрім цього, свобода панорами корисна для збереження «швидкотривалих творів», термін існування яких обмежений, і єдиним способом збереження яких є фотографування: малюнки на асфальті крейдою, малюнки на людському тілі фарбами, “піщані замки”

тощо. Свобода панорами звільняє від необхідності пошуку автора таких творів, що по суті є неможливим [4, с. 60].

Проте свобода панорами є дуже дискусійним питанням у сфері авторського права і часто піддається критиці. В першу чергу, через порушення інтелектуальних прав авторів будівель та скульптур, щодо яких надається вільне відтворення. Розглядаючи права авторів комплексно, менше страждають немайнові права (або не страждають зовсім), оскільки свобода панорами передбачає обов’язкове зазначення автора твору. В даному випадку, деякі науковці навіть вважають, що захист цих прав покращується. За відсутності свободи панорами, правами авторів нехтують або свідомо, або через неможливість знайти інформацію ні про автора споруди чи скульптури, ні щодо контактів для надсилання запиту про отримання дозволу. При цьому, зі свого боку, автори майже ніколи не звертаються до суду для захисту своїх прав.

Щодо порушення майнових прав думки висловлюються різкіше. В низці країн використання свободи панорами з комерційною метою вважається їх порушенням і забороняється законом. В Україні Постановою Кабінету міністрів “Про затвердження мінімальних ставок винагороди (роялті) за використання об'єктів авторського права і суміжних

прав” визначено, що у разі використання зображення певного архітектурного об’єкта під час виготовлення сувенірної продукції, виробник повинен сплатити автору за мінімальною ставкою авторської винагороди. Окрім цього, у коментарях до Законопроєкту №1677 Комітетом з питань європейської інтеграції було зазначено, що відповідно до статті 22 Конституції України, при прийнятті нових законів або внесенні змін до чинних законів не допускається звуження змісту та обсягу існуючих прав і свобод. Тому, позбавлення права суб’єкта авторського права отримувати винагороду у випадку комерційного використання його твору зі збереженням за ним його особистих немайнових прав може розглядатися як суттєве звуження змісту та обсягу існуючих прав і свобод [3]. Також, свобода панорами з дозволом на комерційне використання суперечить положенням ст. 440 та 441 ЦКУ, відповідно до яких, відтворення твору, як об‘єкту авторського права, будь-яким способом у будь-який спосіб є його використанням, що розглядається як майнове право інтелектуальної власності на твір, яке належить його авторові, якщо інше не встановлено договором чи законом.

Ще одним цікавим поглядом на ситуацію є авторське право на фотографічні твори. Так, у справі за позовом до видавництва, з вимогою вилучення з

обороту книги, через використання фотографій творів образотворчого мистецтва без зазначення автора, відповідач заперечував вимоги, посилаючись на те, що фотографічні твори, використані ним у книзі, є окремим об'єктом авторського права. За його словами, такі фотографічні твори є оригінальними та не є репродукціями творів позивача, оскільки під час їх створення фотографом було внесено його власну творчу складову. І хоча суд став на сторону позивача, дана справа цікава в контексті подальших досліджень балансу між свободою панорами та забезпеченням прав авторів.

В Україні існував Законопроєкт № 1677, який мав на меті запровадження свободи панорами. Зокрема, передбачалось доповнення ст. 21 Закону України “Про авторське право і суміжні права” такою нормою: “Без згоди автора (чи іншої особи, яка має авторське право), але з обов’язковим зазначенням імені автора і джерела запозичення, допускається відтворення будь-яким способом, крім механічно-контактного копіювання, творів образотворчого, ужиткового мистецтва, архітектури, містобудування і садово-паркового мистецтва, які знаходяться у громадських та публічно доступних місцях (за винятком експозицій виставок і музеїв), а також використання зображень, відеограм таких творів”.

Свобода панорами закріплена у країнах по всьому світу, зокрема в більшості країн Європи, а також у США [2, ст. 110]. Проте зміст поняття не є однаковим: в різних країнах свобода панорами може бути як з дозволом на використання з комерційною метою, так і без нього. Окрім цього, відрізняється предметна складова, адже хоча переважно мова йде про архітектурні споруди та пам'ятники, в деяких країнах це розширюється до фресок, графіті та інших пласких об'єктів (Швейцарія). Враховуючи написане, здавалося б, прийняття "свобода панорами" має бути складовою Євроінтеграції. Більше того, відповідно до Закону України «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу», питання свободи панорами належить до пріоритетних сфер, в яких здійснюється адаптація законодавства України до законодавства Європейського Союзу [3]. Проте, сама по собі свобода панорами досі залишається дискусійною у країнах ЄС, а відповідно до Директиви 2001/29/ЕС Європейського парламенту і Ради від 22 травня 2001 р., запровадження у національному законодавстві свободи панорами не є обов'язковим та лишається виключно на розсуд держави. На сьогодні, серед країн Європи є такі, що значно обмежують свободу панорами (Франція), або не мають її зовсім (Італія).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України "Про авторське право і суміжні права" від 01.12.2022 р. № 2811-IX // Відомості Верховної Ради України. - 2023. - № 16. - Ст. 118.

2. Улітіна О. В. Деякі питання авторського права на фотографічні твори: свобода панорами / О. В. Улітіна // Науковий вісник Ужгородського Національного Університету. Серія: Право. - 2015. - Т. 1, № 34. - С. 110-112.

3. Проект Закону України "Про внесення доповнень до Закону України "Про авторське право і суміжні права"" від 29.12.2014 р. № 1677 // Верховна Рада України. - URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=1677&skl=9 (дата звернення: 30.04.2023).

4. Коршакова О. М. Проблематика охорони фотографічних творів / О. М. Коршакова // Актуальні проблеми вітчизняної юриспруденції. - 2017. - Т. 1, № 6. - С. 60-61

ГОРОДЕЦЬКИЙ Назар
студент, КПІ ім. Ігоря Сікорського

ОХОРОНА ВИНАХОДІВ У КРАЇНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Анотація. Питання охорони об’єктів інтелектуальної власності з кожним роком набуває все більшої актуальності, що зокрема слід пов’язувати із науково-технічним прогресом. Окрім того, важливим є вивчення практики Європейських країн, що зумовлено євро-антлантичним вектором розвитку держави та євроінтеграційними процесами. В контексті даної роботи було досліджено питання охорони винаходів у країнах Європейського Союзу, вивчено основні нормативно-правові акти та надано їм оцінку.

Ключові слава: *інтелектуальна власність, охорона винаходів, винахід, Європейський Союз, законодавство ЄС*.

Питання прав інтелектуальної власності завжди цікавило велику кількість людей. Переважно такими є особи творчих галузей діяльності, а відтак практикам задавалися масово питання, щодо правового регулювання даного питання. Варто відмітити, що на законодавець вирішуючи питання передачі інтелектуальних прав створив певну ієрархічну систему,

яка своїй сукупності відповідає як на питання матеріальних так і процесуальних аспектів.

Перш за все, варто сказати, що в умовах сучасності правова охорона у праві інтелектуальної власності є способом захисту від тих чи інших несприятливих ризиків та факторів. Такими ризиками, безпосередньо, є робота із недобросовісними контрагентами, можливість зниження іміджу та рейтингу, у результаті здійснення діяльності, яка може порушувати права інтелектуальної власності. Модернізація економіки щороку набуває все більших обертів, що позначається в тому числі і на праві інтелектуальної власності. Постійно створюються об'єкти, що використовуються суспільством для вдосконалення процесу вироблення сучасних технологій, модернізації суспільства та окремих його елементів.

Суть охорони прав на об'єкти інтелектуальної власності полягає в тому, що автор об'єкта інтелектуальної власності отримує від держави виключні права на створений об'єкт інтелектуальної власності на певний період часу.

У Європейьскому законодавстві питання охорони винаходів є окремим інститутом у праві інтелектуальної власності, а також в цілому у позитивіському напрямку законодавчого регулювання. Так, охорона об’єктів

авторського права відбуваєтьсяодразу на трьох рівнях. Серед таких першим є безпосередньо міжнародні угоди, наступним – в межах європейських угод. Щодо третього рівня то він являє собою сукупність двох перших, адже виражений в імплементованому законодавстві країн-членів ЄС.

Варто відзначии, що існують і інші наукові підходи, які визначають захист прав на винаходи в Європі дворівнивими[14]. З одного боку, Директивою № 98/71/ЄС Європейського Парламенту та Ради від 13 жовтня 1998 р. про правову охорону промислових зразків було проведено гармонізацію національного законодавства держав-членів щодо промислових зразків та водночас було визнано за доцільне створення наднаціональної системи охорони прав на промислові зразки на рівні Спільноти і поспіль ухвалено відповідний Регламент Ради (ЄС) № 6/2002 від 12 грудня 2001 р. про промислові зразки Спільноти [15].

Переходячи конкретно до питання охорони варто відмітити, що Регламентом Ради ЄС №6/2002, зокрема запроваджено:

- єдиний правовий режим на рівні Спільноти;
- усунуто явні штучні відмінності їх охорони в окремих членах ЄС;
- створено рівні умови конкуренції для всіх учасників ринку;

- забезпечено правову основу дрібносерійного виробництва товарів на основі концепції прогресивного маркетингу;
- усунуто колізії в національних системах реєстрації промислових зразків.

Варто також відмітити, що неабиякого значення в питанні становлення охорони винаходів мало прийняття, ще в 1925 році Гаазької угоди про міжнародне депонування промислових зразків, яка була переглянута у Лондоні у 1934 р., а у 1960 р. у Гаазі переглянута і доповнена Монакським додатковим актом у 1961 р. та Стокгольмським додатковим актом у 1967 р. У 1994 р. було прийнято Угоду Світової організації торгівлі (СОТ) ТРІПС (Угода ТРІПС) яка також заклала основні стандарти щодо наявності, обсягу та використання прав на патенти [16].

Щодо створення патентної системи то така ідея була реалізована внаслідок прийняття 5 жовтня 1973 р. у Мюнхені Конвенції про видачу Європейського патенту. В доволі широкому колі дана конвенція відома, як Європейська патентна конвенція.

Варто відмітити, що законодавство ЄС дає можливість короткострокової охорони незареєстрованого права інтелектуальної власності. Так, з одної сторони це є прояв еластичності правової охорони та зрозумілим і доволі практичним рішенням

зважаючи на виклики сьогодення. З іншої сторони це також є і недоліком, який набуває особливого значення під час маркетингового прорахунку в життєвому циклі товару та його експортоспроможності. Слід погодитися, що такі випадки дієйсно є рідкісними, проте вони все ж таки існують. При цьому вартим уваги є і те, що ніхто не заперечує в переростанні короткострокової охорони в довгострокову. Їх зближує те, що як зареєстровані, так і незареєстровані винаходи у країнах-членах ЄС охороняються при тій умові, що відповідають двом основним критеріям, серед яких новизна та індивідуальність виробу[18, с.108]. Більше того, вони альтернативно мають можливість піддаватися охороні законодавства про недобросовісну конкуренцію.

Таким чином, можемо чітко говорити і констатувати факт, що «індивідуальність» є новим та уже загальноприйнятим поняттям у ЄС, а враховуючи європейську спрямованість нашої держави, має бути сприйнятим і на теренах України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кравченко О.А., Подоляка С.М. Система органів правління в сфері охорони прав на об’єкти інтелектуальної власності в Україні. Інтелектуальна власність. 2004. С. 13-18.

2. Бондаренко С. Система захисту авторського права і суміжних прав в Україні. Національна безпека і охорона. 2001. С. 61-64.
3. Боярчук О. М. Цивільно-правова охорона суміжних прав в Україні : автореф. дис... канд. юрид. наук : 12.00.03; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2002. 19с.
4. Ієвіня О.В., Мироненко В.П., Павловська Н.В., Пилипенко С.А. Право інтелектуальної власності: схеми та роз’яснення: Навч. посібник. К.: КНТ, 2007. 264с.

ГРАЧОВА Олександра
студентка, КПІ імені Ігоря Сікорського
ДУБНЯК Марія
к.ю.н., старший викладач кафедри інформаційного, господарського та адміністративного права, КПІ ім. Ігоря Сікорського,
с.н.с., наукової лабораторії теорії цифрової трансформації і права, Наукового центру Цифрової трансформації і права, ДНУ ІІБП НАПрН України
ORCID: https://orcid.org/0000-0001-7281-6568.

ОСОБЛИВОСТІ СПЛАТИ ПОДАТКІВ НА ПІДСТАВІ РЕЖИМУ ДІЯ-СІТІ

В умовах постійної глобалізації та цифровізації, усі сфери суспільного життя зазнали змін та нововведень. Оскільки, саме на підставі залучення інформаційних технологій , відбувається покращення та вдосконалення економічного сектору, що є основоположним у підтримці стабільності держави загалом. Однією із галузей, що зазнали одних із найбільших аспектів модернізації є податкове право.

Таким чином, актуальним є висвітлення усіх основних аспектів здійснення цифрового оподаткування суб'єктів господарювання, в тому числі, суб’єктів IT-business.

Мета даної роботи полягає у аналізі особливостей здійснення цифрового оподаткування в Україні.

Загалом, поява інформаційних технологій запроваджує зміни щодо питання цифрового оподаткування. Відтак, вперше основні заходи щодо цифрового оподаткування є Законі України «Про стимулювання розвитку цифрової економіки в Україні» (надалі- Закон) [1]. Даний нормативний акт став основним, на підставі якого на юридичній арені вперше було визначено категорію осіб, які підпадають під можливість здійснювати оподаткування своєї діяльності на основні правового режиму «Дія. Сіті».

Відтак, відповідно до п.9 ч.1 ст.1 Закону України «Про стимулювання розвитку цифрової економіки в Україні», правовий режим Дія Сіті - сукупність правових норм, якими визначаються права та обов’язки особи, що виникають, змінюються та припиняються у зв’язку із зверненням про набуття, набуттям та втратою статусу резидента Дія Сіті, а також особливості регулювання відносин за участю резидента Дія Сіті і щодо участі у його статутному капіталі[1].

Таким чином, законодавець навів тлумачення терміну режиму Дія Сіті, що в свою чергу надає всебічне охоплення і аналіз даного поняття з метою подальшого застосування на практиці.

Вагомого аспекту потребує визначення суб'єктів господарювання, на яких поширюється можливість здійснювати електронне оподаткування загалом. Відтак,у Законі під такою особою, враховуючи норми п.11 ч.1 ст.1 розуміється юридична особа, яка відповідно до цього Закону набула статусу резидента Дія Сіті та згідно з інформацією, що міститься у реєстрі Дія Сіті, перебуває у зазначеному статусі [1].

Отже, українська нормативна база містить тлумачення статусу резидента Дія Сіті.

Варто зауважити, що на підставі прийняття вищенаведеного Закону, було прийнято окремі зміни в Податковому кодексі України, приписи якого встановлюють особливості сплати податків для резидентів Дія Сіті,зокрема у п.170.14 1.2 ПКУ [2].

Зокрема, оподаткуванню підлягають такі види доходів фахівців: заробітна плата; винагорода за гіг-контрактом; авторська винагорода за створення службового твору та передання прав на службові твори.

До таких доходів застосовують ставку податку на доходи фізичних осіб 5%. Але в разі якщо річний дохід фахівця у вигляді заробітної плати, винагороди за гіг-контрактом чи авторської винагороди перевищує 240 тис. євро, тоді до суми перевищення застосовують іншу ставку податку – 18 %. Відобразити такі доходи у річній

декларації та сплатити необхідні податки фахівець має сам , що передбачено пп. 170.14-^{1}.3 ПК України[2].

Зокрема, враховуючи аспекти щодо реалізації « законотворці прийшли до висновку, що впровадження «Дія City» , що призведе до зростання частки ІТ у ВВП України до 10% замість нинішніх 4%. Прогнозувалось значне зростання доходів у галузі та збільшення робочих місць у зв'язку із спрощеною системою оподаткування [3].

Механізм режиму «Дія Сіті» створює вагомі прибуткові заходи для суб'єктів господарювання щодо покращення економічного потенціалу України. Зокрема, на підставі реєстрації резидента режиму «Дія Сіті» передбачено можливість спрощеної системи оподаткування. Таким чином, враховуючи даний режим, необхідно зауважити про його подальші перспективи і можливості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15 липня 2021 року №1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (дата звернення:01.05.2023)

2.Податковий кодекс України: Закон України від 2 грудня 2012 року №2755-VI. URL: https://zakon.rada.gov.ua/laws/show/2755-17 (дата звернення: 01.05.2023)

3.Дія City» в дії. *Juscutum*. URL: https://juscutum.com/diia-city (дата звернення:02.05.2023)

ГУБІНА Ганна
к.ю.н., Одеський державний аграрний університет

ПРАВОВЕ РЕГУЛЮВАННЯ SMART-КОНТРАКТІВ У СІЛЬСЬКОГОСПОДАРСЬКІЙ ДІЯЛЬНОСТІ В УКРАЇНІ ТА ЄС

Україна є однією з держав, яка продовжує мати статус постачальника та експортера сільськогосподарської продукції в сучасних умовах (наприклад, чинний воєнний стан). Враховуючи сучасні можливості актуальним є застосування у зазначеній вище галузі саме smart-контрактів. Нещодавно Україна отримала статус кандидата в члени ЄС. Отже, постала проблема щодо приведення норм українського законодавства до норм законодавства ЄС щодо smart-контрактів.

Дане явище існує достатньо довгий період і, відповідно, повинно мати необхідне правове регулювання. Однак, законодавча база України не містить жодного нормативно-правового акту з цього питання, що має як позитивні аспекти, так і, навпаки. Про це неодноразово зазначалося у науковій літературі. Також є Закон України «Про віртуальні активи» від 17.02.2022 р. № 2074-IX, що ще не набрав чинності. На нашу думку, він і не буде чинним, бо нещодавно у

законодавстві ЄС відбулася значна подія – це голосування за Закон про дані у новій редакції, де визначені деякі аспекти smart-контракту [1]. До нього також були спроби врегулювати дане питання: Європейський акт про управління даними [2], Закон про штучний інтелект [3], Закон про цифрові послуги [4], Закон про цифрові ринки [5]… Проте, в них відсутнє пряме врегулювання саме розглядаємих контрактів.

В Законі про дані було вилучено визначення поняття «smart-контракт», що надає можливість кожному, хто його застосовує, тлумачити, розуміти на власний розсуд. Це є неприпустимим і потребує внесення змін, бо, представляється, є помилковим висувати будь-які вимоги до таких контрактів, коли відсутнє саме визначення, що закріплено на законодавчому рівні. Із аналізу даного закону можна встановити, що лише стаття 30 в ньому напряму пов’язана зі smart-контрактами [1]. Її чинна редакція, вважаємо, не відповідає самої суті smart-контракту: відсутність можливості внесення змін після його розгортання у блокчейні. А будь-які зміни в ньому передбачають, відповідно, розгортання нового такого контракту [6]. Також із змісту даної статті досліджуємого закону незрозуміло щодо того, хто буде фактично безпечно припиняти та переривати такий контракт. Так, Хайн Даувен пропонує три варіанта: 1)

керування одним користувачем, тобто одна фізична або юридична особа має повноваження активувати вимикач або призупинити функцію smart-контракту. Перевагою є найшвидший час реагування в разі надзвичайної ситуації, він централізує владу та контроль, потенційно викликаючи занепокоєння щодо довіри та вразливості до зловмисних дій/учасників, а недоліками - один користувач може не мати необхідного досвіду для прийняття найкращого рішення в кожній ситуації, що може призвести до неоптимальних результатів, а також існує ризик втрати закритого ключа, прикріпленого до цього окремого користувача, що може зробити виконання функцій неможливим у майбутньому; 2) керування кількома підписами (багато підписів), тобто кілька користувачів авторизують активацію перемикача вимкнення або призупинення функції, як правило, за допомогою попередньо визначеного порогу підписів. Перевагою можна вважати те, що відбувається розподіл повноважень щодо прийняття рішень і зменшення ризику неправильного використання або помилок. Недоліками є недосить висока швидкість виконання; 3) децентралізовані автономні організації, тобто рішення приймаються колективом зацікавлених сторін, які голосують за пропозиції з використанням заздалегідь визначених правил і механізмів управління. Позитивними аспектами є посилення довіри шляхом

розподілу повноважень щодо прийняття рішень між спільнотою та/або компаніями, зменшуючи ризик централізації та зловмисних дій, а негативними – у порівнянні з іншими варіантами швидкість виконання може бути найповільнішою [7]. Вважаємо, що погодитися з точкою зору Хайн Даувена щодо оптимального вибору не є можливим, бо потрібно розробити такий варіант згідно вимог норм чинного законодавства ЄС, який відповідає безпосередньо досягненням науко-технічного прогресу та є універсальним, класичним у будь-якому випадку.

Ще однією проблемою, на наш погляд, у статті 30 Закону про дані є така норма: «…захист конфіденційності комерційних таємниць: переконайтеся, що smart-контракт розроблено для забезпечення конфіденційності комерційних таємниць…» [1]. Під комерційною таємницею розуміють «інформацію, яка відповідає всім наступним вимогам: а) вона є секретною в тому сенсі, що вона не є загальновідомою або легкодоступною для осіб у колах, які зазвичай мають справу з відповідним типом інформації, як тіло чи точна конфігурація та збірка його компонентів; б) має комерційну цінність, оскільки є секретною; с) особа, яка на законних підставах контролює інформацію, вжила розумних заходів для збереження її в таємниці» (стаття 2 Директиви (ЄС)

2016/943 Європейського Парламенту та Ради від 08.06.2016 р. про захист нерозкритих ноу-хау та ділової інформації (комерційної таємниці) від їх незаконного придбання, використання та розголошення) [8]. Вбачається, що дотриматися конфіденційності комерційної таємниці у даному контракті не є можливим.

Виходячи з вище проведеного аналізу, на наш погляд, здійснена спроба щодо правового врегулювання деяких аспектів smart-контрактів у законодавстві ЄС потребує подальшого вдосконалення, бо застосування чинної редакції статті 30 Закону про дані, наприклад, під час укладення таких контрактів у сільськогосподарській діяльності може викликати багато проблем та негативних наслідків особливо, де укладаються договори зі складними процесами (наприклад, договір контрактації, контракт на вирощування та постачання м’ясної продукції).

На думку автора, норми статті 30 Закону про дані більше відповідають створенню чи появи нового виду контракту, що є відмінний від smart-контракту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Report on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

https://www.europarl.europa.eu/doceo/document/A-9-2023-0031_EN.html#_ftn29.
2. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.
3. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52021PC0206.
4. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014.
5. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925.
6. Introduction to Smart Contracts. https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html.
7. Hein Dauven. The EU’s Data Act | Balancing Regulations and Innovation in the Age of Smart Contracts. https://dusk.network/news/the-eus-data-act-balancing-regulations-and-innovation-in-the-age-of-smart-contracts.
8. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

ГУМЕНЮК Денис
студент, КПІ ім. Ігоря Сікорського
ГОЛОВКО Ольга
к.ю.н., ст. дослідник,
ст. науковий співробітник лабораторії
теорії цифрової трансформації і права
наукового центру цифрової трансформації
і права ДНУ "ІІБП НАПрН" України,
ст. викладач кафедри інтелектуальної власності
та приватного права КПІ ім. Ігоря Сікорського

ЦИФРОВА МЕДІАЦІЯ ТА ЇЇ ПЕРЕВАГИ І РИЗИКИ ЯК СПОСОБУ ВРЕГУЛЮВАННЯ КОНФЛІКТУ

Для того, що б зрозуміти саму сутність цифрової медіації, слід розпочати з розуміння самого поняття медіації. На сьогодні, вже існує визначення цьому терміну.

Медіація - це приватне та конфіденційне використання посередників для виходу з конфліктної ситуації. Вона дає можливість уникнути втрати часу в судових розглядах та додаткових і непередбачуваних матеріальних витрат. Іншими словами, можна сказати, що медіція- це процес вирішення конфлікту, при якому незалежна третя сторона (медіатор) допомагає спірним

сторонам знайти взаємовигідне рішення без втручання суду чи інших органів влади.

Так виглядає процес медіації в своєму стандартному вигляді. Але з плином часу і сьогоднішніх технічних можливостей має місце наступне поняття, а саме Цифрова медіація. Значної відмінності яка б дозволяла нам говорити про те, що це зовсім різні поняття за своєю природою не має. Цифрова медіація – це процес вирішення конфліктів, в якому медіатор використовує цифрові технології для полегшення спілкування та обміну інформацією між сторонами. Цифрова медіація може відбуватися в різних форматах, таких як відеоконференції, онлайн-чати, електронна пошта, або через спеціалізовані платформи для медіації.

Оскільки у нас вже є сформоване поняття цифрової медіації, пропоную поговорити про те, які можливості вона відкриває, яким чином вона може бути корисна та які має недоліки і які ризики може нести.

Нам вдалося виокремити основні переваги цифрової медіації, до яких ми відносимо:

Зручність: Учасники можуть брати участь в медіації з будь-якого місця, де є доступ до Інтернету, забезпечуючи зручність і швидкість вирішення спору.

Економічність: Цифрова медіація зазвичай менш витратна, оскільки не потрібно витрачати кошти на

подорожі та оренду приміщень для проведення зустрічей.

Ефективність: Цифрова медіація може бути більш ефективною, оскільки учасники можуть ділитися електронними документами та матеріалами в режимі реального часу, а також мати швидкий доступ до інформації, необхідної для вирішення спору.

Конфіденційність: Цифрова медіація може забезпечити більшу конфіденційність, оскільки учасники можуть брати участь в медіації з власних приміщень, забезпечуючи конфіденційність обміну інформацією.

Міжнародний характер: Цифрова медіація може забезпечити міжнародний характер, оскільки учасники можуть брати участь в медіації з будь-якої точки світу.

Збереження часу: Цифрова медіація може бути більш швидкою, оскільки не потрібно витрачати час на подорожі до зустрічей та зустрічі в реальному часі.

Загалом, цифрова медіація може бути вигідною для учасників, які шукають швидке, ефективне вирішення спору, але такий шлях урегулювання конфлікту, може мати негативні наслідки для певної сторони. Оскільки цифрова медіація, не є ідеальним способом вирішення конфлікту і також має свої негативні сторони.

Використання цифрових технологій в медіації може створювати нові виклики та проблеми, такі як:

1. Забезпечення конфіденційності даних

2. Забезпечення безпеки та приватності. Інтернет-платформи можуть бути не надійними для зберігання конфіденційної інформації. Сторони можуть відчувати незручність чи небезпеку передачі чутливої інформації через ці інтернет-платформи.

3. Зниження якості взаємодії через відсутність безпосереднього контакту між сторонами. Однією з найбільших переваг традиційної медіації є можливість особистого контакту між сторонами. За використання цифрових технологій у медіації відсутність особистого контакту може спричинити відчуття віддаленості між сторонами і зменшити їхню можливість досягнути домовленості.

4. Проблеми з технічною підтримкою: Якщо одна з сторін або обидві сторони не мають достатньої технічної підтримки або доступу до необхідних технічних засобів, таких як веб-камера або мікрофон, це може створити проблеми з виконанням медіації через відеозв'язок.

Тому, при використанні цифрових технологій в медіації, важливо дотримуватись певних принципів та стандартів, щоб забезпечити ефективність та якість

процесу медіації, а також зменшити можливість виникнення нових проблем.

Висновок: ми поговорили про позитивні та негативні сторони цифрової медіації як способу вирішення конфлікту, нам також вдалося з'ясувати саме поняття цифрової медіації, але навіть з урахуванням всього вищесказаного, неможливо сформувати об'єктивну позицію, яка б могла говорити про те, що цифрова медіація завжди допоможе врегулювати спір і дійти бажаного результату і навпаки. Все залежить від сторін і конфлікту між ними, в певних випадках медіацію буде корисною, в інших може тільки погіршити ситуацію, тому перед тим, як використовувати цей процес, сторони повинні чітко усвідомлювати всі ризики, негативний результат до якого вона може призвести. Але дещо ми можемо сказати з упевненістю, цей інститут ще перебування на етапі свого становлення в суспільстві, але він розвивається, процес медіації стає все більш відомим, в майбутньому він буде мати всі шанси що б вийти на один рівень з судовим способом врегулювання конфлікту. Ми обрали цю тему для дослідження через те, що вона є відносно новою, що дає нам можливість сформувати власну позиції і ставлення до цього процесу тим самим також розповісти про нього більше.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України "Про медіацію" від 23.02.2021 № 1337-IX. URL: https://zakon.rada.gov.ua/laws/show/1337-20.
2. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Господарський процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text

ДЕРКАЧ Олена

аспірант, НН Інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

ПРАВОВІ ПРОБЛЕМИ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЗБРОЙНИХ КОНФЛІКТАХ

Штучний інтелект (ШІ) – може бути використаний в різних аспектах військової діяльності, таких як розвідка та розвідувальні операції, управління зброєю та бойовим обладнанням, оцінка ситуації на полі бою та прийняття рішень. В умовах війни використання ШІ здійснюється в нових формах та задля вирішення специфічних завдань та досягнення особливих цілей. Поширення ШІ набуває глобальних

масштабів, а методика його використання стає універсальною. Однак на сьогоднішній день досі не існує жодного універсального міжнародного нормативно-правового акту, який би регулював застосування штучного інтелекту в контексті бойових дій. Та можна зазначити, що через початок війни у 2014 році, а потім і повномасштабне вторгнення у 2022 році РФ на територію суверенної та незалежної держави України, багато країн замислились та почали розробляти нормативну базу щодо створювання, використання та несення відповідальності за можливі наслідки при використання ШІ в умовах війни.

Окремі аспекти регулюються Женевськими конвенціями, що були прийняті у 1949 році та доповнені у 1977 році, які містять низку положень щодо захисту цивільних осіб [1], які не беруть безпосередньої участі у війні, а також положення про заборону використання зброї та методів бойових дій, які можуть завдати непропорційної шкоди цивільному населенню та майну - у сьогоднішній війні не виконуються і не дотримуються у жодному пункті, починаючи від захисту та збереження життя цивільного населення і закінчуючи поводження з військовополоненими [2]. Однак, ці конвенції не містять згадок про штучний інтелект, тому як на той час це було не актуально і

відповідно не потребувало правового регулювання через відсутність такого поняття, як штучний інтелект.

Варто зауважити, що деякі країни світу вже розпочали розробляти нормативні акти, що містять положення про використання штучного інтелекту під час збройних конфліктів. Причиною прискоренням цих процесів стала війна в Україні.

Наприклад, Міністерство оборони США випустило етичні принципи для штучного інтелекту у листопаді 2020 року "Ehtical Principles for Artificial Intelligence" [4]. Стратегія розвитку штучного інтелекту Міністерства оборони США - це документ, в якому викладено підхід Міністерства до впровадження та використання технологій штучного інтелекту у своїх операціях. Стратегія була опублікована в лютому 2019 року і спрямована на те, щоб дозволити Міністерству оборони ефективно впроваджувати ШІ в усі аспекти своєї місії, включаючи ведення бойових дій, розвідку та бізнес-операції.

Цей документ включає в себе наступні пункти:

1. Поважати закон і діяти чесно
2. Прозорість і підзвітність
3. Об'єктивність і справедливість

Деякі з ключових принципів етики ШІ включають захист приватності та безпеки даних, розуміння та управління ризиками, уникнення дискримінації та

забезпечення справедливості та інклюзивності, забезпечення прозорості та зрозумілості, розвиток навчання та підвищення свідомості.

Ці принципи мають на меті забезпечити використання ШІ для досягнення соціальних та економічних цілей в межах етичних норм та стандартів ("Department of Defense AI Strategy") [3]. Стратегія Міністерства оборони США у сфері штучного інтелекту є важливим компонентом більш широких зусиль уряду Сполучених Штатів, спрямованих на збереження своєї технологічної переваги в глобальному ландшафті, а також на забезпечення безпеки американського народу.

У Франції окремі аспекти кібербезпеки регулюються Законом "Military Programming Law" [5], що є джерелом Директиви NIS (Network and Information Security Directive, що є законодавчим актом Європейського союзу 2016 року, стосовно кібербезпеки). Ця система дозволила ідентифікувати операторів життєво важливих об'єктів інформаційних технологій, як приватних, так і державних, які експлуатують або використовують об'єкти, що вважаються важливими для виживання нації.

Крім того, закон містить положення про захист прав людини та заборону використання військової технології для порушення прав людини. Це може мати важливе значення для розробки та використання систем

штучного інтелекту, які можуть впливати на права людини, наприклад, системи автоматизованого прийняття рішень. Загалом, хоча закон про військове програмування Франції не містить конкретних положень про штучний інтелект, він встановлює загальні принципи безпеки та захисту прав людини, які можуть бути застосовані до розробки та використання штучного інтелекту військового призначення.

Законодавча база України наразі містить декілька законів та правових документів, в яких є згадки про деякі аспекти, що стосуються штучного інтелекту. Наприклад, Закон України "Про захист персональних даних", Закону України "Про кібербезпеку".

Хоча уряд України розробляє «Концепцію розвитку штучного інтелекту в Україні до 2030 року», все одно в українському законодавстві відсутні тлумачення і нормативні документи, які регулюють питання застосування і регулювання використання штучного інтелекту., яке наразі набуло істотного значення в реаліях сьогодення. Знову ж таки існування міжнародних законодавчих актів, які можуть застосовуватись до цього питання, не дає вичерпних понять про настання відповідальності за порушення використання ШІ в збройних конфліктах. Вивчаючи дане питання можна стверджувати, що на сьогоднішній день штучний інтелект широко та масово

використовується збройними силами, безпосередньо, у війні між Україною та РФ, а саме автоматизовані бойові системи, системи розвідки та контролю, але при цьому завдається шкода цивільному населенню при використанні військовими систем, складовою яких є ШІ. Тобто існує прецедент, а чіткої нормативної бази, в якій мають бути зазначені причини, немає, як і правових наслідків за результатами використання ШІ .

Джерел, нормативних документів надто мало, практично немає, а бланкетні норми, на мою думку, не працюватимуть, до прикладу в Міжнародному суді, та судах на місцях, так як немає механізму встановлення причинно-наслідкового зв'язку, а саме – хто винен, та хто буде нести відповідальність і згідно якого нормативного документу- розробник, оператор, чи сама система дала збій? Такі обставини уже ставлять під сумнів законність винесених судами рішень.

Отже, враховуючи вище викладене, можемо констатувати необхідність створення спеціальних комісій, залучення міжнародних неурядових (громадських) організацій, такі як Червоний хрест, що працюють з конфліктами, та на міжнародному рівні вони виступають більше як наглядачі, розробляють інформаційні звіти, з якими може ознайомитись будь-хто зацікавлений. Доцільно розробляти пропозиції, проводити міжнародні консультації, з обов'язковим

залученням правників різних галузей права, для розробки нормативної бази та впровадженням її в міжнародне законодавство та подальшої імплементації в національне законодавство.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Женевські конвенції про захист жертв війни 1949 року URL:https://www.ombudsman.gov.ua/uk/zhenevski-konvenciyi-pro-zahist-zhertv-vijni-1949-roku
2. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року URL : https://zakon.rada.gov.ua/laws/show/995_199#Text
3. Artificial intelligence initiatives within the department of defense Senate Hearing, From the U.S. Government Publishing Office (2019) URL : https://www.govinfo.gov/content/pkg/CHRG-116shrg46003/html/CHRG-116shrg46003.htm
4. The U.S. Department of Defense Adopts Ethical Principles for Artificial Intelligence (2020) URL:https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
5. The French Military Programming Law (Lpm) 2019-2025 And The Capacities Of The Armed Forces (2022) URL :https://www.ccomptes.fr/system/files/2022-07/20220511-press-release-The-French-military-programming-law-2019-2025-and-capacities-of-armed-forces.pdf

ДУБНЯК Марія

к.ю.н., старший викладач кафедри інформаційного,
господарського та адміністративного права,
КПІ ім. Ігоря Сікорського,
с.н.с., наукової лабораторії теорії цифрової трансформації і
права,Наукового центру цифрової трансформації і права,
ДНУ ІІБП НАПрН України
ORCID: https://orcid.org/0000-0001-7281-6568.

ЕТИКА ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ЄВРОІНТЕГРАЦІЇ: ВІД ПРИНЦИПІВ ДО ПРАКТИКИ

Впровадження технологій штучного інтелекту *(далі ШІ)* у різні галузі формує ряд практичних проблем. Для сфери інтелектуальної власності — питання правового режиму і захисту об’єктів створених за допомогою технологій ШІ. У сфері медицини і охорони здоров’я — проблема достовірності медичних прогнозів та розроблених ліків. У судовій та правоохороній системах — проблема прогнозування рецидиву злочинцем під час ухвалення рішення суддею, частіше притягнення до відповідальності представників маргінальних груп, використання технологій ШІ для запобігання злочинності. У сфері публічного управління — механізми контролю та балансу в процесі

впровадження технологічних рішень у процес прийняття рішень. У сфері зайнятості та праці — феномен технологічного безробіття.У сфері екології та захисту навколишнього природного середовища — проблема вуглецевого сліду, обробки та моніторингу даних у сфері довкілля, обліку об’єктів та речовин, які шкідливо впливають на довкілля, доступу громадськості до екологічної інформації.

Проблеми формування етичних принципів розробки технологій штучного інтелекту займаються держави, спеціальні урядові групи, наукові центри при всесвітньо-відомих університетах, та окремі науковці.

Спеціалізовані центри, які діють за підтримки Інституту майбутнього життя та меценатів, таких як: Leverhulme Center for the Future of Intelligence (LCFI) у Кембриджі, One Hundred Year Study of AI (AI100) у Стенфордському університеті, The Institute for Ethics in AI в Оксфордському університеті.

Корпорації: Amazon, DeepMind, Facebook, Google, IBM та Microsoft створили ініціативу Partnership on Artificial Intelligence to Benefit People and Society. Державні установи напрацьовують аналітичні звіти з окремих питань, наприклад, Доповідь Білого дому “Про майбутнє штучного інтелекту” та “Звіт про робототехніку та право” Комітету з правових питань Європейського Союзу, чи Рекомендації з етики щодо

надійного ШІ (08.04.2019) [1], Рекомендації щодо політики та інвестицій для надійного ШІ (26.06.2019) [2], підготовлених Групою експертів високого рівня з ШІ (AI HLEG).

2010 рік - принципи для проектувальників, розробників і користувачів роботів [1].

2017 рік - Асіломарські принципи штучного інтелекту [2].

2018 рік - принципи відповідальної практики у сфері ШІ від компанії Google [3].

2018 рік - Торонтська декларація: захист прав на рівність і недискримінацію в системах машинного навчання [4].

2019 - рік Група експертів високого рівня Європейської комісії зі штучного інтелекту (AI HLEG) опублікувала “Керівництво з етики для надійного штучного інтелекту” [5], “Рекомендації щодо політики та інвестицій для надійного штучного інтелекту” [6].

2020 рік - з метою просування етичного підходу до штучного інтелекту Папською академією життя (Pontifical Academy For Life), технологічними компаніями Microsoft, IBM, FAO та міністерством інновацій Італії було підписано документ “Римський заклик до етики штучного інтелекту” (Rome Call for AI Ethics) [7].

Рух за просування і популяризацію “Римського заклику” дістав самостійний напрям академічних досліджень алгор-етика (“algor-ethics”) — напрям етичних роздумів щодо використання алгоритмів, особливо у сфері освіти та права.

Висновки: Більшість етичних кодексів розробки технологій ШІ та робототехніки містить рекомендації про дотримання оціночних категорій, таких як: справедливість, відповідальність, підзвітність, які відносяться до теоретичних питань соціальної етики впровадження технологій.

За понад десятирічний відрізок часу предмет регулювання в етичних кодексах змінився, від принципів регулювання роботів як пристроїв, до принципів регулювання розробки алгоритмів, нейромереж, вибору та аналізу вхідних та вихідних даних, які враховують особливості проектування та розробки такого програмного забезпечення.

Етичні кодекси враховують не лише рекомендації та стандарти для розробників, а і впровадження цих принципів для урядів країн, з метою дотримання високих стандартів прав людини під час прийняття рішень про використання технологій ШІ у публічному секторі.

Коло стейкхолдерів у сфері етики технологій розширилось. Це вийшло за межі ідей наукових

фантастів і академічних шкіл. Воно включає експертів спеціальних урядових груп, технологічні корпорації, галузеві професійні об’єднання, а з 2020 року і релігійні конфесії. З одного боку, це означає, що питання регулювання новітніх технологій нормами етики привертає увагу широкого кола спеціалістів з різних галузей знань (програмістів, інженерів, аналітиків даних, філософів, соціологів, правників), що дозволяє віднайти спільні точки конвергенції. З іншого боку, відсутність зобов’язуючих норм і санкцій, які можуть гарантуватись лише системою правового регулювання, підкреслює проблему пошуку правових механізмів перетворення етичних норм у правове регулювання, що буде предметом окремого дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Principles of robotics (2010) by EPSRC. URL: https://webarchive.nationalarchives.gov.uk/ukgwa/20210701125353/https://epsrc.ukri.org/research/ourportfolio/themes/engineering/activities/principlesofrobotics/
2. Ethical Guidelines for Artificial Intelligence Research. AI-Ethics: Law, Technology and Social Values. URL: https://ai-ethics.com/research-principles/
3. Google AI principles (2018) URL: https://ai.google/responsibilities/responsible-ai-practices/?category=general

4. The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems. (2018) https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems
5. Ethics guidelines for trustworthy AI (2019) URL: https://web.archive.org/web/20200226023934/https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
6. Policy and investment recommendations for trustworthy Artificial Intelligence (2019) URL: https://web.archive.org/web/20200226023934/https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence
7. Rome Call for AI Ethics (2020) URL: https://www.romecall.org/the-call/

ЗАБАРА Ігор

к.ю.н., доцент, доцент кафедри міжнародного права
ННІМВ КНУ імені Тараса Шевченка

ДО ПИТАННЯ ВИЗНАЧЕННЯ МІЖНАРОДНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ ПРИ ЗАСТОСУВАННІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

У широкій темі відповідальності спробуємо розглянути інститут відповідальності при застосуванні технологій Інтернету речей з позицій міжнародного права.

Досить тривалий час інститут міжнародно-правової відповідальності держави за інформаційну і комунікаційну діяльність розглядався з позицій поширення інформації традиційними засобами (радіомовлення, телебачення, поширення друкованої, візуальної та аудіо продукції). При цьому міжнародно-правова відповідальність передбачалась виключно за поширення протиправної, неправдивої або перекрученої інформації, а також за порушення технічних умов використання частот, орбіт при здійсненні комунікацій (електронних комунікацій). Ця тематика залишається і до сьогодні актуальною [1].

Разом з тим, зміни, які відбуваються у суспільних відносинах, що пов’язані з появою і розвитком ще одного вагомого напрямку використання ІКТ – Інтернетом речей теж викликають широке коло правових питань, вагомими серед яких постають проблеми, пов’язані з інститутом міжнародно-правової відповідальності.

Сучасна проблематика інституту міжнародно-правової відповідальності за правопорушення при використанні новітніх інформаційно-комунікаційних технологій в сучасних умовах постає досить широко. Тож, в рамках нашої конференції обмежимось розглядом кола питань, пов’язаних із розглядом інституту відповідальності при застосуванні технологій Інтернету речей з позицій міжнародного права.

Зазвичай, говорячи про інститут відповідальності загалом, та інститут міжнародно-правової відповідальності зокрема, вибудовують авторську, або вже закріплену, схему подачі матеріалу, в якій надається визначення, суб’єктний склад, складові елементи та розглядаються окремі правові норми.

На нашу думку, у зв’язку з досить складним предметом дослідження, яким виступає Інтернет речей, варто відійти від традиційної схеми і запропонувати зосередитись на питаннях правовідносин, в нашому випадку - міжнародно-правових відносин

відповідальності. Для цього варто охопити коло тих питань, які нададуть бачення сучасним аспектам визначення міжнародно-правової відповідальності при застосуванні технологій Інтернету речей.

1. Виходитемо з того, що можемо говорити про відповідальність широкого кола суб'єктів, як в рамках національних юрисдикцій (якщо протиправні діяння здійснюються в межах території однієї держави), так і у відносинах між державами (оскільки при застосуванні технологій Інтернету речей можуть бути транскордонні впливи).

2. Зауважимо, що питання міжнародно-правової відповідальності не будуть значно відрізнятись від тих поглядів (концепцій, підходів), які використовуються при розгляді питань міжнародно-правової відповідальності при використанні сучасних інформаційно-комунікаційних технологій ІКТ [2].

3. Разом із питаннями (проблематикою) відповідальності, які умовно можна визначити як такі, що виникають із використання Інтернету речей «на благо», неодмінно будуть слідувати питання (проблематика) із використання Інтернету речей «на зло» (з військовими, терористичними і кримінальними цілями).

4. Питання міжнародно-правової відповідальності міститимуть як комунікаційну (кібернетичну), так і інформаційну складову.

У зв’язку з цим.

5. Визначаючи питання міжнародно-правової відповідальності, (враховуючи можливі впливи на саму «архітектуру Інтернету речей», так само як і впливи через цю «архітектуру» на особу, суспільство, державу) варто виходити з наступного кола питань, які охоплюють загрози при використанні Інтернету речей, зокрема:

загрози апаратні – для пристроїв, сенсорів і датчиків;

загрози для програмного забезпечення;

загрози для прав людини (за групами прав);

загрози для здоров’я людини, тварин, природного навколишнього середовища.

6. «Вважаємо, що вплив на кібернетичні системи держав будуть здійснювати кілька чинників, серед яких:

а) кількість кінцевих пристроїв, що отримуватимуть найрізноманітнішу інформацію (прогнозовано – 1 млн. кінцевих пристроїв на 1 кв. км);

б) нові засоби і способи швидкісної передачі інформації (LiFI, квантовий зв’язок);

в) засоби і технології, що працюватимуть із гігантськими обсягами зібраної, переданої та отриманої інформації (Super Data Base) [2].

7. У зв'язку зі збільшенням кількості як кінцевих пристроїв, так і нових засобів і способів передачі інформації, широко постане питання їх впливу на здоров'я людини, тварин, природного навколишнього середовища.

8. Вважаємо, що вплив на права людини буде залежати від того, яким шляхом може піти сучасне суспільство («міжнародне співтовариство, наділене міжнародною правосуб'єктністю» [3]) і, залежно від цього, в яких саме суспільно-політичні умовах розвиватиметься Інтернет речей – у використанні технологій для створення відкритого суспільства, або використанні технологій для посилення контролю над громадянами (фізичними особами).

Виходячи з наведеного, можна окреслити такі кола міжнародно-правових відносин відповідальності:

(1) міжнародно-правові відносини відповідальності держав за міжнародні зобов'язання, пов'язані з боротьбою з військовими, кримінальними та терористичними злочинами у сфері інформаційно-комунікаційних технологій;

(2) міжнародно-правові відносини відповідальності держав за міжнародні зобов'язання, пов'язані з

порушенням прав людини, викликаних технологіями Інтернету речей;

(3) міжнародно-правові відносини відповідальності держав за міжнародні зобов'язання, пов'язані з впливом на здоров'я людини, тварин, природного навколишнього середовища.

На нашу думку, вартими уваги є подальші дослідження окремих аспектів режиму міжнародно-правової відповідальності міжнародно-правові відносини відповідальності держав за інформаційну діяльність суб'єктів міжнародного права, зокрема пов'язаних із протиправним використанням державами сучасних технологій Інтернету речей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Забара, І.М. (2016). *Проблеми забезпечення відповідальності держави за інформаційні міжнародно-протиправні діяння*, Матеріали конференції «Проблеми відповідальності держави». Київ, Національний авіаційний університет, 87-99.

2. Забара, І.М. (2019). *До питання визначення проблематики міжнародно-правової відповідальності за правопорушення при використанні новітніх інформаційно-комунікаційних технологій*, Матеріали конференції «Інтернет речей: проблеми правового регулювання та впровадження». Київ, Комітет Верховної Ради України з питань цифрової

трансформації, НДІІП НАПрН України, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 58-61.
3. Буткевич, В.Г. (2012). Виклики міжнародному праву в умовах глобалізації світу. *Право України*, 3-4. 12-50.

КАГРАМАНОВА Юлія
асистент кафедри ІПЗАС ДУТ
СВЕРДЛЮК Богдан
асистент кафедри ІПЗАС ДУТ

ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІОТ В ОСВІТІ

Сьогоднішні трансформаційні зміни в системі освіти є результатом стрімкого розвитку інноваційних технологій та цифровізації, яка стала невід'ємною частиною нашого життя [1]. Україна вже здійснила низку заходів, щоб реформувати галузь. Наразі необхідно готувати студентів до зростаючої конкуренції на ринку праці. Для досягнення цієї мети потрібно розробити нові інноваційні навчальні програми, які відображатимуть радикальні зміни в обчислювальній

техніці. Однією з таких змін є Інтернет речей (IoT), який передбачає підключення до Інтернету різних пристроїв, включаючи комп'ютери та смартфони. Сьогоднішня освіта без Інтернету речей неможлива, тому він глибоко вкорінений у наші заклади освіти, а електронне, дистанційне та змішане навчання є звичайною практикою в українській системі.

На сьогодні дуже мало наукових праць, які розглядали б впровадження Інтернету речей в освіту. Лише декілька університетів мають реальний досвід використання IoT з точки зору безпеки, віртуальних лабораторій та інтерактивних методів проведення занять в очному форматі. З переходом на дистанційне навчання було знайдено можливість швидше впроваджувати IoT в освітній процес.

Студенти, особливо ті, які навчаються в закладах вищої та перед-вищої освіти, все частіше відмовляються від традиційних паперових книг на користь планшетів та ноутбуків. Завдяки цьому, вони можуть самостійно рухатися вперед у своєму темпі та отримувати більш якісний освітній досвід як вдома, так і в аудиторії, маючи доступ до більшого об’єму інформації. Це може вимагати від студентів та викладачів підвищення рівня компетенції, що значно покращить ефективність навчання. Застосування нових

технологій також зменшує необхідність в ручномій перевірці тестів та виконанні інших рутинних завдань.

У 2020 році, внаслідок поширення COVID-19, багато закладів освіти по всьому світу були закриті або перейшли на дистанційне навчання. Це призвело до того, що всі стали розглядати широке коло питань в Інтернеті, щоб полегшити перехід до структурованого дистанційного навчання.

Інтернет речей може привести до кардинальної зміни взаємодії з користувачами та автоматизації процесів у сфері освіти. Він об'єднує фізичні об'єкти в мережу за допомогою вбудованих датчиків, виконавчих механізмів та інших пристроїв, які збирають та передають інформацію про заклад у режимі реального часу.

Які інструменти Інтернету речей використовуються в освіті? Згідно з аналізом досвіду зарубіжних вчених [3; 4], можна виділити наступні засоби:

Розумні дошки та інші цифрові інтерактивні засоби медіа, які дозволяють викладачам збирати та аналізувати дані, що допомагає оптимізувати навчання та покращувати його результати.

Розумні студентські картки та пристрої для відстеження відвідування закладів освіти, які полегшують контроль та надають можливість

адміністрації мати реальну картину про відвідування закладу студентами.

Бездротові дверні замки, підключені камери спостереження і системи розпізнавання обличчя, які забезпечують безпеку для викладачів, студентів та співробітників.

Дослідницькі програми, удосконалені за допомогою більш просунутих та автоматизованих систем в основних областях навчання, таких як медицина, сільське господарство та техніка.

Сучасні освітні платформи включають електронні книги з можливістю масштабування та збереження, а також смарт-дошки замість звичайних дошок, що дозволяють використовувати їх для письма маркером та відображення пов’язаної з темою графіки та зображень. У додаток до цього, системи голосового керування для викладачів, системи зберігання нотаток, інтелектуальні відеокамери для відеоспостереження, планшети і смартфони з освітніми програмами, змінюють традиційний спосіб роботи шкіл та освітніх систем.

Заклади вищої та середньої освіти можуть застосовувати різноманітні рішення Інтернету речей, незалежно від своєї спеціалізації. Наприклад, викладачі інформатики та інженерії можуть керувати лабораторіями IoT під час практичних занять, медичні коледжі можуть розширити можливості Інтернету

медичних пристроїв, а юридичні коледжі можуть викладати етику, конфіденційність та політику IoT. Також існують віддалені лабораторії з віддаленим доступом, які дозволяють проводити досліди безпосередньо з ПК. Інтернет речей - це не просто оновлення технологій у галузі освіти, але й можливість бути лідером та поширювати зміни на все суспільство, включаючи заклади освіти. Однак, існують деякі проблеми, які необхідно вирішити, щоб використовувати IoT в освіті. Наприклад, великий обсяг підключених пристроїв та даних вимагає значної пропускної здатності та бездротового доступу, що може вимагати модернізації мережного обладнання та програмного забезпечення.

Для визначення застосування IoT-інструментів в дистанційному та змішаному навчанні, автори провели опитування викладачів на міжнародній конференції в червні 2022 року. Опитування включало кілька питань, в тому числі, чи знайомі викладачі з поняттям IoT та які саме інструменти вони використовують у своїй роботі зі студентами.

Узагальнюючи результати опитування, 84% респондентів знайомі з терміном IoT та широко використовують його в своїй практиці, зокрема, електронні книги (16%), різні інтернет-додатки (40%), електронні журнали та віртуальні лабораторії. На

сьогодні неможливо проводити навчання дистанційно без можливостей, які надає Інтернет, тому викладачі повинні максимально ефективно підвищувати свою цифрову компетентність та знайомитись з сучасними технологіями, а також намагатись якісно передавати ці знання студентам, оскільки майбутні фахівці потребують цих знань та вмінь.

Для використання всіх переваг IoT потрібні відповідні інструменти врегулювання та захисту інформації на державному рівні. [2] В Україні до основних нормативно-правових актів, що регулюють розробку та використання сучасних інформаційно-комунікаційних технологій можна віднести: Стратегію розвитку інформаційного суспільства в Україні, Стратегію сталого розвитку «Україна – 2020»; «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну підтримку розвитку індустрії програмної продукції». Та переліком нормативно-правових актів, насамперед таких законів України, як: «Про інформацію», «Про захист персональних даних». Відповідно до ст. 11 Закону України «Про інформацію» інформація про фізичну особу – це відомості про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [5]. Основними даними про особу

(персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Забороняється збирання відомостей про особу без її попередньої згоди за винятком випадків, передбачених законом. Кожна особа має право на Механізми державного управління ознайомлення з інформацією, зібраною про неї. Інформація про особу охороняється Законом.

Питання захисту приватності постає особливо гостро саме з розвитком технологій Інтернет речей. Як зазначається в проекті нового Цивільного кодексу України «право на приватність належить до особистих немайнових прав і на сучасному етапі розвитку вітчизняної правової науки тотожне поняттю права на особисте життя та його таємницю».

Стаття 32 Конституції України передбачає: ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шелевер О.В., Технології інтернет речей в сучасній освіті: перспективи, особливості DOI https://doi.org/10.32782/2663- 6085/2022/50.2.412.
2. Круц Анна Олександрівна., Сучасні тенденції застосування технологій Інтернет речей при впровадженні електронного урядування на місцевому рівні с.16-17 https://ktpu.kpi.ua/wp-content/uploads/2019/12/naukovo-doslidna-robota-studentiv-kruts-2019.pdf 20203.
3. Botta A., De Donato V., Persico V., Pescape A. Integration of cloud computing and the Internet of Things: an overview. Computer systems of the future generation. 2016. URL: https://doi.org/10.1016/j.future.2015.09.0214.
4. Cornel C. and Ph. D., The Role of Internet of Things for a Continuous Improvement in Education. 2015.5.
5. Про інформацію Закон України від 02.10.1992 No 2657-XII. URL: http://zakon2.rada.gov.ua/.6. Про захист персональних даних Верховна Рада України; Закон України від 1 червня 2010 року No 2297-VI. URL: http://zakon2.rada.gov.ua/laws/show/2297-17/print1476025938545625.

КОСТЕНКО Олексій

доктор філософії (Ph.D.) з юридичних наук,
старший дослідник,
завідувач наукової лабораторії теорії цифрової трансформації і права наукового центру цифрової трансформації і права ДНУ ІІБП НАПрН України.

МЕТАВСЕСВІТ: ВСТУПНИЙ ЕТАП ФОРМУВАННЯ ОСНОВ ПРАВОВОГО РЕГУЛЮВАННЯ ВІРТУАЛЬНИХ СЕРЕДОВИЩ

Метавсесвіт (далі - Metaverse) – цифрове середовище, утворене сукупністю цифрових суб'єктів та цифрових об'єктів, що взаємодіють між собою, а також цифрові або інші технології, що забезпечують цю взаємодію [1], або нова концепція віртуального електронного світу, що складається з блокчейну (BCH), штучного інтелекту (AI) [2], електронної ідентифікації суб'єктів та об'єктів (ID), криптовалют (ICO), пристроїв Інтернет речей (IoT), технологій доповненої/віртуальної/розширеної реальності (AR/VR/MR), контенту створеного штучним інтелектом (AIGC), децентралізованих автономних організацій Metaverse (DAO); Аватарів (AV), віртуальних суб'єктів

та об’єктів, віртуальних активів та інтелектуальної і персональної власності на них, захисту персональної інформації та безпека даних в Metaverse, технологій формування цифрових людей/особистостей (Digital Humans) [3]. Metaverse – це набір сучасних технологій, що надають людині можливості недоступні в аналоговому світі, які можуть створити більш безпечний, прозорий і надійний електронний світ або світи.

Метавсесвіт, віртуальна спільнота, яка вже створює потенційні регулятивні проблеми і потребує мультидисциплінарного [4] правового регулювання [5].

Метавсесвіт складається з інфраструктур, з якими взаємодіють аватари. Юридичні питання в метавсесвіті включають захист даних, конфіденційність, статус аватарів [6], права інтелектуальної власності, особисту шкоду, кримінальні правопорушення [7], фінансові порушення [8], тощо.

Велика хартія законів Metaverse розробляється для регулювання суспільних відносин у метавсесвіті та створення нових галузей електронного права [9]. Вона буде служити золотим стандартом права Metaverse, створить нові та посилить діючі закони та правила регулювання суспільних відносин в електронних середовищах.

Очевидним фактом є необхідність у комплексній, мультидисциплінарній законодавчій базі для вирішення унікальних проблем, пов’язаних із Metaverse, а також для забезпечення захисту користувачів і відповідального та етичного регулювання Metaverse.

Для початку роботи над законодавством Metaverse для України доцільно створити базову модель [10], яка буде ґрунтуватися на трьох блоках: технологія, стандарти та право. Саме ці основи повинні формувати стратегії впровадження Metaverse в Україні та протистояти ризикам, викликам та негативним впливам, які він створює у сфері забезпечення економічної безпеки, сферах національної безпеки та особистої інформаційної безпеки. Саме тому першочергового впорядкування потребують наступні сфери правовідносин.

Транскордонна взаємодія в новому середовищі, вирішення питань щодо повноважень урядів або правових систем регулювання та виконання законів у віртуальних середовищах, забезпечення конфіденційності [11], етичні міркування та негативний вплив на вразливих користувачів, спеціальні закони, правила та політики, що збалансуватимуть конкуруючі інтереси різних зацікавлених сторін у Metaverse [12].

Управління та регулювання застосування AI в Metaverse. Законодавство стосовно AI вже на сьогодні

має низку проблем, таких як: предметна кваліфікація штучного інтелекту, характеристика, атрибуція та захист продуктів штучного інтелекту, принцип штучного інтелекту, відповідальність за делікти тощо. Позиція аналогового законодавства – авторські права на роботи повинні належати «виробнику або менеджеру» штучного інтелекту. Проте слід вже продумувати законодавчі інструменти регулювання для епохи появи супер AI.

Управління та правова регуляція AIGC (контент, створений штучним інтелектом). AI віртуального світу бере участь у створенні та розвитку Metaverse як інфраструктури. AIGC поділяється на дві частини: перша – це AI формування зображення, включаючи генерацію скелетної анімації, генерацію виразу обличчя, захоплення руху та інші технології навколо персонажів, а також розпізнавання зображень, генерацію сцен, імпорт ресурсів, візуалізація, моделювання, тощо; друга – логічний AI, включаючи семантичне розуміння, мовні моделі, діалогові роботи та інші технології навколо мовного діалогу, а також загальний AI інтелект з логіки прийняття рішень, моделі прийняття рішень на основі сценаріїв (багатоагентна єдина мета, мультиінтелект кілька цілей), тощо. Управління та правова регуляція DAO (децентралізована автономна організація) автономна

організація, що базується на AIGC, яка може відокремлювати Metaverse від поточного Інтернету.

Законодавче регулювання доповненої реальності (Augmented Reality, AR), яка «плавно» інтегрує інформацію реального світу та інформацію віртуального світу; віртуальної реальності (Virtual Reality, VR), що включає комп'ютерну, електронну інформацію та технології моделювання.

Визначення права на персональну інформацію в контексті права суб'єктів інформації і контроль особистої інформації, якою вони користуються, різними способами, і недопущення інших до її незаконного використання, тобто необхідна глибока деталізація персональної інформації в поєднанні із сферою ідентифікаційних даних та значне розширення прав на їх контроль та захист.

Розробка законодавства про електронні докази, яке повинно забезпечити достовірність аналізу великих даних та можливість миттєвої великомасштабної обробки неструктурованої інформації з метою забезпечення форми доказів, релевантність доказів та їх законність.

Встановлення правового статусу віртуальних (дематеріалізованих) суб'єктів та об'єктів власності, із урахуванням існування різних форм суб'єктів права, норм, різних правових систем та юрисдикцій.

Встановлення правил та норм для віртуальної власності, яка в Metaverse відрізняється від власності в реальному світі. Є наукова думка, що мережева віртуальна власність стосується всієї ексклюзивної віртуальної власності, що існує в кіберпросторі. Однак, визначення віртуальної власності, природа та режим охорони закону детально не визначені, натомість пропонуються наступні правові атрибути або методи захисту віртуальної власності: теорія речових прав, теорія прав кредитора, теорія нових прав власності та теорія прав інтелектуальної власності.

Встановлення статусу цифрових людей (Digital Humans) або електронних особистостей, які є «клоном» людини реального світу в Metaverse, чия поведінка повністю контролюється та перебуває під впливом людини реального світу, і значною мірою відображає риси особистості реального світу [13]. Цифрові люди (Digital Humans) – це технологія, заснована на технології комп’ютерної графіки та технології штучного інтелекту, яка використовує людські обличчя та тіла як шаблони для імітації реалістичного та високоінтерактивного віртуального персонажу.

Техніко-медичне удосконалення людини, дистанційна медична консультація, віртуальна діагностика, пристрої IoT, біоніка 3D, друк інтерфейсу мозок-комп’ютер (BCI), обчислювальна біологія [14].

Фактично українським правознавцям вже сьогодні доцільно активно включатися в роботу щодо формування національних правових норм регулювання Metaverse, які не тільки стануть основою національного Metaverse, але й наддадуть можливість взаємодіяти та залучатися до спільної міждержавної наукової роботи зі створення технічного, етичного та правового регулювання Metaverse.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Костенко О.В. Проблеми правового регулювання Метавсесвіту. Конференція: матеріали V міжнар. наук.-практ. конф., м. Стокгольм, Швеція, 6-8 лют. 2022 р. Стокгольм, Швеція 2022. С. 729–733.URL: https://www.researchgate.net/publication
2. Баранов О.А. Визначення терміну «штучний інтелект». *Інформація і право*. № 1(44)/2023. С. 32–49. URL: http://ippi.org.ua/sites/default/files/5_28.pdf?fbclid=IwAR3FuuOlkhLTnDabyIlSjPGxW7klw3IWiYDCORgCl_ZHl16XC1cYcdMR4Ew (дата звернення: 30.04.2023).
3. Костенко О.В. Штучний інтелект (AI) і Метавсесвіт: правові аспекти. *Юридичний науковий електронний журнал*. 2022. № 8. С.301-308. URL: http://lsej.org.ua/8_2022/66.pdf. DOI: https://doi.org/10.32782/2524-0374/2022-8/66.

4. Dwivedi, Y. K., Hughes, L., Baabdullah, A. M. Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. URL: https://www.sciencedirect.com/science/article/pii/S0268401222000767 (дата звернення: 29.04.2023).
5. Turdialiev, M. The legal issues of metaverse and perpectives of establishment of international financial center in metaverse. URL: https://cyberleninka.ru/article/n/the-legal-issues-of-metaverse-and-perpectives-of-establishment-of-international-financial-center-in-metaverse (дата звернення: 29.04.2023).
6. Cheong, B. C. Avatars in the metaverse: potential legal issues and remedies. URL: https://link.springer.com/article/10.1365/s43439-022-00056-9 (дата звернення: 29.04.2023).
7. Qin, H. X., Wang, Y., Hui, P. Identity, Crimes, and Law Enforcement in the Metaverse. URL: https://arxiv.org/abs/2210.06134 (дата звернення: 29.04.2023).
8. Katterbauer, K., Hassan, S., Cleenewerck, L. Financial cybercrime in the Islamic Finance Metaverse. DOI: https://doi.org/10.57019/jmv.1108783.
9. Kostenko, O., Furashev, V., Zhuravlov, D., Dniprov, O. Genesis of Legal Regulation Web and the Model of the

Electronic Jurisdiction of the Metaverse. DOI: https://doi.org/10.46282/blr.2022.6.2.316.
10. ing, H.,Wang, H., Lin, Y., Wang, W., Dhelim, S. A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges. URL: https://arxiv.org/abs/2111.09673 (дата звернення: 29.04.2023).
11. Kalyvaki, M. Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. Journal of Metaverse. URL: https://dergipark.org.tr/en/pub/jmv/issue/72588/1238344 (дата звернення: 30.04.2023).
12. Fernandez, C. B., Hui, P. Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse. URL: https://ieeexplore.ieee.org/abstract/document/9951378/ (дата звернення: 30.04.2023).
13. Bibri, S. E. The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society. URL: https://www.mdpi.com/1747560 (дата звернення: 30.04.2023).
14. Chen, D., Zhang, R. Exploring Research Trends of Emerging Technologies in Health Metaverse: A Bibliometric Analysis. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3998068 (дата звернення: 30.04.2023).

КОРНІЙЧУК Ілля
Навчально-науковий Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського
КУРДЕЧА Василь
КПІ ім. Ігоря Сікорського

РЕГУЛЯТОРНІ ТА ПРАВОВІ ВИКЛИКИ У ГІБРИДНИХ МІКРОМЕРЕЖАХ З ПІДТРИМКОЮ ІНТЕРНЕТУ РЕЧЕЙ

Людство продовжує шукати чистіші та ефективніші джерела енергії [1, с.1], в результаті цього, гібридні мікромережі стають гарним рішенням. Гібридні мікромережі — це енергетичні мережі, які поєднують відновлювані та невідновлювані джерела енергії. Для ефективного застосування такої системи, потрібно використовувати нові технології, такі як Інтернет речей, штучний інтелект та хмарні сховища на основі блокчейну. Однак для успішної інтеграції таких технологій (рис. 1), необхідно вирішити низку регуляторних проблем [2, с.269]:

Рис. 1. *Алгоритм застосування новітніх технологій*

Гібридні мікромережі з підтримкою Інтернету речей, використовуючи датчики для моніторингу та контролю споживання і використання енергії, можна оптимізувати використання енергії, зменшити кількість відходів та підвищити загальну ефективність. Штучний інтелект, аналізуючи дані в режимі реального часу, може прогнозувати попит на енергію та коригувати її виробництво, зменшуючи витрати та запобігаючи відключення електроенергії [3, с.4]. Використовуючи хмарне середовище на основі блокчейну, можна підвищити захист від кібератак та забезпечити доступність та точність критично важливих даних. Але існують регуляторні проблеми, пов’язані з

використанням цих технологій, включаючи проблеми конфіденційності даних, потенційну упередженість алгоритмів штучного інтелекту, правову та регуляторну невизначеність і проблеми щодо масштабованості (рис. 2).

Рис. 2. Регуляторні проблеми у гібридних мікромережах

Конфіденційність даних та кібербезпека. Наприклад, у мікромережах з підтримкою Інтернету речей існує ризик того, що до конфіденційних даних можуть отримати доступ сторонні особи, що може становити загрозу національній безпеці. Аналогічно, у хмарних сховищах на основі блокчейну існує ризик втрати або викрадення критично важливих даних, що може призвести до перебоїв у виробництві енергії та спричинити масштабні збитки. Одним з потенційних

рішень цієї проблеми є розробка надійних технологій шифрування і автентифікації. Це може допомогти запобігти несанкціонованому доступу до конфіденційних даних і захистити від кібератак. Крім того, можуть з'явитися можливості для покращення кібербезпеки завдяки використанню штучного інтелекту та машинного навчання, які можуть ідентифікувати потенційні загрози та реагувати на них у режимі реального часу.

Правова та регуляторна невизначеність. Наприклад, у випадку зі штучним інтелектом для мікромереж можуть виникнути юридичні питання щодо того, хто нестиме відповідальність, якщо алгоритм припуститься помилки, яка призведе до відключення електроенергії. Аналогічно, у випадку з хмарним сховищем на основі блокчейну може виникнути регуляторна невизначеність щодо використання децентралізованого сховища і того, як воно вписується в існуючі енергетичні норми. Для усунення правової та регуляторної невизначеності потрібна розробка нових політик і нормативних актів, спеціально пристосованих до цих нових технологій. Це може допомогти прояснити відповідальність і зменшити правову невизначеність. Крім того, можуть з'явитися можливості для співпраці з регуляторними органами з метою створення умов, які дозволять тестувати та

експериментувати без ризику правових або регуляторних наслідків.

Масштабованість та інтероперабельність. Хоча ці технології можуть добре працювати в пілотних проектах або в невеликих масштабах, їх може бути складно масштабувати до більших систем або інтегрувати з існуючою енергетичною інфраструктурою. Це може стати перешкодою для широкого впровадження і обмежити потенційні переваги цих технологій. Для вирішення цих питань, потрібно розробити спільні стандарти і протоколи, які дозволять цим технологіям безперешкодно працювати з існуючою енергетичною інфраструктурою.

Сприйняття громадськістю та освіта. Багато з цих технологій є складними і можуть бути незрозумілими для широкої громадськості. Для того, щоб ці технології були успішно інтегровані в енергетичний сектор, необхідно проводити просвітницьку роботу з громадськістю для пояснення їхніх переваг та усунення будь-яких занепокоєнь або непорозумінь.

На закінчення, незважаючи на те, що нові технології в гібридних мікромережах, безумовно, стикаються з регуляторними проблемами, існують також потенційні рішення, які можуть допомогти вирішити ці проблеми. Розробляючи надійні технології

шифрування та автентифікації, уточнюючи правові та регуляторні обов'язки, розробляючи загальні стандарти і протоколи, а також беручи участь у просвітницькій роботі з громадськістю, ми можемо допомогти забезпечити успішну інтеграцію цих технологій в енергетичний сектор і сприяти переходу до більш чистих і ефективних джерел енергії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про альтернативні джерела енергії [Електронний ресурс] : Закон України від 2003, № 24, ст.155: станом на 01 січня 2023 р. — Режим доступу: https://zakon.rada.gov.ua/laws/show/555-15#Text (дата звернення: 30.04.2023). —

2. Корнійчук І. Г., Курдеча В. В. Енергетичне прогнозування та управління з підтримкою інтернету речей для гібридних мікромереж // XVII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2023: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського – 2023. – С. 269.

3. J. Yamnenko, L. Globa, V. Kurdecha and A. Zakharchuk, "Data Processing in IoT Systems based on Fuzzy Logics," 2019 Modern Electric Power Systems (MEPS), Wroclaw, Poland, 2019, pp. 1-4, doi: 10.1109/MEPS46793.2019.9395055.

КРАВЧУК Олексій

суддя-спікер Вищого антикорупційного суду,
професор КПІ імені Ігоря Сікорського,
доктор юридичних наук, професор

ПРЕД'ЯВЛЕННЯ СВІДКУ ДОКАЗІВ ПІД ЧАС ВІДЕОКОНФЕРЕНЦІЇ В КРИМІНАЛЬНОМУ СУДІ

При допиті свідків і потерпілих у кримінальному провадженні в суді можливість поставити запитання про речові докази й документи може бути важливим елементом доведення позиції сторони по справі або спростування позиції протилежної сторони. Хоча КПК України прямо не передбачає можливості пред'явлення свідку документів, звуко- і відеозаписів та речових доказів під час допиту, іноді така потреба виникає. При цьому суд зобов'язаний забезпечити можливість здійснення учасниками кримінального провадження їхніх процесуальних прав на засадах рівності та змагальності. В умовах воєнного стану допит свідків набагато частіше, ніж раніше, проводиться в режимі відеоконференції [1]. При цьому використовується

трансляція (відеозв’язок) з приміщення іншого суду або з допомогою власних технічних засобів свідків, потерпілих – з допомогою спеціального (для судових відеоконференцій) або загальнопоширеного програмного забезпечення.

Оскільки показання свідків – це доказ, що ґрунтується на особистому сприйнятті певної події чи факту, іноді свідку, щоби краще пригадати цю подію чи факт, треба знову побачити певну річ або документ.

Відповідно до ч. 3 ст. 357, ч. 2 ст. 358 КПК учасники судового провадження мають право ставити запитання з приводу речових доказів та документів свідкам, експертам, спеціалістам. За ч. 14. ст. 352 КПК під час дослідження інших доказів свідкам можуть ставити запитання учасники судового провадження, експерт, а також суд. Ці норми сконструйовані так, ніби такі запитання можуть ставитися саме при дослідженні документів або речових доказів. Однак на практиці запитання свідку в суді можна поставити лише при його допиті – це стосується й запитань про речові докази й документи, тому ці правила застосовуються як складова процедури допиту свідків.

Саме ж розміщення норм (у статтях КПК про дослідження речових доказів і документів) вказує на те, що при постановці відповідних питань свідкам ці

докази можуть (або й мають) бути продемонстровані свідкові.

Необхідність пред'явлення свідкові, потерпілому документів, звуко-, відео-записів та речових доказів впливає на порядок дослідження доказів. Як правило, доцільно визначати такий порядок, щоб допит свідків обох сторін і потерпілих проводився після дослідження судом документів і речових доказів (як сторони обвинувачення, так і сторони захисту). Навіть якщо сторони не клопотатимуть про пред'явлення свідку доказів, при допиті питання про докази можуть виникнути, й суду під час допиту краще розуміти, про що йде мова. Тож коли сторони ставлять питання про допит свідка або свідків до дослідження речових доказів і документів, доцільно з'ясувати, чи планують вони ставити запитання свідкам про речові докази або документи. Якщо так, то відповідним чином варто визначити або змінити порядок дослідження доказів. Якщо учасники не планують ставити такі питання свідкам, свідків і потерпілих можна допитати й до дослідження речових доказів і документів.

Якщо учасники планують ставити запитання свідкам про речові докази та документи, які необхідно пред'явити свідку, варто повідомити про це секретаря судового засідання або судового розпорядника перед судовим засіданням, у якому заплановано допитати

відповідного свідка. Бажано завчасно вказати на том і аркуш судової справи, де зберігається документ, назву файлу відео- чи звукозапису, його місце зберігання та таймінг або речовий доказ, який необхідно продемонструвати свідкові. Це потрібно зробити, щоб зайвий раз не втрачати час. Наприклад, речові докази треба завчасно приготувати, попередньо отримавши з відповідного місця зберігання.

Надалі при пред'явленні свідкові речового доказу або документа в ході допиту під час засідання варто зазначати вголос номер сторінки й тому судової справи, назву й таймінг файлу, найменування документа або речового доказу, що пред'являється свідкові і про який йому ставляться запитання. Ці реквізити вказуватимуться в журналі судового засідання й будуть корисними сторонам і суду для подальшої роботи зі справою.

Якщо постає питання про допит свідка в режимі відеоконференції, одним із питань при його вирішенні є те, чи слід буде пред'являти йому при допиті речі, документи, звуко-, відеозаписи. Хоча в умовах ковіду, а надалі воєнного стану віддаленість свідка як підстава для задоволення клопотання про відеоконференцію, як правило, переважає, і тоді питання про те, як продемонструвати свідкові зазначені докази при його допиті – стає здебільшого технічним.

Якщо йдеться про документ, то він може бути відсканований судом із судової справи (або вже наявний у ній в електронній формі) і продемонстрований свідкові за допомогою системи технічного фіксування судового засідання та програмного забезпечення відеоконференцзв'язку.

Аналогічним чином, як правило, може бути продемонстровано звуко- та відеозаписи (хоча в окремих випадках це вимагає спеціального програмного забезпечення, тому може потребувати залучення спеціаліста для участі в дослідженні; оскільки ці докази вже мають бути в розпорядженні суду, то суду, як правило, відомо, чи їх можна відтворити на техніці й програмному забезпеченні суду, чи потрібно залучати спеціаліста). Це ще раз вказує на необхідність завчасного повідомлення суду про потребу пред'явлення свідкові доказу. Електронний документ, скан паперового документа, файл звуко-, відеозапису відтворюються з допомогою системи технічного фіксування судового засідання та транслюються свідкові з допомогою програмного забезпечення відеоконференцзв'язку. Головуючий переконується, чи добре все видно (або й чути) свідкові, задаючи йому запитання. Також про те, що свідкові все добре видно (чути) може свідчити факт, коли він одразу при відтворенні файлу згадує цей документ, і починає

пояснювати, наприклад: «так, це той договір, я його підписував».

Свідкові, що допитується з допомогою відеоконференції через його власні технічні засоби, навіть зручніше побачити відеофайл на екрані власного комп'ютера або почути звуковий файл у власних навушниках, ніж побачити його на телеекрані, підвищеному під стелею в судовій залі.

Речові докази, як правило, немає можливості пред'явити в такий спосіб, і необхідність їх пред'явлення свідкові може передбачати обов'язкову його явку до суду (що не завжди є можливим). Але як видно з наведеного, в КПК йдеться не суто про пред'явлення, а про можливість поставити свідкові запитання про речі й документи. У такому випадку суду слід переконатися, що свідок розуміє, про яку річ або який документ ідеться, цього достатньо. Щодо документа, звуко-, відеозапису таке розуміння може бути досягнуто шляхом демонстрації відсканованого судом документа за допомогою системи фіксування судового засідання та програмного забезпечення відеоконференції.

Постановка свідкові питань про документ з демонстрацією його електронного примірника чи відсканованої копії через відеоконференцію не порушує принцип безпосередності. Він полягає в

безпосередньому сприйнятті судом показань і безпосередньому дослідженні судом документа. Цей документ має бути доступний для ознайомлення сторін, яким надана можливість вказати суду на певні особливості документа. Сторони повинні мати можливість почути показання свідка в суді, поставити йому необхідні питання в ході прямого чи перехресного допиту. Право поставити свідкові питання про документ також ураховує принцип безпосередності дослідження, а не суперечить йому, адже суд безпосередньо почує відповіді свідка на поставлені йому питання про документ.

Більш детально питання пред'явлення свідкові, потерпілому доказів – речей, документів, звуко- і відеозаписів під час допиту в суді розглядався нами в статті: [2].

Висновки. При допиті свідка, потерпілого в режимі відеоконференції в кримінальному провадженні в суді йому можуть бути поставлені запитання щодо доказів – речей, документів, звуко- і відеозаписів. При цьому свідкові, потерпілому може бути продемонстровано відповідний доказ (як правило, – крім речових доказів) з допомогою системи технічного фіксування судового засідання, що транслюються свідкові з допомогою програмного забезпечення відеоконференцзв'язку. Якщо звуко-, відеофайл є

зашифрованим, може бути залучений спеціаліст та використовуватися інше спеціальне програмне забезпечення або програмно-технічні засоби. В разі виникнення потреби демонстрації свідкові доказів під час допиту, ці докази мають бути досліджені до допиту свідка, а суд має бути завчасно (як правило при вирішенні питання про виклик свідка) попереджений про таку необхідність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кравчук О., Сікора К. Відеоконференція з власних технічних засобів у кримінальному судочинстві під час воєнного стану. Кримінальна юстиція в україні: реалії та перспективи: матеріали Круглого столу (23 вересня 2022 року). Львів : Львівський держ. університет внутр. справ, 2022. С. 174–178. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/5018

2. Кравчук О. Пред’явлення свідку доказів під час допиту в кримінальному суді. Just Talk. 23 лютого 2023 р. https://justtalk.com.ua/post/predyavlennya-svidku-dokaziv-pid-chas-dopitu-v-kriminalnomu-sudi

КУШНІРУК Олександр

студент, КПІ ім. Ігоря Сікорського

ГОЛОВКО Ольга

к.ю.н., ст. дослідник,
ст. науковий співробітник лабораторії
теорії цифрової трансформації і права
наукового центру цифрової трансформації
і права ДНУ “ІІБП НАПрН” України,
ст. викладач кафедри інтелектуальної власності
та приватного права КПІ ім. Ігоря Сікорського

ПРАВОВА ОХОРОНА ПЕРСОНАЖІВ

Розвиток сучасних економічних відносин та підприємницької діяльності в країні став передумовою використання результатів творчої діяльності для створення індивідуалізованих засобів цивільного обороту учасників, їх товарів і послуг. Сьогодні одним з найбільш актуальних питань, пов’язаних з охороною прав на результати творчої діяльності, є передача прав на літературні твори та їх окремі структурні елементи (назви, персонажі), наприклад, для використання в якості торговельних марок і фірмових найменувань, для

реєстрації промислових зразків (автономні автомобілі, дрони тощо).

Одним із типових способів комерційного використання персонажів є індивідуалізація товарів і послуг за допомогою торговельної марки, якою є ім’я або зовнішній вигляд (зображення) персонажа, в тому числі використання таких знаків у рекламі товарів і послуг. Популярні персонажі, в тому числі герої мультфільмів, залучаються до приватного обігу окремо від усього твору.

Персонаж (фр. personnage, від лат. persona - маска актора в античному театрі, у переносному значенні - носій маски, актор, особа, яку він зображує) - образ актора, який постає у творі як об’єкт оповіді і розглядається передусім як якась жива або умовна істота. По суті, термін «персонаж» - це збірний термін для всього спектру зображувальних засобів.

Щодо елементів твору, які охороняються, то до них належать: зовнішня форма (його мова, в тому числі спеціальні наукові знаки і символи, за допомогою яких виражаються авторські засоби і прийоми створення художнього образу, тобто вся сукупність використаних ним зображувально-виражальних засобів) та внутрішня форма (утворена авторською послідовністю уявлень наукових понять, логікою, системою розкриття наукових ідей і розташуванням матеріалу) сформована,

спеціальною аргументацією та науковим апаратом, методами розкриття наукових ідей [5].

Ватро звернути увагу на те, що у чинному українському законодавстві ні Цивільний кодекс України, ні Закон України «Про авторське право і суміжні права» не згадують про охорону персонажів літературних творів, а от про охорону авторського права, захист авторських прав, однак, згадується в Законі України «Про охорону прав на знаки для товарів і послуг», частина 4 статті 6 Закону містить підстави для відмови в реєстрації знака для товарів і послуг [1].

Як правило, персонажі у творі можуть отримати правову охорону за умови, що останній є результатом самостійного створення і виражений в об’єктивній формі. Деякі вчені стверджують, що основна можливість охорони персонажів засобами авторського права грунтується на твердженні, що і зображення, і мова твору належать до правової категорії творів [6].

Закон України «Про охорону прав на знаки для товарів і послуг» перелічує підстави для відмови в реєстрації знаків для товарів і послуг, а саме відтворення імен, відомих з наукових, літературних і художніх творів або цитат і персонажів з них, а також позначень художніх творів і їх фрагментів без згоди суб’єкта авторського права чи його правонаступника, а

також позначень художніх або його правонаступника (ч. 4 ст. 6 цього Закону) [2].

Звернемо увагу на практику застосування судами норм законодавства у справах про захист авторського права і суміжних прав: часто у судових рішеннях зустрічається позиція суду про те, що персонажі охороняються як окремі об’єкти авторського права лише в тому випадку, якщо вони створені однією особою. Виходячи з цих положень, суди застосовують їх при вирішенні спорів між автором і власником художнього твору. На думку деяких вчених, одним із додаткових аспектів бренду в сучасних рекламних кампаніях є корпоративний герой. За великим рахунком, такий герой є «обличчям» бренду, що уособлює його індивідуальність і зближує його зі споживачем на емоційному рівні. Наявність корпоративного героя як частини бренду може мати значний вплив на імідж продукту, а отже, і на його продажі. Залежно від реальності існування героя можна вирізнити дві категорії: вигадані (різноманітні істоти, персонажі) та реальні люди [7].

Також варто розглянути питання застосування персонажів у складі складних об’єктів. Складним об’єктом, за загальним правилом, визнається результат інтелектуальної діяльності, який сам по собі складається з декількох охоронюваних результатів

інтелектуальної діяльності (наприклад кінофільм, який має містити в собі декількох персонажів). У такому випадку особа, яка організувала створення складного об’єкта (якщо мова йде про кінофільм – продюсер), набуває виключне право на складний об'єкт на підставі договорів про відчуження виключного права з авторами або ліцензійних договорів, укладених з власниками виключних прав на відповідні результати інтелектуальної діяльності. Міжнародна організація охорони інтелектуальної власності визначає комерційне використання персонажа як пристосування або вторинне використання вигаданого персонажа та його властивостей (імені, художнього образу, зовнішності) автором або уповноваженою третьою особою для різноманітних товарів і послуг з метою заохочення потенційних споживачів купувати ці товари або послуги через наявність у них симпатії до певного персонажа [8].

Використання персонажів у промислових зразках та засобах індивідуалізації юридичних осіб, товарів, робіт, послуг та підприємств також має свої особливості. Формуючи визначення промислового зразка з юридичної точки зору, можемо дійти висновку, що це - право, що надається в багатьох країнах в рамках системи реєстрації для захисту оригінальних декоративних і нефункціональних характеристик

промислового виробу або продукту [8]. Технічні характеристики продукту в сучасному світі, як правило, відносно ідентичні, що пов’язано з великою конкуренцією, запобіганням утворення монополії на ринку та з перспективою на майбутнє (покращенням технічних характеристик товару в майбутньому, запасом інновацій, нових функцій та особливостей виробу). Саме тому правова охорона промислових зразків відіграє важливу роль у захисті відмінної риси продукту споживач, адже обирає товар, керуючись зовнішніми характеристиками та ціновою політикою.

Дуже часто у продажу можна зустріти товари із зображеннями персонажів відомих брендів або мультфільмів, відеоігор та книг. Це можуть бути різноманітні сувеніри для блогів, канцелярські товари чи іграшки, що імітують зовнішній вигляд персонажів. Однак слід пам’ятати, що персонажі є об’єктом авторського права, оскільки вони є творчим результатом автора і мають правову охорону. Крім того, ім’я або зображення персонажа може бути зареєстровано як торговельна марка. Тому суб’єкти господарювання, які займаються виробництвом або продажем таких товарів, повинні дбати про дотримання прав інтелектуальної власності, оскільки вони можуть бути притягнуті до відповідальності за завдані збитки.

Відповідно до частини 1 статті 15 Цивільного кодексу України кожна особа має право на захист у разі порушення, невизнання або оспорювання її цивільного права. Правовласники мають право вимагати компенсації у разі незаконного використання їхніх творів. Розмір компенсації варіюється від 10 до 50 000 мінімальних заробітних плат. При пред'явленні вимоги про виплату компенсації автору не потрібно доводити розмір збитків або факт їх заподіяння, що робить компенсацію найзручнішим способом захисту авторських прав [1].

Успішне використання прав на промислові зразки дозволяє компаніям підвищити свою конкурентність і, таким чином, отримати стратегічну перевагу. Якщо промислові зразки, створені компаніями, захищені правами інтелектуальної власності, вони набувають певної вартості і не можуть бути використані без дозволу власника. Це означає, що необхідно зареєструвати відповідні права на цей об'єкт інтелектуальної власності, щоб інші особи не могли використовувати його на власний розсуд і для власної вигоди.

Визначимо головні особливості правової охорони персонажів у складі торгівельних марок, промислових виробів тощо. По-перше, основним способом захисту прав на комерціалізований персонаж є реєстрація

торгової марки. Якщо є намір виготовити продукт або надати послугу з персонажем, авторського права може бути недостатньо для захисту прав у суді. У більшості випадків знадобиться зареєстрована торгова марка [3].

По-друге, Закон України «Про охорону прав на знаки для товарів і послуг» забороняє реєстрацію в Україні торговельної марки, яка відтворює персонажі загальновідомого твору без згоди власника авторського права або його правонаступника. Згідно з «Методичними рекомендаціями щодо деяких питань проведення експертизи заявки на знак для товарів і послуг», опублікованими на офіційному веб-сайті Українського відомства інтелектуальної власності, з метою застосування підстави, передбаченої абзацом 2 пункту 4 статті 6 Закону України «Про охорону прав на знаки для товарів і послуг», якщо наукові, літературні та художні твори, їх цитати та персонажі є загальновідомими в різних регіонах України[9] .

По-третє, торговельна марка, на відміну від авторського права, є територіально обмеженою, тобто діє в тій країні, в якій вона зареєстрована. Для того, щоб захистити права персонажа в інших країнах, можна скористатися Мадридською міжнародною реєстрацією торговельних марок [4].

Всесвітня організація інтелектуальної власності визначає комерційне використання персонажа як

пристосування або вторинне використання вигаданого персонажа та його якостей (імені, художнього образу, зовнішності) автором або уповноваженою ним третьою особою для різних товарів і послуг з метою спонукання потенційних споживачів до придбання цих товарів або послуг через симпатію до певного персонажа. На нашу думку, у Цивільному кодексі України слід передбачити «право на персонажа» як особисте немайнове право фізичної особи. Воно поширюється не лише на зображення, образ але й на інші елементи, які персоналізують особу чи її сценічний образ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Цивільний кодекс України: Закон України від 16 січня 2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 01.05.2023).

2. Про охорону прав на знаки для товарів та послуг: Закон України від 15.12.1993 р., № 3689-XII. URL: https://zakon.rada.gov.ua/laws/show/3689-12#Text (дата звернення: 01.05.2023).

3. Про охорону прав на промислові зразки: Закон України від 15 грудня 1993 р. № 3688-XII. URL: https://zakon.rada.gov.ua/laws/show/3688-12#Text (дата звернення: 01.05.2023).

4. Мадридська угода про міжнародну реєстрацію знаків: угода від 14.04.1891 р. № 995-134. URL:

https://zakon.rada.gov.ua/laws/show/995_134#Text (дата звернення: 01.05.2023).
5. Якименко Ю. Способи захисту авторських прав / Ю. Якименко // Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія «Юридичні науки». - 2015. -№ 6. – С. 37-41.
6. Білоусов В. М. Поняття, ознаки й елементи літературного твору / / Часопис Київського університету права. — 2003. — № 2. — С. 40-44.
7. Кузьменко Т.С. Правова охорона додаткових компонентів бренду / Т.С. Кузьменко / Актуальні проблеми політики. – 2009. – №38. – С. 608-614.
8. Кулініч О.О. Порушення авторських прав на персонажі художніх творів при реєстрації права на торговельні марки: вирішення спорів за законодавством України / О.О. Кулініч, Л.Д. Романадзе // Часопис цивілістики. – 2012. -№13. – С. 95-98.
9. Коваль І.Ф. Щодо правового статусу вищого суду з питань інтелектуальної власності / І.Ф. Коваль // Теорія і практика інтелектуальної власності. – 2016. – №5. – С. 39-44.

ЛЮБАРСЬКА Світлана
студентка, КПІ ім. Ігоря Сікорського
КУРДЕЧА Василь
КПІ ім. Ігоря Сікорського

ВРАХУВАННЯ ПРАВОВИХ ВИМОГ ПРИ ОБРОБЦІ ГРАФІЧНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІОТ

Розвиток цифрової індустрії призводить до стрімкого зростання кількості пристроїв мереж Інтернету речей. В свою чергу це призводить до необхідності правового регулювання як вимог до створення таких систем так і самої роботи мереж Інтернету речей. Особливої уваги слід звернути на мережі Інтернету речей, що працюють із графічними зображеннями та відеоданими, отриманими з фото- та відеокамер, фотодатчиків тощо. Дана робота присвячена врахуванню правових вимог[1, с.1] при обробці графічної інформації в мережі Інтернету речей.

Аналіз існуючих рішень показує, що методи обробки графічної інформації в IoT включають [2, с.263]:

- відстеження комп’ютерного зору,
- аналіз даних зображень,
- формування та обробку відеопотоків

- розпізнавання образів,
- віртуальну реальність.

Опис методів обробки графічної інформації можна сформувати наступним чином:

Відстеження комп’ютерного бачення – це програмний інструмент, який виявляє об’єкти та відстежує їх рух, але для цього потрібні спеціалісти та можуть вийти з ладу, якщо пристрій вийде з ладу через вірус або інші проблеми.

Аналіз даних зображень дозволяє витягти значущу інформацію з цифрових зображень, але це може зайняти багато часу та бути дорогим залежно від конкретної системи.

Формування та обробка відеопотоків – дозволяє створювати потік даних, що може бути переданий до хмарного середовища для подальшої обробки та збереження. Потенційно дану процедуру можливо виконувати на кінцевих та проміжних вузлах.

Розпізнавання шаблонів дозволяє автоматизовано розпізнавати шаблони та шаблони в даних, але це може бути важко реалізувати, надзвичайно повільно та вимагає більшого набору даних для отримання підвищеної точності.

Віртуальна реальність, яка імітує досвід за допомогою відстеження пози та 3D-дисплеїв біля очей, не підходить для вирішення наявних проблем.

При цьому розглядувані методи стикаються з рядом проблем. До таких технічних проблем з обробкою графічної інформації в IoT можна віднести (рис.1):

Зберігання та передача графічної інформації через мережу IoT може бути проблематичною через велику кількість даних.

Якість зображення може відрізнятися, а передача через мережу може спричинити спотворення, що ускладнить визначення деталей і характеристик зображення.

Обмежені можливості обробки даних пристроїв IoT можуть вплинути на точність результатів обробки графічної інформації.

Збір і передача графічної інформації через мережі IoT може викликати проблеми безпеки, наприклад несанкціонований доступ до інформації.

Існує потенційний ризик того, що пристрої IoT можуть збирати графічну інформацію в різних форматах файлів або протоколах зв’язку, що може призвести до труднощів з обробкою та аналізом даних.

При розгляді цих проблем необхідно звертати увагу в тому числі і на юридичні аспекти. Особливо у галузі збору, зберігання та передачі графічної інформації, необхідно дотримуватись правил і законодавчих норм.

Перше що потрібно врахувати це Закон України "Про захист персональних даних". Згідно з цим Законом, персональні дані[1, ст.1] - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Обробка персональних даних може здійснюватися тільки відповідно до вимог цього Закону.

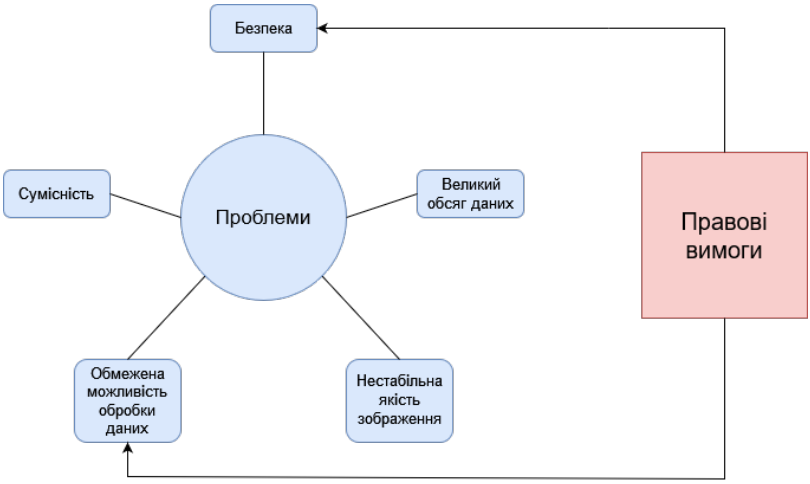

Рис.1. Вплив правових вимог на існуючі технічні проблеми з обробкою графічної інформації в мережах Інтернету речей.

Авторські права на графічну інформацію також є важливою темою. Захист авторських прав на графічну інформацію в інтернеті речей може включати в себе такі заходи, як:

Правові повідомлення: розміщення правових повідомлень на своєму веб-сайті або на пристроях, що використовують цю інформацію.

Технічні заходи: захист від копіювання, шифрування та технічні обмеження.

Юридичні заходи: у разі порушення авторських прав на графічну інформацію, власник може подання позов у суд про порушення авторських прав.

Існуючі методи вирішення цих проблем:

Щоб зменшити розмір зображення та час передачі даних через мережу IoT, можна використовувати стиснення даних.

Алгоритми обробки зображень, такі як виявлення контурів, сегментація зображень і класифікація зображень, можуть бути використані для вирішення завдань обробки графічної інформації.

Штучний інтелект можна використовувати для вирішення проблем, пов’язаних з обробкою графічної інформації[3, с.248].

Заходи безпеки даних, такі як шифрування даних і автентифікація користувачів, можуть бути застосовані для забезпечення безпеки даних, що передаються через мережу IoT.

Стандартизація форматів зображень і протоколів зв’язку може допомогти подолати проблеми сумісності

між різними пристроями IoT, які збирають і передають графічну інформацію.

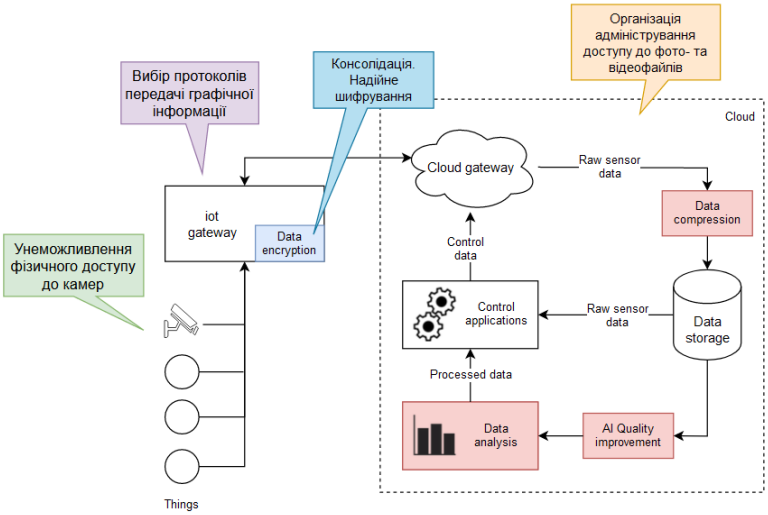

Рис.2. Модифікована система із врахуванням юридичних вимог.

Першим кроком захисту(з технічної точки зору) персональних даних є унеможливлення фізичного доступу на кінцевих вузлах до камер для збору особистої інформації.

Наступний крок – вибір протоколів для оптимізації передачі графічної інформації: прямим потоком від камер до IoT gateway і від нього по TCP до Cloud gateway. Також має бути використане надійне шифрування для того щоб неможливо було отримати інформацію до її потрапляння в Cloud.

Наступний крок - організація адміністрування - доступу до фото- та відеофайлів, що знаходяться в сховищі (як на особистому сервері так і в хмарному середовищі), тобто має бути чіткий контроль того хто і як отримує доступ до інформації.

В публікації було розглянуто технічні проблеми обробки графічної інформації, вплив на них правових вимог та запропоновано рекомендації по створенню мереж Інтернету Речей з урахуванням правових вимог підчас технічної реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 04.05.2023).
2. Любарска С.І., Курдеча В.В. Аналіз та порівняння методів обробки графічної інформації в мережі Інтернету речей. XVII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2023: Зб. матеріалів конф., К.: КПІ ім. Ігоря Сікорського. – 2023. – С.263.
3. L. Globa, V. Kurdecha, I. Ishchenko and A. Zakharchuk, "An approach to the Internet of Things system with nomadic units developing," 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, Ukraine, 2017, pp. 248-250, doi: 10.1109/CADSM.2017.7916127

МАРТИЩЕНКО Богдан

студент, КПІ ім. Ігоря Сікорського

ГОЛОВКО Ольга

к.ю.н., ст. дослідник,
ст. науковий співробітник лабораторії
теорії цифрової трансформації і права
наукового центру цифрової трансформації
і права ДНУ "ІІБП НАПрН" України,
ст. викладач кафедри інтелектуальної власності
та приватного права КПІ ім. Ігоря Сікорського

ЗАКОНОДАВСТВО УКРАЇНИ ПРО МЕДІА: ЄВРОІНТЕГРАЦІЙНИЙ АСПЕКТ

Актуальність. Медіа на сьогоднішній день відіграють досить важливу роль в житті суспільства. Вони не лише висвітлюють актуальні новини, відіграють розважальну роль але й фактично є показником розвитку держави, розвитку демократичного суспільства, одначасно висвітлюючи такий розвиток. З огляду на казане у дані роботі нами було здійснено дослідження поняття медіа, здійснено пошук джерела етимології поняття. Окрім того, основну увагу зосереджено на дослідження правового підгрунття діяльності медіа в Україні.

***Ключові слова*:** *ЗМІ, медіа, нормативно-правовий акт, законодавство України про медіа.*

Підвищена увага дослідників до проблем масових комунікацій і медіа, що активізувалися в останні роки, стала реакцією на бурхливий розвиток електронних соціальних мереж та комунікаційних інтернет-сервісів. Дослідницький інтерес проявився в різних галузях наукового знання і знайшов своє вираження як у різноманітних теоріях, що всебічно висвітлюють різні аспекти даної тематики, так і в ряді колізій концептуальної та методологічної неузгодженості. Не секрет, що інтерес до проблем комунікації завжди виявлявся з різних боків, з різних позицій та галузей науки. Цей всебічний інтерес став причиною розвитку цілого комплексу міждисциплінарних досліджень, таких як наприклад візуальні дослідження (visual studies), медіа дослідження (медіа-теорія, медіафілософія або media studies), цифрові дослідження (digital studies) тощо. Не виключенням є і правова наука. Оскільки на сьогоднішній день, ЗМІ являються фактично «четвертою» гілкою влади, а також зважаючи на важливість незалежного медіа, як ознаки демократичної країни, визначальним на наш погляд є вивчення питання законодавства України про медіа.

Для суворішої з наукової точки зору структури медіа, визначимо спочатку саме поняття «медіа», яке

багатьма вченими та фахівцями-практиками трактується і як «технічний засіб комунікації», і як «технологія або пристрій для зберігання, запису та відтворення інформації», і як «сукупність інформаційних засобів та прийомів», і як «ЗМІ», «масмедіа», «засіб масової комунікації». Це частково пояснюється тим, що дослідники наголошують на неможливості знайти точний еквівалент цього поняття.

Англійське "media" є скороченням від "media of communication(s)", що означає "засоби комунікації". Англійське «media» може бути скороченням від «media of mass communica-tion(s)», що означає, відповідно, «засоби масової комунікації».

Перейдемо до вивчення питання законодавства України про медіа. Слід зазначити, що основою законодавчого регулювання діяльності засобів масової інформації є Закон України «Про медіа». При цьому, слід зазначити, що даний нормативно-правовий акт є абсолютно новим для України, оскільки був прийнятий 13.12.2022 року. Слід зазначити, що даний нормативно-правовий акт став якісною доробкою українського законодавця, оскільки фактично став результатом удосконалення законодавства, шляхом заміни одним нормативно-правовим актом ряду уже неактуальних. Окрім того, необхідність прийняття цього нормативно-правового пов’язується із тим, що це було однією із

вимог для вступу України до Європейського союзу. Сама ж мета закону випливає по суті із преамбули, де відмічено, що цей Закон спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення [1].

Сам же закон визначає [2]:

- процедуру ліцензування та реєстрації суб’єктів у сфері медіа;
- процедуру реєстрації іноземних лінійних медіа;
- відповідальність суб’єктів у сфері медіа за порушення вимог законодавства;
- особливості правового регулювання в умовах дії збройної агресії;
- статус національного регулятора;
- впроваджує механізм співрегулювання і розробки разом з органом спільного регулювання актів.

Слід зазначити, що вказаний нормативно-правовий акт не є абсолютним регулятором правовідносин, що виникають в процесі діяльності засобів масової інформації. Так, відповідно до статті 3 Закону України «Про медіа» законодавство у сфері медіа складається з Конституції України, цього Закону, законів України "Про електронні комунікації", "Про забезпечення функціонування української мови як державної", "Про кінематографію", "Про рекламу", "Про суспільні медіа України", "Про інформацію", "Про систему іномовлення України", "Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста", інших законів України, що регулюють діяльність у сфері медіа, а також міжнародних договорів, що регулюють діяльність у сфері медіа, згода на обов’язковість яких надана Верховною Радою України.

Висновок. Виходячи із вищезазначеного слід зазначити, що на сьогоднішній день законодавство України про медіа отримало новий поштовх у розвитку. Безумовно, такий поштовх в першу чергу зумовлений необхідністю виконання вимог Європейського Союзу до України, зокрема для подолання надмірних приватних інтересів у медіапросторі України, впровадження в українському законодавстві положень Директиви Європейського парламенту і Ради 2010/13/ЄС, проте в

будь-якому випадку це розвиток та необхідні для держави зміни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про медіа. Закон України від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 01.05.2023).
2. Офіційний веб-сайт Національної ради України з питань телебачення і радіомовлення. Національна рада надає роз’яснення щодо впровадження Закону «Про медіа». URL: https://www.nrada.gov.ua/natsionalna-rada-nadaye-roz-yasnennya-shhodo-vprovadzhennya-zakonu-pro-media/

МИШАКОВА Альона

Львівський національний університет імені Івана Франка

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ РОСІЄЮ ДЛЯ ПОШИРЕННЯ ПРОПАГАНДИ В УКРАЇНІ

Рейтингова група NewsGuard у травні 2023 року заявила, що виявила 49 несправжніх новинних вебсайтів в усьому світі. Матеріали, націлені на залучення реклами, на них генеруються чат-ботами зі штучним інтелектом: ChatGPT, OpenAI Inc тощо.

Про штучний інтелект вперше почали говорити в 1950-х. З того часу ШІ, переживши кілька “зим”, продовжував лише нарощувати масштаби. Зараз це одна з галузей, що розвивається настрімкіше. Потенційні можливості застосування ШІ величезні, вже зараз останній може самостійно створити відео чи фото, виявити шахрайство, керувати автомобілем і навіть комунікувати зі своїм користувачем.

Наприкінці 2022 року світ сколихнув штучний інтелект ChatGPT, який може підтримувати діалог та створювати тексти на різні теми. Цей бот швидко обробляє масиви даних та імітує людську діяльність,

маючи в запасі величезну кількість інформації з Інтернету.

З початком роботи ChatGPT виявилось, що він також вміє генерувати дезінформацію та пропаганду, зокрема розповідає про панування неонацизму в Україні та волевиявлення народу Криму.

Журналісти The Washington Post вставили, що в набори даних, якими “годують” ШІ, входять російські пропагандистські ЗМІ, наприклад ресурс RT.

У 2023 році Україна піднялася на 79 сходинку в Індексі свободи ЗМІ. Торік країна займала 109 місце. Автори рейтингу вказують, що крім традиційних дезінформації та пропаганди, тепер і штучний інтелект масово “сіє хаос у медіасвіті”. Зокрема, спотворює реальність, створюючи фейковий контент.

Ще до нападу на Україну росія роками вела проти нас інформаційну війну, використовуючи дезінформацію, фейки та пропаганду. З розвитком штучного інтелекту росіяни взяли в роботу і його.

Так, на початку повномасштабного вторгнення українців атакували “діпфейками” - створеним штучним інтелектом синтезом зображень різних людей. Зокрема, росіяни поширили фейкову "заяву Володимира Зеленського", в якій він начебто закликав українців скласти зброю. На відео голова президента непропорційно велика, а голос набагато глибший за

справжній. Через низьку якість цього “діпфейку” він не спрацював.

Щоб дискредитувати українських політиків, було також створено фейкового міського голову Києва Віталія Кличка, який спілкуючись із мерами Берліна, Мадрида та Варшави нібито просив повернути з Німеччини в Україну чоловіків на війну.

Також у соціальних мережах поширювали відео із нібито українським політиком Юрієм Луценком після бою в Соледарі. У ролику обличчя військового помітно штучно збільшується та зменшується у розмірах.

Штучний інтелект також навчили “малювати” картинки за заданими текстами. Українські ЗМІ активно використовували цю можливість, наприклад, щоб показати “людський” образ міст чи результати апокаліпсису в рф. Втім, часто ці світлини маніпулювали людськими емоціями та завдавали шкоди. Так, штучний інтелект згенерував фото “хлопчика, який вижив під час ракетного удару в Дніпрі”. Ця світлина викривлює реальність та певним чином ідеалізує трагедію, бо дитина на ілюстрації не виглядає, як реальні діти, яких витягують з-під завалів.

Хто саме допоміг штучному інтелекту створити цей знімок, - невідомо. Але допис із цим фото стрімко поширився у Facebook з майже скрізь ідентичним підписом "Цей малюк вижив…”. Що ця ілюстрація

згенерована ШІ ніде не вказувалось, а сам метод поширення світлини соцмережами нагадував роботу російських ботоферм.

Помічено випадки, коли російські пропагандистські ЗМІ ставили позицію ШІ як експертну думку. Так РІА Новини взяли коментар у ChatGPT щодо ситуації з монахами УПЦ московського ппатріарахату в Києво-Печерській лаврі. А згідно з опитуванням виконаного InMind на замовлення міжнародної організації Internews, 12% українців з різних причин досі читають російські медіа.

Україна також активно використовує штучний інтелект на полі бою. Так, у травні 2023 року останній ідентифікував за допомогою фото особу російського військового, який пограбував квартиру в Ірпені. Серед іншого, ШІ встановив 70 учасників незаконного збройного формування “Самооборона Криму”. Штучний інтелект українські журналісти також використовують, щоб виявити російську пропаганду в медіа.

На перший погляд, потенційні небезпеки розвитку ШІ, а це збільшення генерації пропагандистського контенту та часу на фактчекінг, несуть Україні більше шкоди, ніж користі. Однак, більшість інформації в Україні про перебіг різних військових операцій є закритою. Тож можна

передбачити, що до закінчення війни і навіть якийсь час після перемоги суспільство не знатиме усіх деталей про методи та засоби, які використовували наші спецслужби, щоб подолати ворога.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Rise of the Newsbots: AI-Generated News Websites Proliferating Online [Електронний ресурс] – Режим доступу до ресурсу: https://www.newsguardtech.com/special-reports/newsbots-ai-generated-news-websites-proliferating/.
2. 2023 World Press Freedom Index – journalism threatened by fake content industry [Електронний ресурс] – Режим доступу до ресурсу: https://rsf.org/en/2023-world-press-freedom-index-journalism-threatened-fake-content-industry?data_type=general&year=2023
3. Пам'ятаєте, державні ЗМІ дуже любили розповідати про болгарів, «захоплених» Росією? Їх замінив ChatGPT [Електронний ресурс] – Режим доступу до ресурсу: https://meduza.io/feature/2023/04/13/pomnite-gosudarstvennye-smi-ochen-lyubili-rasskazyvat-o-bolgarah-voshischennyh-rossiey-ih-zamenil-chatgpt.
4. Inside the secret list of websites that make AI like ChatGPT sound smart [Електронний ресурс] – Режим доступу до ресурсу: https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/?fbclid=IwAR1qeP1lkzurJQXt13r075CS6Pi9tc6vvEBhCzNxHmfXAH4cYixzXpGBpRk

РОЗГОН Ольга

к. ю. н, доцент
НДІ правового забезпечення інноваційного розвитку
НАПрН України, Харків
ORCID 0000-0001-6739-3927

АНАЛІЗ ПРАВОВОГО РЕГУЛЮВАННЯ ФОТОГРАФІЧНИХ ТВОРІВ НА МАТЕРІАЛЬНОМУ НОСІЇ ТА ФОТОГРАФІЧНИХ ТВОРІВ У ЕЛЕКТРОННІЙ (ЦИФРОВІЙ) ФОРМІ

Наразі актуальним є оцифрування об’єктів матеріальної та нематеріальної культурної спадщини, якими можуть бути твори мистецтва, і створення платформ для їхньої популяризації в Україні та за кордоном. У результаті впровадження технології оцифрування творів мистецтва у процес розвитку роботи музеїв виникають *цифрові фотографії*.

Твір вважається створеним із моменту первинного надання йому будь-якої об’єктивної форми (письмової, речової, *електронної* (цифрової) тощо) (ст. 9 Закону України «Про авторське право та суміжні права»).

Отже, допускається можливість створення твору в цифровій формі.

Цифрова фотографія дуже легко поширюється. При цьому всі «копії твору» не втрачають своєї якості в порівнянні з першою версією цифрової фотографії.

Так, у ст. 24 Закону України «Про авторське право та суміжні права» встановлене без дозволу суб'єкта авторського права та безоплатно інтерактивне надання доступу до *твору в електронній (цифровій) формі* за допомогою терміналів у приміщенні бібліотек, музеїв із відкритим доступом для відвідувачів, архівами або організаціями зі збереження фондів аудіо-, відеозаписів, за запитом фізичної особи з метою навчання, наукового або приватного дослідження за таких умов: 1) виключення можливості створення копій цього твору для використання поза приміщенням закладів; 2) надання одночасно доступу лише до *однієї копії цього твору*. Таким чином, цією статтею підтверджується, що у *твору в цифровій формі є копії об'єкта авторського права та/або суміжних прав* і є можливість для музеїв вільно використовувати такий твір із відкритим доступом.

Копія — відтворений у будь-якій об'єктивній формі об'єкт авторського права та/або суміжних прав. Копія твору, виконана у будь-якій матеріальній формі, є примірником твору (п. 27 ст. 1 Закону України «Про

авторське право та суміжні права»). Як бачимо у ст. 1 цього закону *копія* використовується у розумінні об'єктивної форми (матеріальної або електронної (цифрової), а примірник твору — це стосовно матеріальної форми твору.

Авторське право на твір є чинним із моменту *створення твору*. Український законодавець установив, що *авторське право* на твір і право власності на *електронний (цифровий) об'єкт*, в якому втілено (зафіксовано) такий твір, не залежать одне від одного (ч. 1 ст. 10 Закону України «Про авторське право та суміжні права»).

Цифровий об'єкт — це об'єкт, що складається з набору бітових послідовностей. Інформація про вміст — це та інформація, яка є первинною метою збереження. Вона складається з об'єкта даних вмісту (фізичного або *цифрового об'єкта*, тобто бітів) і пов'язаної з ним інформації про представлення, необхідної для того, щоб зробити об'єкт даних вмісту зрозумілим для визначеної спільноти. Наприклад, *об'єкт даних вмісту* може бути *зображенням*, яке надається як бітовий вміст одного файлу CD-ROM разом з іншими файлами на тому ж CD-ROM, які містять представницьку інформацію [2].

Оригінальність є основною вимогою законодавства про *авторське право*: лише ті твори, які

демонструють певний мінімальний рівень цієї ознаки, користуються захистом. Але жоден з основних міжнародних договорів про авторське право прямо не визначає, що це таке та якого рівня твір повинен досягти, щоб виникло авторське право.

У п. 35 ст. 1 Закону України «Про авторське право та суміжні права» від 01.12.2022 р. № 2811-IX встановлено, що *оригінальність твору* — ознака (критерій), що характеризує твір як результат *власної інтелектуальної творчої діяльності* автора та відображає творчі рішення, прийняті автором під час створення твору.

Фотографії, які не мають ознак оригінальності (не є фотографічними творами). Охорона об’єктів авторського права поширюється лише на форму вираження об’єктів авторського права. Охороні підлягають усі *оригінальні твори* — оприлюднені та неоприлюднені, завершені та незавершені, незалежно від їх призначення, жанру, обсягу, а також *способу вираження* (ст. 7 Закону України «Про авторське право та суміжні права»).

Згідно з п. 56 ст. 1 Закону України «Про авторське право та суміжні права» *твір — оригінальне інтелектуальне творіння* автора (співавторів) у сфері науки, літератури, мистецтва тощо, виражене в об’єктивній формі. А в п. 35 ст. 1 зазначена *вимога*

щодо особистої (власної) інтелектуальної творчої діяльності застосовується при визначенні оригінальності твору.

Хоча європейські Директиви з авторського права не містять чіткого визначення терміну «твір», Суд Європейського Союзу (Court of Justice of the European Union — (CJEU)) розробив дві умови, які повинні бути виконані одночасно для отримання авторського права: по-перше, повинен бути *оригінальний* об'єкт, тобто *власне інтелектуальне творіння автора*; по-друге, тільки вираження цього творіння може охоронятися авторським правом як твір.

Важливий аспект у захисті фотографій за законодавством ЄС можна знайти в Директиві 2006/116/ЄС (Copyright Term Directive) [1], яка визнає охороноздатними об'єктами *не тільки фотографії*. Як бачимо, остання частина ст. 6 Директиви дозволяє державам-членам надавати охорону «іншим фотографіям». У загальних рисах охорона, яку деякі держави-члени визнають за «іншими фотографіями», визначається негативно, тобто пропонуючи охорону фотографіям, які не кваліфікуються як фотографічні твори європейські країни, які визнають цю форму (7 EU members plus 2 EEA members), зазвичай надають права, подібні до звичайного авторського права (проте існують значні винятки). При цьому Directive 2006/116/EC не

містить вказівки, що «*інші фотографії*» або «*неоригінальні фотографії*» повинні бути захищені авторським правом. Цей критерій є спрощеним критерієм оригінальності.

У світлі вищевикладеного видається, що *акти оцифрування текстів і зображень*, безумовно, виходять за межі фотографічних творів, оскільки «тільки мистецтво автора оригіналу, а не фотографа» повинно бути видимим. Той же висновок, здається, справедливий і для оцифрування об'єктів, у всіх тих випадках, коли оцифрування є *простим цифровим відтворенням об'єкта*. Тим не менш, слід мати на увазі, що рівень оригінальності не повинен помилково встановлюватися на занадто високому рівні: вільний і творчий вибір творчого фотографа, який необхідно оцінювати в кожному конкретному випадку, може, особливо у випадках «художнього» фотографування творів мистецтва, вважатися авторським [3].

Отже, твори *мистецтва як* музейні культурні цінності існують у матеріальній формі, а також можуть бути відтворені у цифровій формі як *цифрові фотографії*. Цифрова фотографія творів у контексті цифрової форми подання є результатом оцифрування музейних культурних цінностей. Фотографічний твір у цифровій формі — це твір у електронній (цифровій) формі з можливістю робити копії цього твору,

інформація про який закодована у цифровому об’єкті, що складається з набору бітових послідовностей.

Авторське право на твір є чинним із моменту *створення твору*, навіть якщо він у такій об’єктивній *електронній* (цифровій) формі.

Залишається дискусійним питання, наскільки твір у цифровій формі можна визнати за українським законодавством оригінальним. Відомо принаймні два підходи до визначення *оригінальності фотографічного твору*, а саме об’єктивний і суб’єктивний. Перший передбачає, що стороння особа (експерт-мистецтвознавець чи суддя) здатна сама визначити *творчий характер твору*, а другий — лише автор може пояснити, як він задумав і створив твір. Суд повинен кваліфікувати це з урахуванням усіх обставин справи (наприклад, чи були відомі автору більш ранні схожі твори) [4]. Така ознака (критерій), як *оригінальність твору,* має охарактеризувати твір як результат *власної інтелектуальної творчої діяльності* автора та відображає творчі рішення, прийняті автором під час створення твору. Цифрова фотографія матиме ознаки оригінальності, якщо цей твір у цифровому форматі створений завдяки творчому внеску автора твору в цифровому форматі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights.
2. Digital Object: An object composed of a set of bit sequences. (CCSDS 650.0-M-2 – Reference Model for an Open Archival Information System (OAIS), p.1-11, Section 1.7.2).
3. Margoni T. (2014). The Digitisation of Cultural Heritage: Originality, Derivative Works and (Non) Original Photographs. *SSRN Electronic Journal*. URL: https://doi.org/10.2139/ssrn.2573104.
4. Томаров І. (2016). Оригінальність фотографії у судовій практиці. *Legal Shift*, URL: http://www.legalshift.com.ua/?p=948.

ПЕЧЕРОВА Ніна

кандидат юридичних наук, доцент кафедри адміністративного права, права інтелектуальної власності та цивільно-правових дисциплін Київського університету інтелектуальної власності та права Національного університету «Одеська юридична академія»

ПОНЯТТЯ ВІРТУАЛЬНОГО АКТИВУ, ПРАВОМОЧНОСТІ ЩОДО РЕАЛІЗАЦІЇ ПРАВА ВЛАСНОСТІ НА ВІРТУАЛЬНІ АКТИВИ, ПРАВОЧИНИ З ВІРТУАЛЬНИМИ АКТИВАМИ

Ринок віртуальних активів є прикладом ринку, що динамічно розвивається. Разом з розвитком відповідного ринку має розроблятися і його правове регулювання. Підґрунтям для правового регулювання даного ринку і розуміння правовідносин, що у ньому складаються мають скласти норми таких галузей права як цивільне, інформаційне, податкове, а також інших галузей права. Важливу допомогу у розробленні такого регулювання може надати і вивчення досвіду європейських країн. На сьогодні, в нашій державі був розроблений Закон України «Про віртуальні активи» від

17.02.2022 року (далі – Закон) [1]. І хоча даний Закон не набрав чинності, він відіграє безумовно важливу роль у спробах нашої держави покласти початок регулюванню даної сфери суспільних відносин.

Перш ніж переходити до розгляду безпосередньо правомочностей щодо реалізації права власності на віртуальні активи, а також правочинів із віртуальними активами розглянемо, що собою власне представляють віртуальні активи. Зауважимо, що ключову допомогу при розгляді та опрацюванні даних питань надає Закон України «Про віртуальні активи» про який було зазначено вище [1].

Відповідно до ч. 1 ст. 1 згадуваного Закону під віртуальним активом розуміється нематеріальне благо, що є об’єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів. Віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об’єкти цивільних прав [1]. В той же час не можна не звернути увагу на п. 3, 6, 7, 10, 11, 12 ч. 1 ст. 1 Закону, де надається визначення забезпеченому віртуальному активу, ринку віртуальних активів, системі забезпечення обороту віртуальних активів, учасникам ринку віртуальних активів. Так, під забезпеченим віртуальним активом відповідно до п. 3 ч.

1 ст. 1 Закону розуміється віртуальний актив, що посвідчує майнові права, зокрема права вимоги на інші об’єкти цивільних прав. Під незабезпеченим віртуальним активом розуміється актив, що не посвідчує жодних майнових або немайнових прав згідно із п. 6 ч. 1 Закону. Під оборотом віртуальних активів розуміються усі правовідносини, які стосуються віртуальних активів, які виникають між учасниками ринку віртуальних активів, а також між ними та державою згідно із п. 7 ч. 1. Під ринком віртуальних активів розуміється сукупність учасників ринку віртуальних активів та правовідносин між ними щодо обороту віртуальних активів згідно із п. 10 ч. 1 ст. 1 Закону. Щодо системи забезпечення обороту віртуальних активів, то, виходячи із положень п.11 ч.1 ст. 1 Закону розуміється програмний або програмно-апаратний комплекс обміну електронними даними, який забезпечує ідентифікацію та оборотоздатність віртуальних активів. Щодо учасників ринку віртуальних активів згідно із п. 12 ч. 1 ст. 1 Закону розуміється постачальники послуг, пов’язаних з оборотом віртуальних активів, а також будь-які особи, які здійснюють операції з віртуальним активами у своїх інтересах [1].

Предметом окремого аналізу, зокрема, серед вище викладеного потребує п. 7 ч. 1 ст. 1 Закону, згідно якого,

як вже було зазначено вище «під оборотом віртуальних активів розуміються усі правовідносини, які стосуються віртуальних активів, які виникають між учасниками ринку віртуальних активів, а також між ними та державою» в контексті відносин між «учасниками ринку віртуальних активів та державою».

Уваги в контексті розгляду, що собою представляє віртуальний актив представляє положення ч.3 ст. 2 Закону, а саме, що дія Закону не застосовується до правовідносин, пов’язаних із випуском, обігом, зберіганням і погашенням електронних грошей, а також до правовідносин, що виникають під час емісії, обігу, викупу цінних паперів та виконання зобов’язань за ними, укладання і виконання деривативних контрактів, заміни сторони деривативних контрактів та вчинення правочинів щодо фінансових інструментів на ринках капіталу, експлуатації програмних або програмно-апаратних комплексів обміну електронними даними, в яких забезпечується здійснення зазначених правовідносин щодо фінансових інструментів, а також відносини, що виникають під час провадження професійної діяльності на ринках капіталу та організованих товарних ринках [1].

При цьому, виходячи із вище викладеного та повертаючись до наданого визначення віртуального активу, а саме, що під віртуальним активом розуміється

нематеріальне благо, що є об’єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі, існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів, віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об’єкти цивільних прав [1] можна прийти до висновку, що під віртуальним активом слід розуміти фактично сукупність даних в електронній формі. Дані ж дані в електронній формі є відображенням об’єкту цивільних прав, що має вартість. Самі ж ці дані розуміються як нематеріальне благо.

В контексті розпоряджання віртуальними активами важливим є розгляд положень, що представляє собою гаманець віртуального активу, а також ключ віртуального активу.

Так, згідно із п. 2, 5 ч. 1 ст.1 Закону під гаманцем віртуального активу розуміється програмне забезпечення або програмно-апаратний комплекс, що надає його користувачу інформацію про належні йому віртуальні активи та можливість розпоряджатися ними в системі забезпечення обороту віртуальних активів за допомогою ключа віртуального активу [1], тобто ключовим є те, що програмне забезпечення або програмно-апаратний комплекс формує гаманець віртуального активу, а також надає користувачеві

інформацію про належні йому віртуальні активи і можливість розпоряджатися ними в системі забезпечення обороту віртуальних активів.

Таким чином, саме програмне забезпечення або програмно-апаратний комплекс безпосередньо пов’язаний із розпорядженням віртуальними активами.

Важливим є і положення про ключ віртуального активу. Так, під ключем віртуального активу розуміється набір технічних засобів, реалізованих у системі забезпечення обороту віртуальних активів, що надають змогу контролювати віртуальний актив [1]. Дане положення також є вкрай важливим в контексті сек’юритизації віртуального активу, а саме унеможливлення доступу до розпоряджання таким активом особи, яка на це не має права.

Важливими питаннями в контексті поставленої теми є наступні положення вже згадуваного Закону, а саме щодо фінансових віртуальних активів. Так, відповідно до ч. 6 ст. 4 Закону фінансовими віртуальними активами є емітований резидентом України забезпечений віртуальний актив, що забезпечений валютними цінностями (далі – ЗВА(ВЦ), емітований резидентом України забезпечений віртуальний актив, що забезпечений цінним папером або деривативним фінансовим інструментом (далі – ЗВА (ФІ). При цьому важливо зауважити, що згідно із ч.

7 ст. 4 віртуальні активи не є засобом платежу на території України та не можуть бути предметом обміну на майно (товари), роботи (послуги)[1].

Особливу актуальність в контексті реалізації правомочностей щодо реалізації права власності на віртуальні активи має стаття 5 Закону, яка визначає створення віртуальних активів, введення віртуальних активів у цивільний оборот та виведення віртуальних активів із цивільного обороту. Так, відповідно до ч.1 даної статті моментом створення віртуального активу є момент, з якого перший власник отримує можливість володіти, користуватися та розпоряджатися віртуальним активом у системі забезпечення обороту відповідного віртуального активу, якщо немає можливості достовірно встановити інший момент створення віртуального активу, виходячи з технічних можливостей[1]. Тобто, момент створення віртуального активу збігається в часі з моментом отримання першим власником можливостей щодо володіння, користування та розпоряджання у системі забезпечення обороту відповідного віртуального активу, але при цьому якщо немає можливостей встановити інший момент створення віртуального активу, виходячи з технічних особливостей.

При цьому, під системою забезпечення обороту відповідного віртуального активу розуміється згідно п.

11 ч. 1 ст. 1 Закону програмний або програмно-апаратний комплекс обміну електронними даними, який забезпечує ідентифікацію та оборотоздатність віртуальних активів [1]. Таким, чином моментом створення віртуального активу є момент, з якого перший власник отримує можливість володіти, користуватися та розпоряджатися віртуальним активом у програмному або програмно-апаратному комплексу обміну електронними даними, який забезпечує ідентифікацію та оборотоздатність таких віртуальних активів (система забезпечення обороту віртуальних активів) при цьому, якщо немає можливості достовірно встановити інший момент створення віртуального активу, виходячи з технічних особливостей знову ж таки програмного або програмно-апаратного комплексу обміну електронними даними, який забезпечує ідентифікацію та оборотоздатність віртуальних активів (система забезпечення обороту віртуальних активів).

Згідно із ч. 2 ст. 5 Закону оборот віртуального активу починається з моменту його створення та здійснюється до моменту припинення обороту віртуального активу. Оборот на території України ЗВА (ВЦ) здійснюється в порядку, встановленому Національним банком України. Оборот на території України віртуальних активів крім ЗВА (ВЦ), здійснюється в порядку, встановленому Національною

комісією з цінних паперів та фондового ринку згідно з ч. 3, 4 ст. 5 Закону [1].

Згідно ч. 5 ст. 5 Закону особа, яка несе зобов'язання за забезпеченим віртуальним активом, має забезпечити припинення обороту віртуального активу, якщо об'єкти цивільних прав, якими його було забезпечено, ним втрачені або вибули з цивільного обороту з тих чи інших підстав, а можливість заміни забезпечення такого віртуального активу не передбачена правочином про створення відповідного забезпеченого віртуального активу або правочином про відчуження такого віртуального активу [1]. Таким чином, ч. 5 ст. 5 визначено випадки за яких особа, що несе зобов'язання за забезпеченим віртуальним активом має припинити оборот віртуального активу по-перше, якщо об'єкти цивільних прав, якими його було забезпечено, ним втрачені або вибули з цивільного обороту з тих чи інших підставах; по-друге можливість заміни забезпечення такого віртуального активу не передбачена правочином про створення відповідного забезпеченого віртуального активу або правочином про відчуження такого віртуального активу. Таким чином, віртуальний актив є «певним чином» в той же час «відокремленим» від об'єкту цивільних прав, яким такий актив забезпечено.

Важливим в контексті розгляду питання правомочностей щодо реалізації права власності на віртуальні активи є положення ч. 5 ст. 5 Закону, а саме об’єктом забезпечення віртуального активу є інший об’єкт цивільних прав, права вимоги на який посвідчує такий віртуальний актив. Об’єкт забезпеченя віртуального активу визначається правочином, згідно з яким такий віртуальний актив створено. Майнові права, зокрема права вимоги, на об’єкт забезпечення віртуального активу передаються набувачу такого віртуального активу [1]. Щодо питання правочину згідно якого такий віртуальний актив створено, то дане питання може бути предметом окремого розгляду.

Відповідно до ч. 1 ст. 6 Закону право власності на віртуальний актив набувається за фактом створення віртуального активу, вчинення та виконання правочину щодо віртуального активу, на підставі норм закону або рішення суду і засвідчується володінням ключа такого віртуального активу, крім випадків, передбачених частиною третьою цієї статті [1]. Тобто підґрунтям для набуття права власності на віртуальний актив є факт створення віртуального активу, вчинення правочину щодо віртуального активу, виконання правочину щодо віртуального активу, відповідно до норм закону, за рішенням суду. Ключ віртуального активу є засвідченням володіння віртуальним активом.

Важливо відзначити, що згідно ч. 2 ст. 6 Закону умовами набуття, умовами переходу та обсягу прав на віртуальні активи можуть виражатися у формі алгоритмів та функцій системи забезпечення обороту віртуальних активів, у межах якої здійснюється оборот віртуальних активів [1].

Зміст права власності на віртуальний актив включає право володіти віртуальним активом, право користуватися віртуальним активом та право розпоряджатися віртуальним активом на свій розсуд, якщо це не суперечить закону, зокрема шляхом передачі права власності на віртуальний актив згідно ч. 5 ст. 6 Закону. Володіння, користування та розпоряджання віртуальним активом фіксується у системі забезпечення обороту віртуальних активів відповідно до ч.6 ст. 5. Важливим положенням є ч. 7 ст. 5 Закону, якою встановлюється, що якщо законом встановлено вимоги щодо форми або істотних умов правочину про розпоряджання об’єктом забезпечення віртуального активу, такі вимоги підлягають виконанню також під час вчинення правочину щодо розпоряджання таким віртуальним активом [1].

Відповідно до ч. 1 ст. 7 Закону під розпоряджанням забезпеченим віртуальним активом розуміється розпоряджання майновим правом на об’єкт забезпечення цього віртуального активу [1].

Виходячи із вище викладеного у даній роботі подальший науковий інтерес представляють питання із узгодження у майбутньому положень чинного цивільного законодавства (зокрема, договірних положень) в контексті того, що як було вже зазначено «під розпоряджанням забезпеченим віртуальним активом розуміється розпоряджання майновим правом на об’єкт забезпечення цього віртуального активу» із розвитком законодавства у сфері регулювання віртуальних активів, адже як відомо відповідно до ч. 1 ст. Цивільного кодексу України цивільним законодавством регулюються особисті немайнові та майнові відносини (цивільні відносини), засновані на юридичній рівності, вільному волевиявленні, майновій самостійності їх учасників [2].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Закон України «Про віртуальні активи» від 17.02.2022 року URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text

2.Цивільний кодекс України від 16.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

САВЧЕНКО Віктор

к.ю.н, доцент,
науковий співробітник Оксфордського університету;
доцент кафедри цивільно-правових дисциплін
Харківського національного університету імені В.Н. Каразіна

«СУРОГАТНА ВОЛЯ» ШТУЧНОГО ІНТЕЛЕКТУ: ФІЛОСОФСЬКО-ПРАВОВИЙ АНАЛІЗ

В умовах цифрового розвитку суспільства, використання штучного інтелекту (далі – ШІ) стає все більш активним. Технології штучного інтелекту стають все більш розвинутими та доступними для професійного та приватного використання. Якщо раніше, використання ШІ було актуальним для великих корпорацій, урядів та дослідницьких установ, то сьогодні будь-яка людина застосовує цю технологію у повсякденному житті: додатки в мобільному телефоні, електронна комерція, наукова діяльність, ігри, творчість тощо.

Поширення та зростання можливостей ШІ вимагає розуміння його природи та наявності у нього специфічної волі.

ШІ сьогодні не є суб’єктом прав, та використовується лише як інструмент для реалізації волі користувача. Проте ШІ самостійно здійснює обробку зображень, прийняття рішень, розпізнавання та обробку мови (Link та ін., 2018). ШІ це здатність машини працювати інтелектуально, точно зчитуючи вхідні дані та застосовуючи ці знання для досягнення визначених цілей і діяльності за допомогою гнучкого дизайну (Trifonov та ін., 2018). Фактично, ШІ здійснює самостійну інтелектуальну діяльність на підставі закладених в нього алгоритмів. ШІ був розроблений як сурогатний аналог людської інтелектуальної діяльності, а значить, він виконує дії, які для людини визначаються правами на свободу літературної, художньої, наукової і технічної творчості (Цивільний кодекс України, 2023, ст.270).

Реалізація цих прав людиною є способом виразу свободи волі. Е. Фром пропонує розглядати свободу волі в декількох розуміннях: 1) природна (ненормативна) - можливість приймати рішення на основі власної волі; 2) позитивна (нормативно) - прийняття рішень відповідно до власної волі і на основі нормативних приписів; 3) дійсна (реальна, фактична) - гарантована ймовірність приймати рішення відповідно до власної волі і на основі нормативних приписів (Fromm, 1994). На основі цього можна говорити про

правове розуміння свободи волі як можливості прийняття рішень, яка нормативно гарантована і обмежена. Внутрішня свобода волі корелюється з недоторканністю права на свободу мислення та не підлягає обмеженням, проте зовнішній прояв свободи волі через волевиявлення обмежується правовими приписами. Імперативні норми майже не залишають місця для свободи волі, а диспозитивні, характерні для приватного права, створюють механізми для правомірного волевиявлення.

Фактично, свобода волі, це можливість приймати рішення та реалізовувати їх, відповідно до визначених правил. Виходячи з цього слід провести аналогію з діями ШІ.

Обробивши інформацію, ШІ інтелект приймає відповідне рішення. Наприклад, проаналізувавши фотографію, ШІ робить висновок про недостатність рівню її експозиції та приймає рішення про підвищення яскравості. Процес обрахунку даних можна порівняти з внутрішньою волею людини, коли вона аналізує інформацію та приймає рішення. Процес покращення зображення ШІ, можна порівняти з зовнішньою формою свободи волі людини, волевиявленням.

Проте ШІ приймає рішення відповідно до закладених в нього алгоритмів, через що можна припустити відсутність у нього власної волі. В той же

час, людина також приймає рішення під впливом зовнішніх факторів, наявної інформації та знань, власного досвіду тощо. Тобто людина керується власними алгоритмами, які можуть набувати форму рефлексів, інстинктів тощо. З позиції детермінізму, свобода волі ґрунтується на причинному зв’язку явищ. Теологічний детермінізм прив’язують з конструкцією «якщо Бог передбачив, що я буду діяти певним чином, то я повинен діяти так», але допускає не вирішене питання щодо того, чи обов’язково Бог знає наперед, що я буду діяти певним чином (Lucas, 1970). Біологічний детермінізм представляє твердження, що теперішній стан людських суспільств є специфічним результатом біологічних сил і біологічної «природи» людського виду, а усі детерміністські теорії описують певну модель суспільства, яка відповідає соціально-економічним упередженням (Dialogue. The critique: Sociobiology: Another biological determinism, 1976). В біологічному детермінізмі свобода волі пов’язана з генами, через що ми приймаємо рішення не самостійно, адже нас обмежують закладені в нас гени.

Таким чином можна порівняти детерміністське розуміння свободи волі з алгоритмічною волею ШІ. Застосування детерміністичних теорій для правового розуміння свободи волі призведе до юридичного колапсу, адже будь-які вчинки людини можна буде

пояснити зовнішнім впливом. Проте слід визнати той факт, що людина приймає рішення на підставі закладених в неї умов: біологічних, суспільних, культурних, власного досвіду та знань тощо. Це дає підставу припустити, що сьогоденний стан волі ШІ дуже близький до етапу детерміністського розуміння свободи волі людини.

Зовнішній прояв свободи волі людини відбувається за певними правилами, які визначені нормами моралі та права. Так само і волевиявлення ШІ обумовлюється закладеними в нього алгоритмами.

ШІ це сурогатне відображення людського інтелекту, зі схожими властивостями до аналізу, самовдосконалення та прийняття рішень. Так само як природа, еволюція або Бог заклали в людину можливість до інтелектуальної діяльності, так і розробник закладає сурогатну версію цього у ШІ. Людський інтелект призвів до розвитку свободи волі, а тому можна припустити, що і ШІ згодом отримає більш вдосконалену «сурогатну волю». Ми вважаємо, що аналіз «сурогатної волі» ШІ потребує окремого детального дослідження, з акцентом на порівняльний метод, з метою проведення аналогій між волею людини та ШІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Link, J., Waedt, K., Zid, I., & Lou, X. (2018). Current challenges of the joint consideration of functional safety & cyber security, their interoperability and impact on organisations: How to manage RAMS+ S (reliability availability maintainability safety+ security). In *12th International Conference on Reliability, maintainability, and Safety (ICRMS)* (p. 185–191).

2. Trifonov, R., Nakov, O., & Mladenov, V. (2018). Artificial intelligence in cyber threats intelligence. In *International conference on Intelligent and innovative computing applications (ICONIC)* (2018).

3. Цивільний кодекс України, Кодекс України № 435-IV (2023) (Україна). https://zakon.rada.gov.ua/laws/show/435-15#Text

4. Fromm, E. (1994). *Escape from Freedom*. Holt McDougal.

5. Lucas, J. R. (1970). Theological determinism: Omniscience and foreknowledge. In *The freedom of the will* (p. 71–77). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198243434.003.0014

6. Dialogue. The critique: Sociobiology: Another biological determinism. (1976). *BioScience*, *26*(3), 182–186. https://doi.org/10.2307/1297246

ФЕДОРЕНКО Світлана

Курсант 2-го курсу, Навчально-наукового інституту права та фахівців для підготовки до підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ

ЮНІНА Марина

доцент, доцент кафедри Цивільного права та процесу, Дніпропетровського державного університету внутрішніх справ

НОВІТНІ АСПЕКТИ РЕЄСТРАЦІЇ ШЛЮБУ ЧЕРЕЗ ЄДИНИЙ ДЕРЖАВНИЙ ПОРТАЛ «ДІЯ»

Насамперед потрібно зауважити на тому, що розвиток сучасного суспільства відбувається у швидко змінному світі, який постійно змінюється під дією процесів діджиталізації. Даний процес стає магістральним напрямком трансформації усіх сфер нашого життя і поступово змінює принципи та механізми їх функціонування, розвитку. Зокрема, в Україні все більш поширюється інтерес до діджиталізації, що у перекладі з англійської мови означає «оцифровування» або «приведення в цифрову

інформацію» [1, с. 330], що спонукає на пошук нових теоретико-методичних підходів щодо забезпечення ефективного управління, в умовах діджиталізації, під якою прийнято розуміти трансформацію, проникнення цифрових технологій в повсякденне життя громадян нашої країни, що певним чином його полегшує.

Зазначимо, що ще у 2020 році Україна стала першої державою в світі, яка створила та надала для використання Єдиний державний портал, що має назву «Дія». Даний портал є досить зручним у користуванні та дозволяє громадянам нашої держави швидко оформити, чи зберігати в електронному вигляді необхідні документи, зокрема: паспорт, ідентифікаційний код, довідку про місце реєстрації тощо. Також відповідний портал надає можливість: оформити довідку про несудимість; допомогу при народженні дитини чи щомісячне відшкодування вартості послуг із догляду за дитиною до трьох років; подати позов до суду; зареєструвати автомобіль або отримати послугу, пов’язані із документами водія; оформити низку ліцензій, дозволів чи отримати витяги з реєстрів тощо [2].

Крім цього, платформа-портал «Дія» розміщена в захищеному дата-центрі та відповідає світовим стандартам захист від кіберзагроз. Тобто усі дані про користувачів зберігаються у зашифрованому вигляді,

що само по собі унеможливлює їх перехоплення або викрадення.

Необхідним є зазначити, що у зв’язку із повномасштабною війною в нашій країні на законодавчому рівня були закріплені доволі суттєві зміни, які самі по собі спрощують укладення шлюбу в умовах воєнного стану. Взагалі шлюб являє собою сімейний союз жінки та чоловіка, зареєстрований в органі державної реєстрації актів цивільного стану (частина 1 статті 21 Сімейного кодексу України) [3]. Наразі зареєструвати шлюб стало можливим саме через портал «Дія», так як в умовах війни не завжди можливим є прийти до органу державної установи для подачі заяви та проведення офіційної реєстрації шлюбу.

Звернемо увагу на те, що виходячи із нововведень, можливим стало подати заяву про державну реєстрацію шлюбу саме на порталі «Дія», при чому також можна одразу обрати місце, час, формат та зал, де пройде сама церемонія.

Даний процес реєстрації займає мінімум особистого часу, а скористатися такою послугою можуть громадяни України, старші 18 років та які мають е-підпис. Правильна послідовність здійснення всіх дій, полягає у наступному: 1) авторизуватися на порталі «Дія» та перейти у розділ «Сім’я»; 2) обрати послугу «Заява про шлюб»; 3) заповнити заяву та

обрати час і місце реєстрації; 4) сплатити адміністративний збір (становить від 0,85 гривень до 1649,85 гривень, у залежності від обраних послуг та дня реєстрації шлюбу); 5) підписати заяву електронним підписом; 6) потрібно, щоб ваш партнер авторизувався у своєму кабінеті на порталі, перейшов на заяву за посиланням з пошти та підписав її електронним підписом [4, с. 1]. Після здійснення всіх вищевикладених дій, обраний орган державної реєстрації актів надішле результат розгляду заяви та деталі церемонії на електронну адресу, а в подальшому необхідним є тільки в конкретний час та дату прибути до ДРАЦС.

Отже, можна зробити висновок, що ще у 2020 році Україна стала першою державою в світі, яка створила та надала для використання Єдиний державний портал, що має назву «Дія». У свою чергу, в умовах сучасності наша країна зробила все можливе задля того, щоб забезпечити сприятливі умови для осіб, які мають бажання зареєструвати шлюб. Так, відтепер зареєструвати шлюб стало можливим саме через портал «Дія», так як в умовах війни не завжди можливим є прийти до органу державної установи для подачі заяви та проведення офіційної реєстрації шлюбу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Філиппова С.В., Свінарьова Г.Б. Діджиталізація як середовище та фактор змін системи управління підприємством. Вісник Хмельницького національного університету, 2020. С. 330-335.

2. Мінцифри запустило портал державних послуг «Дія»: Урядовий портал. Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/news/mincifri-zapustilo-portal-derzhavnihposlug-diya (дата звернення 15.04.2023)

3. Сімейний кодекс України від 10.01.2002 року №2947-III. URL: https://zakon.rada.gov.ua/laws/show/2947-14#Text (дата звернення 15.04.2023)

4. Барсукова О. На порталі «Дія» тепер можна подати заяву про шлюб, 2023. URL: https://life.pravda.com.ua/society/2023/02/27/253085/ (дата звернення 15.04.2023)

ЧЕСНИЦЬКИЙ Данило

студент, КПІ ім. Ігоря Сікорського

ГОЛОВКО Ольга

к.ю.н., ст. дослідник,
ст. науковий співробітник лабораторії
теорії цифрової трансформації і права
наукового центру цифрової трансформації
і права ДНУ “ІІБП НАПрН” України,
ст. викладач кафедри інтелектуальної власності
та приватного права КПІ ім. Ігоря Сікорського

ОХОРОНА ПРАВА НА TRADE DRESS В УКРАЇНІ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

Одним із питань, що виникають у світовій практиці у зв'язку з регулюванням прав на дизайн, є питання порядку охорони дизайну та його елементів. Перелік об'єктів, якими може бути дизайн, у світі, в т.ч. в Україні, в основному однаковий. Так, дизайн може бути засобом індивідуалізації (позиційний товарний знак у вигляді червоної підошви туфель Christian Louboutin), об'єктом патентного права (промисловий зразок сумки Hermes), об'єктом авторського права.

Захист дизайну як кожного з наведених об'єктів права інтелектуальної власності має певні недоліки, жоден з них не можна назвати бездоганним для охорони дизайну.

Trade dress визначається як комерційний вигляд товару в цілому (зовнішній вигляд та відчуття), який ідентифікує або вказує на джерело походження товару та виділяє його для споживачів. З судової практики випливає, що trade dress можуть бути визнані: форма, колір, розташування матеріалів на лінії дитячого одягу, дизайн обкладинки журналу, порядок виставлення вина в магазині [4].

Якщо ж говорити про trade dress в Україні, слід зазначити, що це питання не є цілком пропрацьованим у національному законодавстві. Так, національне законодавство не виділяє такого поняття, як фірмовий стиль суб’єкта господарювання, а тому українським суб’єктам господарювання доводиться охороняти trade dress чи не всіма можливими способами відразу. Так, розглядаючи судову практику відносно теми, слід зазначити справу за позовом ТзОВ «Стародавній Херсонес», до ТзОВ «Барбарис 2012», ТзОВ «Токіо сіті», ТзОВ «Кепі Енд» про припинення незаконного використання знака для товарів та послуг, припинення незаконного використання складеного твору та стягнення компенсації [1]. Хоча позов і було задоволено

частково, але все ж судом досліджувався дизайн екстер`єру та інтер`єру ресторанів, меблювання, аксесуари, декор, кольорова гама та виходячи із подібності інтер’єрів приймалось рішення про задоволення позову.

Продовжуючи дослідження trade dress в Україні слід також наголосити про часткову захищеність даного поняття через Закон України «Про захист від недобросовісної конкуренції» згідно з яким вбачається, що неправомірним є використання як чужої торговельної марки (знаку для товарів і послуг), так і рекламних матеріалів, оформлення пакування товарів, інших позначень без дозволу (згоди) суб`єкта господарювання, який раніше почав використовувати їх або схожі на них позначення у господарській діяльності, що призвело чи може призвести до змішування з діяльністю цього суб`єкта господарювання, копіювання зовнішнього вигляду продукції [2].

Натомість якщо надавати оцінку такому захисту, слід зазначити, що дане питання через відсутність належної практики ускладнюється під час фактичного захисту порушених прав у суді.

Саме тому, як вже відмічалось раніше, суб’єктам господарювання доводиться використовувати інші, складніші способи захисту. Такими до прикладу може

бути реєстрація кольору або ж поєднання кольорів, як торгових марок. Яскравим прикладом може слугувати італійська компанія Унидельта С. п.А. (свідоцтво № 127798), яка зареєструвала блакитний колір для неметалічних гайок, механічного фітингу для неметалічних труб, а також хомутів для таких труб. Ще одним прикладом може слугувати реєстрація темно-рожевого кольору (свідоцтво на ТМ № 74157) світовим виробником товарів для будинку і гігієни Reckitt Benckiser для своєї продукції, серед якої засоби для прання і видалення плям, препарати для пом'якшення тканини, а також різні мийні засоби.

Продовжуючи дослідження підходів до захисту прав, можна також говорити про можливість реєстрації етикетки, як торгової марки. Проте, тут одразу виникає проблема, адже цілісно етикетку зареєструвати неможливо. Так, на етикетці окрім зображувального елементу також повинні бути присутні штрих-код, склад продукції, інформація про виробника товару чи імпортера. Натомість завдяки євроінтеграційним процесам у 2020 році в Україні було прийнято новий закон "Про захист прав на знаки для товарів і послуг", який регулює використання Trade dress в Україні відповідно до стандартів ЄС. Так, відповідно до ч. 4 ст. 5 вказаного Закону об'єм охорони торгової марки, що надається, визначається зображенням знаку і переліком

товарів і послуг, внесеним в реєстр [3]. Наявність штрих-коду, складу продукції, інформації про виробника товару чи імпортера буде причиною для відмови у реєстрації. Натомість відсутність такої інформації у зареєстрованій ТМ надалі може викликати проблеми для вирішення ступеня подібності з оскаржуваною етикеткою.

Висновок. Виходячи із наведеного вище, слід зазначити, що питання охорони права на trade dress в Україні фактично відсутнє. Так, теоретично, застосовуючи різні можливі способи захисту, які регламентовані в Україні, домогтися цілі все ж можливо, проте наявність чіткої регламентованої процедури конкретно щодо права на trade dress значно краще захищала б суб’єктів інтелектуальної власності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Постанова Київського апеляційного господарського суду від 16.07.2015 р. Справа № 910/11324/13. URL: http://reyestr.court.gov.ua/Review/46969768 (дата звернення: 01.05.2023).
2. Про захист від недобросовісної конкуренції. Закон України від 07.06.1996 № 236/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text (дата звернення: 01.05.2023).
3. Про охорону прав на знаки для товарів і послуг. Закон України від 15.12.1993 № 3689-XII. URL: https://zakon.rada.gov.ua/laws/show/3689-12#Text (дата звернення: 01.05.2023).
4. Trade Dress Definition URL: http://www.law.cornell.edu/wex/trade_dress (дата звернення: 01.05.2023).

ШКУРАЙ Олександр

Студент, КПІ ім. Ігоря Сікорського

ГОЛОВКО Ольга

к.ю.н., ст. дослідник,
ст. науковий співробітник лабораторії
теорії цифрової трансформації і права
наукового центру цифрової трансформації
і права ДНУ “ІІБП НАПрН” України,
ст. викладач кафедри інтелектуальної власності
та приватного права КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЄС

Постановка проблеми. Науковий прогрес дав поштовх до нових функцій технології штучного інтелекту, внаслідок чого перед суспільством постають нові моральні, економічні та правові дилеми про сприйняття розуму індивіда, інтелектуального процесу людини та права інтелектуальної власності. Є декілька важливих питань стосовно яких, треба прийти до мажоритарного консенсусу, за для полегшення процесу наукового дискурсу, та подальшого правового регулювання суспільних відносин з так званим

“штучним інтелектом”. Це питання: 1) Що таке штучний інтелект ; 2) чи мають правову охорону об’єкти, створені повністю або частково з використанням штучного інтелекту, якщо так, то яким об'єктом вони є та хто є первісним автором таких об'єктів ; 3) передбачити яке майбутнє чекає авторське право для того, щоб забезпечити належне регулювання.

Визначення Штучного Інтелекту

Фахівці, що працюють над дослідженням категорії Штучний Інтелект (далі - ШІ), намагаються визначити, яку поведінку треба вважати розумною, та створити працюючі моделі цієї поведінки. Дослідники ставлять запитання про те, як за допомогою нових теорій і моделей навчитися розуміти принципи й механізми інтелектуальної діяльності. Практичною метою є створення методів і техніки, необхідної для програмування «розумності» і її передача комп’ютерам, а через них – різним системам і засобам.

Під терміном інтелект, зокрема від латинської мови, прийнято вважати розумові здібності людини. Також інтелектом ми називатимемо здатність мозку вирішувати інтелектуальні задачі шляхом придбання, запам’ятовування і цілеспрямованого перетворення знань у процесі навчання на досвіді і адаптації до різноманітних обставин. Відповідно штучний інтелект розумітимемо, як властивість автоматичних систем

брати на себе окремі функції інтелекту людини, наприклад, вибирати й ухвалювати оптимальні рішення на основі раніше отриманого досвіду й раціонального аналізу зовнішніх дій [4].

У вищенаведеному визначенні поняття інтелекту під терміном «знання» мається на увазі не лише та інформація, яка надходить до мозку через органи чуття. Такого типу знання надзвичайно важливі, але недостатні для інтелектуальної діяльності. Об’єктам нашого навколишнього середовища притаманна властивість не лише впливати на органи чуття, але й перебувати один із одним у певних відносинах. Щоб здійснювати в навколишньому середовищі інтелектуальну діяльність (або хоча б просто існувати), необхідно мати в системі знань модель цього світу.

У цій інформаційній моделі навколишнього середовища реальні об’єкти, їх властивості й відносини між ними не лише відображаються і запам’ятовуються, але і, як на цьому наголошено в даному визначенні інтелекту, можуть «цілеспрямовано перетворюватися». При цьому важливим є те, що модель зовнішнього середовища формується «в процесі навчання на досвіді і адаптації до різноманітних обставин».

На сьогодні, ШІ навколо якого йдуть сперечання – це інтелектуальні системи, алгоритми і методи, які обробляють дані для вирішення дуже складних задач,

які вираженні у комп’ютерному коді. Важливою його частиною є машинне навчання (Machine Learning).

Сучасний ШІ працює за принципом “змішування” декількох підходів в моделюванні штучного інтелекту: моделювання структури й механізму роботи мозку людини, моделювання інтелектуальної діяльності, створення змішаних людино-машинних систем. Наприклад комп'ютерна програма Midjourney, яка користується ШІ, змішує певну кількість існуючих візуальних об'єктів, в результаті чого з'являється новий візуальний об’єкт, який імітує стилі, способи, методи та інші ознаки об'єктів, на яких він базувався.

Як це працює ? Ці зображення з'являються за допомоги методу дифузії з додатковою допомогою нейромережі, метод був винайдений у 2015 році дослідниками ШІ зі Стенфордського університету. На діаграмі нижче, взятій з дослідження Стенфордської команди, показано дві фази процесу дифузії з використанням навчальних даних у формі спіралі [5].

Під час першого етапу (перша діаграма) на зображення або іншого типу даних, накладається візуальний шум. На кожному етапі ШІ фіксує, як додавання шуму впливає на зображення. На останній етап дані будуть розсіяні у практично випадковий шумм.

Другий етап майже однаковий, тільки працює він навпаки і дивитись на нього треба зправо наліво. Зафіксувавши кроки, які перетворюють певне зображення на шум, ШІ виконує ті самі дії у зворотному напрямку, генеруючі копію оригінального зображення. Таким чином ШІ показує свою головну ознаку яка відрізняє його від звичайної комп'ютерної програми, а саме починає навчатись, створювати тенденції, категорії, алгоритми та сама обирає яку техніку та особливості застосувати у індивідуальних випадках.

Чи є об'єкт згенерований за цією формулою, новим твором ?Штучний інтелект не може претендувати авторські права, на згенеровані ним об'єкти, що споріднює його з тваринами. Це пов’язано з тим, що концепт авторських прав від самого початку стосувався лише людей і їхньої творчості. Самим очевидним прикладом тут може бути рішення Судових органів США у справі “Naruto v. Slater” , яке стосується визначення об'єктів інтелектуальної власності створених не людиною.А саме спір між організацією PETA, яка намагалися заявити позовні вимоги від імені примата “Наруто” проживаючого на території природного заповіднику Індонезії, позовні вимоги подавали на правах того, що Наруто є недієздатною особою і не може сам представляти свої інтереси в суді.

Висновком суду, було затверджено, що мати авторські права, може тільки людина. Тварини не мають авторських прав за законодавством США; тварини не можуть виступати в суді, тому організація PETA не може виступати представником недієздатної особи [6].

Чи не може за такою логікою, статися так, що всі об’єкти, створені за допомогою штучного інтелекту та штучним інтелектом безпосередньо, не будуть охороноздатними?

Американський науковий дискурс, має кілька підходів стосовно визначення прав об’єктів, створених за допомогою штучного інтелекту та штучним інтелектом безпосередньо. Зокрема, є підхід, що автором має вважатися особа, яка використовує штучний інтелект для створення твору, або це має бути співавторство користувача та розробника/власника штучного інтелекту залежно від обставин.

Але хтось все таки має права на результати створені за допомогою ШІ, то хто це ?Це може бути людина, наприклад якщо дії які вона вчинила, вплинули на вигляд об'єкта. Наприклад особа визначила та запрограмувала параметри ШІ на те щоб підібрати певний твір, на основі якого програма згенерує новий об'єкт. Такий стан речей не є чимось новим для нашого суспільства, відображення цього є у статті 33 Закону України “Про авторське право та суміжні права”, в якій

зазначається, що твори, створені фізичними особами з використанням комп’ютерних технологій, не вважаються неоригінальними об’єктами, згенерований комп’ютерною програмою [1].

1 січня 2023 року набрав чинності новий Закон України “Про авторське право і суміжні права”. У цьому законі результат роботи штучного інтелекту підпадає під правове регулювання як не оригінальний об’єкт, згенерований комп’ютерною програмою, що охороняється правом особливого роду (sui generis) [1].

Sui generis – це набір спеціальних положень, які відрізняються від загальних. Вони регулюють об’єкти, створені внаслідок роботи комп’ютерної програми. Ці об’єкти не містять творчого підходу та генеруються без участі людини. Як результат, особисті немайнові права на такі об’єкти не виникають, адже вони можуть належати лише фізичній особі, але аж ніяк не штучному інтелекту.

Такі права з нетиповим родом походження діятимуть з моменту, коли комп’ютерна програма згенерувала результат, а їхній строк чинності спливає через 25 років з цього моменту. Якщо штучний інтелект згенерував результат, використавши інший об’єкт авторського права, тоді користуватись таким результатом ШІ можна лише у випадку, якщо не порушені авторські права щодо цього об’єкту.

Наприклад, якщо штучний інтелект створив кліп, використовуючи уривки захищеного авторським правом відео – потрібно дотримуватися авторських прав щодо використаного контенту.

Як Європейська правова система на сьогодні регулює питання Штучного інтелекту ? Європейський суд з прав людини (далі - ЄСПЛ) розглянув справу “Centrum för rättvisa проти Швеції” (заява № 35252/08), що стосується автоматизованого радіоелектронного перехоплення сигналів [2].

Заявник стверджував, що під час своєї роботи щоденно спілкується з особами, організаціями та компаніями у Швеції та за кордоном за допомогою електронної пошти, телефону та факсу. Проте він побоюється, що його розмови перехопить радіоелектронна розвідка. Таке підслуховування є автоматизованим і повинно стосуватися лише певних сигналів. Дані, зібрані за допомогою цих процедур, можуть стосуватися як змісту розмови, так і асоційованих комунікаційних даних. Дані можуть бути перехоплені в радіоефірі – зазвичай, за допомогою радіозв’язку та супутників – і з кабелів.

ЄСПЛ заявив, що Суд пам’ятає про потенційно шкідливий вплив радіоелектронної розвідки на захист приватності. Однак, Суд визнає важливість такої системи, як та, що була розглянута у цій справі, для

національної безпеки. Стосовно цього він зауважує аналогічні висновки Венеціанської комісії

У підсумку, судом було прийнято таке рішення : суд вважає, що шведська система радіоелектронної розвідки передбачає належні та достатні гарантії проти свавілля та ризику зловживання.

Дуже схожий випадок відбувся з провідними IT компаніями Microsoft, GitHub та OpenAI, в сторону яких був направлений гнів через використання плагіну на основі ШІ, під назвою “Copilot” .

Copilot – це програма, що працює на базі технології OpenAI та прямо у редакторі створює рядки коду для айтівців. Програма навчається завдяки загальнодоступному коду з GitHub [7]. Юридичний простір відкрив дискусію, багато хто сказав, що ця програма порушує права інтелектуальної власності та авторські права фахівців IT сфери, оскільки базується на “піратстві програмного забезпечення у безпрецедентних масштабах”. Грантуючись на таких поглядах, Метью Баттерік, правник, звернувся з груповим позовом проти компаній до федерального суду Сан-Франциско [3].

Проте, Microsoft, GitHub та OpenAI подали заяву, в якій стверджують, що “Copilot нічого не вилучає з відкритого вихідного коду, доступного для громадськості. Натомість Copilot допомагає

розробникам писати код, генеруючи пропозиції на основі того, чого він навчився з публічного коду” [8].

2023-го року у місцевому суді Сан-Франциско, штату Каліфорнія прийнято позов до платформ Midjourney, DeviantArt та Stability AI, який подали художниці Сара Андерсен, Келлі МакКернан і Карла Ортіс. Причина позову – штучні інтелекти використовували картини художниць без їхньої згоди. У позовних вимогах, автори творів запросили майнові компенсації за завдані збитки через порушення авторських прав, правил платформи DeviantArt, закону DMCA та законів про захист від недобросовісної конкуренції [10].

Наразі судовий процес тіки розпочато, але поки авторки вимагають від відповідача гарантій, які унеможливлять їх порушенню прав у майбутньому. В тому числі, через видалення їх творів з баз и даних ШІ – [9].

Висновки. Нині автор та здатність до творчості ототожнюються з людиною. Своєю чергою це є підставою для відмови в охороноздатності об’єктам, які створені за допомогою штучного інтелекту та штучним інтелектом безпосередньо. Винятки становлять ті випадки, коли штучний інтелект залишається засобом. У такому разі автором вважатиметься особа, яка використовувала цю технологію.

Враховуючи наявні пропозиції з удосконалення авторського права щодо таких об’єктів, можна сказати, що популярною пропозицією є створення просвітницької діяльності тлумаченням основ технології ШІ. А наразі сучасне законодавство здатне більш иенш справедливо урівноважувати проблемні питання з сфери відносин інтелектуальної власності з ШІ, наприклад за допомогою дуже популярних MIT ліцензій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про авторське право та суміжні права: Закон України від 15.04.2023 Документ 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#n461 ;

2. Справа ЄСПЛ “Centrum för rättvisa проти Швеції” (заява № 35252/08). URL: https://privacy.khpg.org/1604922627 ;

3. USA District Court Northern District of California San Francisco Division
Case 4:22-cv-06823-JST Document 5. URL: https://www.theverge.com/2023/1/28/23575919/microsoft-openai-github-dismiss-copilot-ai-c;

4. А. С. Савченко, О. О. Синельніков. Методи та системи штучного інтелекту. URL: https://pdf.lib.vntu.edu.ua/books/2020/Savchenko_2017_176.pdf ;

5. Дослідження Стенфордського університету. URL: https://colab.research.google.com/github/huggingface/notebooks/blob/main/diffusers/stable_diffusion.ipynb ;

6. . Naruto v. Slater, No. 16-15469 (9th Cir. 2018). United States Court of Appeals for the Ninth Circuit. 2018.
URL:
https://cdn.ca9.uscourts.gov/datastore/opinions/2018/04/23/16-15469.pdf ;
7. Github. URL: https://github.com/features/copilot ;
8. USA District Court Nothern Districk of California Okland Division Case 4:22-cv-06823-JST Document 50. URL: https://www.documentcloud.org/documents/23589440-microsoft-and-github-motion-to-dismiss?responsive=1&title=1 ;
9. UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION Case 3:23-cv-00201 Document 1. URL:https://ipwatchdog.com/wp-content/uploads/2023/02/Andersen_et_al_v._Stability_AI.pdf ;
10.THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 U.S. Copyright Office Summary.URL: https://www.copyright.gov/legislation/dmca.pdf ;

ЯРОШЕНКО Валерія

Львівський національний університет імені Івана Франка

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ЗАСОБУ РОСІЙСЬКОЇ ПРОПАГАНДИ В ІНФОРМАЦІЙНОМУ ПОЛІ УКРАЇНИ І ГРУЗІЇ

Не так давно OpenAi анонсував 2 масштабні моделі штучного інтелекту DALL-E and Chat GPT. Ці нейронні мережі базуються на машинному навчанні для створення нескінченної кількості унікального текстового та візуального контенту для користувачів з будь-якої точки планети. Можливо, OpenAI була першою компанією, яка випустила свої продукти для громадськості, але вона не єдина, хто розвивається у цій сфері; такі компанії, як NVIDIA, Google і менші стартапи що розробляють ШІ, працюють над подібними механізмами.

Ці генеративні моделі ШІ дозволяють користувачам вводити команди для створення есе, музичних текстів, простого коду тощо.

Протягом останнього десятиліття екстремістські групи адаптуються під нову реальність,

використовуючи штучний інтелект для поширення дезінформації у власних цілях.

Екстремістські відеоігри і певне наповнення соціальних мереж знайшли свій шлях до різноманітних інтернет-платформ. На відміну від екстремістської пропаганди минулого, ці нові цифрові медіа-продукти дозволяють екстремістським групам взаємодіяти з аудиторією анонімно і безпрецедентно.

Екстремістські групи на таких платформах, як Twitter, Tumblr, Facebook і особливо TikTok, створюють вірусні пости, щоб залучити підписників, викликати страх і згуртувати своїх існуючих і потенційних новобранців. У 2019 році було виявлено різноманітні облікові записи ІДІЛ у TikTok, які публікували вміст, що провокує насильство, змішаний із запам’ятовуючими професійно записаними бойовими гімнами (тобто Nasheed) та емодзі, щоб націлити користувачів платформи та продемонструвати силу групи.

У той час як звичайні форми екстремістської пропаганди, подібні до згаданих вище, вимагають навченого персоналу для планування, створення та поширення цих матеріалів, поява генеративних моделей штучного інтелекту може дозволити різноманітним екстремістським недержавним акторам створювати

більшу кількість пропагандистських продуктів, більш комплексних – із значно меншою затратою сил.

Проросійська пропагандистська активність спостерігається зокрема в Сакартвело, особливо в Telegram, який використовується для поширення новин про війну щохвилини. Після того, як найпопулярніша соціальна медіа-платформа Сакартвело, Facebook, видалила ультрарадикальні та насильницькі групи в рамках боротьби з дезінформацією та маніпулюванням інформацією, ці самі актори стали дедалі активнішими в Telegram і Tik-Tok, які певним чином стали їхньою альтернативою.

Класичними способами поширення російської пропаганди є публікація фейків в телеграм каналах, зокрема тих, що підтримують ультраправі рухи - «Альт-Інфо», «Грузинський марш» і Союз православних батьків.

Головний посил дезінформації в Сакартвело сьогодні полягає в тому, що «якщо ми помітно підтримаємо Україну, то ми спровокуємо росію; Тоді росія вторгнеться, а чи ми цього хочемо, ми хочемо того, що відбувається в Україні? - Хіба ви не бачите, що Україна залишилась одна і санкції не працюють? Хіба ви не бачите, що західний світ від неї відмовився?» — це спроба нав’язати проросійські наративи.

21-23 березня 2023 року кремлівські ЗМІ (Украина.ру та news-kiev.ru) та окремі російськомовні (1, 2, 3) грузинсько-мовні (1, 2) акаунти у Facebook опублікували карикатурні зображення президента України, як обкладинки American Newsweek та FRANC-TIREUR Це візуальна маніпуляція, а одна з обкладинок ймовірно була згенерована штучним інтелектом.

3 квітня на сторінці «Православна сторінка» у Facebook була опублікована фотографія, на якій перед храмом палає вогнище та навколо нього стоять люди з різнокольоровими прапорами ЛГБТ-спільноти. Цитуючи пост, це «православний храм в чужій країні» і «чим більше ви терпите ЛГБТ-пропагандистів, тим більше вони собі дозволяють».

Фотографія з вогнем та різнокольоровими прапорами перед церквою - відвертий фейк. На це вказують кілька деталей, такі як глючна графіка, несправжні контури та неприродний вигляд прапорів. Крім того, на одній зі сторінок Facebook 31 березня було опубліковано ту саму фотографію та написано, що вона згенерована платформою штучного інтелекту Midjourney.

Наразі російські пропагандисти та екстремістські групи адаптуються до можливостей штучного інтелекту у поширенні дезінформації швидше, ніж держструктури та кіберполіція створюють їм протидію.

Закони та нормативні акти повинні зіграти певну роль, принаймні в деяких сферах з найвищим ризиком, сказав Метью Ферраро, адвокат WilmerHale та експерт з юридичних питань навколо ШІ.

Ще одним аспектом є те ще, що штучний інтлект може обслуговувати величезну кількість юзерів одночасно, з мінімальною затратою часу на створення контенту.

Деякі стартапи зі штучного інтелекту намагаються запобігти неправильному використанню своїх продуктів, розробляючи альтернативні програми, які допомагають ідентифікувати шаблони, які можуть вказувати, чи зображення, тексти, відео чи звуки були створені за допомогою генеративних моделей. Ці програми одного разу можна буде інтегрувати в платформи соціальних медіа, сервіси потокової передачі музики та навіть ігрові платформи, що може заважати штучно створеному вмісту, який використовується для зловмисних цілей, знайти вихід із темних куточків Інтернету. Крім того, критично важливо, щоб компанії зі штучним інтелектом, про які йдеться в цьому матеріалі, розширили свої команди з довіри та безпеки. Ці команди можуть придумати найгірші способи використання функцій цих програм, а потім запровадити правила та плани на випадок їх неправильного використання. У цій статті

стверджується, що, незважаючи на те, що вживаються важливі кроки для запобігання неправильному використанню генеративних моделей ШІ, існують явні вразливості, якими можуть легко скористатися екстремістські актори.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Georgia law takes aim at Deepfake photos, videos [Електронний ресурс] – Режим доступу до ресурсу: https://content.next.westlaw.com/Document/I8be77e48d81811eabea4f0dc9fb69570/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true.
2. How Russian propaganda reacted to the protests in Georgia [Електронний ресурс] – Режим доступу до ресурсу: https://disinfo.detector.media/post/how-russian-propaganda-reacted-to-the-protests-in-georgia.
3. Russian Propaganda Information Front In Georgian Language On Telegram [Електронний ресурс] – Режим доступу до ресурсу: https://isfed.ge/eng/blogi/rusuli-propagandis-qartulenovani-sainformatsio-fronti-telegramze294

Післямова

Актуальність проекту «Європейська інтеграція: законодавство та Інтернет речей»у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE для України пов’язана з процесами європейської інтеграції у сфері цифрової трансформації, здебільшого, щодо процесу впровадження сучасних технологій Інтернету речей (IoT).

Йдеться про дослідження ролі ЄС у глобалізованому світі, зокрема, законодавства ЄС, яке стосується сфери інформаційних цифрових технологій в епоху розвитку досягнень четвертої технологічної революції.

Для реалізації цієї мети ми запропонували запровадити нову дисципліну - “Євроінтеграція: законодавство та Інтернет речей”. Вона призначена для залучення широкого кола студентів, науковців, представників зацікавлених державних органів і громадських та неурядових організацій, практикуючих юристів, ІТ-спеціалістів.

Залучені учасники проекту можуть набути та вдосконалити свої професійні навички з:

1) правових питань впровадження IoT;

2) законодавства ЄС у галузі інформаційних технологій;

3) порівняльно-правового аналізу національного законодавства та законодавства ЄС у сфері IoT.

Це передбачає вивчення змісту, складу, особливостей, системних ризиків та бар'єрів використання IoT, а також роз'яснення політики ЄС щодо його розвитку.

Центральними темами курсу є юридичні питання забезпечення кібербезпеки, пов'язаної з IoT, в контексті захисту критичної інформаційної інфраструктури персональних даних та ідентифікації суб'єктів та об'єктів, що стосуються технологій
IoT, використання роботів та штучного інтелекту,
технологій хмарних обчислень та блокчейну.

Проект базується на інноваційних формах навчання. Це сприяє набуттю навичок самостійного пошуку, виявлення та вирішення юридичних проблем, пов'язаних із використанням IoT. У цьому проекті також впроваджений інноваційний мультидисциплінарний підхід. Це дозволяє поєднувати знання з технічних та правових аспектів IoT. Це стає можливим завдяки унікальному поєднанню професіоналів з політехнічних та юридичних дисциплін Національного технічного університету України «Київський політехнічний інститут Ігоря Сікорського».

Наукове видання

ЗБІРНИК МАТЕРІАЛІВ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНТЕРНЕТ РЕЧЕЙ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

05 травня 2023 року