SOCIAL, LEGAL, AND TECHNOLOGICAL DETERMINANTS OF THE FORMATION OF PROFESSIONAL CONFIDENTIALITY IN THE DIGITAL AGE: A GENERAL-THEORETICAL APPROACH

Taras Pashchuk,
Senior Lecturer at the Department of Law and Finance
Separate Structural Subdivision of the Higher Education
Institution "Open International University of Human Development
'Ukraine'" Lutsk Institute of Human Development
Attorney-at-Law

ORCID: https://orcid.org/0000-0001-9585-492X
E-mail: ptv1215@gmail.com

Abstract. TThis article presents a general theoretical study of the social, legal, and technological determinants shaping the regime of professional secrecy in the context of society's digital transformation. It argues that the rapid development of information technologies, cloud services, cross-border data processing, digital platforms, and artificial intelligence systems is significantly altering the nature of social relations related to the storage and use of professionally confidential information, which requires a rethinking of traditional doctrinal approaches to the content of professional secrecy and the mechanisms for its legal protection.

The author argues that modern risks of confidentiality breaches are linked not only to the unlawful conduct of individual actors but also to the functioning of digital infrastructure, algorithmic information processing systems, generative artificial intelligence, software, and cross-border digital services. In this regard, the author proposes viewing professional secrecy not exclusively as an obligation to maintain the confidentiality of information, but as a multi-level legal regime for controlling its processing throughout its entire lifecycle.

The authors formulate an original approach to understanding information control as a legally guaranteed ability to define the scope of entities, digital services, and technological processes permitted access to professionally confidential information, while ensuring the traceability of operations involving its use. The paper argues for the advisability of legally enshrining the principle of digital professional autonomy, which will ensure the right of a professional to independently determine the admissibility of using digital technologies when working with confidential information, provided that cybersecurity requirements, data localization, algorithmic transparency, and cryptographic protection are observed.

At the same time, based on a critical analysis of Ukrainian and European legal regulations, it has been established that improving Ukrainian legislation should be carried out by modernizing sector-specific regimes of professional secrecy, taking into account contemporary technological challenges and the provisions of European legislation in the field of personal data protection and the regulation of artificial intelligence. The author concludes that digital infrastructure and artificial intelligence systems should be regarded as independent sources of legal risks requiring special legal regulation, and that the protection of professional secrecy must be based on a combination of legal, organizational, and technological safeguards for the protection of confidential information.

Key words: professional secrecy; digitalization; artificial intelligence; confidential information; information control; digital professional autonomy; information security; personal data; legal regulation; digital technologies.

Introduction. The comprehensive digitization of social relations, which over the past decade has transformed the ways in which information is created, processed, and disseminated, has necessitated a fundamental reevaluation of traditional conceptions regarding the nature and functional purpose of professional secrecy as a special legal regime restricting access to certain information. Thus, while in an industrial society the risks of confidentiality breaches were largely associated with unlawful actions by individual actors, today the sources of threats are increasingly algorithmic data processing systems, cloud services, machine learning technologies, cross-border information flows, and digital platforms, whose activities effectively extend beyond the boundaries of the traditional jurisdictional model of legal regulation. In fact, professional secrecy today finds itself at the center of a fundamental conflict between the constitutional value of information privacy and the economic logic of the digital environment, within which personal and work-related information is viewed as a resource for technological development, predictive analytics, and the functioning of artificial intelligence (hereinafter "AI").

The relevance of this issue is confirmed by statistical data from international institutions and regulatory bodies. In particular, according to the GDPR Enforcement Tracker, as of March 2026, more than 2,685 cases of sanctions for violations of personal data protection laws had been recorded in European Union member states, and the total amount of fines exceeded 6.1 billion euros [1]. At the same time, a significant portion of these proceedings concerned the failure to adequately ensure the confidentiality of information to which individuals had access in the course of their professional activities. In turn, according to DLA Piper's annual report, an average of 443 data breach reports were recorded daily in Europe throughout 2025, a 22% increase compared to the previous year [1]. Overall, this trend points to the systemic nature of the information security crisis and highlights the inadequacy of traditional legal mechanisms for protecting confidential information in the digital environment.

The heightened attention to this issue stems primarily from its impact on those areas of social relations

in which professional confidentiality serves as a legal guarantee of an individual's right to privacy. For example, according to the IBM Cost of a Data Breach Report 2024, the average cost of a single data breach in the healthcare sector was $9.77 million, the highest figure among all sectors of public activity [2]. The published statistical data clearly show that the unlawful disclosure of information is no longer merely an ethical or disciplinary issue; it has evolved into a factor capable of affecting the functioning of entire sectors of public administration, the justice system, healthcare, and national security. Therefore, in light of the above, the confidentiality of professional information should be understood as an independent component of an individual's informational sovereignty, the violation of which has consequences far broader than the mere disclosure of information [3, p. 193].

The implementation of AI systems in areas traditionally associated with the protection of professional secrecy also requires further scientific study. Modern generative models are used in the preparation of legal documents, medical diagnostics, audits, the operations of financial institutions, and public administration. However, practice shows that there are cases where confidential data effectively becomes part of the datasets used to train algorithms. According to research by IBM and the Ponemon Institute, in 2025, approximately 20% of reported cybersecurity incidents were linked to the use of unauthorized AI tools ("shadow AI"), and the average additional financial loss resulting from such breaches exceeded $670,000. Notably, only a small fraction of organizations had adequate mechanisms in place to control AI access to confidential information [4].

Equally telling are specific real-world cases that already highlight the inadequacy of established approaches to protecting professional confidentiality. In particular, as part of proceedings against the Royal Free London NHS Foundation Trust, the UK data protection regulator established that medical information on approximately 1.6 million patients had been transferred to DeepMind for the purpose of training medical prediction algorithms without properly informing the data subjects. Despite the purported public benefit of such a project, this situation revealed a fundamental conflict between technological efficiency and an individual's right to medical confidentiality [5; 6, p. 359]. Similar issues were the subject of legal review in France during the operation of the Health Data Hub platform, where the Conseil d'État and the CNIL examined the balance between the public interest in the use of large sets of medical data and the guarantees of medical confidentiality, as well as the requirements of the GDPR [7]. In Germany, the legislature's response to similar technological challenges was the reform of §203 StGB, which legally regulated the possibility of involving IT providers and other third parties in the processing of professionally confidential information, provided that specific safeguards for its protection are observed [8]. In fact, the examples cited demonstrate that the source of risk is not an individual offender, but primarily the operational model of the digital environment.

Furthermore, contrary to traditional concepts that link professional secrecy exclusively to the duty of confidentiality of an authorized person, the modern legal reality requires a broader doctrinal approach. In this regard, it is worth noting that the confidentiality of information is ensured not only by the conduct of a lawyer, a doctor, a notary, or an auditor, but also by the activities of software developers, database administrators, operators of electronic platforms, cloud service providers, and entities that are not, in fact, in traditional professional-fiduciary legal relationships with the holder of the relevant information. Consequently, the classical concepts of professional secrecy, formed back in the days of an analog society, are only limitedly capable of responding to modern technological challenges.

Focusing on the theoretical and legal dimensions of the issue under study, we must address the question of how the regime of professional secrecy itself is determined. Academic literature traditionally analyzes it through the prism of the sectoral affiliation of the relevant legal relationships [9, pp. 132–136], while social and technological factors remain insufficiently explored. At the same time, contemporary processes of digital transformation convincingly demonstrate that the nature of professional secrecy is determined not so much by the legal nature of the information as by a combination of external factors that give rise to the need to protect it. Clearly, therefore, social changes, the transformation of trust models, the proliferation of digital platforms, the algorithmization of decision-making, and the development of AI must be considered as independent determinants shaping the modern regime of professional secrecy.

The purpose of this article is to identify the socio-legal and technological determinants shaping the regime of professional secrecy in the context of digitalization, to critically re-examine existing doctrinal approaches to its content, and to develop conceptual foundations for modernizing the legal regulation of confidential professional information in the context of AI development, European digital policy, constitutional guarantees of privacy, and contemporary security challenges.

Research methods. The methodological foundation of this study consists of a combination of general scientific and specialized legal methods of inquiry, the use of which enabled a comprehensive analysis of the transformation of the legal regime governing professional secrecy in the context of digitalization. In particular, the dialectical method made it possible to trace the evolution of scientific concepts regarding professional secrecy under the influence of digital technologies and the development of AI systems. The formal-legal method was applied in analyzing the provisions of the Constitution of Ukraine, the Civil Code of Ukraine, and Ukrainian laws governing information relations, personal data protection, cybersecurity, and the use of cloud services, as well as relevant European Union legislation, primarily the GDPR and the AI Act. In turn, the comparative legal method was used to compare the Ukrainian and European models of legal regulation of professional secrecy in the context of digital transformation, as well as to identify opportunities for adapting certain foreign approaches to the national legal system. The systemic-structural method made it possible to

identify the interrelationship between the institution of professional secrecy, the personal data protection regime, information security, and the legal regulation of AI systems. Using legal modeling methods, practical scenarios were formulated that reflect the current risks of using generative AI when working with professionally confidential information, and original approaches were proposed to improve the mechanisms for its legal protection.

Results. The study demonstrates that the traditional understanding of professional secrecy - as the duty of a person who has received confidential information in the course of their professional activities to maintain its confidentiality - does not fully correspond to the current conditions of digitalization. It has been established that the source of the risk of confidentiality breaches is increasingly not the behavior of an individual entity, but rather the specific features of the functioning of digital infrastructure, cloud services, cross-border information systems, and generative AI.

It is proposed to view professional secrecy as a multi-level legal regime for controlling confidential information throughout its entire processing lifecycle. A doctrinal understanding of information control is formulated as a legally guaranteed ability to determine the permissible scope of entities, digital services, and technological processes that may access professionally confidential information.

The paper argues for the advisability of legally enshrining the principle of digital professional autonomy, according to which a professional must have a legally guaranteed right to determine the permissibility of using digital technologies when working with confidential information, provided that requirements for cybersecurity, algorithmic transparency, data localization, and cryptographic protection are met. It is demonstrated that the modernization of Ukrainian legislation should be carried out not by creating a universal law on professional secrecy, but by adapting specialized sector-specific regimes to contemporary digital challenges, taking into account the provisions of European legislation in the field of data protection and AI regulation.

Discussion. Professional secrecy in modern legal doctrine is traditionally defined as a special legal regime governing confidential information, access to which a person obtains exclusively in connection with the performance of professional activities and is determined by the existence of a special relationship of trust between the holder of the information and the party seeking the relevant assistance [10, pp. 53–54]. This understanding remained sufficient for a long time for the functioning of an analog model of society, when the vast majority of information flows were under the de facto control of the person legally obligated not to disclose such information. However, as noted earlier, the digitization of public administration, the rapid proliferation of cloud services, the use of generative AI models, and the development of cross-border information systems and automated data processing platforms have revealed a fundamentally different nature of modern threats. In fact, confidential information increasingly leaves the sphere of a specialist's actual control even before it is directly used, passing through a significant number of software, technical, and organizational intermediaries, whose legal status is defined only fragmentarily by current Ukrainian legislation.

In this regard, it is worth noting that Ukrainian lawmakers continue to rely on the established model of professional secrecy, which is centered primarily on the conduct of a specific individual. This approach is evident in the provisions of the Constitution of Ukraine dated June 28, 1996, No. 254k/96-VR [11], the Civil Code of Ukraine dated January 16, 2003, No. 435-IV [12], the Law of Ukraine "On Information" dated October 2, 1992, No. 2657-XII [13], the Law of Ukraine "On the Protection of Personal Data" dated June 1, 2010, No. 2297-VI [14], procedural legislation, and special regulatory acts that establish specific types of professional secrecy. Despite the diversity of legal frameworks, what they have in common is the presumption that the primary source of risk is the person who obtained confidential information while performing professional duties. It is around such a person that disciplinary, civil, administrative, or criminal liability is established, whereas software environments, digital platforms, AI systems, or operators of international cloud infrastructure effectively remain outside the scope of the traditional framework of professional liability.

Given the current state of digital transformation, this regulatory approach no longer reflects the nature of social relations. The reason lies primarily in the transformation of the very mechanism of information circulation. Whereas attorney-client, medical, or notarial confidentiality previously existed primarily in physical form, confidential information is now automatically replicated in backup copies, event logs, data centers, backup systems, cybersecurity measures, remote administration services, third-party software products, and information databases used to power machine learning algorithms. Consequently, a specialist's actual control over information is significantly reduced, although the legal obligation to ensure its non-disclosure continues to rest solely with the specialist.

This contradiction is particularly evident in the practical application of the Law of Ukraine "On the Protection of Personal Data" [14]. Formally, the owner of a personal data database is responsible for ensuring proper processing procedures; however, the actual operation of modern information systems involves a significant number of data processors, cloud providers, software vendors, AI operators, international data processing centers, and other entities, whose activities also affect the level of confidentiality of professional information. Consequently, there are cases in which the legal obligation and the actual ability to ensure its fulfillment are distributed among various participants in the digital environment, even though the law continues to assume their formal unity.

In light of this, we believe that modern professional secrecy should not be viewed exclusively as a duty of confidentiality on the part of a member of the relevant profession. Rather, it is appropriate to define it as a multi-level legal regime for controlling confidential

information throughout its entire life cycle - from the moment of receipt to its final destruction, archiving, or anonymization. The proposed definition much better reflects the true nature of digital information processes, as the focus of legal analysis shifts from the behavior of an individual to the entire system of legal, organizational, and technological safeguards for confidentiality.

Rejecting the traditional understanding of professional secrecy, some foreign authors propose effectively equating it with the general regime for the protection of personal data [e.g., D. Erdos [15]]. However, such an approach appears somewhat controversial. Personal data constitutes only one component of confidential information. Attorney-client privilege, bank secrecy, the confidentiality of pretrial investigations, and auditor or notary confidentiality encompass a significant volume of information that may not fall under the category of personal data at all, yet requires a significantly higher level of legal protection. Clearly, therefore, the mechanical extension of personal data legislation to all types of professional secrecy does not eliminate existing gaps; on the contrary, it creates additional conflicts between sector-specific laws.

Another illustrative example is a practical scenario that could be simulated today in almost any law firm. Suppose, while preparing a procedural document, an attorney uses a generative AI system, inputting into it materials from criminal proceedings, the client's personal data, information about witnesses, medical records, and the results of forensic examinations. From the perspective of national legislation, there may be no breach of attorney-client privilege if the relevant information has not become known to third parties. However, from a technological standpoint, such data has already left the controlled professional environment and been transferred to an external digital service provider, whose operational algorithms remain unknown to the user. This raises a perfectly logical question: Can professional secrecy be considered preserved simply because the actual leak of information has not yet been confirmed? In our view, a negative answer is more consistent with the modern nature of information security, since the transfer of confidential information to an uncontrolled digital environment already creates a legally significant risk of a breach of professional secrecy.

At the same time, European legislation is gradually shifting the focus from responding to violations that have already occurred to preventing risks from arising. The General Data Protection Regulation (GDPR) is built around the principles of accountability, data minimization, purpose limitation, and data protection by default [16]. The European Union's AI Act, in turn, establishes specific requirements regarding information confidentiality, cybersecurity, risk management, human oversight, and transparency in the operation of AI systems, particularly when used in areas related to the exercise of public authority or the realization of fundamental human rights [17].

It should be noted that a fundamental flaw in the current legal regulation of professional secrecy appears to be the preservation of an anthropocentric model of legal liability, under which a breach of confidentiality is presumed to be the result of wrongful conduct by a specific individual. Taking the above into account, we conclude that the category of professional secrecy should be viewed through the lens of the doctrine of information control. By the latter, in our view, we mean the legally guaranteed ability to define the scope of entities, technological processes, and digital services permitted access to confidential information, while ensuring the constant traceability of any operation involving such information. In fact, the lack of a regulatory framework for this approach today gives rise to the greatest number of conflicts when using generative AI. The law regulates an individual's access to information but provides almost no guidance on the permissibility of access by software, autonomous agents, machine learning algorithms, or systems capable of performing further analytical processing of confidential data sets.

Incidentally, this issue has already been addressed at the level of European Union law. The aforementioned Regulation (EU) 2024/1689 (AI Act [17]) introduced a risk-based regulatory framework for AI systems, within which what matters most is not so much the nature of the software product as the consequences of its use for fundamental human rights, information security, and the functioning of state institutions. In light of the above, provisions regarding mandatory risk management, documentation of the lifecycle of high-risk systems, ensuring human oversight, maintaining logs of algorithm operations, and conducting continuous monitoring after the system is put into operation are of significant importance. Referring to these provisions, it should be noted that the European Union legislature has effectively recognized a technological system as an independent source of legal risk, whereas the Ukrainian model continues to focus primarily on the behavior of natural persons.

At the same time, unconditionally replicating the European experience can hardly be considered justified. The reason lies, first and foremost, in differences in the structure of national legislation. The Ukrainian model of professional secrecy was developed based on the principle of sectoral autonomy, as a result of which medical, legal, banking, notarial, and auditing secrecy are regulated by different normative acts, employ different conceptual frameworks, and entail distinct legal consequences for breaches of confidentiality. Consequently, the implementation of certain provisions of the AI Act is possible only if they are adapted to each specific regime of professional secrecy. In turn, an attempt to create a universal law on professional secrecy, in our opinion, would have the opposite effect, as it would inevitably lead to duplication of existing legal frameworks and give rise to numerous conflicts with sector-specific legislation.

In the context of this study, it is also appropriate to address the criminal law dimension of this

issue. In particular, Article 182 of the Criminal Code of Ukraine dated April 5, 2001, No. 2341-III, provides for liability for violating the inviolability of private life [18], while certain types of professional secrecy are protected by special provisions of criminal law. Nevertheless, an analysis of the provisions of the relevant articles leads to the conclusion that their structure is focused primarily on classical forms of information disclosure. In contrast, the use of generative AI models, Retrieval-Augmented Generation technologies [19], corporate language models, or agent systems is not always accompanied by the transfer of information to another person in the traditional sense. Confidential information may be used for training models, statistical analysis, generating vector representations, optimizing algorithms, or establishing semantic relationships without a person directly becoming aware of the relevant information. Consequently, a debatable question arises regarding the legal nature of such use. It appears that the established concept of "disclosure" no longer encompasses all possible forms of unauthorized use of professional confidential information.

In the day-to-day operations of military hospitals, mental health rehabilitation centers, prosecutors' offices, law enforcement agencies, and judicial institutions, automated electronic document management systems, telemedicine platforms, remote counseling services, automated document translation tools, and software hosted on foreign digital infrastructure are currently in use. Let's consider a scenario in which a military psychologist prepares a report on a service member's psychological and emotional state using a language model deployed on servers outside Ukraine. Formally, medical confidentiality requirements may still be met if third parties do not have access to the document. However, the mere copying of information into an information environment governed by foreign law already poses risks of losing state control over confidential information. Taking into account the provisions of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" dated October 5, 2017, No. 2163-VIII [20], the Law of Ukraine "On the Protection of Information in Information and Communication Systems" dated July 5, 1994, No. 80/94-VR [21], as well as the Law of Ukraine "On Cloud Services" dated February 17, 2022, No. 2075-IX [22], such a situation must be assessed not only through the lens of medical confidentiality but also as a potential risk to the state's information security.

Even when secure software is used, questions remain regarding the retention periods for information, the possibility of its subsequent use to improve algorithms, the location of server infrastructure, the group of individuals with administrative access to the digital system, and the legal liability of the software developer in the event of a breach of confidential information. Current Ukrainian legislation does not provide a convincing answer to any of these questions, even though each of them directly affects the actual level of guarantees for professional secrecy.

In light of the above, it appears appropriate to enshrine the principle of ***digital professional autonomy*** in law. This principle is proposed to be understood as the legally guaranteed right of a professional to independently determine the admissibility of using information technologies when working with confidential information, provided that the state-established criteria for cybersecurity, data localization, algorithmic transparency, cryptographic protection, and auditing of information systems are met. First and foremost, the introduction of such a principle would help eliminate one of the most glaring gaps in current legislation, where the responsibility for maintaining professional secrecy falls on an individual who is effectively unable to influence the technical processes underlying the operation of digital infrastructure.

In contrast, some researchers argue for the broadest possible use of generative AI without imposing specific legal restrictions, citing the high efficiency of these technologies as justification. However, this position does not appear sufficiently convincing. The economic expediency of automating professional activities cannot take precedence over constitutional guarantees of privacy, attorney-client privilege, medical confidentiality, or an individual's right to the inviolability of confidential information. Any digital technology must be evaluated through the lens of the principle of legal proportionality, according to which increasing the efficiency of the state or a private entity does not justify creating disproportionate risks to fundamental human rights.

Conclusions. This study provides grounds for asserting that the digitization of social relations, the spread of cloud technologies, cross-border data processing, and AI systems are driving a fundamental transformation of traditional approaches to understanding professional secrecy.

The model established in legal doctrine, according to which professional secrecy is viewed primarily as the duty of an authorized person not to disclose confidential information, no longer reflects the true nature of modern information processes, since the source of risk is increasingly not the behavior of a specific individual, but rather the characteristics of how digital infrastructure, algorithmic data processing systems, and software environments function.

The study demonstrates that professional secrecy should be viewed as a multi-level legal framework for controlling confidential information throughout its entire lifecycle - from the moment of receipt to archiving, anonymization, or destruction. The proposed approach shifts the emphasis from an exclusively personal duty of non-disclosure to a system of interrelated legal, organizational, and technological safeguards designed to ensure an adequate level of information security in the digital environment.

Moreover, one of the most significant outcomes of the study was the formulation of a doctrinal approach to the category **of information control,** which is proposed to be understood as the legally guaranteed ability to define the scope of entities, digital services, and technological processes permitted access to professionally confidential information, while ensuring the traceability of operations related to its processing. In our view, this approach most fully corresponds to the contemporary nature of digital

legal relations and allows for the elimination of a number of conflicts that arise during the use of generative AI systems.

It has also been demonstrated that it is advisable to enshrine in law the principle of digital professional autonomy, according to which a professional must be granted a legally guaranteed right to determine the permissibility of using digital technologies when working with confidential information, provided that state-established requirements regarding cybersecurity, data localization, algorithmic transparency, cryptographic protection, and auditing of information systems. Clearly, implementing this approach will help resolve the existing discrepancies between a specialist's legal liability and their actual ability to control the technological processes of information processing.

At the same time, a comparative legal analysis has shown that the modernization of national legislation should not be carried out by creating a single, universal law on professional secrecy, but rather through the systematic updating of sector-specific regimes, taking into account modern technological risks, the provisions of European legislation on personal data protection, and AI regulation. At the same time, the implementation of foreign experience must take into account the specific features of the domestic legal system, which will help avoid duplication of regulatory provisions and the emergence of new legislative conflicts.

In this regard, future research should focus on developing theoretical and applied foundations for the legal regulation of generative AI use in professional activities, establishing criteria for the permissibility of processing professionally confidential information by digital systems, improving mechanisms for allocating legal liability among professional entities, software developers, and digital infrastructure providers, as well as developing new approaches to the protection of professional secrets under criminal and information law in the context of the continued development of AI technologies.

REFERENCES

1. CMS. (2026). Numbers and Figures. Retrieved from https://cms.law/en/int/publication/GDPR-Enforcement-Tracker-Report/numbers-and-figures [in English].
2. IBM. (2024). Cost of a Data Breach Report 2024. Retrieved from https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf [in English].
3. Yarema, O.H. (2022). Zmist informatsiinoho suverenitetu u konteksti derzhavnoho suverenitetu [The content of information sovereignty in the context of state sovereignty]. Yurydychnyi naukovyi elektronnyi zhurnal [Legal Scientific Electronic Journal], (3), 191–194. https://doi.org/10.32782/2524-0374/2022-3/43 [in Ukrainian].
4. McCallion, J. (2025). AI breaches aren't just a scare story any more – they're happening in real life. IT Pro. Retrieved from https://www.itpro.com/security/data-breaches/ai-breaches-arent-just-a-scare-story-any-more-theyre-happening-in-real-life [in English].
5. Hern, A. (2017). Royal Free breached UK data law in 1.6m patient deal with Google's DeepMind. Retrieved from https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act [in English].
6. Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. Health and Technology, 7, 351–367. https://doi.org/10.1007/s12553-017-0179-1 [in English].
7. Conseil d'État. (2022). Intelligence artificielle et action publique: construire la confiance, servir la performance [Artificial Intelligence and Public Policy: Building Trust, Enhancing Performance]. Retrieved from https://www.conseil-etat.fr/publications-colloques/etudes/etudes-a-la-demande-du-gouvernement/intelligence-artificielle-et-action-publique-construire-la-confiance-servir-la-performance [in French].
8. Strafgesetzbuch. §203. Verletzung von Privatgeheimnissen [Breach of privacy]. Retrieved from https://www.gesetze-im-internet.de/stgb/__203.html [in German].
9. Kokhanovska, O.V. (2006). Teoretychni problemy informatsiinykh vidnosyn u tsyvilnomu pravi [Theoretical Problems of Information Relations in Civil Law]. Kyiv: VPTs «Kyiv. un-t». [in Ukrainian].
10. Yemelianov, S.L. (2011). Stan ta rozvytok pravovoho instytutu profesiinoi taiemnytsi v Ukraini [The state and development of the legal institution of professional secrecy in Ukraine]. Pravo i bezpeka [Law and Security], 5(42), 52–57. [in Ukrainian].
11. Verkhovna Rada of Ukraine. (1996). Konstytutsiia Ukrainy [Constitution of Ukraine], Law №254к/96-BP. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [in Ukrainian].
12. Verkhovna Rada of Ukraine. (2003). Tsyvilnyi kodeks Ukrainy [Civil Code of Ukraine], Law №435-IV. Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#Text [in Ukrainian].
13. Verkhovna Rada of Ukraine. (1992). Pro informatsiiu [On Information], Law №2657-XII. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].
14. Verkhovna Rada of Ukraine. (2010). Pro zakhyst personalnykh danykh [On Personal Data Protection], Law №2297-VI. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].
15. Erdos, D. (2016). European Union Data Protection Law and Media Expression: Fundamentally Off Balance. International and Comparative Law Quarterly, 65(1), 139–183. https://doi.org/10.1017/S0020589315000512 [in English].
16. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [in English].
17. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [in English].
18. Verkhovna Rada of Ukraine. (2001). Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine], Law №2341-III. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian].
19. Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W.T., Rocktäschel, T., Riedel, S., & Kiela, D. (2020). Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. Advances in Neural Information Processing Systems, 33, 9459–9474. https://doi.org/10.48550/arXiv.2005.11401 [in English].
20. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Basic Principles of Ensuring Cybersecurity of Ukraine], Law №2163-VIII. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].
21. Verkhovna Rada of Ukraine. (1994). Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh [On the Protection of Information in Information and Communication Systems], Law №80/94-BP. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian].
22. Verkhovna Rada of Ukraine. (2022). Pro khmarni posluhy [On Cloud Services], Law №2075-IX. Retrieved from https://zakon.rada.gov.ua/laws/show/2075-20#Text [in Ukrainian].