UDC 340.1:343.98
DOI: 10.32518/sals2.2025.144

Соціально-правові студії. 2025. Т. 8, № 2
Social & Legal Studios. 2025. Vol. 8, No. 2

Legal regulation of the concept of "bot farms" as a response to manipulation of Internet users

Dina Dryzhakova*
Postgraduate Student
Taras Shevchenko National University of Kyiv
01033, 60 Volodymyrska Str., Kyiv, Ukraine
https://orcid.org/0009-0004-7585-5860

Abstract. The aim of this study was to develop a legislative definition of bot farms, thereby creating a basis for legal regulation of their use. The research employed the formal-legal and comparative-legal methods. The issue of bot farms is an emerging area of interest, prompted by increasing trends in the use of bots for purposes such as propaganda, fraud, and disinformation. Bots can be categorised into the following groups: one-day bots, classic bots, foreign bots, non-standard bots, and bots with complex behaviour. Furthermore, the study identified the purposes and areas of activity of bot farms, which include generating artificial traffic for financial gain, and conducting propaganda, disinformation, and the promotion of narratives and specific viewpoints within society. The study also examined the legislative regulation of the creation and operation of bot farms. A comparative analysis was conducted of the legal norms in European Union countries and the United States of America concerning the spread of artificial intelligence and the use of bots. The legal framework addressing liability for the use of bot farms for criminal purposes was reviewed. Relevant legislative proposals were analysed, the adoption of which could influence prosecution for disinformation and the deployment of criminal bots under martial law. Specific cases involving the exposure of bot farms were considered, along with the distinctive legal mechanisms used to counteract the activities of illegal bot farms, based on the experiences of foreign jurisdictions. The practical value of the study lies in the fact that it showed that Ukrainian legislation is not adapted to regulate the development of bot technologies, especially AI-based bots, and therefore needs to be revised by the legislator to combat the growing risks of disinformation and manipulation

Keywords: cybersecurity; artificial intelligence; criminal liability; social networks; fake information; propaganda

Introduction

Bot farms have emerged as a formidable instrument in the Russian Federation's information warfare strategy, specifically aimed at fracturing Ukrainian society, fomenting discord, and undermining international support for Ukraine. The predominant concentration of these bot farms was in Kyiv, Odessa, Lviv, and Zaporizhzhia, where they generated fraudulent identities and online groups to disseminate pro-Russian narratives and misinformation (Kostenko *et al.*, 2022). Bot farms, or "botnets", have been increasingly used to propagate unlawful material intended to destabilise public order in Ukraine, compromise its worldwide image, and diminish its diplomatic initiatives. This tendency has raised significant worries about cybersecurity since botnets are used for many illicit operations, including the manipulation of public opinion and the incitement of territorial alterations. In the wake of the Russian Federation's full-scale invasion, bot farms have attracted considerable scrutiny for their involvement in misinformation efforts aimed at both the general populace and state authorities. These bots have been deliberately used to undermine frontlines and occupied areas, jeopardise national security, and disseminate disinformation that diminishes the legitimacy of the Ukrainian government.

Globalisation and digitalisation have created novel strategies for influencing Internet users, making information security a vital component of national security (Tkachenko *et al.*, 2025). Since the start of the invasion, bot farms have become a vital component of Russia's hostile information operations. In 2022, the Security Service of Ukraine documented more than 4,500 cyberattacks, inflicting material damage equal to that of military operations (National Cybersecurity Coordination Centre, 2023). In 2025, the information landscape is a comprehensive battlefield, using sophisticated technologies and instruments. Ukrainian law currently lacks essential definitions for phrases such as "bot", "bot farm", and "cyberwarfare", underscoring the pressing need for comprehensive legal frameworks to tackle these modern issues.

As the concepts of bot and bot farm are relatively new, there is still insufficient research on the topic within the scientific community. The creation of large volumes of fake accounts is carried out with the intent to disseminate disinformation and pursue criminal objectives (Kravchuk *et*

Suggested Citation

Article's History: Received: 16.03.2025 Revised: 27.05.2025 Accepted: 25.06.2025

Dryzhakova, D. (2025). Legal regulation of the concept of "bot farms" as a response to manipulation of Internet users. *Social & Legal Studios*, 8(2), 144-154. doi: 10.32518/sals2.2025.144.

*Corresponding author

al., 2024). This practice can inflict harm both on individual citizens and on the state as a whole by spreading panic among the population, discrediting public authorities in the eyes of civil society, and damaging Ukraine's reputation on the international stage. H.M. Fadhil *et al.* (2022) introduced a machine learning approach for botnet identification. Their methodology used several classification algorithms to identify dangerous bots throughout networks, demonstrating how artificial intelligence may improve the efficacy of botnet detection. The model enhanced the accuracy and efficiency of botnet detection by the use of data mining methods, significantly impacting real-time network security management. P. Rataj (2025) offered a legal analysis of botnet defence, emphasising the convergence of cybersecurity and data protection legislation inside the European Union. He examined the legal frameworks inside the EU and their applicability to the protection of personal data in the context of botnet attacks. His study emphasised the difficulties of implementing cybersecurity legislation against botnet operators while upholding privacy rights and suggested enhancements to existing legal norms to tackle the escalating hazards presented by bots in digital contexts.

I. Mbona and J.H.P. Eloff (2022) used Benford's rule, a statistical notion often utilised in fraud detection, to discern irregular patterns in bot behaviour. Through the analysis of numerical data distribution in social media activity, they demonstrated the efficacy of this technique in identifying bots that diverge from typical user behaviours, so providing an additional instrument for botnet identification. In another study, I. Mbona and J.H.P. Eloff (2023) explored the categorisation of social media bots as either malicious or benign by means of semi-supervised machine learning methodologies. Their study focused on differentiating between malicious bots employed for disseminating misinformation and benign bots that may fulfil legal functions, such as customer service or automated content distribution. The research provided significant insights into the automation of dangerous bot identification on social media platforms using machine learning, aiding continuing efforts to counter digital manipulation and enhance online security.

Q. He *et al.* (2022) introduced an innovative method for detecting essential bots inside a botnet using the principles of gravitational law. The authors devised an approach that predicts the most important bots inside a network by applying this model to large-scale botnet infections. This strategy proved essential for identifying the most harmful bots during a botnet assault and is especially valuable for comprehending the dissemination and effects of botnets in real-time networks. J.M. Hodgins (2022) examined the use of social media bots to influence political outcomes. Author underscored the need for proactive steps and legislation to avert foreign meddling in democratic processes by concentrating on the role of bots in disseminating misinformation and undermining public opinion. This highlighted the increasing apprehension over the utilisation of bots for political manipulation, which was subsequently examined by T. Shadmy (2022), who proposed a legislative framework that reconciles free expression with the need to mitigate the dissemination of misinformation. Both works emphasised the necessity of legal measures to counteract the impacts of bots on public opinion and election integrity.

The aim of this study was to investigate and define the concept of bot farms in the context of cybersecurity measures, to develop a legislative definition informed by international experience, and to establish effective and relevant mechanisms for countering and preventing the use of bot farms in actions aimed at undermining Ukraine's national security. The objectives of the study include defining the concept of bots and bot farms, identifying the features of their operation, and examining the legal regulation of bot farm activities.

Materials and methods

In the course of conducting research to establish legal regulation in the field of cybersecurity and cyberspace, the following regulatory legal acts were studied: Code of Ukraine on Administrative Offenses (1996), Criminal Code of Ukraine (2001), Law of Ukraine No. 2657-XII "On Information" (1992), Law of Ukraine No. 2849-IX "On Media" (2022). Draft laws submitted for consideration to the Verkhovna Rada of Ukraine and designed to resolve gaps in liability for the criminal use of bots to harm national security were also used, namely: Draft Law of Ukraine No. 11115 "On Amendments to Certain Laws of Ukraine on Regulation of the Activities of Information Sharing Platforms Through Which Mass Information is Distributed" (2024), Draft Law of Ukraine No. 9223 "On Amendments to the Criminal and Criminal Procedure Codes of Ukraine Regarding the Establishment of Liability for Certain Actions Against the Foundations of National Security of Ukraine" (2023).

In order to fully and comprehensively study this topic, special methods of scientific knowledge were used, such as formal-legal, logical-legal, comparative-legal, and legal analysis methods. Using the formal-legal method, the regulatory framework regulating the US and European Union in the field of cybersecurity was studied, in particular, United States Senate Bill No. 1001 "Bots: Disclosure" (2018), BOTS Act (2016), Digital Services Act (2022) and the Code of Practice on Disinformation (2022) in order to determine the international practice of legal regulation of bots and bot farms. Using the legal dogmatic method, the concept of bot farms was defined in the context of their role in undermining information security.

At the initial stage of the study, the problem was identified. Also, the concept of a bot was clarified, their classification, features of creation and application were studied. The nature of bots and the procedure for their creation were studied. The next stage of the study was the determination of the regulatory and legal regulation of relations in the information environment, the establishment of levels of responsibility for offenses in cyberspace. After that, the legal mechanisms for regulating relations in the field of information security in the USA and the EU were studied. The Explanatory Note to the Draft Law of Ukraine No. 11115 (2024) was also studied regarding the detection and neutralisation of bot farms by special services in Ukraine since the beginning of the full-scale invasion of the Russian Federation. At the final stage of the study, the main directions for improving national legislation in the field of information security were identified.

Results

On average, Internet users spend more than two hours per day on social networks. The Internet has become a primary platform for communication on current events, culture, and politics, thereby increasing the significance of influencing what is seen and discussed online. Against this backdrop,

fake accounts – or bots – are present on every social network and exist in vast numbers. Bots are automated social media accounts created to perform specific actions and imitate the behaviour of genuine users. A botnet, or collection of such accounts, constitutes a network of bots that are programmed to execute identical tasks, unified by a shared objective and closely interconnected through mutual subscriptions (Makhortykh *et al.*, 2022).

Bots are, therefore, specially designed programmes that automatically perform the same actions as ordinary users. These bots may closely resemble legitimate accounts, complete with individual profiles and activity histories. They can post comments, publish content, and give likes on social networks. Bots are capable of fulfilling a broad range of functions, including entertainment, search, broadcasting, viewing, "liking", subscribing, and content publication (Shynkar & Levchenko, 2023). By nature, bots serve as a convenient interface for users interacting with various web services. As such, bots will continue to evolve technologically to better replicate human behaviour, particularly through the integration of artificial intelligence (Rawat *et al.*, 2023). The development of AI has enabled the generation of an unlimited number of synthetic images of non-existent individuals. AI-based bots can now comprehend natural language, analyse messages, and identify user needs. Furthermore, bot management software – referred to as "bot harvesters" – has become increasingly common, allowing the control of dozens or even hundreds of such accounts (Ye *et al.*, 2024). To influence public opinion, increase socio-psychological tension, and disseminate criminal disinformation, Russian special services actively deploy various informational and technical tools, including botnets, microblogs, and social networks, to undermine national information security. Social networks, in particular, are among the least protected mediums for countering the spread of false, anti-Ukrainian content (Dzyana & Dzyanyy, 2023).

Draft Law of Ukraine No. 9223 (2023) establishes legal provisions addressing the creation, acquisition, utilisation, or sale of accounts within automated information systems, electronic communication networks, and social media platforms. The legislation seeks to combat the spread of misinformation and the manipulation of public sentiment via these accounts. It specifically criminalises the usage of accounts that deliberately harbour false information about the user and are used to disseminate and spread incorrect data, including impersonating unverified persons or obstructing the actions of individuals and legal bodies. Actions detrimental to Ukraine's sovereignty, territorial integrity, defence capabilities, or national security are subject to sanctions that may include fines or restrictions on personal freedom. The proposed legislation further suggests that the Security Service of Ukraine be designated as the authority for the pre-trial investigation of certain offences. The legislation does not expressly define "bot farms", but its provisions include acts often linked to these operations; therefore, it seeks to mitigate misinformation and protect national security.

One of the state's principal responsibilities is to monitor information resources – such as online publications, social media platforms, blogs, forums, and personal pages – to identify those disseminating disinformation, inciting interethnic hatred, or promoting violence and intolerance, with the aim of blocking or disabling such resources (Kovalchuk, 2025). Recently, the use of bot farms to negatively impact Ukraine's information space has escalated significantly. Through fake accounts, information is disseminated that provokes panic among the population and discredits Ukrainian authorities both domestically and internationally (Zoltick & Maisel, 2023).

Criminal bot farms are being actively used by Russian propaganda to conduct information and psychological operations that adversely affect the psychological well-being of the Ukrainian population, influence public opinion about the military, and incite panic through the dissemination of propaganda, disinformation, and selective exaggeration or suppression of information. The most vulnerable to such influence are populations residing in the occupied territories and in the aggressor state itself; however, populations in EU countries and those living in Ukrainian-controlled areas are also subject to this negative impact. Representatives of the Russian special services utilise every available tool to deploy bots and bot farms, including platforms such as Facebook, Telegram, Viber, TikTok, and others, employing both technological and psychological strategies to intensify the impact of information on public perception. These activities are further facilitated by objective factors such as electricity outages across much of the occupied territories and the absence of Ukrainian telecommunications. Disinformation, in this context, refers to the public dissemination of unverified or knowingly false information that may adversely affect the exercise of citizens' legitimate rights and interests or threaten the national security of the state (Zelenov, 2024). "Fake" can be defined as false information presented through fabricated websites, impersonated social media profiles, or accounts mimicking other individuals. Bots, in turn, are specialised programmes that manage accounts and strategically post comments at specific times to maximise impact (Odilla, 2023). Bots are classified into several categories, as presented in Table 1.

Table 1. Bot classification

Name	Characteristic
Mayflies	Created automatically for a short period of time to perform single tasks. They are usually easy to detect because they create social media profiles without a photo or with an empty news feed.
Classic bots	Created for a longer period using scripts, the account filling is more complete, but images of people are never used
Alien bots	Correspond to the characteristics of classic bots, but the accounts have foreign names because they are created on foreign bot farms.
Non-template bots	These accounts match the characteristics of a real person. They are more complex, but there is no segmented audience that allows you to distinguish a bot from a real user.
Bots with complex behavior	Systems that are created using complex programs and that accurately mimic the behaviour of real people on social networks

Source: compiled by the author based on F. Odilla (2023)

Bot farms are understood as facilities where numerous bots are created with the intent of performing specific tasks. In essence, a bot farm is an operational base for individuals who generate large numbers of bots for the purpose of engaging in criminal activities (Harbinja *et al.*, 2023). Generally, bot farms function in two principal directions. The first involves the creation of bots to generate artificial traffic as a means of financial gain. The second concerns the execution of propaganda, dissemination of disinformation, and promotion of particular narratives and ideological viewpoints within society (Ahmad *et al.*, 2023). Upon examining this issue, several key reasons can be identified for the widespread use of bot farms in Ukraine. These include: the promotion of specific political views and narratives among the population; the shaping of public opinion in ways that serve the interests of the aggressor; fraudulent activities; and the theft of citizens' personal data by bots for subsequent misuse.

To combat and prevent the spread of disinformation, bot activity, and other manipulative information technologies within Ukraine, the Centre for Countering Disinformation under the National Security and Defence Council has been operational since its establishment on 11 March 2021. The Centre's primary functions include countering disinformation in the military domain, addressing crime in the information sphere, regulating information policy across all sectors, and engaging in scientific and technical initiatives. Its principal focus is on combating disinformation on the Internet and in the media. At the legislative level in Ukraine, the mechanism for countering disinformation – depending on the type of legal liability – involves three key areas, which are presented in Table 2.

Table 2. Sectors of legal regulation of disinformation

Sector	Regulatory and legal acts
Civil liability	Constitution of Ukraine (1996) Article 278 of the Civil Code of Ukraine (2003) Law of Ukraine No. 2657-XII "On Information" (1992) Law of Ukraine No. 2849-IX "On Media" (2022)
Administrative and legal liability	Article 173-1 of the Code of Ukraine on Administrative Offenses (1996)
Criminal liability	Articles 109, 110, 250, Section 2, Article 361 of the Criminal Code of Ukraine (2001)

Source: compiled by the author

It is evident that the existing legal framework for the prevention and prosecution of cyber offences remains incomplete and inadequate, as many innovative technologies operate outside the boundaries of current legislation. The existing legal framework in Ukraine, encompassing statutes such as the Code of Ukraine on Administrative Offenses (1996), the Criminal Code of Ukraine (2001), and Law No. 2657-XII "On Information" (1992), fails to sufficiently address the problem of bot farms and the utilisation of bots for disinformation and manipulation. These laws mostly address concerns such as fraud and privacy infringements, but they are deficient in explicit regulations governing the development, utilisation, and effects of automated systems, such as bots, that affect public opinion or compromise national security. The Criminal Code of Ukraine addresses offences such as fraud and identity theft, but it fails to identify or criminalise the use of bot farms in relation to political manipulation or misinformation operations.

Law of Ukraine No. 2657-XII "On Information" (1992) pertains to information dissemination but fails to delineate the regulation of automated or artificial intelligence-driven content development, which is essential to the functioning of bot farms. Moreover, Draft Law of Ukraine No. 9223 (2023) establishes penalties for actions undermining national security, such as disseminating false information through automated accounts. However, it does not have the comprehensiveness to address the intricate dynamics of contemporary bot farm operations, underscoring the necessity for more precise and updated legislation to combat these emerging threats.

In an effort to regulate legal relations within the information space, Draft Law of Ukraine No. 11115 (2024) has been submitted to the Verkhovna Rada. The authors of this draft law highlight that although the Law of Ukraine No. 2849-IX "On Media" (2022) defines information sharing platforms, their activities are not sufficiently regulated. Providers of such platforms are not classified as media entities, and as a result, they are not legally obliged to protect users' personal data, block illegal content, or hold channel owners accountable for the distribution of such content. The draft law proposes the following mechanisms for regulating the activities of information sharing platforms:

1. Defining providers of information sharing platforms as distinct entities within the media sector. This proposal conforms to the Law of Ukraine No. 2849-IX "On Media" (2022), which governs media operations in the digital realm. Classifying online platforms as media businesses would expand regulatory authority to include internet-based services that disseminate material to the public. This is legally robust since it incorporates these platforms inside the media system, mandating compliance with duties akin to those of conventional media outlets, hence enhancing responsibility in information dissemination.

2. Establishing that such platforms operate specific accounts or channels through which mass information is disseminated. This proposal aligns with Ukrainian legal standards on media regulation and information dissemination. It recognises the responsibility of platforms in regulating and overseeing content dissemination, assuring their accountability for the material disseminated via their channels. This provision aims to improve transparency and traceability of content sources in response to the proliferation of disinformation on digital platforms, along with Ukraine's current legislative framework regarding information security and transparency.

3. Introducing legislative obligations for information sharing platform providers by analogy with the existing requirements for video sharing platforms. The analogy to video sharing platforms, as shown in the Directive of the European Parliament and of the Council No. 2018/1808 (2018) and Ukraine's media rules, is a rational strategy for regulating online material dissemination. This encompasses

responsibilities such as content moderation, removal of unlawful information, and safeguarding user protection. This idea aims to eliminate regulatory discrepancies between traditional media and contemporary digital platforms by applying uniform standards to all information-sharing platforms. Nonetheless, there may be apprehensions over the balance between these responsibilities and the freedom of speech, as well as the potential for excessive control that hinders innovation and communication.

4. Requiring providers to appoint a representative in Ukraine for official communications. This requirement extends to all platforms registered within the European Union. This stipulation aligns with the Regulation of the European Parliament and of the Council No. 2022/2065 (2022) and the General Data Protection Regulation (2016), which necessitate that platforms appoint a designated representative in the territory of their operations. This idea might strengthen Ukraine's capacity to enforce its laws against international platforms and guarantee adherence to national norms. It may also enhance collaboration with global technology firms, particularly on content moderation and data security. This clause may provoke apprehensions about jurisdictional issues and the extraterritorial applicability of Ukrainian law, especially for platforms functioning inside the EU and other countries.

Additionally, a group of People's Deputies led by Georgy Mazurashu submitted Draft Law of Ukraine No. 9223 (2023). This draft proposes to supplement the Criminal Code of Ukraine (2001) with a new Article 114-3 "Use of accounts for the purpose of spreading false information or for influencing decision-making, actions, or omissions". The draft law was developed in alignment with Ukraine's Information Security Strategy, approved by Presidential Decree No. 685/2021 "On the Decision of the National Security and Defence Council of Ukraine "On the Information Security Strategy" (2021), to strengthen legal accountability for the dissemination of false information. Given that social media platform owners often respond inadequately to reports concerning fake profiles and pages involved in information attacks, it has become necessary to address the issue through legislative amendments. These changes aim to strengthen the role of specially authorised state bodies in their interactions with social media owners and administrators.

In order to counter and prevent the negative consequences caused by disinformation, law enforcement agencies in Ukraine have been actively engaged in dismantling bot farms. Since the beginning of the full-scale invasion, media outlets have regularly reported on the detection and shutdown of such operations. In 2022 alone, the Security Service of Ukraine (SBU) dismantled five bot farms comprising more than 100,000 fake accounts. These accounts were used to spread disinformation among the populations of Ternopil, Kharkiv, Poltava, Cherkasy, and Transcarpathia. The bot farms operated across various platforms, including some promoting the ideology of the aggressor state, which are banned in Ukraine. During searches, SBU representatives seized: 100 sets of GSM gateways; nearly 10,000 SIM cards from various mobile operators, used to conceal illegal activity; and computer equipment containing evidence of criminal operations. Criminal proceedings were initiated under Article 110 of the Criminal Code of Ukraine (2001) – Encroachment on the Territorial Integrity and Inviolability of Ukraine – which carries a penalty of up to 15 years' imprisonment (Cyber Police of Ukraine, 2023).

At the legislative level, there is currently no officially defined concept of "destructive content" or "destructive information"; however, related terms such as "harmful", "prohibited", and "illegal" information are commonly referenced. The significant increase in harmful content is a global issue. To address this, many countries – including Germany, the United Kingdom, France, Austria, and Turkey – have enacted relevant legislation aimed at regulating the online environment and fostering a safe informational space (Ivan & Manea, 2022). For instance, in 2020, the Turkish Parliament passed amendments to Law of Turkey No. 5651 "On Regulation of Broadcasts via Internet and Combating Crimes Committed by the Means of Such Publications" (2007) stricter control over social networks and the content disseminated on their platforms. This law, especially the need for social media corporations to establish official representative offices in Turkey, aids in combating bot farms by ensuring that platforms are directly responsible for the material they host and distribute (Gulati & Gulati, 2024). Encouraging Turkish individuals to oversee content-related complaints and evaluate compliance with national legislation facilitates the identification and elimination of detrimental or fraudulent activities, including the operations of bot farms that disseminate misinformation or influence public sentiment. The legislation's requirement for platforms to retain user data in Turkey improves law enforcement's capacity to monitor and investigate illegal activity, such as bot farm operations (Cantekin, 2020). Prospective sanctions, such as fines, advertising prohibitions, or traffic limitations, function as formidable deterrents, motivating platforms to establish more rigorous monitoring and moderation systems, therefore limiting the expansion of automated bots and their nefarious applications. Under this law, companies must establish official representative offices in Turkey to process content-related complaints.

The only piece of bot-specific legislation enacted in the United States to date is Bill of the Senate of the California No. 1001 "Bots: Disclosure" (2018). This law makes it unlawful to "use a bot to communicate or interact with another person online with the intent to mislead the other person as to the artificial identity of the person, to knowingly mislead the person as to the content of the communication, to induce the purchase or sale of goods or services in a commercial transaction, or to influence the outcome of an election". The legislation defines a "bot" as "an automated online account where all or substantially all of the actions or postings of that account are not the result of the actions of a real person". However, this law does not prohibit the use of all bots; rather, it stipulates that no liability arises if the use of bots is clearly disclosed (Kovac, 2022). The implementation of Bill of the Senate of the California No. 1001 (2018) is fundamentally based on transparency requirements. It stipulates that bots used for communication with the goal to deceive in commercial or political settings must be explicitly identified as non-human. Failure to provide such disclosure renders the bot user legally accountable. Enforcement procedures rely on consumer complaints, enquiries by governmental agencies, or civil litigation instead of proactive oversight. The law's restricted jurisdiction, applicable only to contacts with California citizens, coupled with the lack of a designated enforcement agency, has limited its practical efficacy and posed obstacles in achieving widespread compliance across platforms.

The BOTS Act (2016) is a legislative measure in the United States that pertains to the regulation of automated systems, including bots, within the wider digital landscape. This legislation explicitly criminalises the use of bots for deceptive purposes, especially in instances where they are employed to mislead individuals about their identity or the nature of the content they engage with. Often used for misinformation and propaganda, the Act offers a legal framework that may guide national legislation in Ukraine. Considering that the principal objective of bot farms often involves manipulating public perception through the artificial inflating of interaction or the promotion of certain ideological narratives, the Act's emphasis on bot transparency and disclosure corresponds with Ukraine's need to establish similar measures. This statute underscores the legal accountability for the conduct of automated accounts, serving as a crucial reference for Ukraine as it endeavours to enhance its legal frameworks on cybersecurity, information security and misinformation. The Act exemplifies the balance between public safety and freedom of speech by concentrating on the fraudulent applications of bots, rather than imposing sweeping restrictions on automated online interactions. This equilibrium is especially pertinent as Ukraine faces the deployment of bots by adversarial forces, including Russian agents, which are used not just to influence public sentiment but also to undermine national security.

Artificial Intelligence Act (2024) is a significant EU law designed to regulate the implementation of AI systems according to their risk assessment. The Act specifically targets high-risk AI applications, including those used for misinformation and manipulation via bot farms. The Act's stipulations about transparency, accountability, and human oversight of AI systems provide essential guidance for Ukrainian legislators aiming to govern AI-operated bot farms, which often use intricate algorithms to mimic human behaviour and evade discovery. The Act mandates that AI systems presenting substantial hazards to public safety or fundamental rights adhere to rigorous transparency and risk assessment standards. This precisely corresponds with Ukraine's need to establish more robust legal definitions and frameworks for AI technologies that facilitate bot farms, especially those used in cyberwarfare and psychological operations. Digital Service Act (2022) is an extensive regulatory framework aimed at fostering a safer online environment by ensuring platforms are responsible for the material they host and the algorithms they use. It requires corporate platforms to adopt steps to reduce the dissemination of illicit material, including misinformation, and to enforce enhanced transparency standards for targeted advertising and automated content moderation.

Digital Service Act (2022) is especially pertinent to bot farms since it imposes substantial responsibilities on digital platforms to vigilantly oversee and regulate the operations of automated systems. Regulation provides a framework for Ukraine to hold both platforms and bot operators responsible. The stipulations of the Regulation for transparent content control and the need for platforms to promptly address harmful material might be implemented in Ukrainian digital environments, where bots are used to distort political debate and disseminate disinformation. Furthermore, its focus on the significance of risk management strategies corresponds with the study's conclusions that bot farms pose a systemic danger to national security. The Code of Practice on Disinformation (2022), revised by the European Commission, fortifies prior initiatives to address online misinformation by broadening the range of parties engaged and intensifying the responsibilities of technology platforms. The Code mandates platforms to enhance transparency in political advertising, collaborate with fact-checkers, and guarantee that their algorithms do not facilitate the dissemination of incorrect information. This self-regulatory mechanism is essential for addressing the role of bots in amplifying misinformation. The Code of Practice on misinformation offers Ukraine a chance to foster enhanced cooperation among governmental bodies, technology firms, and civil society in combating bot-driven misinformation. By implementing analogous measures to those in the Code, Ukraine might mandate platforms to proactively address bot-driven misinformation and hold them responsible for adverse effects on national security.

A significant step in countering propaganda was the adoption of the Code of Practice on Disinformation by the European Commission (2018). This Code was the first self-regulatory document of its kind globally, designed to encourage companies to collaborate in addressing the challenge of disinformation. The Code was signed by representatives of leading online platforms, including Facebook, Google, Twitter, YouTube, and Microsoft (Pagallo *et al.*, 2023). By signing, these platforms committed to establishing systems for verifying the websites on which advertising is placed. They are also required to disclose specific actions taken and to grant independent third parties' access to their platforms to monitor compliance. Additionally, the Code calls for limitations on the misuse of advertising systems by distributors of disinformation. To ensure accountability, signatories must submit regular compliance reports. Notably, a strengthened version of the Code of Practice on Disinformation (2022) was signed and published. The updated Code includes a broader array of stakeholders, allowing a wider range of entities to contribute through commitments relevant to their specific fields. These commitments include demonetising the spread of disinformation, enhancing transparency in political advertising, reinforcing cooperation with fact-checkers, and facilitating researcher access to data. The Code's stipulations, such as eliminating misinformation, augmenting openness in political advertising, and fostering collaboration with fact-checkers, are crucial for mitigating the impact of bot farms, which often create fraudulent accounts to disseminate deceptive material or ideas. The Code enhances openness in political advertisements and facilitates improved data access for academics, hence enabling more efficient detection and monitoring of bot operations. Moreover, its focus on cooperation with fact-checkers facilitates the identification and refutation of false narratives disseminated by bot farms, so aiding in the reduction of their detrimental effects on democratic processes and public confidence. The Code establishes a systematic framework for social media platforms and other stakeholders to combat the detrimental actions of bot farms.

Established democratic states, like the United States and EU member states, refrain from imposing excessively stringent rules on bot use, opting instead to create frameworks that enable social media platform proprietors to adopt self-regulatory measures. This methodology is pertinent to Ukraine, as the legislative framework governing bot farms and cybersecurity is insufficiently established, lacking explicit regulations about the legal status of information-sharing platforms. To rectify these deficiencies, it is imperative to revise current legislation, including the Law of Ukraine No. 2657-XII

"On Information" (1992), by clearly defining and codifying concepts such as disinformation and harmful content. The existence of harmful material should provide the legal foundation for criminalising bot farm operations and ensuring accountability for those responsible. In light of these changes, information policy must prioritise measures that effectively combat the dissemination of illicit material. National security services are essential to this process, diligently monitoring media channels to detect and mitigate risks to national information security (Kharchenko *et al.*, 2017). Neutralising bot farms, particularly those generating substantial quantities of malicious bots, continues to be one of the most efficacious strategies in the fight against misinformation.

Currently, there is no standardised legal definition for bot farm, and the topic remains insufficiently explored. The expanding magnitude and influence of bot farms indicate that this problem is beyond economic interests and now represents a substantial danger to national and international security. Global strategies for bot regulation, especially those emphasising the need for distinct frameworks to tackle misinformation, election integrity, and speculation, vary in their breadth and aim. Some laws, such as those proposed in Ukraine aim primarily to address the impact of bots on elections and national security, while others, like the EU's strategy, include more extensive controls on information manipulation, including the economic and social ramifications of misinformation. Understanding these differences and the reasons behind them, whether to reduce speculation, ensure fair voting, or fight misinformation, can impact Ukraine's law-making efforts. Consequently, it is imperative for Ukraine to implement a comprehensive and clearly articulated regulatory framework that tackles the many concerns presented by bot farms, using international best practices while conforming to its national security objectives.

Discussion

The regulation of bot farms and misinformation is an urgent issue, with international frameworks and state law changes striving to address these difficulties. Draft Law of Ukraine No. 11115 (2024) and Draft Law of Ukraine No. 9223 (2023) are initiatives aimed at regulating bot farms, emphasising openness and responsibility for information-sharing platforms. Nevertheless, the present analysis concluded that these proposed legislations remain insufficient in handling the technological complexities of bot farms. K. Mezei and B. Szentgáli-Tóth (2023) observed that Ukrainian legislation aimed at combating misinformation inadequately addresses the rapidly advancing technology used by bot farms. This evaluation corresponded with the results of the present research, which indicated that Ukraine's legislative framework is deficient in explicit definitions and thorough regulations governing automated networks that influence public opinion.

Conversely, international frameworks like the Regulation of the European Parliament and of the Council No. 2016/679 (2016) and the Regulation (EU) 2022/2065 (2022) provided more comprehensive tools for regulating bot activity. These regulations emphasised platform accountability, openness, and data safeguarding, as articulated by L. Böck *et al.* (2022). The present analysis concured with these methodologies since they extended beyond the basic regulation of misinformation to address the foundational architecture of bot networks. Nonetheless, the proposed legislation in Ukraine did not adequately address these overarching issues, limiting its efficacy. Draft Law of Ukraine No. 11115 (2024) mandated that platforms designate representatives in Ukraine, so guaranteeing responsibility for detrimental information. Although this represented progress in enhancing openness, it fails to directly confront the technology aspects of bots and bot farms.

H.K. Gidey *et al.* (2023) examined the architectural issues faced by cognitive bots, highlighting their advanced skills that surpass traditional bot behaviour. Their results indicated that as bots advance with AI, they increasingly replicate human behaviour and decision-making processes, complicating detection and regulating efforts. This finding corresponded with the present analysis, which underscored the escalating danger presented by AI-driven bots and the need for legal frameworks to evolve in response to these breakthroughs.

The research conducted by F. Gallwitz and M. Kreil (2022) on botnet data monitoring under the Regulation of the European Parliament and of the Council No. 2016/679 (2016) advocated for a more proactive strategy in bot regulation, highlighting the need for data protection measures to mitigate automated manipulation. This differs from the Ukrainian strategy, which emphasises punitive actions over preventative and data-informed solutions. The current research agreed with F. Gallwitz and M. Kreil (2022), supporting the idea of adding better data security measures and active strategies to find and stop harmful bot activities.

O.M. Yaroshenko *et al.* (2022) examined the legal control of artificial intelligence, specifically in the context of labour law, in industrialised nations. They contended that AI, particularly regarding autonomous systems such as cognitive bots, presents considerable regulatory concerns. This aligned with the present study's assessment of Ukraine's proposed legislation, which inadequately addresses the implications of AI in bot operations. The authors underscored the need for legal frameworks that explicitly address the extensive implications of AI, including labour law and security issues. The present research agreed with this viewpoint, saying that AI's involvement in bot activities requires a transition from conventional legal frameworks to more extensive, technology-specific legislation. E. Aïmeur *et al.* (2023) emphasised the significance of collaboration with fact-checkers and improving platform transparency to address misinformation. Their research underscored the inadequacies of depending on voluntary self-regulation by platforms, indicating that more rigorous procedures are necessary. This result diverged from the more permissive stance seen in Draft Law of Ukraine No. 11115 (2024), which heavily depends on platform proprietors to manage content regulation internally. The present research advanced this argument by stating the need for a more complete regulatory framework that encompassed not just transparency but also explicit rules for bot detection and responsibility for automated content generation.

D. Gesmann-Nuissl and S. Meyer (2022) emphasised the consumer protection dimensions of bot regulation, contending that openness in bot use is crucial for protecting consumers from manipulation. Their results correspond with the present research, which advocates for the compulsory disclosure of bots to enhance public confidence. Nonetheless, the research challenged the proposed legislation for its lack of explicit restrictions regarding bot behaviour and its effects on users. This disparity highlights a substantial deficiency in Ukraine's strategy: while the legislation emphasised platform responsibilities, it neglected to address

the particular detriments inflicted by bots, including psychological manipulation and market distortion. J. Hutson *et al.* (2023) examined the difficulties of regulating developing technologies such as cognitive bots, which possess more advanced skills than conventional bots. This corresponds with the study's conclusions, emphasising the need for legislative changes that adapt to technological progress. The suggested laws in Ukraine do not effectively deal with these issues, and this study highlighted the need to clearly define and regulate advanced bot technologies, especially those using AI and machine learning, to keep the laws relevant as technology rapidly evolves.

While the present analysis recognised the significance of the proposed legislation in Ukraine, it determined that these regulations insufficiently tackle the intricacies of bot farm operations. The research endorsed the suggestions of global frameworks, promoting more extensive and technologically informed regulation. By synthesising global research results and emphasising transparency alongside the technological infrastructure of bots, Ukraine may establish a more robust legal framework to address misinformation and bot farm activities.

Conclusions

This research aimed to examine and provide a legislative definition for "bot farms", emphasising the establishment of a comprehensive legal framework for their regulation. The study effectively accomplished this objective by investigating the increasing use of bots in cybercrimes, including misinformation, propaganda, and fraud. It delineated the principal attributes of bot farms, including their ability to produce substantial quantities of fraudulent accounts for the propagation of modified information, and underscored the escalating danger these operations pose to national security, especially in relation to Ukraine's current crisis. The research, via comparative examination of foreign legal frameworks such as those of the European Union and the United States, underlined the need for analogous regulatory methods in Ukraine, particularly with the intricacies of automated systems like bots.

The study conducted a comprehensive analysis of current Ukrainian legislation and legal initiatives, including Draft Laws No. 9223 and No. 11115, and assessed potential enhancements to mitigate the rising danger of bot farms. It determined that, while certain advancements have occurred, substantial deficiencies persist in the proper definition and regulation of automated bot networks. Key results indicate the inadequacy of existing legal definitions of "bot" and "bot farm" in Ukraine's legal framework, with the absence of comprehensive regulations to oversee their utilisation in both local and foreign spheres. The research highlighted the difficulties in regulating misinformation while protecting freedom of speech, a worry reflected in international legislative initiatives such as the EU's Digital Services Act and California Senate Bill No. 1001.

This study revealed that Ukraine's legislative system needs to develop explicit definitions of bot farms and associated activities, while prioritising cybersecurity and national security. The research indicated that Ukraine must use more efficient strategies for identifying and dismantling bot farms, especially since they persist in influencing public perception and security. By using worldwide best practices and conforming to global cybersecurity standards, Ukraine may enhance the protection of its information space from dangerous bot activities. The results emphasised the essential need for legislative frameworks that address bot farms' activities while also improving openness in digital content distribution to avert abuse.

Future studies need to investigate the formulation of more precise legal definitions for bot farms and related technologies, together with the actual use of these concepts within Ukraine's legal framework. Subsequent research may concentrate on technical innovations in bot identification, including the use of AI and machine learning and their integration into the legal framework to improve enforcement. The ongoing global discussion about regulating artificial intelligence and its effects on digital manipulation needs close attention, as these developments will significantly impact future laws related to bot farm activities.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of interest

None.

References

[1] Ahmad, A., Waseem, M., Liang, P., Fahmideh, M., Aktar, M.S., & Mikkonen, T. (2023). Towards human-bot collaborative software architecting with ChatGPT. In *Proceedings of the 27th international conference on evaluation and assessment in software engineering* (pp. 279-285). New York: Association for Computing Machinery. doi: 10.1145/3593434.3593468.

[2] Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: A review. *Social Network Analysis and Mining*, 13(1), article number 30. doi: 10.1007/s13278-023-01028-5.

[3] Bill of the Senate of the California No. 1001 "Bots: Disclosure". (2018, September). Retrieved from https://calmatters.digitaldemocracy.org/bills/ca_201720180sb1001.

[4] Böck, L., Fejrskov, M., Demetzou, K., Karuppayah, S., Mühlhäuser, M., & Vasilomanolakis, E. (2022). Processing of botnet tracking data under the GDPR. *Computer Law & Security Review*, 45, article number 105652. doi: 10.1016/j.clsr.2021.105652.

[5] Cantekin, K. (2020). *Turkey: Parliament passes law imposing new obligations on social media companies*. Retrieved from https://www.loc.gov/item/global-legal-monitor/2020-08-06/turkey-parliament-passes-law-imposing-new-obligations-on-social-media-companies/.

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

[7] Code of Practice on Disinformation by the European Commission. (2018, April). Retrieved from https://ec.europa.eu/newsroom/dae/redirection/document/87534.

[8] Code of Practice on Disinformation. (2022, June). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[9] Code of Ukraine on Administrative Offenses. (1996, October). Retrieved from https://zakon.rada.gov.ua/go/80731-10.

[10] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/254%D0%BA/96-%D0%B2%D1%80#Text.
[11] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2341-14.
[12] Cyber Police of Ukraine. (2023). *Over 4,000 bots to discredit the Ukrainian Defense Forces and spread propaganda in favour of Russia: Vinnytsia Region police liquidated a large-scale bot farm*. Retrieved from https://cyberpolice.gov.ua/news/ponad--botiv-dlya-dyskredytacziyi-syl-oborony-ukrayiny-ta-poshyrennya-propagandy-na-koryst-rosiyi-policzejski-vinnychchyny-likviduvaly-masshtabnu-botofermu-7868/.
[13] Decree of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy". (2021, December). Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#n5.
[14] Directive of the European Parliament and of the Council No. 2018/1808 "On the Amending Directive No. 2010/13/EU "On the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities". (2018, November). Retrieved from http://data.europa.eu/eli/dir/2018/1808/oj.
[15] Draft Law of Ukraine No. 11115 "On Amendments to Certain Laws of Ukraine on Regulation of the Activities of Information Sharing Platforms Through Which Mass Information is Distributed". (2024, March). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/43884.
[16] Draft Law of Ukraine No. 9223 "On Amendments to the Criminal and Criminal Procedure Codes of Ukraine Regarding the Establishment of Liability for Certain Actions Against the Foundations of National Security of Ukraine". (2023, April). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/41788.
[17] Dzyana, H., & Dzyanyy, R. (2023). Public administrative activity in the conditions of contemporary uncertainty: Information and communication aspect. *Democratic Governance*, 16(1), 37-51. doi: 10.23939/dg2023.01.037.
[18] Explanatory Note to the Draft Law of Ukraine No. 11115 "On Amendments to Certain Laws of Ukraine on Regulation of the Activities of Information Sharing Platforms Through Which Mass Information is Distributed". (2024). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/pubFile/2274626.
[19] Fadhil, H.M., Makhool, N.Q., Hummady, M.M., & Dawood, Z.O. (2022). Machine learning-based information security model for botnet detection. *Journal of Cybersecurity and Information Management*, 9(1), 68-79. doi: 10.54216/JCIM.
[20] Gallwitz, F., & Kreil, M. (2022). Investigating the validity of botometer-based social bot studies. In F. Spezzano, A. Amaral, D. Ceolin, L. Fazio & E. Serra (Eds.), *Proceedings of the 4th multidisciplinary international symposium "Disinformation in open online media"* (pp. 63-78). Cham: Springer. doi: 10.1007/978-3-031-18253-2_5.
[21] Gesmann-Nuissl, D., & Meyer, S. (2022). Siri 2.0 – conversational commerce of social bots and the new law of obligations of data: Explorations for the benefit of consumer protection. *Robotics*, 11(6), article number 125. doi: 10.3390/robotics11060125.
[22] Gidey, H.K., Hillmann, P., Karcher, A., & Knoll, A. (2023). Towards cognitive bots: Architectural research challenges. In P. Hammer, M. Alirezaie & C. Strannegård (Eds.), *Proceedings of the 16th international conference "Artificial general intelligence"* (pp. 105-114). Cham: Springer. doi: 10.1007/978-3-031-33469-6_11.
[23] Gulati, J., & Gulati, G.C. (2024). Analysing the algorithm of zoombombing as a cybercrime in digital era: Legal risks and challenges. *Journal of Electrical Systems*, 20(4), 2445-2452. doi: 10.52783/jes.2751.
[24] Harbinja, E., Edwards, L., & McVey, M. (2023). Governing ghostbots. *Computer Law & Security Review*, 48, article number 105791. doi: 10.1016/j.clsr.2023.105791.
[25] He, Q., Wang, L., Cui, L., Yang, L., & Luo, B. (2022). Gravity-law based critical bots identification in large-scale heterogeneous bot infection network. *Electronics*, 11(11), 1771. doi: 10.3390/electronics11111771.
[26] Hodgins, J.M. (2022). Countering Russian subversion during federal elections in Canada in the era of social media and fake news. *ITSS Verona Magazine*, 1(1).
[27] Hutson, J., Banerjee, G., Kshetri, N., Odenwald, K., & Ratican, J. (2023). Architecting the metaverse: Blockchain and the financial and legal regulatory challenges of virtual real estate. *Journal of Intelligent Learning Systems and Applications*, 15(1), 1-23. doi: 10.4236/jilsa.2023.151001.
[28] Ivan, D.L., & Manea, T. (2022). AI use in criminal matters as permitted under EU law and as needed to safeguard the essence of fundamental rights. *International Journal of Law in Changing World*, 1(1), 17-32. doi: 10.54934/ijlcw.v1i1.15.
[29] Kharchenko, V., Ponochovnyi, Y., Qahtan, A.-S.M., & Boyarchuk, A. (2017). Security and availability models for smart building automation systems. *International Journal of Computing*, 16(4), 194-202. doi: 10.47839/ijc.16.4.907.
[30] Kostenko, O., Jaynes, T., Zhuravlov, D., Dniprov, O., & Usenko, Y. (2022). Problems of using autonomous military AI against the background of Russia's military aggression against Ukraine. *Baltic Journal of Legal and Social Sciences*, 4, 131-145. doi: 10.30525/2592-8813-2022-4-16.
[31] Kovac, M. (2022). Autonomous artificial intelligence and uncontemplated hazards: Towards the optimal regulatory framework. *European Journal of Risk Regulation*, 13(1), 94-113. doi: 10.1017/err.2021.28.
[32] Kovalchuk, D. (2025). Utilising large language models for automated real-time cyber threat analysis. *Bulletin of Cherkasy State Technological University*, 30(1), 48-58. doi: 10.62660/bcstu/1.2025.48.
[33] Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., & Ukhach, V. (2024). Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security*, 2(2), 28-38. doi: 10.62566/lps/2.2024.28.
[34] Law of the Turkey No. 5651 "On Regulation of Broadcasts via Internet and Combating Crimes Committed by the Means of Such Publications". (2007, May). Retrieved from https://mbkaya.com/turkish-internet-law/.
[35] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2657-12#Text.
[36] Law of Ukraine No. 2849-IX "On Media". (2022, December). Retrieved from https://zakon.rada.gov.ua/go/2849-20.

[37] Makhortykh, M., Urman, A., Münch, F.V., Heldt, A., Dreyer, S., & Kettemann, M.C. (2022). Not all who are bots are evil: A cross-platform analysis of automated agent governance. *New Media & Society*, 24(4), 964-981. doi: 10.1177/14614448221079035.
[38] Mbona, I., & Eloff, J.H.P. (2022). Feature selection using Benford's law to support detection of malicious social media bots. *Information Sciences*, 582, 369-381. doi: 10.1016/j.ins.2021.09.038.
[39] Mbona, I., & Eloff, J.H.P. (2023). Classifying social media bots as malicious or benign using semi-supervised machine learning. *Journal of Cybersecurity*, 9(1), article number tyac015. doi: 10.1093/cybsec/tyac015.
[40] Mezei, K., & Szentgáli-Tóth, B. (2023). Some comments on the legal regulation on misinformation and cyber attacks conducted through online platforms. *Lexonomica*, 15(1), 33-52. doi: 10.18690/lexonomica.15.1.33-52.2023.
[41] Odilla, F. (2023). Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. *Crime, Law and Social Change*, 80(4), 353-396. doi: 10.1007/s10611-023-10091-0.
[42] Pagallo, U., Bassi, E., & Durante, M. (2023). The normative challenges of AI in outer space: Law, ethics, and the realignment of terrestrial standards. *Philosophy & Technology*, 36, article number 23. doi: 10.1007/s13347-023-00626-7.
[43] Public Law of the United States of America No. 114-274 "BOTS Act 2016". (2016, September). Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/3183.
[44] Rataj, P. (2025). Botnet defense under EU data protection law. *Computer Law & Security Review*, 56, article number 106080. doi: 10.1016/j.clsr.2024.106080.
[45] Rawat, R., Oki, O., Chakrawarti, R.K., Adekunle, T.S., Lukose, J.M., & Ajagbe, S.A. (2023). Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments. *Informatica*, 47(9), 51-62. doi: 10.31449/inf.v46i9.4538.
[46] Regulation of the European Parliament and of the Council No. 2016/679 "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, April). Retrieved from http://data.europa.eu/eli/reg/2016/679/oj.
[47] Regulation of the European Parliament and of the Council No. 2022/2065 "On a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)". (2022, October). Retrieved from http://data.europa.eu/eli/reg/2022/2065/oj.
[48] Shadmy, T. (2022). Content traffic regulation: A democratic framework for addressing misinformation. *Jurimetrics Journal*, 63.
[49] Shynkar, T., & Levchenko, T. (2023). Manipulative technologies in terms of information security. *Society. Document. Communication*, 8(2), 270-286. doi: 10.31470/2518-7600-2023-19-270-286.
[50] Tkachenko, O., Chechet, A., Chernykh, M., Bunas, S., & Jatkiewicz, P. (2025). Scalable front-end architecture: Building for growth and sustainability. *Informatica (Slovenia)*, 49(1), 137-150. doi: 10.31449/inf.v49i1.6304.
[51] Yaroshenko, O.M., Melnychuk, N.O., Zhygalkin, I.P., Silchenko, S.O., & Zaika, D.I. (2022). Problems of legal regulation of artificial intelligence in labour law of developed countries. *Informatologia*, 55(1-2), 160-169. doi: 10.32914/i.55.1-2.13.
[52] Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective. *Telecommunications Policy*, 48(10), article number 102851. doi: 10.1016/j.telpol.2024.102851.
[53] Zelenov, D. (2024). Psychological mechanisms of influence of disinformation and fake news on the formation of public opinion on Ukrainian European integration: Analysis of Russian propaganda. *Scientific Studios on Social and Political Psychology*, 30(2), 25-35. doi: 10.61727/sssppj/2.2024.25.
[54] Zoltick, M.M., & Maisel, J.B. (2023). Societal impacts: Legal, regulatory and ethical considerations for the digital twin. In N. Crespi, A.T. Drobot & R. Minerva (Eds.), *The digital twin* (pp. 1167-1200). Cham: Springer. doi: 10.1007/978-3-031-21343-4 37.

Правове регулювання поняття «бот-ферми» як відповідь на маніпулювання користувачами Інтернету

Діна Дрижакова
Аспірант
Київський національний університет імені Тараса Шевченка
01033, вул. Володимирська, 60, м. Київ, Україна
https://orcid.org/0009-0004-7585-5860

Анотація. Метою цього дослідження була розробка законодавчого визначення поняття бот-ферм, чим створити основу для правового регулювання їх використання. У дослідженні використовувалися формально- та порівняльно-правовий методи. Питання бот-ферм є новою сферою інтересів, викликаною зростаючими тенденціями використання ботів для таких цілей, як пропаганда, шахрайство та дезінформація. Ботів можна розділити на такі групи: одноденні боти, класичні боти, іноземні боти, нестандартні боти та боти зі складною поведінкою. Крім того, у дослідженні було визначено цілі та сфери діяльності бот-ферм, які включають генерування штучного трафіку для отримання фінансової вигоди, а також проведення пропаганди, дезінформації та просування наративів і певних точок зору в суспільстві. У дослідженні також розглянуто законодавче регулювання створення та функціонування бот-ферм. Було проведено порівняльний аналіз правових норм країн Європейського Союзу та Сполучених Штатів Америки щодо поширення штучного інтелекту та використання ботів. Було розглянуто правову базу, що регулює відповідальність за використання бот-ферм у злочинних цілях. Було проаналізовано відповідні законодавчі пропозиції, прийняття яких може вплинути на переслідування за дезінформацію та використання злочинних ботів в умовах воєнного стану. Було розглянуто конкретні випадки, пов'язані з викриттям бот-ферм, а також особливості правових механізмів, що використовуються для протидії діяльності незаконних бот-ферм, на основі досвіду іноземних юрисдикцій. Практична цінність дослідження полягає в тому, що воно показало, що українське законодавство не адаптоване для регулювання розвитку бот-технологій, особливо ботів на основі штучного інтелекту, у зв'язку з чим існує необхідність його перегляду законодавцем для боротьби зі зростаючими ризиками дезінформації та маніпуляцій

Ключові слова: кібербезпека; штучний інтелект; кримінальна відповідальність; соціальні мережі; фейкова інформація; пропаганда