

If we talk about the fact that the state should not interfere with normal activities, then, in our opinion, regardless of whether a religion is recognized as the state or not, other religious organizations should not be humiliated or limited in their rights. No one can be forced to become a member of a state church. This opinion of the ECHR was expressed in the case of “Asatruarfelagid against Iceland” and also in the case of “Darby against Sweden” [5]. We believe that all states should be secular, that is, religion should be separated from the state. We do not at all belittle the role of the church. After all, if the church is completely removed from the state, people will have no moral values and laws left, and such a state will become atheistic.

Conclusion. To sum up, the negative obligations of the state consist in the obligation not to interfere with the normal activities of religious organizations and to respect the autonomy of religious organizations, while the positive obligations consist in taking certain actions to ensure the enjoyment of certain rights.

References:

1. Конвенція про захист основоположних прав і свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 05.01.2025)
2. Справа Європейського суду з прав людини “Свідки Єгови проти Греції”. URL: <https://hudoc.echr.coe.int/fre?i=001-80394> (дата звернення: 05.01.2025)
3. Guide_Art_9_UKR Council of Europe European Court of Human Rights, 2015 рік, свобода думки, совісті і релігії, стаття 9 Конвенції URL: <https://www.echr.coe.int> (дата звернення: 29.12.2021)
4. Справа Європейського суду з прав людини “Х проти Сполученого Королівства ”. URL: <https://hudoc.echr.coe.int/fre?i=001-74930> (дата звернення: 05.01.2025)
5. Справа Європейського суду з прав людини “Асатруарфеллагід проти Ісландії ”. URL: <https://hudoc.echr.coe.int/fre?i=001-113920> (дата звернення: 04.01.2025)
6. Англо-український словник. URL: <https://www.lingvolive.com/en-us> (дата звернення: 07.01.2025).

LEGAL MECHANISMS FOR ENSURING DIGITAL RIGHTS IN DEMOCRATIC STATES: CHALLENGES AND PERSPECTIVES

ARTEM SHERUDA, PhD student

MYKHAILO V. SHEPITKO, Professor, Doctor of Science in Law, Scientific Adviser

SVITLANA S. MYKYTIUK, Associate Professor, PhD in Law, Language Adviser

Yaroslav Mudryi National Law University in Kharkiv

The advent of modern digital technologies has initiated profound transformations within contemporary society, specifically manifesting in the digital reconfiguration of social relations. This transformation is characterized by the widespread integration of advanced digital technologies across diverse spheres of human activity.

Digital transformation directly influences the realization of fundamental human rights and contributes to the emergence of new human and citizen rights as participants in the global information and digital space. The results of digitalization require reflection and adequate formulation of the legal mechanisms for regulating, implementing, and protecting both existing rights and those that are just beginning to form, with the aim of ensuring sustainable socio-economic development and the realization of constitutional rights and freedoms of individuals and citizens [3, p. 18-19].

As O. Hiliaka notes, in this context, the most important task of legal science becomes the development of a model for the legal regulation of digital technology usage, which would ensure a balance between preserving fundamental societal and legal values and the development of new technologies aimed at improving the quality of life. Furthermore, digitalization and the spread of new technologies in the economy themselves present a new challenge for the development of law at the present stage, which requires comprehensive theoretical study and analysis [2, p. 17].

In the context of the research, it is essential to explore the legal framework for digital rights in democratic states. Given the need for legal regulation of digital rights, the Council of the European Union and the European Parliament have concluded an Agreement on Amendment 138 of Article 1, Section 3(a) of *Directive 2009/136/EC*, which states that Internet users are presumed innocent and have the right to privacy in networks. Important legal acts in the EU also include *Regulation (EU) 2016/679 (GDPR)* and *Directive (EU) 2016/680* [1, p. 335].

Ukraine adopted the Law of Ukraine *On Personal Data Protection* in 2010, which, despite numerous amendments, still lacks provisions on the protection of digital identity, taking into account the specific nature of the cyber environment [5]. In contrast, the *EU Regulation (GDPR)*, which has been in effect since 2018, directly applies to all EU member states. It mandates the appointment of a data protection officer for certain types of data processing and grants broader rights to data subjects. Unlike the Ukrainian law, which defines the rights and obligations of data subjects but does not require the appointment of a data protection officer, the *GDPR* demonstrates a stronger commitment to safeguarding personal data, particularly to prevent identity theft and misuse. Additionally, while the Ukrainian law imposes administrative sanctions for data processing violations, the *GDPR* grants supervisory authorities significant powers to impose administrative sanctions, including substantial fines, reflecting a punitive approach to preventing data protection violations.

It is worth noting the fact that the rapid development of new digital technologies, such as artificial intelligence, big data, and blockchain, poses significant challenges to legal mechanisms for ensuring digital rights. These technologies not only transform the digital landscape but also introduce complex legal issues related to data protection, privacy, and the safeguarding of fundamental rights. The dynamic and evolving nature of these innovations complicates the establishment of comprehensive regulatory frameworks,

necessitating adaptive legal approaches that can effectively address emerging risks while fostering technological progress.

Cyber threats require special attention, as massive databases storing confidential information regularly attract malicious actors. A successful attack can harm both an organization's reputation and user security by exposing personal data to public access. This highlights the need for clear and transparent rules regarding data collection and use. Consequently, lawmakers worldwide are developing norms and standards to balance commercial interests with citizens' rights to privacy and security.

For example, the *Artificial Intelligence Act (AI Act)* is a European Union regulation that establishes a common legal and regulatory framework for artificial intelligence within the EU. It aims to ensure the safe and ethical use of AI while considering potential risks to society and human rights. Complementing the *General Data Protection Regulation*, the *AI Act* does not alter its provisions but establishes safety, transparency, and accountability requirements for AI system developers and users, safeguarding personal data and fundamental human rights. It mandates risk assessments, mitigation measures, and accountability in AI deployment [4].

In conclusion, the rapid digital transformation of modern society requires the development of adaptive legal mechanisms to safeguard digital rights in democratic states. Emerging technologies such as artificial intelligence, big data, and blockchain challenge existing legal frameworks, demanding innovative approaches to balance technological progress with fundamental human rights protection. While the European Union has established comprehensive regulations like the *GDPR* and *AI Act*, many countries, including Ukraine, continue to face difficulties in aligning national legislation with global standards. Developing flexible and future-oriented legal models is essential to address digitalization challenges and ensure the sustainable development of democratic societies.

References:

1. Бондаренко О., Думчиков, М. Захист цифрової особистості: вивчення досвіду Європейського союзу та України. *Юридичний науковий електронний журнал*. 2024. № 1. С. 334-338.
2. Гиляка О. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. *Вісник Національної академії правових наук України*. 2023. № 30(2). С. 15-30.
3. Петришин О. Гиляка О. Права людини в цифрову епоху: виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. 2021. № 28(1). С. 17-35.
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council 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) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> (date of access: 15.03.2025).
5. The Law of Ukraine No. 2297 VI "On Personal Data Protection". URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (date of access: 15.03.2025).