UDC 342.7:004.738.5:004.056
DOI https://doi.org/10.32782/TNU-2707-0581/2025.5/02

Horielova V. Yu.
V.I. Vernadsky Taurida National University

THE INTERNET OF THINGS AND THE PROTECTION OF HUMAN RIGHTS: ETHICAL AND LEGAL CHALLENGES

The article examines the topical issue of ethics and law of the Internet of Things (IoT), since today, thanks to the improvement of sensor technologies, wireless communication and data processing, IoT has evolved from a concept to an integral element of modernity, transforming almost all spheres of human existence (economy, transport, healthcare and other areas, ensuring process automation, resource optimisation and development of smart systems). The article outlines the ethical aspects of using IoT, in particular, those related to transparency, fairness of algorithms and respect for human rights. It is noted that IoT stimulates the progress of artificial intelligence, while massive data collection and storage create risks of violation of human privacy, which requires strict legal regulation. Thus, the issue of 'algorithm ethics' becomes an urgent one, as algorithm-based solutions can be biased, which requires transparency and human responsibility for technology development. The successful development of IoT requires a combination of legal regulation, technical measures, international standards and educational programmes to ensure a safe and fair digital environment. The article presents a list of problems associated with the practical application of the Internet of Things. The author emphasises the need to develop and implement ethical standards for the Internet of Things (IoT), which is an important means of ensuring security and protecting human privacy in the technological environment. The article also discusses existing international ethical standards for the Internet of Things, including the principles of data protection, security, transparency and responsibility. These principles promote the integration of ethics into the technology development process, ensuring that IoT not only performs technical functions but also complies with ethical standards, in particular in terms of protecting human privacy.

Key words: *Internet of Things, human rights, ethics, privacy, data protection, cybersecurity, artificial intelligence, digital governance, algorithmic transparency, legal regulation.*

Problem Statement. The Internet of Things (IoT) is a technological phenomenon that offers vast opportunities for development; however, it simultaneously poses risks to privacy, security, and human rights. The absence of appropriate regulation and ethical standards exacerbates concerns regarding data usage transparency, algorithmic discrimination, and cybersecurity threats.

Relevance of the Study. The development of the Internet of Things (IoT) is accompanied by its rapid integration into everyday life, which heightens the risk of human rights violations, particularly concerning privacy and security. The relevance of this research lies in the need to establish ethical and legal frameworks for the regulation of IoT and the protection of human rights within the digital environment.

The aim of the study is to analyse the ethical and legal challenges that arise in the context of the use of IoT, as well as to develop recommendations for the creation of a secure and fair digital environment.

Analysis of Recent Research and Publications. The ethical and legal challenges of the Internet of Things (IoT) occupy a central place in contemporary scientific discourse. One of the first comprehensive accounts of the architecture and functions of IoT was presented by L. Atzori, A. Iera, and G. Morabito, who outlined the technological foundations of interaction between devices and humans [1]. The concept of the development of networked systems was further elaborated by J. Gubbi, R. Buyya, and other researchers, emphasising the growing role of data analytics and artificial intelligence [2]. The issues of cybersecurity and legal regulation in the IoT domain were examined in detail by R. Weber and E. Studer, who highlight the complexity of determining legal responsibility within the digital environment [3].

The ethical aspects of digital technologies are examined by L. Floridi and M. Taddeo, who emphasise the need to develop a "data ethics" framework and ensure algorithmic transparency [4]. In the legal context, significant attention is given to the EU General Data Protection Regulation (GDPR), which was systematically interpreted by P. Voigt and A. Von dem Bussche, establishing standards for transparency and control over personal information [5]. The International Organization for Standardization (ISO) has created a technical basis for secure device interaction through ISO/IEC 29182 [6]. Among important legislative initiatives, the American IoT Cybersecurity Improvement Act [7] and the OECD principles on the ethical use of technologies [8] should be noted, as they lay the foundation for a global policy of responsible data governance.

Contemporary research also emphasises the practical consequences of IoT application in various sectors – from medicine [10] to agriculture [13] and industry [14]. At the same time, issues of privacy, algorithmic bias, and user security are becoming increasingly relevant. The concept of "privacy by design" (protection of privacy at the technology development stage) was developed by A. Cavoukian, who regarded it as the foundation for building trust between humans and the technological environment [17; 20]. Therefore, ethical standards have not only a moral but also a regulatory potential, as they form the basis for improving legal mechanisms of IoT oversight. The IEEE Ethically Aligned Design standards and EU initiatives on "ethical artificial intelligence" [24; 26] establish a new paradigm for responsible digital development.

Among Ukrainian researchers, the issues of digital ethics and the protection of human rights in the IoT domain are analysed by V. Horielova, O. Pidopryhora, and L. Koval, who emphasise the need to harmonise national legislation with European standards. The Ukrainian scientific tradition is gradually adapting these approaches by developing its own ethical frameworks for IoT, focused on prioritising the protection of human rights and freedoms.

Presentation of the Main Material. Despite the active development of foreign scientific thought, the issue of ethical regulation of the Internet of Things (IoT) in Ukraine is still at an early stage, which necessitates a systematic analysis taking into account the national context. The development of the Internet of Things began in the 1990s, when the idea of interconnecting devices via the Internet was formed. Thanks to the improvement of sensor technologies, wireless communication, and data processing, IoT has evolved from a concept into an integral element of the modern digital environment. This technology transforms the economy, transport, healthcare, and other sectors, providing process automation, resource optimisation, and the development of "smart" systems. IoT stimulates the progress of artificial intelligence, machine learning, and big data technologies, which increases the demand for cybersecurity. The Internet of Things, or IoT, represents the concept of integrating physical objects into a single network, enabling interaction between them and with humans. This technology involves the use of sensors, software, and networking tools for collecting, processing, and exchanging data. IoT is aimed at creating an infrastructure that unites objects, from household appliances to industrial systems, in order to enhance efficiency, automation, and process personalisation.

The main elements of the Internet of Things are physical objects, networking technologies, and analytical platforms. Physical objects are equipped with sensors and chips that record the state of the environment or the device itself. Networking technologies provide the transmission of collected information through communication channels such as Wi-Fi or cellular networks, which facilitates the synchronization of device operations. Analytical systems process data, forming the basis for decision-making and adapting device functionality according to conditions or user needs [1].

However, despite the significant potential of IoT, its development is accompanied by a number of challenges. The main risks are associated with the protection of personal data, as devices collect large volumes of information that may be accessible to third parties. Cybersecurity also remains a key challenge, as device vulnerabilities can become a source of threats to users and infrastructure [2]. Equally important are the ethical aspects of IoT use, particularly those related to algorithmic transparency, fairness, and respect for human rights [3]. Thus, although the Internet of Things is an important tool for societal transformation, contributing to progress in various sectors, its implementation requires a responsible approach, which should include the development of ethical standards, legal regulation, and data protection technologies to ensure the safe and fair use of this innovation [4].

Furthermore, the development of the Internet of Things is accompanied by the emergence of numerous challenges related to privacy, security, and personal data management. In response, legal and ethical frameworks are being established to protect user rights, ensure transparency in data usage, and allocate responsibility for potential risks. International legal instruments already aim to regulate IoT activities in various contexts, seeking to ensure the safe functioning of technologies and their compliance with ethical principles [5]. One of the key international documents is the General Data Protection Regulation (hereinafter – GDPR), which establishes the main requirements for the collection, storage, and transfer of personal data. Its application also covers IoT, requiring informed consent from users and ensuring the right to control personal information. The GDPR serves as a foundation for the implementation of transparency and accountability policies in the IoT domain, promoting the global adaptation of data protection standards. In this regard, the International Organization for Standardization (ISO) has developed a series of recommendations for IoT, notably ISO/IEC 29182, which sets technical protocols for device interaction. These standards facilitate the integration of IoT into global networks, ensuring device compatibility and enhancing security. Combined with other ISO standards, this document enables the development of IoT in compliance with fundamental ethical and legal principles [6].

It is also pertinent to highlight the "IoT Cybersecurity Improvement Act" in the United States, which establishes basic security requirements for IoT devices used by government institutions. In China, the "Personal Information Protection Law" (PIPL) imposes strict restrictions on data processing and transfer, aimed at strengthening privacy control [7].

It should be noted that the ethical standards currently being developed within international organisations, such as the OECD, which proposes principles of transparency, trust, and accountability for IoT, are aimed at encouraging manufacturers and developers to adhere to high standards in the creation of secure and reliable devices. In particular, the recommendations include ensuring users' rights to be informed and to control their own data. The importance of the legal and ethical aspects of IoT use is emphasised by their role in building trust in technologies [8]. Despite the diversity of approaches in different countries, all of them are aimed at minimising risks and ensuring fair conditions for the use of the Internet of Things in society.

The practical significance of the Internet of Things (IoT) is most clearly observed in specific sectors, where the technology directly impacts the realisation of human rights–primarily the right to life, security, and healthcare. The Internet of Things is increasingly integrated into everyday life, creating an ecosystem of interconnected devices that enhance efficiency, comfort, and safety. This technology enables the automation of routine processes, reduces costs, and optimises resource use, becoming a key element of digital transformation across multiple sectors [9].

In healthcare, IoT contributes to the improvement of diagnostics and health monitoring: smart sensors and wearable devices allow physicians to obtain real-time data on patients' conditions, thereby enhancing the quality of treatment. Automated drug administration devices and remote monitoring systems minimise human error, reduce risks for patients, and increase safety [10]. In the transport sector, IoT transforms infrastructure into a "smart" system that improves efficiency and reduces accidents: vehicles equipped with embedded sensors predict technical malfunctions and optimise fuel consumption. In urban settings, "smart" traffic lights and traffic management systems help to reduce congestion, promoting the efficient use of roads [11].

In the "smart home" domain, IoT automates the management of lighting, heating, and security, providing comfort and reducing energy consumption. Smart refrigerators and remote control systems for household appliances optimise domestic processes, giving users more time for everyday tasks [12]. In agriculture, IoT implements sensor-based monitoring systems for crop cultivation conditions: data on soil moisture, temperature, and air quality allow for increased yields and reduced costs. Similar technologies are used in animal husbandry to monitor animal health and improve living conditions [13]. In industry, IoT is applied for equipment monitoring, which lowers the risk of accidents, ensures production continuity, and enhances efficiency [14]. In commerce, the Internet of Things transforms traditional business models: smart shelves, sensors, and customer behaviour analysis systems optimise inventory management, improve marketing strategies, and enhance service quality [15]. Thus, the development of IoT provides significant benefits, but also creates challenges related to privacy and cybersecurity. Therefore, the implementation of these technologies requires careful technical and legal regulation, alongside an ethical approach to ensure user safety and trust in the technologies.

The Internet of Things generates substantial volumes of data, which often include sensitive information about users, their habits, and their environment. These data are vulnerable to leaks, unauthorized access, and third-party misuse. An example is the data breach in fitness applications, where collected data allowed the identification of military locations, thereby compromising security [16]. Thus, to minimise such risks, it is necessary to implement stringent data protection measures and inform users about potential threats.

The ethical use of IoT is founded on transparency in data collection and processing, as well as obtaining informed consent from users. Many users are unaware of the extent of information collected and its potential use. Informed consent requires a clear and accessible explanation regarding the collection, storage, and utilisation of personal data. For example, users often agree to privacy policies without reading them, due to the complexity and length of the documents. However, according to international researchers, the need to ensure transparency strengthens trust between users and companies [17].

The automation of processes enabled by IoT can sometimes lead to a loss of user control over decision-making. Smart systems, such as refrigerators, may make purchasing decisions by analysing available products, but this can limit users' autonomy. Moreover, hacker attacks on medical devices, such as pacemakers, pose life-threatening risks, highlighting the need to strengthen security in IoT [18; 19]. Therefore, the development of IoT requires clear legal frameworks that define the responsibilities of developers, manufacturers, and users regarding device safety, timely software updates, and data protection. Legal certainty in this context contributes to the reduction of ethical risks and the enhancement of trust in technologies.

The Internet of Things poses a threat to privacy through the automated collection, storage, and analysis of users' personal data. Smart devices, such as fitness trackers, voice assistants, or video surveillance systems, often capture more data than users may be aware of. These data are used for profiling, behaviour analysis, or commercial advertising, frequently without users' consent. Protecting the right to privacy requires the implementation of stringent regulations, such as the GDPR, which obliges companies to ensure transparency in data collection and obtain informed consent from users [20]. The vulnerability of IoT devices to cyberattacks creates risks to both the physical and informational security of users. Breaches of "smart" homes, vehicles, or medical devices can endanger human life and health. To ensure security, it is necessary to implement modern cybersecurity protocols, mandatory data encryption, and regular software updates. Legal regulation should encourage manufacturers to adhere to high standards of personal data protection [21]. Ensuring transparency in the use of IoT requires openly informing users about the purposes of data collection, as well as the methods of storage and processing. Companies must develop clear and accessible privacy policies, providing users with the right to view, edit, or delete their own data. This fosters trust between users and IoT technology developers.

Furthermore, educational programmes and informational campaigns can help users better understand their rights in the digital age [22]. Children, elderly people, and individuals with disabilities are particularly vulnerable to IoT-related risks. For children, it is important to create devices with limited data collection, protecting them from manipulation and the development of dependency. Elderly individuals may be targeted by cybercriminals due to a lack of awareness about risks. Devices for people with disabilities should take into account specific needs and ensure uninterrupted operation. The development of ethical standards for IoT, aimed at these groups, is an important direction in technological advancement [23]. Protecting human rights in the context of IoT implementation requires a systematic approach that combines technological solutions, legal regulations, and ethical principles. Ensuring privacy, security, and transparency should be a priority in the design of IoT devices, so that technologies contribute to improving quality of life without threatening users' rights and freedoms.

Existing international ethical standards for the Internet of Things (IoT) are aimed at ensuring security, privacy, and social responsibility in the use of this technology. Key initiatives include the IEEE standard "Ethically Aligned Design," which encompasses principles of data protection, security, transparency, and social responsibility. These principles facilitate the integration of ethics into the technology development process, ensuring that IoT not only performs technical functions but also complies with ethical norms, particularly regarding privacy protection and the promotion of fairness [24]. Additionally, the ISO/IEC 27001 and ISO/IEC 27018 standards define requirements for information security and personal data protection in cloud environments, which are directly relevant to IoT. They support the integration of cybersecurity and privacy considerations into IoT-related projects, ensuring that users' data are processed in accordance with international protection standards. The GDPR, in turn, establishes rules for the collection, storage, and processing of personal data, including for IoT devices, emphasising the importance of data minimisation and restricting access to authorised personnel only [25]. International organisations such as the United Nations (UN), OECD, the EU, and IEEE are actively engaged in developing ethical standards for IoT. Their initiatives include the creation of principles for transparency, data protection, security, and social responsibility, promoting the ethical development of IoT. For example, the EU has developed the "Ethical Guidelines for Artificial Intelligence and IoT," while the IEEE implements standards for ethics in the design of IoT devices, ensuring data security and privacy [26].

State regulation plays a key role in shaping ethical norms for IoT, ensuring that technologies comply with social, legal, and ethical requirements. In particular, Ukraine has enacted laws on personal data protection and cybersecurity, which are indirectly relevant to the application of IoT. Ethical approaches to IoT regulation require the integration of international standards, legal norms, and technical measures that guarantee security and privacy. The development and implementation of clear ethical standards will contribute to risk reduction and foster users' trust in IoT. Technologies should be aimed at improving quality of life while maintaining high standards of security and privacy.

Conclusions. The Internet of Things (IoT) today serves not only as a technological innovation but also as a catalyst for profound transformation in legal and social systems. Its integration into everyday life creates new opportunities for the development of the economy, healthcare, transportation, and education, while simultaneously intensifying concerns regarding security, privacy, and the protection of human rights. The main ethical challenges of IoT lie in algorithmic opacity, risks of data misuse, and the erosion of personal autonomy.

The experience of international researchers and regulatory initiatives (notably GDPR, ISO, IEEE, and OECD) demonstrates that the effective functioning of IoT is possible only under conditions of ethical responsibility, technical security, and legal certainty. Ethical standards, based on principles of transparency, fairness, and data governance, should become an integral element in the development and implementation of digital systems.

For Ukraine, a key task is the adaptation of international standards to the national context, the improvement of legislation on personal data protection and cybersecurity, as well as the development of a culture of digital ethics. The combination of legal regulation, educational programmes, and innovative technological solutions will enable the creation of a safe, human-centred digital environment in which the development of IoT does not conflict with fundamental human rights and freedoms.

It appears advisable to develop a unified ethical code for IoT device developers, as well as to strengthen inter-agency coordination in the field of cybersecurity. These measures will contribute to the building of user trust and ensure the sustainable development of Ukraine's digital ecosystem.

Bibliography:

1. Atzori L., Iera A., Morabito G. The Internet of Things: a survey. *Computer Networks.* 2010. Vol. 54, No. 15. P. 2787–2805.

2. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems.* 2013. Vol. 29, No. 7. P. 1645–1660.

3. Weber R. H., Studer E. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review.* 2016. Vol. 32, No. 5. P. 715–728.

4. Floridi L., Taddeo M. What is data ethics? *Philosophical Transactions of the Royal Society A.* 2016. Vol. 374.

5. Voigt P., Von dem Bussche A. *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Springer, 2017. 125 p.

6. ISO/IEC 29182: Framework for Sensor Networks. International Organization for Standardization. URL: https://standards.iteh.ai/catalog/standards/iso/iso-iec-29182 (дата звернення: 04.12.2024).

7. U.S. Congress. *IoT Cybersecurity Improvement Act.* 2020. URL: https://www.congress.gov/bill/116th-congress/house-bill/1668 (дата звернення: 04.12.2024).

8. OECD. *Recommendation of the Council on Artificial Intelligence.* 2019. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (дата звернення: 04.12.2024).

9. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for smart cities. *IEEE Internet of Things Journal.* 2014. Vol. 1, No. 1. P. 22–32.

10. Lee E. A., Seshia S. A. *Introduction to Embedded Systems: A Cyber-Physical Systems Approach.* MIT Press, 2017. 210 p.

11. Kang H. S. et al. Smart manufacturing: Past research, present findings, and future directions. *Int. J. of Precision Engineering and Manufacturing-Green Technology.* 2016. Vol. 3, No. 1. P. 111–128.

12. Grewal D., Roggeveen A. L., Nordfält J. The future of retailing. *Journal of Retailing.* 2017. Vol. 93, No. 1. P. 1–6.

13. Wolfert S., Ge L., Verdouw C., Bogaardt M. J. Big data in smart farming: A review. *Agricultural Systems.* 2017. Vol. 153. P. 69–80.

14. Weber R. H. Internet of Things: Privacy issues revisited. *Computer Law & Security Review.* 2015. Vol. 31, No. 5. P. 618–627.

15. Nissenbaum H. A contextual approach to privacy online. *Daedalus.* 2011. Vol. 140, No. 4. P. 32–48.

16. Ziegeldorf J. H., Morchon O. G., Wehrle K. Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks.* 2014. Vol. 7, No. 12. P. 2728–2742.

17. Cavoukian A. Privacy by design: Leadership, methods, and results. *Information and Privacy Commissioner of Ontario.* 2012. P. 175–202.

18. Tene O., Polonetsky J. Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property.* 2013. Vol. 11, No. 5. P. 239–273.

19. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks.* 2013. Vol. 57, No. 10. P. 2266–2279.

20. Cavoukian A. *Privacy by Design: The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario, Canada, 2011. 20 p. URL: https://www.sfu.ca/~palys/Cavoukian-2011-PrivacyByDesign-7FoundationalPrinciples.pdf (дата звернення: 04.12.2024).

21. Zuboff S. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology.* 2015. Vol. 30, No. 1. P. 75–89.

22. Borenstein J., Herkert J. R., Herkert L. The ethics of autonomous cars. *The Atlantic.* 2017. 110 p.

23. Cavoukian A. Privacy by design: Ethics and innovation in the age of the Internet of Things. *Information and Privacy Commissioner of Ontario.* 2014. 98 p.

24. IEEE. *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems.* IEEE Standards Association, 2019.

25. ISO/IEC 27001:2013; ISO/IEC 27018:2019. Information security management systems – Requirements and practices for protection of personally identifiable information. *International Organization for Standardization.*

26. European Commission. *Ethics Guidelines for Trustworthy AI and IoT.* 2020. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата звернення: 04.12.2024).

Горєлова В. Ю. ІНТЕРНЕТ РЕЧЕЙ І ЗАХИСТ ПРАВ ЛЮДИНИ: ЕТИЧНІ ТА ПРАВОВІ ВИКЛИКИ

У статті досліджується актуальне питання етики та права застосування інтернету речей (IoT), адже на сьогодні завдяки вдосконаленню сенсорних технологій, бездротового зв'язку та обробки даних, IoT еволюціонував від концепції до невід'ємного елементу сучасності, трансформуючи майже всі сфери людського буття (економіку, транспорт, охорону здоров'я та інші сфери, забезпечуючи автоматизацію процесів, оптимізацію ресурсів та розвиток «розумних» систем). У статті зазначені етичні аспекти використання IoT, зокрема, що пов'язані з прозорістю, справедливістю алгоритмів і дотриманням прав людини. Наголошено, що IoT стимулює прогрес штучного інтелекту, водночас масовий збір і зберігання даних створюють ризики порушення приватності людини, що потребує суворого правового регулювання. Актуальним питанням, таким чином, постає проблема «етики алгоритму», адже рішення на основі алгоритмів можуть бути упередженими, що потребує забезпечення прозорості та відповідальності людини за розробку технологій. Успішний розвиток IoT вимагає поєднання правового регулювання, технічних заходів, міжнародних стандартів та освітніх програм, що забезпечить безпечне та справедливе цифрове середовище. У статті наведено перелік проблем, які пов'язані із практичним застосуванням Інтернету-речей. Наголошено на необхідності розробки та впровадження етичних стандартів для Інтернету речей (IoT), що є важливим засобом забезпечення безпеки та захисту приватності людини в технологічному середовищі. У статті також розглянуті існуючі міжнародні етичні стандарти для Інтернету речей, що включають принципи захисту даних, безпеки, прозорості і відповідальності. Ці принципи сприяють інтеграції етики у процес розробки технологій, гарантуючи, що IoT не лише виконує технічні функції, а й відповідає етичним нормам, зокрема в аспектах захисту приватності людини.

Ключові слова: *інтернет речей, права людини, етика, конфіденційність, захист даних, кібербезпека, штучний інтелект, цифрове врядування, алгоритмічна прозорість, правове регулювання.*

Дата надходження статті: 25.10.2025
Дата прийняття статті: 20.11.2025
Опубліковано: 29.12.2025