HUMAN RIGHTS IN THE DIGITAL DIMENSION

2024

Digital Security Lab Ukraine

INTERNATIONAL RENAISSANCE FOUNDATION

Author Team:

Tetiana Avdieieva
Vita Volodovska
Maksym Dvorovyi
Anna Liudva
Serhii Savelii
Yevheniia Stadnik
Karina Levadnia
Viktoriia Tkachenko
Solomiia Yaremenko
Bohdana Yaruta

This report was compiled as a part of the project "Human Rights in the Digital Dimension: Compliance with International Obligations and an Action Plan on the Path to the EU" with the support of the International Renaissance Foundation. It's content is the exclusive responsibility of the authors and does not necessarily reflect the views of the International Renaissance Foundation.

Digital Security Lab Ukraine (DSLU) is a Ukrainian non-governmental organization that supports independent media, journalists, activists, and civil society in strengthening their digital security. The organization promotes human rights standards in the digital sphere by developing analytical materials, participating in legislative processes, and launching advocacy campaigns in Ukraine and around the world.

Website: dslua.org
E-mail: dslua@dslua.org
Facebook: facebook.com/dslua

The International Renaissance Foundation is one of the largest charitable foundations in Ukraine. Since 1990 we have been helping to develop an open society based on democratic values in Ukraine. During its activity, the Foundation has supported about 20 thousand projects. The funding amounted to over $ 350 million.

Website: www.irf.ua
Facebook: www.fb.com/irf.ukraine

ABOUT THE REPORT

Human rights and freedoms, along with their guarantees, define the essence and direction of the state's activities. This constitutional principle is absolute. Any restrictions, even those introduced during martial law or a state of emergency, are justified only to the extent that they do not undermine the inherent value of the individual and the affirmation of their rights as the state's primary duty.

This report provides an overview of the state of human rights protection in the digital environment under the impact of Russia's full-scale invasion and Ukraine's obligations to harmonize its national legislation with EU law as of 2024. The analysis focuses on measures to ensure access to the internet (Section 1) as a prerequisite for the realization of digital rights; the protection of freedom of expression and media freedom online (Section 2); the protection of personal data and privacy in the digital environment (Section 3). The report also explores the impact of artificial intelligence technologies on human rights and measures that can be introduced to prevent potential violations and mitigate associated risks (Section 4). The final section examines the influence of digital technologies on the right to free elections, particularly through the lens of political advertising regulation.

Future annual reports will expand the scope of research to include the impact of digitalization on other fundamental human rights.

The report contains detailed recommendations for reforming national legislation and taking other necessary measures to fulfill human rights obligations in the online environment. These recommendations are based on the conducted analysis, as well as on international treaties to which Ukraine is a party, recommendations and resolutions of the Council of Europe, case law of the European Court of Human Rights, UN recommendations, the EU Charter of Fundamental Rights, and other EU legal acts whose implementation is a prerequisite for Ukraine's European integration.

TABLE OF CONTENTS

INTERNET ACCESS AS A FOUNDATION FOR HUMAN RIGHTS IN THE DIGITAL AGE

The reform of national legislation on electronic communications, notably the enforcement of the Law of Ukraine "On Electronic Communications" in 2022, has unequivocally guaranteed citizens' right to quality and affordable Internet access (universal electronic communications services), a prerequisite for self-expression and the exercise of human rights online. Aligning Ukrainian legislation with EU requirements also aims to ease regulatory pressure and improve market conditions, ultimately leading to higher-quality services for consumers. However, full implementation of the legislative innovations is still underway. The full-scale invasion of Ukraine by the Russian Federation delayed the adoption of numerous secondary acts required to implement the guaranteed rights and programmes in practice, as well as their financing. Additionally, consumers in the temporarily occupied territories remain largely disconnected from Ukrainian networks.

Damage to Internet infrastructure caused by military action poses a serious threat to the enjoyment of the right to Internet access. Joint efforts by the government and businesses have enabled the relatively rapid restoration of services where possible. However, certain government decisions - for example, introducing requirements to ensure uninterrupted network access during emergency power outages - have been criticised for placing excessive burdens on electronic service providers. Smaller Internet providers have also raised concerns about increased tax pressure following changes to the taxation regime, an issue currently being challenged in several court cases.

Despite martial law, no general temporary restrictions on Internet access have been applied in Ukraine. However, the activities of the National Centre for Operational and Technical Management of Electronic Communications Networks of Ukraine (NCON) - which is authorised during this period to issue binding orders to service providers - still require greater legal clarity and transparency.

1.1. Ensuring Universal Access to the Internet

The right to Internet access in Ukraine is enshrined in the Law of Ukraine "On Electronic Communications" which, since 2022, has guaranteed consumers the right to receive universal electronic communications services, including fixed broadband Internet access. The law also specifies minimum standards for such service - notably, a connection speed sufficient to allow access to a range of services, from email and media to social networks, messaging apps, and video calls.

The standards for the quality of universal services are established by the central executive authority in the field of electronic communications (since 1 September 2023, this has been the Ministry of Digital Transformation of Ukraine; previously, it was the Administration of the State Service of Special Communications and Information Protection). Since 2023, the data transmission speed at the endpoint - meaning for the end user - must be at least 30 Mbps.

The government does not regulate the price of universal electronic communications services; costs depend on individual providers. However, providers are required to offer these services at economically justified, transparent, and non-discriminatory prices, and to notify consumers of any price changes at least 20 calendar days before they take effect. Article 100 of the Law of Ukraine "On Electronic Communications" also provides for state monitoring of tariff/price levels. However, the draft resolution of the Cabinet of Ministers

of Ukraine "On Approval of the Procedure for Monitoring Tariff/Price Levels for Universal Electronic Communications Services" was only published for public consultation by the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NCEC) - the competent regulatory authority - in December 2024.

According to several rankings, Ukraine is among the countries with the lowest Internet costs in the world. A 2023 study by Picodi indicated that the average price of an unlimited package with a speed of 100 Mbps in Ukraine was $6.10, the second-lowest in the world. Cable.co.uk, in its *Worldwide Data Pricing* study, measured the cost of 1 GB of mobile data globally and reported that as of 2023, Ukraine ranked 16th worldwide, with an average price of $0.27 per GB. However, analytical materials for the draft Strategy for the Development of the Electronic Communications Sector of Ukraine until 2030 noted that, compared to European countries, the relative cost for the population is the highest (1.36% of household income).

According to data provided by the Ministry of Digital Transformation in these analytical materials, the coverage rate (the share of the population with technical access to the Internet) for mobile broadband access in Ukraine stands at 91%, while fixed broadband access covers 88.4% of the population. Both figures are lower than the averages for the European Union and are therefore identified in the Strategy as areas for improvement. Although the Strategy has not yet been officially adopted, it is considered a roadmap for improving Internet access in Ukraine. Its priorities include the development of 5G technology - the test launch of which was announced by Deputy Prime Minister Mykhailo Fedorov in November 2024 - and achieving mobile broadband coverage for 98% of the population, with an average speed of at least 90 Mbps.

Overall, Ukrainian legislation on Internet access is consistent with EU and Council of Europe standards. Nevertheless, the government must prioritise its full implementation, focus on achieving the defined targets in practice, and invest in the development of new access technologies. To this end, it is necessary to:

- Adopt the Strategy for the Development of the Electronic Communications Sector of Ukraine until 2030 and approve an operational plan for its implementation, with input from stakeholders and civil society,
- Introduce a system for monitoring tariff/price levels for universal electronic communications services to assess their affordability and support the realisation of the right to universal Internet access.

1.2. Special Measures to Guarantee Internet Access for Vulnerable Groups

The Ukrainian legal framework provides guarantees to ensure Internet access for vulnerable social groups. In particular, Article 101 of the Law of Ukraine "On Electronic Communications" effectively establishes the right of consumers belonging to vulnerable groups to receive targeted financial assistance if the cost of universal electronic communications services is deemed unaffordable. The Cabinet of Ministers of Ukraine is responsible for setting the procedure and the amount of such assistance. However, no secondary legislation has yet been adopted at the government level to implement this provision. At present, only a draft Criteria and Indicators for Determining the Affordability of Universal Electronic Communications Services is under public consultation. Application of this provision was suspended for 2024, and the Law of Ukraine "On the State Budget of Ukraine for 2025" has extended the suspension for another year.

Another guarantee concerns the right to Internet access in geographically remote areas. The Law of Ukraine "On Electronic Communications" stipulates that if geographic surveys of network deployment identify a lack of universal services in a given area, the regulatory authority (NCEC) must designate that area as needing access to universal electronic communications services. To address this, a competition may be organised to partially reimburse providers for infrastructure development costs, or a provider may be required to build the network, with reimbursement of the related expenses. The NCEC has approved the respective methodology, and it was registered with the Ministry of Justice of Ukraine in early 2024, although no surveys have yet been conducted.

Separately, Article 100 of the Law of Ukraine "On Electronic Communications" guarantees the promotion of universal electronic communications services for consumers with disabilities and calls for measures to provide them with suitable terminal equipment and specialised tools to ensure equal access, including, if necessary, speech recognition and synthesis technologies. However, no secondary legislation has yet been adopted to set out the mechanisms for implementing this right.

The draft Strategy for the Development of the Electronic Communications Sector of Ukraine until 2030 highlights the challenges in putting the state's positive obligations in this area into practice. One of the main challenges is ensuring both geographic and financial accessibility of universal services, notably developing mechanisms to deliver targeted financial assistance to consumers belonging to vulnerable groups to help them access these services; establishing mechanisms to compensate service providers for losses incurred in fulfilling their obligation to provide universal services; and addressing the lack of detailed secondary legislation in this area.

To achieve the goal of providing at least 75% of Ukrainian households with access to fixed broadband Internet at speeds of up to 1 Gbps, the Strategy sets out, among other measures: (1) making Internet access inclusive for persons with disabilities, including by offering benefits for purchasing technical access devices and specialised software, and by ensuring that electronic communications services are accessible for persons with disabilities; and (2) implementing universal electronic communications services by establishing mechanisms to ensure the geographic and financial accessibility of these services for vulnerable consumer groups.

The draft Strategy is aligned with the National Strategy for Creating a Barrier-Free Space in Ukraine until 2030, which also sets out tasks aimed at promoting digital inclusion. These include expanding technical infrastructure to connect households in rural areas, providing benefits for persons with disabilities, and fostering a competitive environment among fixed broadband Internet service providers in local communities.

Overall, while Ukrainian legislation on Internet access for vulnerable groups is adequate at the normative level, it remains largely declarative. Therefore, the government must prioritise its implementation and focus on achieving the stated goals in practice. To this end, it is necessary to:

- Adopt the Strategy for the Development of the Electronic Communications Sector of Ukraine until 2030,
- Develop and approve, based on this Strategy and the National Strategy for Creating a Barrier-Free Space in Ukraine until 2030, legal acts of the Cabinet of Ministers of Ukraine and relevant authorities that introduce specific measures to improve Internet access for vulnerable groups.

1.3. Ensuring Conditions for Unimpeded Access to Quality Internet Services

The Law of Ukraine "On Electronic Communications" guarantees end users the right to choose their electronic communications service provider freely and to receive services in a timely and high-quality manner. This right is supported *inter alia* by the freedom to conduct business in providing Internet services and by the state's obligation to ensure a competitive environment, particularly through the analysis of electronic communications markets and the application of antitrust measures. Such measures may be applied by the regulatory authority - the NCEC - in accordance with the procedures set out in the legislation.

Regarding Internet access provision, the focus should be on the retail markets for mobile communications access, which also enables Internet access, and fixed broadband Internet access. In 2023, the NCEC identified the mobile communications market as one that may require competition safeguards, given that three operators control 99% of the market. By contrast, the fixed broadband market is competitive: more than 4,000 providers operate in Ukraine, and the largest - PJSC Kyivstar - holds no more than a 16% market share. In 2024, the NCEC launched a review of the mobile communications market to assess the need for competitive safeguards and subsequently identified it as competitive.

At the same time, 2024 saw the emergence of tax pressure on actors in the electronic communications services market, which may reduce the supply of Internet access services. Since late September 2024, the State Tax Service has effectively required all providers to switch from the simplified to the general taxation system, relying on the ambiguous interpretation of the provisions of the Tax Code of Ukraine. This triggered a wave of applications to the NCEC from smaller providers seeking to suspend their activities, a petition to the Cabinet of Ministers, which received a negative response, and opposition from civil society and relevant business associations. Among the threats raised were concerns about the deterioration in the quality and accessibility of Internet services, especially during emergency power outages, higher service costs for consumers due to rising operating expenses, and market monopolisation. More than 100 providers have challenged the State Tax Service's decisions to cancel their registration as single tax taxpayers in court. As of the end of 2024, however, no legislative proposals aimed at clarifying the interpretation of tax law provisions had been registered in Parliament.

To protect market pluralism in Internet access services, it is necessary to:

- Amend the Tax Code of Ukraine and the Law of Ukraine "On Electronic Communications" to provide clear regulation of the status and requirements, including tax requirements, for electronic communications service providers.

1.4. Legality and Justification of Restrictions on Internet Access Services

Restrictions on Internet access services should be considered in general and individual contexts. The first relates to so-called shutdowns – the complete or partial disconnection of Internet access across the entire country or in specific regions. The second concerns restrictions on individual rights to Internet access for certain categories of persons, particularly imprisoned people.

Several provisions allow for shutdowns in Ukraine outside the context of martial law. Most notably, Article 18 of the Law of Ukraine "On the Legal Regime of the State of Emergency" allows for the launch of special rules on the use of communications and information transmission via computer networks if a state of emergency is declared due to mass public disorder. The scope of such restrictions must be set by a presidential decree and then approved by the Verkhovna Rada of Ukraine.

Another important provision is provided by the Law of Ukraine "On Electronic Communications". Article 115 provides that, in order to cease terrorist activities, the provision of electronic communications services to consumers located within a defined area of an anti-terrorist operation may be temporarily restricted. Temporary restrictions may also be introduced by local executive authorities and local self-government bodies, with the approval of the Ministry of Digital Transformation, to facilitate notification and provide communications services for participants in emergency response and recovery operations. In practice, however, such restrictions have not been applied to date.

At the individual level, Internet access restrictions are addressed in the Criminal Executive Code of Ukraine. It grants the prisoners the right to use the Internet under the supervision of the penitentiary administration during their free time, at their own expense or the expense of third parties, by depositing funds into an electronic wallet. That is, where financial means are available, prisoners are not deprived of the right to Internet access while in custody.

Access to the Internet is granted upon application to the penitentiary administration and is provided in accordance with the Internet room schedule. Information on their Internet use is recorded in a special log, along with records of their use of IP telephony and video calls. When accessing the Internet, prisoners can visit a list of websites determined by the penitentiary administration, based on categories approved by the Ministry of Justice. They may access websites of government authorities, local governments, international organisations, the European Court of Human Rights (ECtHR), and websites related to creativity, education, sports, culture, law, and reference information, as well as registered media outlets. Upon request, the penitentiary administration may also grant access to other websites.

However, prisoners are prohibited from engaging in certain activities online. They are forbidden from using social media, accessing pornographic sites, or continuing phone calls if they use aggressive or obscene language. In addition, their correspondence may be monitored, except for correspondence with courts, international organisations, prosecutors, and defence lawyers, which must take place exclusively through an email account registered and supervised by the penitentiary administration. Denials of Internet access rights are subject to appeal under the general procedures for public law disputes, namely within the framework of administrative proceedings.

Although Ukrainian legislation does not create excessive opportunities for shutdowns and reasonably regulates restrictions on individual Internet access rights for the imprisoned, to ensure compliance with international law standards in case of any general Internet access restrictions, it is necessary to:

- Follow procedures for notifying the UN Secretary-General and the Council of Europe about the introduction of the state of emergency,
- Apply the least restrictive measures necessary to achieve the objectives during a state of emergency or anti-terrorist operation,
- Regularly review any restrictions to assess their necessity and proportionality.

1.5. Internet Access Under Martial Law

The Law of Ukraine "On the Legal Regime of Martial Law" allows for measures such as regulating the activities of electronic communications networks and/or service providers, as well as prohibiting the transmission of information via computer networks. Responsibility for this regulation lies with the NCON, which is established by the Administration of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP). Under martial law, the NCON acts as the emergency regulatory body in the electronic communications sector. Legislative amendments adopted in 2022, shortly after the full-scale invasion, formalised the NCON's authority to issue binding instructions to service providers during martial law. These powers include the ability to introduce temporary restrictions on service provision, as outlined in Cabinet of Ministers Resolution No. 812 of 29 June 2004, which governs the NCON's operations. Some NCON instructions also refer to the Regulation on the NCON, approved by SSSCIP Order No. 209 of 11 April 2019 (as amended), although the full text of this regulation is not publicly available.

Despite martial law, Ukraine has not introduced classic Internet shutdowns. Service disruptions have typically resulted from Russian shelling and the resulting power outages. However, in February 2024, the NCON issued an Instruction on maintaining the stability of electronic communications networks under martial law, which has since been amended several times. This Instruction imposed obligations on network and service providers to ensure continuous operation for set periods - for example, by 1 February 2025, 100% of mobile base stations must remain functional for at least 10 hours during outages, and by 1 December 2024, local Internet providers must maintain service for 72 hours. These requirements posed significant challenges for providers, though the Head of SSSCIP later stated that a substantial portion of the requirements had been met.

On 27 February 2022, the NCON issued an order to block autonomous systems (AS) linked to Russia. These systems are clusters of IP addresses associated with Russian Internet providers. Together with two other NCON instructions, this resulted in blocking over 600 autonomous systems, comprising more than 48 million IP addresses, effectively covering almost the entire Russian segment of the Internet. These instructions are set to remain in effect until martial law is lifted, though there is no public information on whether service providers have actually enforced them.

The imposed restrictions may be justified by the need to protect Ukrainian users from cyberattacks, threats, and harmful content originating from the Russian segment of the Internet. Nonetheless, the NCON's legal authority to order the blocking of autonomous systems remains vaguely defined. While such measures may have been justified in the early days of the full-scale invasion, when rapid, discretionary action was necessary for emergency regulation, the state should have ensured clearer legal frameworks for

the NCON's operations in the online space by the third year of the war. This includes improving transparency, particularly through centralised publication of its decisions and clearer guidelines on which decisions should or should not be made public on the SSSCIP website, as is the current practice.

To harmonise Ukrainian legislation with the requirements of the EU, the Council of Europe, and relevant UN recommendations, it is recommended to:

- Amend the Cabinet of Ministers Resolution No. 812 of 29 June 2004 to clarify the NCON's authority to block autonomous systems and introduce clear requirements for publishing NCON decisions that do not contain restricted information,
- Assess the effectiveness of, and revise where necessary, the requirements related to maintaining uninterrupted Internet access, especially with regard to the capacity of smaller business providers to comply,
- Ensure a comprehensive review of NCON decisions related to Internet resource restrictions and other measures introduced under martial law after its cessation.

FREEDOM OF EXPRESSION IN THE DIGITAL ENVIRONMENT

Despite the ongoing full-scale war, the Ukrainian authorities have so far refrained from introducing widespread restrictions on freedom of expression and have continued to actively align national legislation with EU law in the field of media and journalists' rights. Human rights and media organisations play a significant role in maintaining this balance by monitoring potential risks in a timely manner and contributing constructive criticism and proposals for improving regulation.

At the same time, several challenges remain. These include impunity for crimes against journalists and the use of defamation lawsuits as a tool to censor the media; a lack of legal clarity regarding the procedures and grounds for imposing sanctions in the online sphere; unjustified restrictions on access to socially important information; and insufficient resources for strengthening the institutions responsible for effectively implementing European standards in the field of freedom of expression and the media.

2.1. Freedom to Receive and Impart Information Online

2.1.1. Legislative Guarantees for the Freedom to Receive and Impart Information Online

Article 34 of the Constitution of Ukraine guarantees everyone the right to freedom of thought and speech, and to freely express their views and beliefs, which includes the right to freely collect, store, use, and impart information orally, in writing, or in any other way of one's choice. The same provision also sets out the grounds on which freedom of expression may be restricted. Such restrictions must be established by law and are permitted:

- in the interests of national security, territorial integrity, or public order to prevent disturbances or crimes,
- to protect public health,
- to protect the reputation or rights of others,
- to prevent the disclosure of confidentially obtained information,
- to maintain the authority and impartiality of the judiciary.

This provision serves as the cornerstone of the current national system for protecting freedom of expression. Although it does not fully replicate Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention) or Article 19 of the International Covenant on Civil and Political Rights - specifically omitting the requirement that any restriction be "necessary in a democratic society" - it generally provides an adequate legislative framework at the national level. Moreover, the obligation to consider the case law of the ECtHR, which interprets Article 10 of the Convention, is established by Article 17 of the Law of Ukraine "On the Execution of Judgments and Application of the Case Law of the European Court of Human Rights."

The provisions of the Convention and the Covenant are also reflected in specific laws governing the dissemination and receipt of information. Article 5 of the Law of Ukraine "On Information" affirms the right to information, which includes the ability to freely obtain, use, disseminate, store, and protect information necessary for the exercise of one's rights, freedoms, and legitimate interests - provided this does not infringe upon the rights of others or constitute abuse of information as defined in Article 28 of the

same law. Article 6 reiterates the constitutional principles governing the restriction of this right. This body of legislation is supplemented by the legal framework on access to public information, established in the dedicated Law "On Access to Public Information." This law guarantees the openness of information created by public authorities and other information holders, and it establishes mechanisms for challenging violations of the right to access information.

Article 4 of the Law of Ukraine "On Media" also enshrines the freedom of business activity in the media sector, which is grounded in the freedom to express opinions and beliefs and the freedom to impart, share, and receive information. This Law also emphasises the need to observe the three-part test for human rights restrictions when interfering in media activities - including the criterion of necessity in a democratic society, which is present in the Convention but absent from the Constitution.

The right to judicial appeal against any decisions, actions, or inaction by public authorities or local governments, as well as the right to apply to the Ukrainian Parliament Commissioner for Human Rights for the protection of one's rights, is guaranteed by Article 55 of the Constitution of Ukraine. This provision also applies to violations of the right to freedom of expression committed by state representatives and is subject to review within the general framework of administrative justice.

2.1.2. Lawful and Justified Grounds for Website Blocking and Online Content Filtering

Blocking of Internet Resources. As of the end of 2024, there were five mechanisms for blocking websites in Ukraine (excluding those related to the legal regime of martial law). Two of them may be applied by court decision, two require a decision by a regulatory authority which may be appealed in court, and one is based on the application of political-legal sanctions. These mechanisms include:

- Blocking of resources used to distribute child pornography, based on a court decision and carried out by electronic communications service providers, as set out in Article 18(3) of the Law of Ukraine "On Electronic Communications,"
- Blocking of resources providing access to unlicensed gambling, based on a decision by the Commission for Regulation of Gambling and Lotteries (CRGL), to be implemented by the website owner or hosting service provider, pursuant to Article 25 of the Law of Ukraine "On State Regulation of Activities Related to the Organisation and Conduct of Gambling,"
- Prohibition of anonymous online media outlets in cases of three minor or significant violations, or two grave violations within one month, as well as a 14-day temporary prohibition on unregistered online media in cases of five major violations within one month that resulted in fines - based on a decision by the National Council of Television and Radio Broadcasting of Ukraine (National Broadcasting Council), under Article 116(13, 16) of the Law of Ukraine "On Media,"
- Prohibition of registered online media in cases of four grave violations within one month, and prohibition of unregistered online media in cases of three grave violations in the same period, based on a court decision pursuant to Article 116(14, 15) of the Law of Ukraine "On Media,"
- Blocking of access to information resources used to display and promote the symbols, ideas, or programme goals of terrorist organisations or groups, based on a decision of the National Security and Defence Council of Ukraine, enacted by Presidential Decree, under Articles 4 and 5 of the Law of Ukraine "On Sanctions."

The first four mechanisms address illegal content and either ensure judicial oversight of access restrictions or are imposed by an independent regulator after substantial engagement with the violating parties regarding ongoing unlawful actions. In practice, only one of these mechanisms was used in 2024: the CRGL issued a decision to block 105 websites. The National Broadcasting Council received relevant powers at the end of March 2024 but has not yet exercised them, and the Unified State Register of Court Decisions contains no judgments issued under the Law "On Electronic Communications."

The most problematic mechanism is that based on the Law of Ukraine "On Sanctions." A new sanction - blocking access to information resources used to display and promote the symbols, ideas, or programme goals of terrorist organisations or groups - was introduced in 2023. The provision contains no exceptions for the use of prohibited symbols for educational, journalistic, or other legitimate purposes. In addition, its implementation raises concerns about the legal certainty of the sanctions-related decrees themselves. In 2024, this sanction was applied in three Presidential Decrees (against Russian media, media associated with Ihor Huzhva and Anatolii Sharii, and Ukrainian citizen Oleksii Selivanov), none of which specified the exact online resources to be blocked.

Furthermore, the Law "On Sanctions" continues to be used as a basis for blocking websites through a broader provision allowing the imposition of "other sanctions consistent with the principles of this Law." This practice dates back to 2017 and has been repeatedly criticised by experts for failing to meet international human rights standards. Key issues include inconsistent terminology on blocking, application of sanctions to individuals - including Ukrainian citizens and deceased persons - and the unclear duration of sanctions. Experts have also highlighted the need for adequate information explaining the grounds for imposing sanctions on particular subjects. In 2024, this provision was invoked in six Presidential Decrees to block websites, in some cases alongside the previously mentioned type of sanction. As a result, over 800 websites remain blocked under this legal basis. In 2024, the Ukrainian government was notified of the first case communicated to the ECtHR regarding the compliance of this mechanism with the Convention, related to the blocking of Russian social networks in 2017.

Separate legislative proposals in 2024 also sought to modify the sanctions regime, potentially impacting the blocking system. Government-drafted draft law No. 11492, amending the Law "On Sanctions" to ban the use of software products and access to electronic information resources, proposes to introduce a new sanction: "prohibition of access to electronic information resources on the Internet (webpages, websites, other web-based resources), electronic communication networks, electronic communication systems, information systems, and information and communication systems." This draft law is currently under consideration by the Verkhovna Rada Committee on National Security, Defence and Intelligence. While it partially addresses the absence of a clear legal norm permitting Internet site blocking via sanctions, it does not clarify the procedure for enforcing such sanctions. Another draft law No. 12102, adopted in December 2024 and signed by the President in 2025, amends several laws to introduce a procedure for forming and maintaining a list of terrorist organisations. The implementation of this procedure and creation of the list would improve legal clarity regarding the use of so-called "terrorist content blocking" already envisaged in sanctions legislation.

Filtering and Removal of Online Content. Current legislation contains no explicit provisions on content filtering. However, two laws - the Law of Ukraine "On Media" and the Law of Ukraine "On Copyright and Related Rights" - include provisions that could potentially be used to limit access to specific online content.

Article 99(3) of the Law "On Media" empowers the National Broadcasting Council to request that online platform providers and authorised representatives of search engines restrict access to or exclude from search results information that violates Ukrainian law – if any sanction other than a warning has been imposed on the media entity responsible for distributing such information. However, due to jurisdictional challenges discussed in section 2.3.1 of this Report, practical implementation of this provision remains complicated. In 2024, the National Broadcasting Council did not invoke this procedure.

Article 56 of the Law "On Copyright and Related Rights" establishes a procedure for addressing copyright infringements online. It allows access to be restricted only to the specific digital content in violation and, in exceptional cases, to the web page hosting the infringing material. This procedure is non-judicial and involves the website owner or hosting service provider as the entity responsible for restricting access.

To harmonise and implement Ukrainian legislation in this area with EU and Council of Europe standards, it is recommended to:

- Amend the Law of Ukraine "On Sanctions" to clarify the grounds and procedures for website blocking, to prevent its misuse against domestic media, and to ensure that the justification for sanctions is published in the State Sanctions Register,
- Adopt legislation enabling the lawful restriction of terrorist content online, including exceptions for legitimate uses of terrorist symbols on websites for news, educational, historical, or other lawful purposes, in line with EU approaches,
- Upon the adoption of the above legislative changes, review past website blocking decisions based on sanctions to assess their necessity, proportionality, and compliance with the law.

2.1.3. Restrictions on Freedom of Expression Imposed in the Interests of National Security, Territorial Integrity, Public Safety, or to Prevent Disorder or Crime

Provisions aimed broadly at ensuring national security through the restriction of unlawful expressions are embedded in various legislative acts, targeting different categories of subjects depending on the scope of the provision. Key areas of relevance include criminal, administrative offence, and media legislation, as the provisions of Article 28 of the Law of Ukraine "On Information," which define types of abuse of information, are effectively implemented through these legal mechanisms. In addition, separate mention should be made of legislation prohibiting the use of specific symbols, as it remains unsynchronised with criminal, administrative, and media legislation with regard to the application of sanctions.

Criminal and Administrative Offence Law. The Criminal Code of Ukraine contains several provisions that criminalise certain types of speech, regardless of the medium used – including online platforms. Many of these provisions constitute restrictions on freedom of expression intended to protect national security, territorial integrity, public safety, or to prevent disorder or crime. The relevant provisions include:

- Article 109 – public calls for the violent change or overthrow of the constitutional order or seizure of state power: punishable by up to 3 years' imprisonment, or up to 5 years if committed via mass media; confiscation of property may also apply in both cases,
- Article 110 – public calls or dissemination of materials calling for changes to Ukraine's territory or borders in violation of the constitutional order: punishable

by up to 5 years' imprisonment, or up to life imprisonment if resulting in death or serious consequences; confiscation of property may apply in both cases,

- Article 111-1 – public denial of the armed aggression against Ukraine, establishment and entrenchment of the temporary occupation of part of the territory of Ukraine, or public calls to support the decisions and/or actions of the aggressor state, its armed formations and/or occupation administration; calls for cooperation with the aggressor state, its armed formations and/or occupation administration; calls to reject the extension of Ukraine's state sovereignty over its temporarily occupied territories: punishable by disqualification from engaging in certain activities or holding certain positions for a term of 10 to 15 years; conducting information activities in cooperation with the aggressor state and/or its occupation administration, aimed at supporting the aggressor state, its occupation administration or armed formations, and/or enabling it to avoid responsibility for the armed aggression against Ukraine: punishable by imprisonment for a term of 10 to 12 years, with disqualification from engaging in certain activities or holding certain positions for a term of 10 to 15 years, and may be accompanied by confiscation of property. If such activity resulted in the death of persons or other grave consequences, the penalty shall be 15 years' imprisonment or life imprisonment, with all of the above-listed additional penalties,
- Article 258-2 – public calls for terrorist acts: up to 3 years' imprisonment, or up to 5 years if committed via mass media, plus a possible 3-year ban on holding certain positions or engaging in certain activities; confiscation of property may apply in both cases,
- Article 295 – public calls for riots, arson, destruction of property, seizure of buildings or forced evictions threatening public order: up to 3 years' restriction of liberty,
- Article 436 – public calls for aggressive war or incitement of military conflict and the production of related materials: up to 3 years' imprisonment,
- Article 436-1 – public use of symbols of communist or Nazi totalitarian regimes: up to 5 years' imprisonment, or up to 10 years if committed via mass media; confiscation of property may apply. The article also provides exceptions for legitimate uses of such symbols,
- Article 436-2 – justification, recognition as lawful, or denial of the armed aggression of the Russian Federation against Ukraine, which began in 2014, including by presenting it as an internal civil conflict; justification, recognition as lawful, or denial of the temporary occupation of part of the territory of Ukraine; as well as glorification of persons who carried out the armed aggression of the Russian Federation against Ukraine, which began in 2014: punishable by imprisonment for up to 3 years. If such actions involve the production of materials containing such calls – the punishment shall be imprisonment for a term of 3 to 5 years. If mass media are used for such purposes – the punishment shall be imprisonment for a term of 5 to 8 years. In the last two cases, confiscation of property may also be applied,
- Article 442 – direct and public incitement to genocide and production or dissemination of related materials: 3 to 7 years' imprisonment.

In 2024, only one law was adopted in this area to amend the provisions of the Criminal Code in connection with the ratification of the Rome Statute. Its provisions revised Article 442 on incitement to genocide, thereby ensuring alignment with the wording of Article 25 of the Statute.

At the same time, other provisions of the criminal legislation also require revision – in particular, Article 436-1 of the Criminal Code, adopted within the framework of the decommunization laws, as well as a number of provisions (Articles 111-1 and 436-2 of the Criminal Code) passed by the Verkhovna Rada in March 2022 at the onset of the full-scale invasion. The excessive sanctions stipulated in Article 436-1 were highlighted by the Venice Commission in its opinion as early as 2015, yet these provisions have not been amended, despite attempts to introduce relevant draft legislation during the previous parliamentary convocation. Furthermore, the wording of Article 111-1(1) and Article 436-2(1) creates a situation in which a person may be punished twice for the same act under different provisions of the Criminal Code. The lack of harmonisation between these norms can lead to disproportionate negative consequences for individuals found in violation and must be addressed.

Separate attention should also be given to the practice of applying these provisions. A 2023 study by the Human Rights Platform identified longstanding problems within the judiciary when handling cases under the relevant articles of the Criminal Code. National courts do not carry out independent analysis of the content of statements that form the basis of the charges, relying instead on expert opinions without conducting additional assessment. Most court judgments lack quotations or descriptions of the statements that led to criminal liability and contain no analysis of the audience that may have been exposed to the content in question. In some cases, individuals have been held criminally liable merely for liking or reposting content. Courts also continue to treat social media as "mass media," contrary to updated media legislation that classifies online platforms as a separate category of actors. This classification results in the application of provisions with more severe penalties.

The Code of Ukraine on Administrative Offences also contains two provisions whose legitimate objective is to impose restrictions in the interests of national security and public order. Article 173-3 of the Code establishes liability for the public use, display, or wearing of the St. George's/Guard ribbon. In 2024, the ECtHR, in a decision on admissibility in the case of Borzykh v. Ukraine, found such a restriction to be lawful and in line with Article 10 of the European Convention on Human Rights. Article 173-1 of the Code also prohibits the dissemination of false rumours that may cause panic among the population or disturb public order.

Media Law. Article 36 of the Law of Ukraine "On Media" also contains a number of restrictions aimed at protecting legitimate interests in the areas of national security, territorial integrity, and public safety. Its provisions prohibit media from publishing:

- Calls for the violent overthrow or change of the constitutional order, the initiation or conduct of an aggressive war or armed conflict, violation of Ukraine's territorial integrity, or the elimination of Ukraine's independence, as well as information that justifies or promotes such actions,
- Propaganda of or calls for terrorism and terrorist acts, and information that justifies or endorses such acts,
- Information that denies or justifies the criminal nature of the communist totalitarian regime of 1917–1991 in Ukraine or the national-socialist (Nazi) totalitarian regime, that creates a positive image of persons who held leadership positions in the Communist Party (district committee secretary and above), in the highest authorities and administrative bodies of the USSR, Ukrainian SSR (Ukrainian Soviet Socialist Republic), and other Soviet republics (except for cases related to the development of Ukrainian science and culture), employees of Soviet state security bodies, or that justifies the activities of these bodies, the establishment of Soviet rule in Ukraine

or in certain administrative-territorial units, or the persecution of participants in the struggle for Ukraine's independence in the 20th century,

- Information containing the symbols of the communist or national-socialist (Nazi) totalitarian regimes, except in cases provided for by the Law of Ukraine "On the Condemnation of the Communist and National-Socialist (Nazi) Totalitarian Regimes in Ukraine and the Prohibition of Propaganda of Their Symbols,"
- Information containing propaganda of the Russian totalitarian regime, the armed aggression of the Russian Federation as a terrorist state against Ukraine, as well as the symbols of the military invasion of the Russian totalitarian regime, except in cases provided for by the Law of Ukraine "On the Prohibition of Propaganda of the Russian Nazi Totalitarian Regime, the Armed Aggression of the Russian Federation as a Terrorist State Against Ukraine, and the Symbols of the Military Invasion of the Russian Nazi Totalitarian Regime in Ukraine,"
- Information that denigrates or disrespects the state language,
- Information that denies or questions the existence of the Ukrainian people (nation), the Ukrainian statehood, and/or the Ukrainian language.

The standards for applying these restrictions in practice are to be further developed by co-regulatory bodies, which began operating in 2024. One of these bodies, operating in the field of audiovisual media, designated national security-related issues as its priority in 2025. In 2024, the National Broadcasting Council did not impose any sanctions under these provisions against online media or VOD services.

Legislation on the Prohibition of Symbols. Following the full-scale invasion, Ukraine reinforced its memory policy and enshrined additional legal restrictions on the propaganda of certain regimes and their symbols. Two laws were adopted: "On the Prohibition of Propaganda of the Russian Nazi Totalitarian Regime, the Armed Aggression of the Russian Federation as a Terrorist State Against Ukraine, and the Symbols of the Military Invasion of the Russian Nazi Totalitarian Regime in Ukraine" and "On the Condemnation and Prohibition of Propaganda of Russian Imperial Policy in Ukraine and the Decolonisation of Toponymy." Both laws define prohibited content and symbols, as well as exceptions for their lawful use. However, the legislation targeting Russian imperial policy includes an exception for media that may not apply to all types of media except audiovisual ones, as it limits exemption from liability to informational, analytical programmes and documentary films only. A similar shortcoming is also present in the Law of Ukraine "On the Condemnation of the Communist and National-Socialist (Nazi) Totalitarian Regimes in Ukraine and the Prohibition of Propaganda of Their Symbols."

Draft law No. 12062 proposes amendments to the Code of Ukraine on Administrative Offences and the Criminal Code of Ukraine to introduce liability for the propaganda of Russian imperial policy symbols as defined in the relevant law. It envisages administrative fines of UAH 1,700–3,400 for individuals and UAH 3,400–5,100 for officials. Criminal liability is provided for cases where such symbols are used in government or local government institutions and in state or municipal enterprises. The proposed provisions also include references to lawful exceptions for the use of such symbols. However, when introducing such changes, it is important to consider the existing need to align the norms of criminal law to distinguish between different offences, the degree of societal harm caused by the dissemination of certain expressions, and the proportionality of penalties.

To harmonise Ukrainian legislation in this area with the requirements of the EU, the Council of Europe, and relevant UN-level recommendations, it is recommended to:

- Review and amend provisions of the Criminal Code of Ukraine that establish liability for unlawful speech aimed at protecting national security, in order to avoid overlapping provisions and ensure proportionality of sanctions by introducing alternative types of punishment,
- Unify approaches to restricting the display and promotion of symbols, including expanding the exceptions for their legitimate use in media,
- Support the development of co-regulatory media codes that define criteria for classifying information as prohibited for dissemination in Ukraine under Article 36(1), Subparagraphs (1), (4), and (10) to (14) of the Law of Ukraine "On Media,"
- Promote the professional development of judges in adjudicating cases involving the dissemination of unlawful online content, with a view to better applying ECtHR standards.

2.1.4. Restrictions on Freedom of Expression Related to the Protection of Reputation and the Rights of Others

Article 34 of the Constitution of Ukraine guarantees everyone the right to freedom of thought and speech, and to freely express their views and beliefs. However, it also states that these rights may be restricted by law to protect the reputation or rights of others. The ECtHR has repeatedly balanced the right to freedom of expression and the right to respect for private life and reputation in cases against Ukraine under Article 10 of the European Convention on Human Rights, resulting in the gradual adaptation of national legislation to European standards.

Article 30 of the Law of Ukraine "On Information" distinguishes between factual statements and value judgments. No one can be held liable for expressing value judgments. Value judgments do not contain factual data that can be verified or refuted, but may be expressed through certain stylistic means, such as satire, hyperbole, or allegory. If a person believes that such judgments or opinions infringe on their dignity, honour, business reputation, or other personal non-property rights, they have the right to use the legal means provided to respond, as well as to present their own interpretation of the case in the same media outlet to refute the opinions expressed and offer an alternative view. If an opinion is expressed in a crude, offensive, or obscene manner that damages the person's dignity, honour, or business reputation, the person who expressed it in such a manner may be held liable for moral damages. However, such an opinion cannot be refuted, as it is not factual information.

National legislation recognises the concept of "public figures," allowing for broader criticism and intrusion into their private lives. It also prohibits restricting access to information of public interest - for example, information that reveals threats to state sovereignty and territorial integrity of Ukraine; enables the exercise of constitutional rights, freedoms, and duties; exposes human rights violations or attempts to mislead the public; or concerns harmful environmental and other negative consequences of the actions (or inaction) of individuals or legal entities. For journalists, the Law of Ukraine "On State Support for Media, Guarantees of Professional Activity and Social Protection of Journalists" provides additional safeguards and exempts them from liability for disseminating false information if the court determines the journalist acted in good faith and attempted to verify the information.

However, courts do not always correctly apply these legislative guarantees in practice. For instance, in 2024 the Supreme Court overturned the rulings of lower courts and found

their decision to require a public apology on a Facebook group page to be incorrect. The Court aligned its position with the ECtHR judgment in the Editorial Board of Pravoye Delo and Shtekel v. Ukraine, which held that apologies are not a legitimate form of redress for damage to honour, dignity, or reputation, as they are not foreseen by civil law. In other cases, the Supreme Court has also noted misapplication of legal provisions regarding the distinction between facts and value judgments.

Currently, the existing level of implementation of European standards for balancing freedom of expression and the protection of reputation and privacy is insufficient. One of the most common tools for exerting pressure on journalists and media outlets remains so-called strategic litigation against public participation (SLAPPs), which are designed to suppress public discussion, legitimate criticism, or protest, and to deter journalists or other civil society actors from future coverage.

In December 2024, an employee of the State Bureau of Investigation and former prosecutor, Oleksandr Hovorushchak, filed a lawsuit against Slidstvo.Info and journalist Yanina Korniienko over an investigation into his family's acquisition of assets allegedly worth UAH 35,000,000. The official demanded the retraction and deletion of all information related to him and his relatives, as well as UAH 40,000 in moral damages from each defendant. Previously, in 2023, Ukrainian entrepreneur Serhii Semeniuk filed a defamation lawsuit against Slidstvo.Info and author Yanina Korniienko over an investigation into alleged ties between his cleaning companies and Russia. His lawyers reportedly attempted to manipulate the court's automated case assignment system and added a co-defendant to justify filing the lawsuit with a specific district court.

Former judge of the Donetsk District Administrative Court, Liudmyla Arestova, filed a lawsuit in December 2024 for the protection of her honour, dignity, and business reputation against the Ukrainian service of Radio Free Europe/Radio Liberty and the journalist of the Schemes, Heorhii Shabaiev. In her claim, the former judge requests that the information presented in the Schemes investigation regarding her Russian citizenship be declared false and defamatory to her honour, dignity, and business reputation; that photographs of her, which Schemes found in open sources, be removed from the publication; and that compensation in the amount of UAH 180,000 be awarded for moral damages.

A striking example of a SLAPP is the series of lawsuits filed by former Yanukovych-era official Andrii Portnov, which were clearly aimed at discouraging journalists from covering his activities due to the threat of legal action. In 2020, Portnov sued the investigative journalism programme Schemes and its editor-in-chief Nataliia Sedletska, demanding that they retract statements linking him to the arson of a crew member's car and to threats against the newsroom. The Pechersk District Court ruled in Portnov's favour. In September 2024, this decision was upheld by the Kyiv Court of Appeal. The journalists filed a cassation appeal. In another case, in December 2024, the Kyiv Court of Appeal upheld a ruling ordering Hromadske to delete an investigation linking Portnov to activities related to the occupation of Crimea in 2014 and awarded compensation for legal assistance totalling UAH 56,000 and UAH 15,000 for attorney services. The editorial team is preparing an appeal to the Supreme Court.

At the local level, similar lawsuits are also widespread and may have an even greater "chilling effect." In 2023, editor-in-chief of the online publication Volyn Online, Mariiana Metelska, reported that the company group Tekhnotorg had filed a lawsuit against her following an investigation into possible links between their operations and Russia and Belarus. The plaintiffs demanded a retraction and UAH 750,000 in moral damages. The case is currently being heard in a court of first instance.

In December 2024, the Council of Europe presented initial legislative and policy proposals for implementing European and Council of Europe standards on combating the use of SLAPPs in Ukraine. The document offers practical recommendations for updating procedural codes, the Law of Ukraine "On Court Fees," and considers the adoption of a separate law defining SLAPPs, their characteristics, and additional protective measures - including support mechanisms for victims. These proposals are based on Recommendation CM/Rec(2024)2 of the Committee of Ministers to member States on combating the use of SLAPPs, adopted on 5 April 2024. When amending national legislation, it is also important to consider the EU Directive 2024/1069 of the European Parliament and of the Council of 11 April 2024 "on the protection of persons who engage in public participation from manifestly unfounded or abusive court proceedings (strategic lawsuits against public participation)."

To harmonise Ukrainian legislation with the requirements of the EU, the recommendations of the Council of Europe and the UN, it is necessary to:

- Develop and introduce legal amendments to counter SLAPPs, including definitions and key characteristics of SLAPPs, essential procedural safeguards and anti-abuse mechanisms, and protection and support for victims, in accordance with Recommendation CM/Rec(2024)2 of the Committee of Ministers and Directive (EU) 2024/1069,
- Establish mechanisms for monitoring and raising awareness of the harm caused by SLAPPs, including training for judges, prosecutors, and lawyers,
- Initiate professional discussions on amending the Rules of Attorney Ethics to address the unethical nature of SLAPPs and distinguish them from legitimate defamation claims.

2.1.5. Restrictions on Freedom of Expression for the Protection of Morals and Public Health

The Constitution of Ukraine does not list the "protection of morals" as a separate ground for restricting freedom of expression. Therefore, any "moral" reservations are only permissible if they are properly justified by the need to protect national security, territorial integrity, or public order to prevent disorder or crime, to protect public health, to safeguard the reputation or rights of others, to prevent the disclosure of confidential information, or to uphold the authority and impartiality of the judiciary.

The controversial Law of Ukraine "On the Protection of Public Morals," which established "the legal basis for protecting society from the distribution of products that negatively affect public morals," was repealed in 2023 with the adoption of the Law of Ukraine "On Media." Article 36 of the latter prohibits the dissemination via media and video-sharing platforms of pornographic materials, promotion of narcotic drugs and psychotropic substances, and advocacy of cruelty to animals. Violations are subject to a warning or a fine (for online media - up to 10 minimum wages if the warning is not complied with or in the case of repeated significant violations within one month). Dissemination of materials that promote sexual exploitation and violence against children, depict sexual relations involving children, or use child imagery (visual recordings of children) in sexual or erotic performances constitutes a grave violation, for which a fine of up to 15 minimum wages may be imposed on online media entities (for a single violation). Article 42 of the Law "On Media" also regulates the dissemination of certain types of content to avoid harm to children - this will be covered in the following section.

In 2024, discussions continued regarding the decriminalisation of pornography (excluding child pornography). Article 301 of the Criminal Code of Ukraine currently provides for liability for the distribution of works, images, films, and video content of a pornographic nature, with a maximum sentence of up to five years' imprisonment. As early as 2022, a petition calling for the decriminalisation of pornography gathered 25,000 signatures. Later that year, a coalition of civil society organisations called for the decriminalisation of pornography distribution. On 18 September 2023, draft law No. 9623 was registered, proposing amendments to the Criminal Code of Ukraine to guarantee freedom from interference in private life. The proposed amendment to Article 301 would have limited criminal liability to cases involving the distribution of pornographic content without the consent of the person depicted ("revenge porn") or among minors. At the same time, the authors of the draft law proposed to retain criminal liability for the distribution or production of child pornography and extreme pornography (such as involving bestiality, necrophilia, or depictions of violence). No progress was made on the consideration of this draft law.

On 11 November 2024, members of parliament registered a new draft law No. 12191 "On Amendments to the Criminal Code of Ukraine to Improve Its Provisions on Criminal Offences Against Public Order and Morals," which represents a revised and more "compromise-based" version of earlier proposals. The new bill proposes to retain criminal liability for distributing pornographic works, images, or other pornographic items, films, video content, or pornographic computer programmes to children and minors, as well as for coercing children to produce pornographic materials. On 23 December 2024, the Verkhovna Rada Committee on Law Enforcement considered draft law No. 12191 and recommended that parliament adopt it as a basis, with an extended deadline for submitting and reviewing amendments and proposals.

The need to decriminalise pornography for adults is also supported by judicial practice. In many cases, convictions under Article 301 of the Criminal Code of Ukraine have involved actions that are clearly not socially dangerous and only serve to burden the national judicial system. The Better Regulation Delivery Office, as part of the Pornometer project, analysed court data and found that in the first nine months of 2024, 1,104 indictments were filed, representing a 75% increase compared to the same period in 2023. However, only 7% of cases ended in court verdicts over the past two years. During the first nine months of 2024, Ukrainian courts issued 43 convictions, with typical examples including: case No. 367/4183/24, in which a woman received a probation sentence and was barred from working in photo and video production for selling self-made videos via the Telegram messenger; case No. 176/573/24, in which a man was convicted for uploading his photos to a dating site; and case No. 542/1052/23, in which a person was fined UAH 34,000 for sending two erotic videos to their partner.

The Law of Ukraine "On Advertising" contains a range of restrictions aimed at protecting morality and public health. Amendments to this Law in 2023 - introduced to implement certain provisions of the EU acquis on audiovisual advertising - expanded the ban on including in advertising any statements and/or images that are discriminatory and/or incite hatred, enmity, or cruelty towards individuals or groups based on age, ethnicity, sexual orientation, disability, or other grounds. The ban on advertising, sponsorship, and product placement of tobacco products, devices for tobacco consumption without combustion, accessories related to their use, herbal smoking products, electronic cigarettes, refill containers, e-liquids used in electronic cigarettes, and heated tobacco products (HTPs) with electronic heating devices has also been tightened. The law also explicitly introduces mechanisms for self-regulation and co-regulation in the advertising sector through the adoption of codes (rules) for the creation and dissemination of advertisements, especially in relation to: alcohol advertising - aimed at reducing its impact on children; advertisements included in children's programmes of audio

or audiovisual media; and video-sharing platform advertisements for foods and beverages high in fats, trans-fatty acids, salt, sodium, or sugar, whose excessive consumption is not recommended in a balanced diet. Draft law No. 12253 proposes further alignment of the Law of Ukraine "On Advertising" with EU requirements, particularly regarding the definition of discriminatory advertising, and restrictions on the advertising, sponsorship, and product placement of alcoholic beverages, as well as advertising and teleshopping of medical products, among others.

To bring Ukrainian legislation and its implementation in this area into compliance with EU and Council of Europe requirements, it is recommended to:

- Amend the Criminal Code of Ukraine to remove the general prohibition on the possession and distribution of pornography, except in cases involving or targeting minors,
- Develop and adopt legislative amendments establishing effective safeguards to protect individuals from the non-consensual dissemination of intimate images ("revenge porn"),
- Align national advertising legislation with the requirements of the EU Audiovisual Media Services Directive, particularly with respect to restrictions on the advertising, sponsorship, and product placement of goods and services harmful to health.

2.1.6. Restrictions on Freedom of Expression Related to the Protection of Children

Article 42 of the Law of Ukraine "On Media" sets out requirements for the dissemination of content that may harm the physical, mental, or moral development of children. Such content includes:

- Excessive focus on violence, namely the dissemination of statements or depictions of violence that are unjustified or excessive in the context of a particular programme or publication,
- Positive portrayal of self-inflicted injury or suicide, incitement to such acts, or excessive and unjustified detail regarding the means and circumstances of suicide,
- Depictions of animal cruelty, methods of animal killing, and close-up images of dying or brutally mutilated animals, except where such depictions are necessary to promote humane treatment of animals, provided viewers are warned of the graphic scenes,
- Positive portrayal of vandalism,
- Positive portrayal of criminal activity or glorification of perpetrators, excessively detailed modelling of criminal acts and/or depictions of actions that may be dangerous for children to imitate,
- Positive portrayal of addiction to narcotic, toxic, or psychotropic substances, tobacco, or alcohol, as well as other substances used or that may be used for intoxication, or encouragement of their use, production, distribution, or acquisition - excluding works of art,
- Obscene expressions, language, or gestures, except when used in works of art or in reporting on current events and news with the nature of regular press information,
- Encouragement or incitement to participate in gambling, except as provided by the laws of Ukraine,

- Close-up depictions of deceased, dying, or brutally mutilated persons, except where necessary for the identification of a person and subject to viewer warnings of graphic scenes.

On the Internet, such content may be shown by VOD services only under the condition of using a conditional access system, warning about the presence of such content, and marking it with special symbols in the catalogue. Online media may distribute the above-mentioned content only if proper warnings are in place about its potential harmfulness to children.

The restrictions set by this provision are proportionate and not excessive, and have been recognised as compliant with the requirements of the EU Audiovisual Media Services Directive. In addition, the legislation provides that the interpretation criteria for these restrictions will be developed by co-regulation bodies, which were only registered in 2024 and will begin active work on developing relevant co-regulation codes in 2025. In 2024, the National Broadcasting Council imposed a sanction in only one case of online-related violation: the unregistered Kryvyi Rih online media outlet Svoi received an order for publishing a photo of a minor in an article without proper justification. The media outlet removed the image following the regulator's action.

Article 36 of the Law "On Media" also prohibits the distribution in Ukraine of materials that encourage the sexual exploitation and abuse of children, depict sexual relations involving children, or use the image of children (visual recordings of children) in performances of a sexual or erotic nature. Under the law, such a violation is considered grave, and media outlets involved may be immediately subject to a fine. However, no such violations by media were recorded by the National Broadcasting Council in 2024.

Of note is the practice of industry-based norm-making – joint coordination acts developed by audiovisual media representatives under the supervision of the media regulator since 2016, which directly address the protection of children's rights in the media. In January 2024, it was announced that the text of the sixth such act had been agreed, focusing on the coverage of pre-trial investigations involving children. However, the act's text was not subsequently published, which may indicate that work on it continues or has been postponed until the co-regulation bodies under the Law "On Media" become operational. These bodies will take such coordination acts into account when drafting their own codes in 2025.

Articles 301-1 and 301-2 of the Criminal Code establish liability for actions related to accessing, importing, producing, and distributing child pornography – including via information and communication technologies – as well as for conducting or attending performances of a sexual nature involving minors. These provisions were introduced in 2021 to implement the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, and align with its Articles 20–21, which mandate criminalisation of such acts. In 2024, no convictions were issued under Article 301-2, while 84 convictions were handed down under Article 301-1 of the Criminal Code of Ukraine.

To harmonise and implement Ukrainian legislation in this area with EU, Council of Europe, and UN standards, it is recommended to:

- Support the development of media co-regulation codes that define the criteria for determining content that may harm the physical, mental, or moral development of children.

2.1.7. Restrictions on Freedom of Expression Related to the Authority and Impartiality of the Judiciary

Article 34 of the Constitution of Ukraine permits restrictions on the right to freedom of thought and speech and the free expression of views and beliefs in accordance with the law for the purpose of maintaining the authority and impartiality of the judiciary. Article 6(3) of the Law of Ukraine "On the Judiciary and the Status of Judges" prohibits interference in the administration of justice, exerting influence on a court or judge in any manner, contempt of court, and the collection, storage, use, or dissemination of information with the aim of discrediting the court or influencing its impartiality. In particular, Article 376 of the Criminal Code of Ukraine establishes criminal liability for interfering in any form with the activities of a judge with the intention of obstructing the performance of their official duties or compelling the adoption of an unjust decision. According to Article 48(4) of the Law of Ukraine "On the Judiciary and the Status of Judges," a judge is obliged to report interference in their judicial activity to the High Council of Justice and the Prosecutor General.

In 2023, a post by the head of the Anti-Corruption Action Center, Vitalii Shabunin, which criticised the ability of certain judges of the High Anti-Corruption Court to perform their duties, prompted a referral to the High Council of Justice (HCJ). The HCJ interpreted the post as possible interference with the judiciary under Article 376 of the Criminal Code. This approach to interpreting criticism may have negative consequences for civil society, journalists, and activists engaged in judicial oversight, as any criticism of judges could be viewed as interference, creating a risk of criminal prosecution.

According to the Registry of Judges' Notifications of Interference (the Registry), a total of 73 notifications in 2024 concerned criticism of judges, allegations of corruption, and similar issues raised during court proceedings, in media publications and investigations, on social media, or in parties' submissions to the court. No decisions have yet been issued by the HCJ regarding eleven of these notifications. Eleven notifications concerned media investigations and publications (in ten of those cases, the HCJ did not find any interference in judicial activity). In 52 out of 73 cases, the HCJ determined that there were no grounds to believe there was a risk of interference in judicial activity. Nonetheless, notifications, articles, and social media posts alleging corruption by judges or threats against them frequently served as the basis for the HCJ to refer cases to the prosecutor's office for further investigation.

In 2024, there was a continued trend of restricting access to information about judicial activity, undermining the principle of openness of court decisions, hearings, and information about court proceedings (Article 11(1)) of the Law of Ukraine "On the Judiciary and the Status of Judges"). Due to the full-scale invasion, access to the Unified State Register of Court Decisions was restricted in 2022 to protect the security of judges and trial participants, as well as information security. Despite partial restoration of access following pressure from civil society, certain court decisions remained inaccessible in 2024 (as documented by DEJURE Foundation). Moreover, on 23 May 2024, draft law No. 7033-d was adopted at first reading with recommendations for revision. The draft law disproportionately restricts access to certain categories of court decisions, including those related to crimes against national security - information that may be of public interest.

Since 2023, access to information about the judiciary has continued to be significantly limited, reflecting a regression in judicial transparency. In particular, decisions of the Supreme Court and the actions of judicial governance bodies such as the High Qualification Commission of Judges and the High Council of Justice have frequently and unjustifiably

restricted public access to important information about judges' activities, citing the need to protect confidentiality or national security. This lack of transparency undermines public trust in the judiciary and calls for reform to strike a balance between confidentiality and public oversight.

To align Ukrainian legislation with the standards of the Council of Europe, the EU, and UN guidance documents, it is recommended to:

- Ensure transparency of the judiciary by expanding access to the Unified State Register of Court Decisions, with appropriate security measures, consideration of the public interest, and clear oversight of the legal grounds for restricting access to judicial decisions,
- Harmonise restrictions on access to information and define clear justifications and criteria that ensure a balance between security, confidentiality, and the right to information.

2.2. Media Freedom

2.2.1. Freedom of Media Activity, Pluralism, and Editorial Independence

The Law of Ukraine "On Media" defines its purpose as ensuring the exercise of the right to freedom of expression, the right to receive diverse, reliable, and timely information, ensuring pluralism of opinions and the free dissemination of information, protecting Ukraine's national interests and the rights of media service users, regulating activities in the media sector in accordance with the principles of transparency, fairness, and impartiality, and fostering a competitive environment, equality, and media independence. In line with the Constitution of Ukraine and the EU Audiovisual Media Services Directive, the Law prohibits censorship and unlawful interference in the activities of media sector entities by state authorities, local self-government bodies, civil society organisations, political parties, media owners, or any other individuals or legal entities.

At the same time, the Directive is not the only EU act requiring media pluralism and guarantees of freedom of media activity, and the mere codification of principles in law does not ensure their genuine implementation in practice. The European Media Freedom Act (EMFA) - a regulation adopted by the EU in April 2024 - aims to safeguard media pluralism and independence in the context of digital transformation of the media landscape. While the document is directly applicable in EU Member States, it also requires them to introduce a set of legal guarantees into national legislation to give practical effect to EMFA provisions. In 2024, it was included in the list of EU acts subject to screening for alignment with Ukrainian national legislation, making its implementation an important step on Ukraine's path toward EU integration, especially given the EU's increased attention to media reform.

General principles regarding user access to diverse, editorially independent media content; the editorial and functional independence of public broadcasting; proper justification and proportionality of regulatory measures applied to media by public regulators; and media ownership transparency are already enshrined in the current Law "On Media." However, these provisions alone cannot fully protect against forms of pressure or censorship not directly related to the exercise of regulatory powers. For example, in October 2024, Ukrainian Pravda reported prolonged and systemic pressure from the Office of the President on the editorial team and individual journalists of the online media outlet, including blocking government speakers from engaging with Ukrainian Pravda journalists or participating in events, as well as pressuring businesses to halt advertising cooperation

with the outlet. Such incidents highlight the need for public scrutiny and a broader review of the system of accountability for obstructing journalistic activity (see Section 2.2.3).

The European Media Freedom Act provides for amendments to national legislation requiring the assessment of the impact of media market concentration on pluralism and editorial independence, separately from the assessment conducted under the Law of Ukraine "On the Protection of Economic Competition." This assessment should consider the effect on the availability of media services in the market, safeguards for editorial independence, the economic viability of media without concentration, and the commitments undertaken by parties to the concentration regarding the promotion of media pluralism and editorial independence. The media regulator should play an active role in conducting this assessment, meaning the powers of the National Broadcasting Council should be expanded, along with strengthening its expertise to carry out such analysis.

The EMFA also places significant emphasis on the transparency and non-discriminatory allocation of state funding for media. Public funds or any benefits provided, directly or indirectly, by public authorities or their legal entities to media or online platforms for state advertising or service contracts must be allocated transparently, objectively, proportionally, and without discrimination, and be published in advance via electronic and user-friendly means. Funding competitions must be open. Media entities receiving state support are obliged to disclose such support. The Law "On Media" will also need to include a general obligation for media that provide news content and coverage of current events to ensure internal editorial freedom and disclose any potential conflicts of interest that may affect their reporting.

The implementation of these provisions will require, among other things, a review of current approaches to state budget funding and the elimination of potential abuses.

To harmonise and implement Ukrainian legislation with EU and Council of Europe standards, it is necessary to:

- Develop a comprehensive plan for implementing the requirements of the European Media Freedom Act into national legislation, with the involvement of media representatives, civil society, and experts from the EU and Council of Europe,
- Strengthen the financial and expert capacity of the National Broadcasting Council to implement the proposed changes, particularly in relation to assessing the impact of media concentration on pluralism and editorial independence.

2.2.2. Protection of Journalistic Sources and Confidentiality of Communications

Article 25 of the Law of Ukraine "On Information" grants journalists the right not to disclose the source of information or any information that could lead to the identification of such sources, except when required to do so by a court decision based on the law. Article 65 of the Criminal Procedure Code of Ukraine stipulates that journalists may not be questioned as witnesses regarding information that contains confidential professional data provided under the condition of non-disclosure of the authorship or source. Additionally, information held by a media outlet or journalist that was provided under the condition of non-disclosure is considered legally protected (Article 162) and access to it is permitted only if it is impossible to prove certain circumstances by other means.

At first glance, national legislation appears to guarantee the protection of journalistic sources and the confidentiality of their communications, but in reality, the existing provisions do not meet the minimum standard established by the EU's European Media

Freedom Act. Moreover, even the guarantees currently in place are not effectively implemented in practice.

In 2021, the ECtHR issued a ruling in the case of journalist Nataliia Sedletska, finding Ukraine in violation of Article 10 of the European Convention on Human Rights. The applicant complained that court orders granting the Prosecutor General's Office of Ukraine access to information about incoming and outgoing calls from her mobile phone constituted unjustified interference with her right to protect journalistic sources. The Court noted several violations leading to unlawful interference with her rights: unjustified consideration of the request for access to data without the applicant's participation or notification, insufficient justification provided by domestic courts for collecting extensive protected information on her personal and professional contacts over a 16-month period, and limited opportunities for the applicant to challenge the court order.

Meanwhile, while specific legal guarantees for protecting journalistic sources exist in cases involving temporary access to property and documents, such guarantees are absent in relation to temporary seizure of property, arrest of property, searches, or covert investigative (search) actions. These procedures currently lack any balancing of investigative interests with the protection of journalistic sources or their confidential communications.

The European Media Freedom Act seeks to unify approaches to protecting journalistic sources and communications across the EU by establishing minimum safeguards. For Ukraine, aligning its national legislation with this Act is part of the accession negotiations with the EU. One key necessary reform is to extend protections not only to journalists, but also to other media workers and individuals who, through regular or professional relations with a media service provider or its editorial office, may possess or disclose such information.

Ukrainian legislation provides that access to confidential communications in the context of criminal proceedings may only be granted for the detection or prevention of serious or particularly serious crimes, which aligns with the EU approach. However, investigations used to justify access to confidential communications (including through spyware) must directly concern the person entitled to these protections, not be conducted within the framework of unrelated criminal proceedings.

Current national legislation requires that individuals be notified when investigative actions result in access to their confidential personal data as part of criminal investigations. Individuals may also request such information under personal data protection laws. However, the enforcement of these guarantees in practice requires strengthening, particularly in terms of safeguards against abuse. Oversight powers could be exercised by an independent regulatory body in the field of personal data protection (see Section 3.4.1).

Ukrainian legislation currently does not regulate the use of surveillance technologies, including spyware, which does not preclude their practical application. General guarantees for the protection of journalistic sources and confidential communications extend to surveillance cases involving special software. However, considering the intrusiveness of such technologies, their complexity in detection and oversight, the law should provide specific safeguards to ensure their legal use, including narrowly defined grounds, transparent procedures for application and oversight. Therefore, national legislation, particularly regarding the powers of security services, law enforcement bodies, and other state authorities, must be supplemented with adequate safeguards against the arbitrary use of such invasive surveillance tools.

In 2024, no legislative amendments were developed to strengthen the protection of journalistic sources. On the contrary, at the end of 2023, draft law No. 10242 was registered in Parliament, proposing amendments to the Criminal Code of Ukraine to establish criminal liability for unauthorised interference, distribution, or dissemination of information processed in public electronic registers, and to increase criminal liability during martial law for offences in the field of information and communication systems. Media and human rights organisations called on the Verkhovna Rada not to support this draft law, as it poses significant threats to freedom of speech, journalists' work, and the protection of journalistic sources and whistleblowers in Ukraine. Under the guise of combating "data misuse," the draft creates a tool that could be used to persecute journalists investigating corruption or abuse of power. The increased liability also opens the door for covert investigative actions against journalists, including surveillance and wiretapping, which severely undermines international standards on source protection.

To harmonise and implement Ukrainian legislation with EU and Council of Europe requirements, it is necessary to:

- Expand the list of individuals entitled to protection against the disclosure of journalistic sources or confidential communications - including other media professionals and individuals who, through regular or professional relations with a media service provider or editorial office, may possess or disclose such information,
- Amend national legislation to ensure effective judicial oversight in all cases of access to information about journalistic sources or confidential communications, as well as implement other standards set out in the European Media Freedom Act,
- Regulate the use of spyware in line with EU requirements and conditions (only when alternative measures are insufficient, only in cases of serious or particularly serious crimes committed by the person concerned, with mandatory judicial oversight, regular review, and subsequent notification about applied restrictions) or establish a ban on the use of such tools.

2.2.3. Protection Against Obstruction of Journalistic Activity in the Digital Environment

Ukrainian media and journalists are frequently targeted by cyberattacks and online threats. Investigations into such cases are typically delayed and ineffective, creating an atmosphere of impunity that encourages further violations. In 2024, the Institute of Mass Information (IMI) recorded 58 cases of cyberattacks against journalists and media outlets. The Women in Media NGO in 2024 documented 29 verified cases of online attacks against female journalists, including doxing, hate speech, defamation, and even threats of rape, death, and physical violence.

According to IMI, Russian actors continued to intimidate journalists in 2024, remaining the most frequent source of threats (45 cases) and cyberattacks (35 out of the 58 recorded incidents). Specifically, IMI reported three waves - in October, November, and December - of anonymous bomb threats sent via identical emails to multiple media outlets and journalists across various Ukrainian regions. Throughout 2024, Russian hackers hijacked Ukrainian TV broadcasts to disseminate propaganda and targeted both national and regional media websites that reported on Russian war crimes.

At the same time, threats and other forms of pressure on independent media also came from within Ukraine: IMI recorded 21 cases of obstruction and 19 cases of indirect pressure on journalists by Ukrainian actors.

The online outlet Ukrainian Pravda reported threats against investigative journalist Mykhailo Tkach in May 2024. Another incident related to a separate investigation occurred in October, but also received no adequate response from law enforcement. The Commission on Journalistic Ethics urged the authorities to give proper attention to reports from any journalists, media, or professional organisations raising concerns about such incidents and to take all appropriate follow-up measures.

Ukrainian civil society organisations also issued a statement opposing the persecution of anti-corruption activists and investigative journalists by law enforcement agencies. In April 2024, Slidstvo.Info reported that an employee of the Security Service of Ukraine may have instructed military enlistment officials to serve a draft summons to a Slidstvo.Info journalist investigating luxury property owned by the head of the SBU Cybersecurity Department. The outlet filed a complaint with law enforcement regarding persecution and obstruction of journalistic activity. The State Bureau of Investigation launched a criminal case, but the pre-trial investigation has been delayed, raising doubts about its effectiveness.

In 2024, Ukrainian courts issued 10 convictions for crimes against journalists. All of them concerned incidents of physical obstruction, property destruction, and threats made during the course of journalistic work.

To ensure adequate protection of journalists from obstruction in the digital environment, it is necessary to:

- Strengthen inter-agency coordination in investigating crimes against journalists, including those committed in the digital space,
- Enhance the effectiveness of oversight mechanisms to ensure thorough investigations of cases involving obstruction of journalists, and promote cooperation between investigative bodies, human rights defenders, and media organisations.

2.2.4. Independent and Effective Media Regulatory Authority

The National Broadcasting Council is an independent, permanent, collegiate state body that carries out state regulation, oversight, and control in the media sector based on the Constitution of Ukraine, the Law "On Media," and other laws of Ukraine. The status, powers, and appointment procedure of the regulatory authority generally comply with EU requirements - specifically, the Audiovisual Media Services Directive and the EMFA. Council of Europe experts, in assessing the provisions of Ukraine's new Law "On Media," also noted positive changes, including strengthened independence guarantees through an improved procedure for selecting candidates for National Broadcasting Council membership, the creation of co-regulation mechanisms, and the introduction of requirements for the justification and objectivity of decisions. Their analytical opinion also emphasised the importance of holding an independent and transparent competition, as well as involving the public in nominating candidates and overseeing the competition process. These aspects are currently covered by Articles 76 and 77 of the Law of Ukraine "On Media."

However, the actual implementation of legal guarantees is key to ensuring the regulator's independence and effectiveness. Since the media law came into force in 2023, the National Broadcasting Council has not received the funding provided for by law. The Law "On the State Budget of Ukraine for 2024" also suspended the provisions of Article 78 of the Law "On Media" concerning the guaranteed salaries of members of the regulatory body and staff of the regulator's secretariat. Similar restrictions

were introduced by the 2025 budget. Given the significant expansion of the National Broadcasting Council's responsibilities, the lack of sufficient resources poses a serious threat to the implementation of media reform. In its 2024 Enlargement Policy report on Ukraine, the European Commission highlighted the need to ensure sufficient funding and human resources for the National Broadcasting Council to fulfil its mandate.

Another issue that may undermine the regulator's independence and its capacity to effectively exercise its powers is the reintroduction of the mandatory state registration procedure for the National Broadcasting Council's regulatory acts by the Ministry of Justice of Ukraine. The current provisions of the Law "On Media" stipulate that such acts are not subject to state registration, as the National Broadcasting Council is a separate constitutional body and is not part of the system of executive authorities that are subordinate or accountable to the Cabinet of Ministers of Ukraine. However, the Law "On Law-Making Activity," adopted in August 2023 and set to enter into force one year after the end of martial law, reinstates this so-called "justice clearance" procedure. Draft law No. 12111, "On Amendments to Certain Laws of Ukraine Regarding Media Activities," which passed its first reading in December 2024, aims to address this issue by exempting the National Broadcasting Council's acts from the registration requirement.

The need to amend the Constitution of Ukraine to improve the procedure for forming the National Broadcasting Council's composition also remains an open question. The Constitution currently divides the appointment of an equal number (half) of the members of the regulatory body between the Parliament and the President of Ukraine. In practice, delays by either appointing entity in selecting candidates can result in the entire regulator's work being blocked. Additionally, the full name of the National Broadcasting Council no longer fully reflects the scope of its mandate – today it covers not only television and radio but also other forms of media and online platforms.

To align Ukrainian legislation and its implementation practices with EU and Council of Europe requirements, it is necessary to:

- Ensure appropriate funding for the National Broadcasting Council in full compliance with the Law of Ukraine "On Media,"
- Repeal the application of the justice clearance procedure to legal acts adopted by the National Broadcasting Council as an independent regulatory authority in the media sector,
- Following the end of martial law, consider amending the Constitution of Ukraine to enhance the independence of the National Broadcasting Council and bring its status and operational guarantees in line with EU law.

2.3. Freedom of Expression and Online Platforms

2.3.1. State Obligations to Protect the Rights of Users of Online Platforms

The effective Ukrainian legislation contains limited provisions regulating online platforms and protecting users from potential abuse. Even the existing norms are largely unenforced in practice due to the lack of jurisdiction over the most popular companies.

Online platforms under Ukrainian jurisdiction are subject to the Law of Ukraine "On Electronic Commerce" and the Law of Ukraine "On Consumer Rights Protection," but their current versions contain only general provisions on state protection of rights and do not impose specific obligations on any type of platform. Only the new version of the Law "On Consumer Rights Protection," adopted in 2023 and set to come into force after

the end of martial law, will introduce certain guarantees for marketplace users, particularly regarding access to information.

A specific category of platforms – video-sharing platforms – is additionally regulated under the Law of Ukraine "On Media" in accordance with Article 28b of the updated EU Audiovisual Media Services Directive. Article 23 of the Law "On Media" establishes the following obligations for video-sharing platform providers:

- To publish the terms of service and make them accessible to users,
- To include in the terms of service a prohibition on the dissemination of programmes, advertisements, and user content that contain illegal material or violate copyright and related rights,
- To implement age verification for users seeking access to content that may harm the physical, mental, or moral development of children, and to ensure the availability of parental control systems to protect children from such content,
- To introduce transparent and understandable mechanisms for assessing and processing user complaints about information hosted on the platform that may violate legislation or the terms of service; to ensure effective complaint resolution and inform users of the outcomes, as well as to provide a transparent, simple, and effective appeal process against platform decisions,
- To establish procedures for exercising the right to reply or correct inaccurate information and to ensure users are informed about corrections or replies, both in the descriptive information of the relevant video and via notices before accessing the video,
- To include in the terms of service requirements related to the dissemination of advertising as set by law, and to allow users to indicate whether their videos contain advertising,
- To implement effective media literacy tools and raise user awareness of such tools.

The Directive, like the Law "On Media," encourages co-regulation mechanisms for developing tools to enforce these obligations. The law also replicates the Directive's provision allowing platform users access to courts to protect their rights. As of the end of 2024, the National Broadcasting Council had not registered any video-sharing platform providers operating in Ukraine.

With regard to platforms under foreign jurisdiction, current Ukrainian law recognises the impossibility of directly regulating their activities and instead promotes a cooperation-based approach to user rights protection. The aforementioned Law "On Media" introduced the concept of an "information-sharing platform," which is intended to cover platforms such as Facebook, Instagram, X (Twitter), and others. The National Broadcasting Council is authorised to sign agreements or memorandums with such platforms. The content of these memorandums is clearly defined only in the context of national referendum legislation and includes requirements and restrictions on content dissemination on platforms accessible in Ukraine, co-regulation mechanisms, cooperation to counter disinformation during referendum preparation and conduct, ensuring transparency in campaigning, and establishing open advertising libraries. As of the end of 2024, no such memorandums had been signed with any platform.

Amidst this and the growing influence of platforms like Telegram – now a primary source of news for the majority of Ukrainians – voices have grown louder in 2024 in favour of stricter regulation of online platforms. Regulatory efforts are led by the Ministry of Digital Transformation, which is responsible for implementing the EU Digital Services

Act (DSA) in Ukraine. In August 2024, it was reported that a draft law to implement key provisions of the DSA had been prepared and was awaiting review by the European Commission for compliance with the Act. The draft envisages requirements for both states and platforms to build infrastructure for user rights protection, including notice-and-action mechanisms, out-of-court dispute resolution bodies for illegal content, and greater transparency of recommendation systems.

In March 2024, Members of Parliament registered draft law No. 11115 amending certain laws of Ukraine concerning the regulation of the activities of information-sharing platforms through which mass information is disseminated. The draft proposes introducing obligations, similar to those already mentioned for video-sharing platforms, for a broader category of entities defined in the draft law as "information-sharing platforms through which mass information is disseminated." This approach partially ensures alignment with the DSA, as it generally reflects the requirements related to notice-and-action mechanisms and the need for terms of service to comply with human rights standards. It also partially takes into account the provisions of the DSA concerning the nomination of local legal representatives in cases where a platform is not under the jurisdiction of Ukraine or a European Union Member State. However, the adoption of these provisions will not suffice to claim full implementation of the DSA and will require further refinement.

To harmonise Ukrainian legislation and its implementation in this area with the requirements of the EU, the Council of Europe, and UN recommendations, it is necessary to:

- Finalise the draft law introducing the provisions of the EU Digital Services Act in Ukraine, based on the European Commission's assessment and with public participation,
- Develop an approach for establishing jurisdiction over foreign online platforms that avoids excessive restrictions on their operations in Ukraine while better safeguarding the rights of Ukrainian users and aligning with the EU Digital Services Act,
- Submit draft law No. 11115 on amendments to certain laws of Ukraine regarding the regulation of information-sharing platforms through which mass information is disseminated, for further revision; and ensure continued coordination of all initiatives related to the regulation of online platforms with the work of the Ministry of Digital Transformation, with the aim of aligning them with EU standards in the field of digital governance.

2.3.2. Status and Obligations of Online Platforms Regarding Compliance with Freedom of Expression Principles

The Law of Ukraine "On Electronic Commerce" regulates the status of internet intermediaries and their immunity from liability. Article 9(4) of the Law effectively reproduces the EU E-Commerce Directive provision on the immunity of hosting service providers, which was later incorporated into the EU Digital Services Act. They are not liable for the dissemination of information by third parties if they have no knowledge of illegal activity or facts and circumstances indicating such illegality, and if, upon gaining such knowledge, they act expeditiously to disable or remove access to the information. This provision may apply to platforms under Ukrainian jurisdiction and is consistent with DSA requirements. However, only the Law of Ukraine "On Copyright and Related Rights," in Articles 56-58, elaborates the implementation of these norms concerning content-sharing service providers. This approach aligns with the DSA and the EU Directive on Copyright and Related Rights in the Digital Single Market. At the same time, Ukrainian

legislation does not prohibit the state from imposing a general obligation on platforms to monitor illegal activity on their networks.

In cases where online media act as intermediaries - such as when they allow comments on articles or host user-generated content sections (columns or blogs) - they may also benefit from immunity provided by the Law of Ukraine "On Media." Article 117(5) of the Law exempts online media from liability for information shared by users in comment sections or user-generated content sections on the media's website, provided the media restricts access to such content within three working days of receiving a complaint from consumers or an order from the National Broadcasting Council.

The Law "On Media" also explicitly grants the National Broadcasting Council the authority to approach providers of information-sharing platforms and search engines to restrict the dissemination in Ukraine of programs or user-generated information that violates content-related restrictions. These powers may serve as a legal basis for issuing orders regarding illegal content, as referenced in Article 9 of the DSA, which are directed at online platforms. However, non-compliance with these obligations does not entail practical consequences for platforms due to the jurisdictional limitations outlined above.

The aforementioned draft law No. 11115, which proposes amendments to several Ukrainian laws on the regulation of information-sharing platforms through which mass information is disseminated, suggests introducing an obligation for such platforms to remove illegal content upon the decision of the National Broadcasting Council. This obligation would be enforced through liability ranging from 5 to 25 minimum monthly wages per day of violation (as of the end of 2024, UAH 40,000 to UAH 200,000) for each piece of content not removed. However, this approach does not align with the DSA, which, although it provides for significant penalties for breaches of its requirements, focuses on regulating the procedures and processes that platforms must establish and maintain. Imposing substantial liability for failing to remove a single post or piece of content would constitute a disproportionate interference.

To harmonise Ukrainian legislation and its implementation in this area with the requirements of the EU, the Council of Europe, and UN recommendations, it is necessary to:

- Finalise the draft law intended to implement the provisions of the EU Digital Services Act in Ukraine, in accordance with the conclusions of the European Commission and with the involvement of civil society,
- Submit draft law No. 11115, which proposes amendments to certain laws of Ukraine regarding the regulation of information-sharing platforms through which mass information is disseminated, for further revision; and ensure ongoing coordination of all initiatives related to the regulation of online platforms with the activities of the Ministry of Digital Transformation, with the aim of ensuring their compliance with EU standards in the field of digital governance.

2.3.3. Independent and Effective Regulatory Body in the Field of Online Platforms

In its 2024 Enlargement Policy report on Ukraine, the European Commission highlighted the importance of developing an "independent regulatory capacity" in the field of digital services and establishing a roadmap with concrete steps to align regulation with the EU Digital Services Act (DSA). These steps should include, among other things, the identification of competent authorities responsible for implementing online platform regulations. The DSA allows for the appointment of multiple competent authorities to share responsibilities for implementation. These may include regulators in the areas

of data protection, consumer protection, electronic communications, or media. However, each EU Member State, even if several authorities are assigned implementation roles, is required to designate a single public authority responsible for oversight and coordination - referred to as the Digital Services Coordinator.

The selection of competent authorities and the Digital Services Coordinator will be critical to building an effective regulatory system for online platforms in Ukraine. To date, the Ministry of Digital Transformation has not publicly presented its vision for this institutional framework. Potential options include establishing a new institution or assigning additional powers to existing state authorities that meet the DSA's criteria, particularly those that are independent.

For example, the National Broadcasting Council already holds specific responsibilities for video-sharing platforms under the Law of Ukraine "On Media." In accordance with the EU Audiovisual Media Services Directive, the National Broadcasting Council may hold platforms accountable for, among other things, failing to implement age-verification systems for content that could harm children, or lacking mechanisms that allow users to report the distribution of illegal content.

Another potential candidate is the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NCEC), which has experience regulating a category of internet intermediaries - namely, providers of electronic communications services that qualify under the DSA as *mere conduit*. Although the effective Law of Ukraine "On Electronic Communications" does not establish the obligations required of such entities under the DSA, the NCEC has experience working with a large number of entities that will be subject to the new digital services legislation. At the same time, both the NCEC and the National Broadcasting Council currently lack sufficient financial and human resources to carry out additional powers due to the suspension of guaranteed funding.

It should be noted that a new regulatory body is also required in the field of personal data protection, in line with the EU General Data Protection Regulation, as well as in the future for the regulation of artificial intelligence under the EU Artificial Intelligence Act. This underscores the need for a comprehensive approach to the formation of a new institutional system of regulatory bodies across the domains of media, technology, and human rights.

To harmonise Ukrainian legislation with the requirements of the EU and the Council of Europe, it is necessary to:

- Develop a unified and coordinated approach to the creation/appointment of new regulatory bodies in the areas of digital services, data protection, and artificial intelligence, including alignment of their status and powers and the procedures for cooperation with other competent authorities,
- Ensure, both legally and in practice, adequate funding and resources for competent authorities to effectively perform their duties under the EU Digital Services Act,
- Once martial law is lifted, consider constitutional amendments to strengthen the independence of the National Broadcasting Council and to establish a general legal framework for the operation of independent regulatory authorities.

2.4. Freedom of Expression Under Martial Law

2.4.1. Restrictions on Freedom of Expression During Martial Law

On 4 April 2024, Ukraine updated its derogation declaration from obligations under the International Covenant on Civil and Political Rights and the European Convention on Human Rights. The declaration continues to contain provisions allowing Ukraine to impose additional restrictions on the rights guaranteed by Articles 19 and 10 of the respective international instruments, which safeguard the right to freedom of expression. The text of the declaration remains general and does not specify concrete measures that may be introduced to limit freedom of speech during martial law.

The Law of Ukraine "On the Legal Regime of Martial Law" permits the regulation of media activities by military command and military administrations, under procedures established by the Cabinet of Ministers. However, such a regulatory procedure has not been adopted. In 2022, the Commander-in-Chief of the Armed Forces of Ukraine issued Order No. 73 "On the Organisation of Interaction Between the Armed Forces of Ukraine, Other Defence Forces, and Media Representatives During Martial Law," which was last amended in February 2024. According to experts, these amendments liberalised access to front-line areas (the so-called "red zone"), enabled unsupervised activity in the "yellow zone," and allowed individual bloggers to receive accreditation - positive developments for online media operations.

The Law of Ukraine "On Media" includes Chapter IX, which introduces restrictions aimed at limiting the influence of the aggressor state in Ukraine's information space. These restrictions apply during the period of aggression and throughout a five-year transitional period (subject to annual review) following the revocation by the Verkhovna Rada of the aggressor state designation. Article 119 of the Law prohibits the dissemination of four types of unlawful content during armed aggression:

- Information portraying the armed aggression against Ukraine as an internal conflict, civil conflict, or civil war, if it incites hostility or hatred, or calls for violent change, overthrow of the constitutional order, or violation of territorial integrity,
- False materials regarding the armed aggression and actions of the aggressor state, its officials, or controlled individuals or organisations, where such content incites hostility or calls for violent change or violations of territorial integrity,
- Programs or materials (excluding news and analytical programs) featuring individuals listed in the Register of Persons Who Pose a Threat to National Security,
- Musical recordings, videos, or clips performed by singers who are or were citizens of the aggressor state after 1991 and/or produced by individuals or entities who were citizens or are registered in the aggressor state.

Additionally, coverage of the activities of aggressor state authorities in news or analytical programming must be accompanied by a disclaimer regarding the aggressor state status. The first two types of content listed above are considered grave violations for online media and may lead to sanctions. The other violations are classified as significant, leading to less severe accountability. In 2024, the National Broadcasting Council did not hold any online media accountable for breaches of these legal provisions. The Law "On Media" also foresees the development of co-regulation codes governing the creation and dissemination of content related to the aggressor state designation and the first two content categories listed above. The first codes are expected to be adopted in 2025.

Nonetheless, questions remain about the legal quality of these restrictions. For example, the criteria for inclusion in the Register of Persons Who Pose a Threat to National Security remain vague. Although in 2024 the Ministry of Culture and Strategic Communications cited grounds for listing 22 individuals (e.g., in the order dated 22 October 2024), many individuals added before the Media Law was enacted remain listed without proper review. Similar concerns about legal certainty have been raised in relation to the broadcast ban on Russian music and the creation of so-called white lists of Russian artists.

Another category of media restrictions stems from the principle of origin and founding country of media actors. Article 120 of the Law prohibits certain individuals from acting as media entities in Ukraine. In practice, this means Russian nationals and legal entities, as well as Ukrainian companies directly or partially (2% or more) owned or funded by Russians or Russian legal entities, cannot obtain media licences or register as media entities. This restriction has been in effect since 2015 and was extended in 2023 to include online media.

Among general restrictions on the right to receive and disseminate information during martial law are amendments to the Criminal Code of Ukraine. Article 114-2, introduced in 2022, establishes criminal liability for disseminating information about the delivery, movement, or stockpiling of weapons, ammunition, or military supplies in Ukraine during martial law, including their movement within the country (punishable by 3 to 5 years' imprisonment). It also criminalises dissemination of information about the movement or deployment of the Armed Forces of Ukraine or other lawful military formations, if identification on the ground is possible (punishable by 5 to 8 years' imprisonment). These offences apply only if such information has not already been published by the military, intelligence, or other authorised bodies. Aggravating circumstances can increase the penalty to 8-12 years. In 2022-2023, 112 convictions were issued under this Article, with 85 more in 2024. Social media platforms, especially Telegram, are most commonly used for unauthorised information dissemination. A review of case law indicates difficulties in distinguishing liability under this article and Article 111 of the Criminal Code of Ukraine, which establishes liability for high treason. The Supreme Court considers the search for, collection, and transmission to representatives of a foreign aggressor state of information about the location of military equipment, personnel of the Armed Forces of Ukraine, and other military formations involved in repelling the armed aggression of the Russian Federation to constitute high treason, as such actions contribute to the potential or actual efforts of a foreign state, foreign organisation, or their representatives to harm the national security of Ukraine.

Additionally, attempts to restrict the use of the Telegram messenger, which is linked to Russia, deserve mention. On 19 September 2024, the National Cybersecurity Coordination Centre , under the National Security and Defence Council, issued a recommendation decision to restrict Telegram use on official devices in government bodies, military units, and critical infrastructure. Several educational institutions later followed suit.

To ensure that restrictions on freedom of expression during martial law are justified and proportionate in accordance with international human rights standards, it is necessary to:

- Clearly define the scope of derogations from freedom of expression obligations in the event of extended martial law and update the relevant declaration,
- Ensure full implementation of the updated Order No. 73 to improve access for accredited online media to conflict zones and support objective war reporting,

- Update legislation concerning the formation of the Register of Persons Who Pose a Threat to National Security and the white lists of artists from the aggressor state to ensure legal certainty,
- Support the development of co-regulation codes for media that define criteria for classifying information as prohibited under Article 119(1), subparagraphs (1) and (2), and Article 119(2) of the Law of Ukraine "On Media,"
- Following the end of martial law, ensure a proper transition to full guarantees of freedom of expression and media freedom, taking into account restrictions established by the Law "On Media,"
- Review amendments to the Criminal Code to eliminate overlaps between articles that establish liability for unauthorised dissemination of information on military equipment or troop positions.

2.4.2. Legal Basis and Procedure for Blocking Internet Resources During Wartime

Among the procedures for website blocking that currently exist in Ukraine, two are applicable under martial law. These procedures involve the activities of the National Broadcasting Council and the National Centre for Operational and Technical Management of Electronic Communications Networks of Ukraine (NCON), and are governed by the Laws of Ukraine "On Media" and "On Electronic Communications," respectively.

Article 123 of the Law "On Media" allows the National Broadcasting Council to block websites exclusively of on-demand audiovisual media services (so-called VOD services) and audiovisual service providers of the aggressor state (essentially websites that provide access to packages of TV channels), if they meet a number of legal criteria (such as having a structure of ownership involving a representative of the aggressor state, being financed by it, or being targeted at the territory and audience of that state). One of the criteria for targeting includes offering access to media or content the dissemination of which is restricted in Ukraine. Once one of these criteria is established through the due procedure, the service is added to the List of On-Demand Audiovisual Media Services and Audiovisual Service Providers of the Aggressor State. A decision to add a service to the List may be appealed in court.

In the decision to add a service to the List, the media regulator must indicate both the grounds for inclusion and the list of actions to restrict access to the service. One such action is notification to the NCEC about the list of websites used to provide the service, to which access must be restricted by electronic communications service providers in Ukraine. This notification must be sent within three working days from the date of the decision, after which the NCEC has three more working days to inform operators, who must restrict access to the websites within the following three working days. In practice, the implementation of this provision in 2024 resulted in five services being added to the List. The regulator duly published the decisions, and the List includes links to the corresponding decisions. In total, 15 websites providing access to these services - mainly those targeting the aggressor state - were blocked.

More problematic from the standpoint of international standards are the restrictions imposed by the NCON, which were already partially discussed in Section 1.1.5 of this Report. Data from the Human Rights Platform indicate that 11,754 websites had been blocked as of August 2023. These blockings continued in 2024: 131 NCON orders to block domain names and IP addresses were published on the State Service for Special Communications and Information Protection's website over the year. In previous periods, this blocking procedure was also applied to websites selling alcohol and tobacco products

and gambling websites - categories not directly related to national security, which is the primary purpose this procedure is meant to address. The NCON also introduced a phishing domain filtering system, which has been criticised by the Internet Association of Ukraine due to concerns over the NCON's mandate and the risk of the system being used to block websites not associated with fraud.

To harmonise Ukrainian legislation and its implementation in this area with EU, Council of Europe, and UN standards and recommendations, it is necessary to:

- Adopt amendments to Cabinet of Ministers Resolution No. 812 of 29 June 2004, clarifying the scope of NCON's powers regarding the blocking of autonomous systems, and introducing clear requirements for the publication of NCON orders that do not contain restricted-access information,
- After the end of martial law, ensure a review of NCON decisions on access restrictions to internet resources and other limitations that have been introduced.

RIGHT TO RESPECT FOR PRIVATE LIFE IN THE DIGITAL ENVIRONMENT

The effective legislation on personal data protection does not reflect many of the procedural and technical innovations already implemented at the EU level. For example, the Law of Ukraine "On Personal Data Protection" lacks provisions on the right to be forgotten, the requirements to have a data protection officer, procedures for conducting data protection impact assessments, and other key elements. To align with European standards, it is necessary to implement the principles of the General Data Protection Regulation and to establish an independent data protection authority capable of ensuring compliance with the law.

In addition, Ukraine must adopt several other EU legal acts, such as the Data Act, the Artificial Intelligence Act, and the Data Governance Act. Proper implementation of these frameworks requires a comprehensive update of national legislation, including the introduction of a list of prohibited practices in the area of data protection. Ukraine must also ensure appropriate safeguards in relation to state surveillance and introduce a ban on the use of spyware and malicious software targeting vulnerable groups such as journalists, activists, and human rights defenders. These measures are especially relevant in the context of additional restrictions introduced under martial law.

3.1. Personal Data Protection

3.1.1. Legislative Safeguards for the Protection of Personal Data

The fundamental principles of personal data protection in Ukraine are set out in the Law of Ukraine "On Personal Data Protection." The law generally reflects the safeguards required under the EU's General Data Protection Regulation (GDPR): it outlines the principles and legal grounds for data processing, lists the rights of data subjects, and prohibits the processing of sensitive data categories, subject to certain exceptions. However, many of the law's provisions are phrased in broad and vague terms, leaving room for legal uncertainty. The law also lacks the formal concepts of a "controller" and "processor" as defined under the GDPR. Instead, it refers to "owner" and "manager" of personal data, which only partially reflect the roles of those entities.

The definition of "controller" (or rather the one mirroring it) in Ukrainian law remains ambiguous. According to Article 2 of the law, a personal data owner is a "natural or legal person who determines the purpose of processing personal data, defines the scope of such data, and determines the procedures for their processing, unless otherwise provided by law." The Ukrainian definition requires the data owner to determine only the "purpose of processing," while the GDPR requires that the controller determine both the purpose and the "means" of processing. In practice, this means the owner may not supervise how or by what tools the intended purpose is achieved. Since the controller's responsibilities must account for both the purpose and the means of data processing, the absence of one of these elements directly contradicts EU guidance on data protection (paragraph 36).

The law also does not provide for the concept of "joint controllers" or a mechanism for regulating their shared processing of data. This lack of legislative guidance leads to unclear allocation of responsibilities for upholding the rights of data subjects. For example, there is a risk that a controller may fail to fulfill obligations such as responding to data subject requests (e.g. for deletion or rectification), simply because it is unclear whether that controller was originally entrusted with processing the relevant data.

The effective law does not include the principles of privacy by design and privacy by default as outlined in the GDPR, meaning that Ukrainian controllers are not currently obliged to take preventive measures that could help avoid potential violations. The law also fails to establish appropriate mechanisms for responding to violations, notifying individuals of unlawful actions involving their data, or providing effective legal remedies.

The draft law No. 8153 on personal data protection, registered in October 2022, aims to harmonise Ukraine's legal framework with European standards in the area of personal data protection. Unlike the effective law, Chapter V of the draft law is entirely dedicated to the roles of the controller and processor. It mirrors the relevant provisions of the GDPR and describes the responsibilities of these entities, including the concepts of joint controllers, privacy by design and default, and procedures for responding to data protection violations. The draft was adopted in the first reading by the Verkhovna Rada in November 2024 and is currently being prepared for its second reading.

To harmonise Ukrainian legislation with EU and Council of Europe requirements, it is recommended to:

- Update the national personal data protection law aligning it with the GDPR standards,
- Include a dedicated chapter on the roles and responsibilities of controllers and processors in accordance with GDPR, specifically:
  - Align the definition of "controller" with the GDPR definition,
  - Set out the appropriate powers and responsibilities of controllers and processors,
  - Introduce the concept of "joint controllers,"
  - Establish requirements for developing technical and organisational measures to respond to data protection violations (both preventive and proactive).

3.1.2. Compliance with General Principles and Legal Grounds for Personal Data Processing

Article 6 of the Law of Ukraine "On Personal Data Protection" sets out general requirements for the processing of personal data, reflecting the fundamental principles enshrined in the GDPR. Although these principles form the basis for lawful data processing, the law does not explicitly emphasise them and only refers to them indirectly across different provisions. For example, the principle of "data minimisation" is implied in Article 6(3), which states that "the scope and content of personal data must be relevant, adequate, and not excessive in relation to the defined purpose of their processing." Similarly, the principle of "purpose limitation" is reflected in Article 6(1)(3), (5). This article also broadly outlines the principles of lawfulness, fairness, transparency, data accuracy, and confidentiality. Notably, however, the law does not contain a clearly structured list of these principles - they are scattered across various provisions without a coherent structure or internal consistency, making their interpretation and implementation more difficult.

The effective law also does not include the principle of "storage limitation," which stipulates that personal data should be kept no longer than necessary for the purposes for which they are processed, except where otherwise required by law. Nor does it refer to the principles of "integrity" (ensuring appropriate technical and organisational measures for secure processing) and "accountability" (the controller's responsibility to ensure compliance with data protection principles). This gap is largely due to the absence of the concepts of "controller" and "processor" in Ukrainian law, resulting in an incomplete mechanism for assigning and implementing data protection responsibilities.

Provisions on the legal grounds for processing personal data are found in Article 11 of the law and generally align with the requirements of the GDPR. However, when referring to processing based on the need to perform a task by the controller, the Ukrainian law only refers to the "necessity of fulfilling the obligation of the personal data owner as prescribed by law" (Article 11(1)(5)), and does not mention the performance of a task carried out in the public interest as an additional legal basis, as provided in the GDPR. A similar issue is found in Article 7, which addresses the processing of sensitive personal data and defines the conditions under which such processing is lawful. While the law generally reflects most of the legal grounds listed in the GDPR, it omits processing of sensitive data for reasons of "substantial public interest" or for "archiving in the public interest, scientific or historical research purposes, or statistical purposes."

The absence of the concept of "public interest" in this context creates unnecessary restrictions on the ability of private institutions and civil society organisations to process data for socially significant purposes - for example, in research projects, healthcare initiatives, or social welfare programmes.

Unlike the effective law, draft law No. 8153 on personal data protection sets out principles and legal grounds for processing in a more comprehensive manner. Mirroring the GDPR, the draft law provides a clear list of data processing principles and explains their meaning, while also offering a more detailed breakdown of the legal bases for processing. This effectively addresses the effective law's shortcomings.

To harmonise Ukrainian legislation with the requirements of the EU and the Council of Europe, it is recommended to:

- Introduce a clearly defined list of fundamental personal data processing principles and mechanisms for their implementation, including the principles of storage limitation, integrity, and accountability,
- Recognise the processing of personal data for public interest purposes as an additional legal basis,
- Include "substantial public interest" and "archiving in the public interest, scientific or historical research purposes, or statistical purposes" as additional legal grounds for processing sensitive data categories.

3.1.3. Compliance with Data Subjects' Rights

Article 8 of the Law of Ukraine "On Personal Data Protection" generally grants data subjects a wide range of rights, including the right to information, the right to access data, the right to amend or delete data, the right to object to personal data processing, and the right to compensation, among others. However, these legislative provisions lack detail. Aside from listing the rights, the law does not specify mechanisms for their implementation, which complicates the ability of data subjects to understand and exercise their rights.

In terms of the right to access personal data, the law does not clarify what information must be provided to the data subject to ensure this right in accordance with the GDPR. The GDPR requires disclosure of the purpose of processing, data retention periods, sources of the data, and more. Currently, the information obligations of the controller are not substantial, allowing them to decide at their own discretion what information the data subject will receive.

In addition, certain provisions fail to clarify the scope of data subject rights in line with GDPR standards. While the law grants individuals the right to object to the processing

of their personal data (Article 8(2)(5)), it only specifies how this right may be exercised in the context of direct marketing or profiling. The law does not extend the right to object to processing for research or scientific purposes. Similarly, the provision on the right to restrict processing only allows the individual to impose limitations "when giving consent" (Article 8(2)(10)). The law does not address circumstances in which a person may request the controller to retain their data following processing - for example, when contesting the accuracy of personal data or challenging its unlawful processing. Lastly, with respect to protection from automated decision-making, the law does not include protection from profiling or define the legitimate circumstances under which such protection may not apply.

Ukrainian law does not grant data subjects either the "right to be forgotten" or the right to data portability (i.e. the right to obtain a copy of their personal data), both of which are established in the GDPR. The closest equivalent to the right to be forgotten can be found in Article 15(2)(4) of the Law of Ukraine "On Personal Data Protection," which states that personal data shall be deleted or destroyed pursuant to a court decision ordering such action. However, under the effective law, a request for deletion can only be made if the data is processed unlawfully or is inaccurate (Article 8(2)(6)). As a result, the case law on this matter is limited to such complaints. By contrast, Article 21 of draft law No. 8153 on personal data protection explicitly includes the right to be forgotten and a mechanism for its implementation in line with European standards.

The shortcomings of the current legal framework are largely addressed by draft law No. 8153. Mirroring the structure of the GDPR, the draft devotes Chapter IV to the rights of data subjects, describes the mechanisms for exercising these rights in individual provisions, expands their scope, and incorporates regulatory elements that are missing from the effective law.

To harmonise Ukrainian legislation with EU and Council of Europe standards, the updated law should:

- Introduce the right to be forgotten and the right to data portability,
- Clarify the scope of existing rights, specifically:
  - Strengthen the information obligations under the right of access by specifying the list of information that the controller must provide,
  - Extend the right to object to personal data processing to include processing for profiling, direct marketing, and research purposes (including archiving and statistics),
  - Specify additional circumstances under which the right to restrict data processing may be exercised (e.g. contesting the accuracy or lawfulness of the data),
  - Expand the scope of protection from automated decision-making to include protection from profiling.

3.1.4. Internal Mechanisms for Ensuring Compliance with Personal Data Protection Standards

The effective Law of Ukraine "On Personal Data Protection" does not provide for internal mechanisms to safeguard personal data and therefore does not comply with Articles 35-43 of the GDPR. Draft law No. 8153 proposes relevant amendments. In particular, Articles 39-40 of the draft introduce a requirement to conduct data protection impact assessments and largely mirror the relevant GDPR provisions. Similarly, the draft provides a mechanism for appointing a data protection officer, as well as a procedure for passing

a qualification exam for such officers. Article 43 also contains provisions on codes of conduct. However, it does not establish any provisions for monitoring compliance with voluntary commitments, leaving the procedures for adopting and implementing the codes' requirements unclear. At a minimum, this section of the draft requires clarification - either the responsibility for monitoring should be assigned to the supervisory authority, or a separate self-regulatory body should be designated to oversee compliance with the codes. Furthermore, the draft contains no provisions regarding certification procedures, seals, or marks, and thus does not fully comply with GDPR requirements, specifically Articles 42-43.

In practice, such mechanisms are rarely used. For example, in Ukraine, companies that do not target the European market rarely appoint data protection officers. This issue is also present in government bodies, including those that regularly process personal data - such as those administering national digital services like Diia, DiiVdoma, Reserve+, Mriia, and others. A similar approach is taken with data protection impact assessments: they are generally only conducted when there is a need to demonstrate compliance with GDPR standards. There is currently no methodology for carrying out such assessments, although the Ukrainian Parliament Commissioner for Human Rights (Commissioner) has highlighted its importance. Ukraine currently has no functioning codes of conduct. A model code of conduct was published by Kyiv Administrative Service Centre (TsNAP) back in 2019; however, there is no publicly available information on how to join the code or which entities have signed it. This suggests that most public and private actors rely solely on legislative requirements and internal policies, without undertaking any additional commitments under codes of conduct. There are also no effective practices involving certification, seals, or labelling.

To harmonise Ukrainian legislation with the requirements of the EU and the Council of Europe, the following steps are recommended:

- Introduce a legal requirement to conduct data protection impact assessments and define requirements for such processes,
- Develop secondary legislation specifying when data protection impact assessments are mandatory and establish typical procedures for conducting such assessments,
- Amend the personal data protection law to require the appointment of a data protection officer, specify the criteria for such appointments, and define the minimum scope of their responsibilities,
- Support the development and adoption of voluntary codes of conduct in the field of personal data protection,
- Establish a certification/accreditation mechanism for an entity responsible for monitoring compliance with the obligations voluntarily undertaken under such codes by controllers and processors,
- Develop standardised certification, seals, and labelling to demonstrate compliance of data processing practices with legal requirements,
- Create a certification/accreditation mechanism for an entity responsible for issuing certifications, seals, and labels.

3.1.5. Free Circulation of Data

Article 29 of the effective Law of Ukraine "On Personal Data Protection" partially regulates the issue of cross-border data transfers by referencing the rules of Convention 108+. However, it does not comply with the GDPR regarding the right to data portability, the requirement to assess the level of data protection through binding corporate rules or government regulation, or safeguards during cross-border transfers. The law also lacks provisions concerning the activities of online intermediaries and platforms, limiting its applicability in the modern digital context. As previously noted, the effective legislation requires at least harmonisation with the GDPR.

Draft law No. 8153 proposes key changes in this area. Article 23 establishes the right to data portability, while Chapter VI is dedicated to cross-border data transfers and the requirements for entities receiving such data. These include minimum standards for binding corporate rules (Article 47). However, the draft still lacks provisions on the right to data altruism and the associated responsibilities of organisations that enable its implementation, the possibility of data reuse, and service interoperability - particularly as addressed in the EU Data Governance Act. It also fails to outline obligations for intermediaries and online search service providers offering goods and services, including the specifics of data processing and permissible processing practices. Given the ongoing reform of Ukraine's personal data protection legislation, it would be appropriate to consolidate all EU-level requirements and recent developments into a unified regulatory framework.

The circulation of data in the public sector is governed by the Law of Ukraine "On Access to Public Information" and Cabinet of Ministers Resolution No. 835 "On Approval of the Regulation on Datasets to Be Published as Open Data." Article 10-1 of the law defines open data and specifies that it must be provided free of charge, openly, and in a format suitable for automated processing. However, the law does not mention dynamic data, nor does it impose adequate penalties for failing to update or provide timely access to open data due to technical or legal reasons. It also does not prohibit data localisation (except in national security contexts), nor does it provide a framework for the contractual reuse of data not protected by intellectual property or personal data legislation, as foreseen by the EU Data Governance Act.

The Law of Ukraine "On Electronic Communications" also addresses data circulation to some extent, particularly regarding traffic and location data. Article 119 mandates the protection of such information by electronic communications service providers. However, there is no explicit prohibition on the storage or access to communication content alongside traffic data. Article 120 provides protection against spam and unsolicited messages. In addition, the Law of Ukraine "On Information Protection in Information and Telecommunications Systems" and the Procedure for the Transfer, Storage, Operation, and Access to State Information Resources and Their Backups impose certain requirements for data storage, including for government-held data. However, no specific provisions prohibit data localisation or define exceptions.

The Law of Ukraine "On Electronic Commerce" makes only a passing reference to intermediaries and online search service providers, grouping them under the general term "online store." This legislation lacks any provisions regulating how such actors handle data - including personal data - or the terms under which data may be accessed or transferred to third parties. It also does not contain transparency requirements regarding data processing practices. Moreover, Ukrainian legislation does not regulate access to data generated by Internet of Things (IoT) products, including data structure or user access regimes.

In practice, mechanisms for certifying the adequacy of personal data protection in other countries are lacking, and there are no clearly defined restrictions on applying Convention 108+ to the aggressor state. Due to insufficient national oversight, binding corporate rules on data protection are often not enforced and remain declarative. Problems also exist with updating open datasets - particularly dynamic data. The quality of data on the Open Data Portal (regulated by Resolution No. 867) is often relatively low, and users seeking relevant information frequently have to rely on the Law of Ukraine "On Access to Public Information." This makes obtaining needed data significantly more difficult. Amid martial law and related restrictions, requesters are often denied access to public information. At present, there are no effective mechanisms for accessing such information, and disputes are frequently resolved in court.

To harmonise Ukrainian legislation with EU and Council of Europe requirements, it is recommended to:

- Amend the Law of Ukraine "On Personal Data Protection" to strengthen safeguards for personal data during cross-border transfers by aligning with GDPR requirements on binding corporate rules and adequacy assessments,
- Clarify legal provisions prohibiting data localisation and ensure the free circulation of data with EU Member States and (potentially) Convention 108+ signatories, subject to temporary restrictions on the aggressor state during martial law,
- Introduce into national legislation (including the Law of Ukraine "On Personal Data Protection") the concept of data altruism, including the designation of organisations permitted to use such data, limited purposes for its use, and procedures for handling data that is no longer needed,
- Amend the Law of Ukraine "On Electronic Communications" to establish specific requirements for processing location data and define retention periods for traffic and metadata,
- Update localisation legislation (including the Law of Ukraine "On Electronic Communications") to clearly define exceptions for national security or public order, and create mechanisms for data exchange with EU countries under a general data non-localisation principle,
- Codify the right to data portability and access to data generated by IoT products, including how such data is structured, the legal grounds for access, and relevant exceptions (e.g. emergencies, justified requests from public authorities),
- Regulate the activities of intermediaries and online search service providers offering goods and services, and establish requirements for their handling of personal data and associated procedures,
- Amend the Law of Ukraine "On Access to Public Information" to strengthen open data regulations, including obligations to ensure availability and proper formatting, as well as procedures for accessing data from holders (including dynamic data),
- Develop secondary legislation establishing interoperability standards, access to dynamic data, and API specifications by updating Resolution No. 835 and aligning the list of datasets published as open data with the EU Open Data Directive,
- Develop secondary legislation establishing monitoring mechanisms for cross-border data transfers, standard contractual clauses, and data protection security protocols (especially for government agencies),
- Incorporate into educational programmes training for data protection officers and guidance for businesses on data circulation and applicable legal standards, including data protection requirements.

3.1.6. Prohibited Practices in the Area of Data Protection

The effective Law of Ukraine "On Personal Data Protection" does not prohibit decisions that have legal consequences for individuals or otherwise significantly affect them from being made solely on the basis of automated processing of personal data, including profiling. Article 8(13) of the law, which grants the data subject "the right to protection against automated decision-making that has legal consequences for them," requires revision. This issue is discussed in more detail in section 5.4.2 of this report. In addition, the current Ukrainian legislation on personal data protection lacks a definition of "profiling." Draft law No. 8153 seeks to address these gaps by introducing a definition of profiling and allocating detailed provisions on automated decision-making to a separate article (Article 25).

The regulation of AI systems is not yet established at the national level. Accordingly, there is no classification of AI systems based on risk levels or a legal prohibition on the use of AI systems that pose an unacceptable risk to human rights and safety. This contradicts the requirements of the EU Artificial Intelligence Act (AI Act), Article 5 of which outlines prohibited AI systems, such as those for social scoring or categorising individuals based on biometric data. Although the implementation of the EU AI Act into Ukrainian law is planned, including the provisions on prohibited systems, the process will likely take time.

In practice, AI systems are widely used in Ukraine, and the lack of clear legal prohibitions or at least restrictions on the most dangerous systems poses a serious risk to personal data protection. For instance, Clearview AI was found in violation of GDPR in the EU for indiscriminately scraping facial images from the Internet to expand its facial recognition database. Meanwhile, the Ukrainian government actively cooperates with Clearview AI, using it to identify deceased persons, enhance security at checkpoints, and identify Russian war criminals. On the one hand, the use of this system has been highly beneficial for Ukraine during wartime; on the other hand, indiscriminate facial image scraping presents significant risks to data subjects. This example illustrates the need for Ukraine to regulate the use of AI systems that process biometric and other sensitive personal data, including setting clear boundaries for their use.

The current version of the Law of Ukraine "On Personal Data Protection" does not include a prohibition on the commercial use of minors' personal data. Draft law No. 8153 also does not contain such a prohibition. However, Articles 13(10) and 14-2(6) of the effective Law of Ukraine "On Advertising" prohibit actors in the field of audiovisual media and providers of video-sharing and information-sharing platforms from processing children's personal data for commercial purposes such as direct marketing or profiling, including behaviourally targeted advertising. These provisions align with the EU Audiovisual Media Services Directive and Council of Europe standards. Nonetheless, they do not extend to online platform providers in a broader sense, which is inconsistent with the EU Digital Services Act.

The Digital Services Act provides protection against prohibited forms of profiling in marketing not only for minors. It introduces a general ban on online platform providers displaying advertising based on profiling that uses sensitive personal data. In other words, this protection applies to all individuals, regardless of age. The Law of Ukraine "On Advertising" does not yet contain a similar provision.

In practice, there have been cases of advertising based on profiling using sensitive personal data. For example, Cambridge Analytica used Facebook users' personal data without consent (including data revealing political views) to profile voters for the purpose

of targeted political advertising. Such examples underscore the importance of introducing a legal prohibition on profiling based on sensitive personal data in marketing to protect data subjects' rights and safeguard democratic processes.

To harmonise Ukrainian legislation with EU requirements, the following steps are recommended:

- Introduce the definition of profiling into the Law of Ukraine "On Personal Data Protection" in line with the definition provided by the GDPR,
- Specify in legislation that profiling must not result in discrimination against individuals based on sensitive personal data,
- Expand the list of actors prohibited under the Law of Ukraine "On Advertising" from processing minors' personal data for commercial purposes by including online platform providers,
- Legally prohibit online platform providers from displaying advertisements based on profiling that uses sensitive personal data,
- Regulate the use of AI systems by state authorities that process biometric data (e.g. for facial recognition databases), including by introducing safeguards against indiscriminate scraping,
- Establish proportionate penalties for violations of prohibited practices in the field of personal data protection.

3.2. Privacy and Security in the Digital Environment

3.2.1. Protection of Honour, Dignity, and Business Reputation

National legislation guarantees every person the right to defend their honour, dignity, or business reputation against harm caused by the dissemination of false information about them and/or their family members. Individuals may choose the appropriate means of legal protection: compensation for pecuniary and/or moral (non-pecuniary) damage (Article 16(2)(8-9) of the Civil Code of Ukraine); the right to reply or to seek retraction of inaccurate information (Article 277(1)); establishing the falsehood of the disseminated information and seeking a retraction when the source cannot be identified (Article 277(4)); and prohibiting the dissemination of information that violates personal non-property rights (Article 278).

It is important to note that Article 280 of the Civil Code introduces an exception to liability for pecuniary and/or moral damage in cases where a whistleblower unintentionally disseminates false information regarding possible corruption or related offences or violations of the Law of Ukraine "On the Prevention of Corruption." In such cases, the individual whose personal non-property rights were violated by the disclosure has the right to reply.

The Law of Ukraine "On Media," which entered into force on 31 March 2023, standardised the out-of-court procedure and rules for exercising the right of reply and retraction if false information has been disseminated through media channels. Article 43 aligns national norms with the requirements of the Audiovisual Media Services Directive (Article 28). The law establishes timeframes for submitting applications, outlines what information must be included, sets deadlines for review and a comprehensive list of grounds for refusal,

and regulates how retractions and replies must be disseminated. A refusal to publish a correction or reply, as well as actions by an audiovisual, print, or online media entity in publishing a correction or reply that do not comply with the legal requirements, may be appealed in court. At the same time, submitting a request for correction or exercising the right of reply with the media entity is not a mandatory prerequisite (nor an obstacle) for filing a relevant lawsuit in court.

Since registered media actors are required to publicly disclose their identification details (Article 37 of the Law "On Media"), including registration information and contact details, this facilitates the identification of information disseminators for the purpose of filing a court claim. However, the dissemination of false information via anonymous social media channels presents significant obstacles to the effective exercise of the right to legal remedy, as it may be impossible to identify the proper respondent in a defamation case.

It is crucial to recognise that protecting a person's honour, dignity, and business reputation must always be balanced against the right to freedom of expression. The relevant balancing standards are discussed in detail in Section 2.1.5.

In 2022, Article 435-1 was added to the Criminal Code of Ukraine, introducing criminal liability for insulting the honour and dignity of a military servicemember, their close relatives or family members, including the creation and dissemination of materials containing such insults. The prescribed penalty is three to five years of restriction or deprivation of liberty. According to the State Register of Court Decisions, two convictions have been issued under this article in cases involving social media posts that insulted military service members. In case No. 712/4108/22, the offender was sentenced to three years of imprisonment, but the sentence was suspended. In case No. 718/418/23, the court approved a plea bargain under which the offender was ordered to pay a fine of UAH 17,000.

Criminal liability for insults to honour and dignity is not in itself a violation of international human rights standards. However, in practice, it is often difficult for states to demonstrate the existence of a pressing social need and the proportionality of the imposed measures. Even when a sentence is minor or suspended, criminal prosecution constitutes a serious interference with human rights. Notably, when the current Criminal Code of Ukraine was adopted in 2001, provisions criminalising defamation and insult were intentionally excluded due to their limited public harm. Moreover, the concepts of "insult," "honour," and "dignity" are inherently subjective, making civil proceedings better suited for protecting individual rights in such cases.

The application of Article 435-1 to civilians also raises legal concerns, as Article 401 of the relevant section of the Criminal Code clearly states that military offences are those criminal offences against the legally established procedure for military service, committed by servicemembers or conscripts during training. In other words, these provisions apply to a specific category of persons. Scholars have also identified several other inconsistencies and flaws related to the application of these new provisions.

In light of this, to harmonise Ukrainian legislation and law enforcement practice with EU and Council of Europe standards, it is recommended to:

- Review the necessity of Article 435-1 of the Criminal Code of Ukraine in its current version, taking into account the theoretical inconsistencies and practical challenges, and make appropriate amendments to the Criminal Code, including removing "insult to honour and dignity" from the list of criminal offences.

3.2.2. Right to One's Image

In the Ukrainian legal system, an individual's right to the protection of their image is enshrined in various legislative acts. Article 308 of the Civil Code of Ukraine establishes a general prohibition on the public display, reproduction, and distribution of a person's photographs without their consent, except in cases where it is necessary to protect the interests of that person or of others. A similar provision is found in Article 8(1)(9) of the Law of Ukraine "On Advertising," which prohibits the use of a person's image without their consent, given either in written or electronic form. In addition, a photographic work is considered an object of copyright and is therefore subject to the requirements of the Law of Ukraine "On Copyright and Related Rights" (Article 6(1)(9)).

Article 10 of the Law of Ukraine "On the Protection of Childhood" provides safeguards for protecting the image rights of minors, prohibiting the publication of any information about a child that could harm them without the consent of the child's legal representative. Moreover, advertising legislation prohibits the use of a child's image in dangerous situations or in contexts that could harm them (Article 20 (2)).

In the context of the degree of public involvement of a person in civic life - as a factor considered by the ECtHR when balancing privacy and freedom of expression - Ukrainian legislation outlines certain categories of individuals about whom information may be disseminated on lawful grounds. For instance, information about the heads or members of supervisory boards of state or municipal enterprises, or members of the executive or supervisory bodies of business entities, is not considered restricted access information. Similarly, information about unlawful actions committed by public authorities, local self-government bodies, or their officials is not considered confidential. This means that journalistic investigations remain protected, including those involving visual materials.

Ukrainian law does not establish administrative or criminal liability for the unlawful dissemination or publication of a person's image. The Criminal Code of Ukraine currently provides for liability only in cases of illegal reproduction, use, and distribution of photographic works as violations of copyright and related rights (Article 176), as well as for the importation, production, sale, or distribution of pornographic images (Article 301).

In practice, when applying Article 308 of the Civil Code, Ukrainian courts generally follow a consistent approach - publishing a person's image without their consent is prohibited unless it serves a legitimate interest. However, courts have not provided a clear interpretation of the concept of "legitimate interest." If a person independently publishes photographs, for example on social media accessible to an unlimited audience, further use of these now-public and open photos by third parties is considered lawful. Nevertheless, due to the absence of a developed concept of the "right to one's image" in Ukrainian law, courts offer limited commentary on the lawfulness of media use of images, adhering to a rather formalistic and narrow interpretation of the law.

Clarifications are instead introduced at the level of self-regulation - experts from independent bodies assess and analyse cases, identify problematic aspects, and issue recommendations on how journalists should ethically report on such matters. Notably, in practice, individuals whose photos have been published by the media without consent generally do not challenge the lawfulness of publication; complaints are mostly related to defamation, particularly when images are accompanied by false or misleading text. However, the general rule remains that media should not publish a person's photo alongside an article if the image adds no value to the public discussion and merely intensifies or provokes public interest in the media story.

The need to properly balance the right to privacy with the public's right to information has also been emphasised repeatedly by self-regulatory bodies in their individual decisions. These decisions mostly concerned the publication of "high-profile cases" in the media that attracted significant public interest and often involved public officials. For example, in a case involving published materials about the income of the head of the Accounting Chamber, the Commission on Journalistic Ethics concluded that the photos of the official were justified by public interest, as she was a public figure. In contrast, in a case concerning a Telegram post by a journalist about a New Year's party featuring nude dancers, the Commission held that even sensational news must comply with journalistic ethics and respect the privacy rights of individuals - particularly if no public figures are involved.

The Independent Media Council (IMC) has also stressed that when publishing images or reporting on cases (especially criminal ones), media must prioritise the "principle of humanity over sensationalism," which involves avoiding provocative headlines and presenting information in an impartial manner. This principle was clearly expressed in the IMC's decisions concerning materials published by the company "Studio 1+1" and the online portal "Vesti.ua," which reported on crimes of a sexual nature and included photographs of victims along with sensational headlines.

The Ukrainian legal system does not contain any rules regarding the labelling of images generated by AI systems, despite Ukraine's active engagement in the development and use of AI technologies. However, the need for such regulation has been acknowledged in various public policy documents aimed at minimising risks to human rights. For example, voluntary labelling of AI systems is listed as one of the tools for reducing human rights risks in the White Paper on AI Regulation in Ukraine. In addition, to increase transparency in marketing, the Ministry of Digital Transformation recommends labelling AI-generated content and informing users when AI is used in advertising. For more on this, see Section 5.3.2 of this Report.

To harmonise Ukrainian legislation with EU, Council of Europe, and relevant UN recommendations, it is necessary to:

- Implement the concept of the "right to one's image," clarifying the safeguards protecting individuals from unlawful intrusions into their right to privacy,
- Introduce national rules/requirements for the labelling of content generated by AI systems.

3.2.3. Ensuring Anonymity and Security Online

The Law of Ukraine "On Personal Data Protection" contains general provisions on security and anonymity, which apply to the processing of personal data online. In particular, Article 6 stipulates that personal data may be processed with the consent of the individual and for lawful purposes. However, the law does not elaborate on specific guarantees regarding security and anonymity, offering only general data protection assurances, which are insufficient to meet international standards. General provisions are also found in the Law of Ukraine "On Advertising" - prohibiting unsolicited advertising/spam without the consumer's prior consent - and the Law of Ukraine "On Information" - prohibiting the collection, storage, use, and dissemination of confidential information about an individual without their consent, except in cases provided by law. However, these provisions still do not address the specific features of ensuring online security and anonymity.

The Laws of Ukraine "On Electronic Commerce" and "On Electronic Communications" impose obligations to protect personal data on e-commerce entities and electronic

communication service providers, respectively. However, they do not contain specific obligations or procedures for safeguarding personal data. Draft law No. 8153 partially addresses this gap by specifying obligations related to risk-based security measures – for instance, ensuring that access to personal data is granted only to authorised individuals for lawful purposes, protecting data from destruction, loss, alteration, unlawful storage, processing, access, or disclosure, and implementing security measures for data processing. The draft law also proposes notifying consumers of security risks in electronic communication networks or services and includes a separate article on the protection of the confidentiality of private communications. Another positive element is the explicit prohibition of interference in private communication in the form of listening, recording, storing, or transmitting information without the participants' consent. However, the proposed Article 119-4 of the Law "On Electronic Communications" effectively grants subscribers the right to request the tracing of calls they consider malicious or unwanted, but it lacks any guarantees or requirements for such requests. It is also unclear whether the draft law obligates the network or service provider to respond to every such request or whether this is left to their discretion – a lack of clarity that opens the door to potential abuse.

At the same time, draft law No. 8153 proposes allowing providers of electronic communication networks or services to obtain, use, and share information about private communications if necessary to deliver communication services (with prior notification to the user). However, the draft does not contain provisions on the protection of end-to-end encryption or other tools for ensuring user anonymity and data security, as required by international standards. This, in turn, creates potential loopholes for circumventing online security measures, including the use of "backdoors" or access to encryption keys. For instance, the government portal Diia, used by a large portion of the Ukrainian population and containing sensitive personal data, does not fully meet data protection standards and carries the risk of data being shared with third parties.

Another important aspect of personal data protection concerns the collection and use of information by law enforcement agencies. The Law of Ukraine "On the National Police" states that police may access the information systems of other state bodies, provided they comply with the Law "On Personal Data Protection." As noted earlier, this law lacks specific provisions on the online environment, which in practice means that there is no regulation of police access to personal data online. Meanwhile, Article 159 of the Criminal Procedure Code authorises investigators and prosecutors to temporarily access and copy information in electronic information systems "if necessary." They may also search, detect, and record computer data without a search warrant if "there are sufficient grounds to believe" that such data "is relevant to a criminal investigation" (Article 236). As a result, law enforcement and investigative authorities are granted wide discretion in accessing and using personal data online, without detailed rules defining the scope or means of applying such powers, as required under ECtHR jurisprudence.

Ukrainian law does not currently prohibit pseudonymity or anonymity online, but nor does it guarantee them. Meanwhile, draft law No. 9223 effectively proposes prohibiting the use of anonymous or pseudonymous accounts for spreading false information or interfering with the activities of state bodies or other entities to the detriment of national sovereignty. Draft law No. 11115, although it does not contain a direct requirement to disclose the personal data of account holders (only the provider's own data and platform ownership details), it does include provisions on implementing mechanisms for notifying page owners about user complaints concerning posted content and enabling users to challenge the actions of page owners. However, the draft does not clarify the nature of these mechanisms or whether personal data of the account holder would be disclosed to the complainant.

International standards also require the existence of a dedicated body for cybersecurity and supervision of online security and anonymity. Currently, the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" assigns oversight of personal data protection to the Commissioner, who operates across all sectors and is therefore not a specialised supervisory authority in the area of online privacy and anonymity. Draft law No. 6177 proposes the creation of a National Commission for the Protection of Personal Data and Access to Public Information, with one of its tasks being to implement state policy in the area of cybersecurity as it relates to personal data protection - including cooperating with cybersecurity actors in preventing cyber incidents. In general, these powers are aligned with international standards, but further clarification is needed on the scope of this body's authority with respect to online data protection.

The state must also introduce effective protections for online security and anonymity. The Criminal Code of Ukraine establishes liability for violating the secrecy of correspondence using computers (Article 163); unauthorised interference with electronic communications systems and networks (Article 361); and unauthorised actions with information stored in such systems by individuals with access (Article 362). The Code of Administrative Offences imposes fines for failure to comply with the legal requirements for personal data protection that results in unauthorised access or violation of data subject rights (Article 188-39).

As previously noted, the Commissioner is responsible for monitoring personal data protection via the Personal Data Protection Department within the Commissioner's Secretariat. Under the Law "On Personal Data Protection," individuals may submit complaints to the Commissioner regarding the unlawful processing of their data, and the Commissioner may also initiate inspections independently. The Commissioner primarily acts as a mediator, but under the law is authorised to issue mandatory orders to eliminate violations, draft protocols on administrative offences, and submit them to court. The same applies to the Cyber Police Department: according to the Law "On the National Police," individuals can complain to the cyber police, but only the court has the authority to impose sanctions for violations of online data protection legislation.

Another agency is the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum, and Postal Services (NCEC), which has the authority to consider cases related to violations of electronic communications legislation (including data protection in electronic communications networks, as defined by the Law "On Electronic Communications"). However, the Commission's activities are currently focused on matters such as licence reissuance and radio spectrum management, and it has no established practice of overseeing data protection in electronic communications networks. Its broad mandate means it cannot effectively ensure personal data protection online.

To harmonise Ukrainian legislation with EU and Council of Europe standards, it is recommended to:

- Develop detailed legal provisions on personal data protection with respect to ensuring online security and anonymity, including specific obligations for network and service providers under the Law "On Electronic Communications,"
- Introduce legal provisions governing the use of encryption, anonymisation, and pseudonymisation tools,
- Enshrine a prohibition on "backdoors" and other mechanisms that weaken or circumvent security measures or exploit existing vulnerabilities,

- Amend criminal procedure and law enforcement legislation to define mechanisms, scope, and conditions under which prosecutors, investigators, and police may access personal data online, ensuring that restrictions comply with international standards of legality, transparency, and independent oversight,
- Establish a dedicated agency for managing cybersecurity risks and a specialised supervisory body for monitoring compliance with online security and anonymity standards.

3.2.4. Countering Cyberbullying, Revenge Porn, and Gender-Based Online Violence

Online bullying (cyberbullying). The Criminal Code of Ukraine does not contain any specific provisions related to cyberbullying or cyberviolence, which complicates the effective investigation of such cases and the prosecution of perpetrators. Meanwhile, the Code of Ukraine on Administrative Offences (CUAO) in Article 173-4 establishes liability for bullying of participants in the educational process, including cyberbullying - psychological, physical, economic, or sexual violence involving the use of electronic communications, which could or did cause harm to the victim's mental or physical health. The scope of the offence is limited only to minors and the educational process. In some cases, the parents of the "bullies" are held accountable under Article 184 of the CUAO for failure to fulfil their child-rearing duties. Another provision - Article 173-5 of the CUAO - concerns workplace harassment. Unlike bullying in education, this offence does not explicitly cover the online space. Thus, its interpretation is left to Ukrainian courts, which have developed rather inconsistent case law.

According to lawyers, judicial protection is currently ineffective, as objectively severe consequences of cyberbullying against children almost never lead to criminal liability. The maximum administrative sanction is a fine of 1,700 to 3,400 UAH. A 2020 DocuDays study (still the only one of its kind in Ukraine) indicates that despite the number of protocols drafted, due to imprecise legislative wording (e.g., the term "electronic communications"), accountability remains difficult to achieve. Another challenge is that victims often do not know whom to turn to in cases of cyberbullying. Legal journals publish police and support services hotline numbers, but this information is not widely known and is often omitted from media coverage. Human rights defenders also note the absence of legislation on cyberviolence, making it impossible to collect and properly present evidence, especially given the anonymity of the internet. As a result, even though there are relevant articles in the CUAO, their application in practice is extremely limited.

Separate regulation is introduced in Article 42 of the Law of Ukraine "On Media," which prohibits the dissemination of content that excessively focuses on violence, encourages self-harm or suicidal thoughts in children, or promotes obscene language and gestures. More detailed criteria for content falling under these bans are to be developed by co-regulatory bodies within codes of conduct for content creation and dissemination. Such a body in the field of online media has already been established and will soon begin work on drafting the codes. This approach aligns fully with the Audiovisual Media Services Directive, which Ukraine has committed to harmonising with as part of its EU integration process.

Non-consensual sharing of intimate images ("revenge porn"). The current Law of Ukraine "On Personal Data Protection" contains no special provisions beyond the general prohibition on the dissemination of personal data without a legal basis. Draft law No. 8153, intended to replace the current version, also lacks additional clarifications in this regard. The only useful tool it proposes is the introduction of the right to be forgotten, which could potentially allow for the prompt removal of intimate images or videos from the internet or search engines.

More specific provisions can be found in the Criminal Code of Ukraine (CCU). Current criminal legislation includes two articles that protect personal privacy: Article 163 ("Violation of the secrecy of correspondence, telephone conversations, telegraph or other communications transmitted via electronic means") and Article 182 ("Violation of the inviolability of private life"). Both could theoretically be applied to cases involving the dissemination of intimate images without consent. In practice, Ukrainian courts have applied Article 163 in a case where the convicted person grabbed a victim's mobile phone to read her text messages with the convict's husband. There are no known court cases concerning revenge porn or the publication of correspondence content on online platforms. However, publication of such correspondence could potentially be prosecuted under Article 163. Article 182 prohibits the unlawful storage and dissemination of confidential personal information. The maximum penalty is up to three years' restriction of liberty, or up to five years' imprisonment if aggravating circumstances are present (such as repeat offences or significant harm). The Law "On Information" as well as the Laws "On Access to Public Information" and "On Personal Data Protection" recognise photos and videos of individuals as confidential information, which may only be disseminated without consent in cases specified by law and only in the interests of national security, economic well-being, or human rights protection.

In practice, however, individuals are most frequently prosecuted not for distributing intimate images without consent, but for distributing pornography. On one hand, Article 301 of the CCU carries heavier penalties and thus may serve a stronger deterrent function. According to the Better Regulation Delivery Office, within the Pornometer project, 1,104 indictments under Article 301 were submitted to the courts in the first nine months of 2024 - 75% more than the previous year. However, convictions were handed down in only 7% of cases. Most cases end with fines, typically very modest. Moreover, incorrect classification of crimes distorts the assessment of harm, failing to reflect the individual impact on victims. Decriminalisation of pornography may potentially change the situation. A relevant initiative was discussed in 2023 and a new bill was registered this year. Draft law No. 12191 proposes to decriminalise the filming and distribution of intimate videos between consenting adults while retaining liability for: non-consensual pornography (revenge porn, deepfake porn), extreme pornography (e.g., involving violence or animals), and child pornography. These changes broadly align with European standards. Nevertheless, Ukraine still lacks proper regulation of user-generated content platforms, many of which operate under terms of use and moderation policies that do not meet international standards.

Gender-based online violence. Ukraine ratified the Istanbul Convention only in mid-2022, and submitted its first baseline legal assessment report in 2023. Officials who prepared the report identified only a few general provisions in the CUAO and CCU relevant to cyberviolence. For example, Article 173-2 of the CUAO covers acts such as insults, threats, and harassment based on gender that could or did cause physical or psychological harm. The maximum penalty is up to 10 days of administrative arrest, and up to 15 days for repeat offences within a year. However, this article makes no explicit reference to online forms of violence and is unlikely to be applied to such cases. Similarly, Articles 163 and 182 of the CCU do not explicitly cover online violence. Still, case law under Article 182 suggests that perpetrators may be held accountable for certain forms of cyberviolence, such as revenge porn, cyberflashing, and stalking - all of which are listed in the EU Directive on combating violence against women and domestic violence as key examples of gender-based online violence. Another relevant provision is Article 126-1 of the CCU, which prohibits domestic violence and could theoretically apply to threats and psychological abuse in online settings. However, human rights defenders note that cyber police often lack the resources and engagement necessary to prioritise

such cases, focusing instead on national security threats such as deepfakes. Although the updated Law "On Prevention and Counteraction to Domestic Violence" includes tools for reporting gender-based online violence, resource limitations among oversight and enforcement bodies render such provisions ineffective in practice.

Certain categories of gender-based violence content are banned from media publication, with violators subject to sanctions by the National Council of Television and Radio Broadcasting of Ukraine. Article 36 of the Law "On Media" prohibits dissemination of statements that (1) incite hatred, enmity, or cruelty, or (2) advocate discrimination or oppression of individuals based on sex, sexual orientation, or gender identity. Detailed criteria for content falling under this prohibition are to be developed by co-regulatory bodies through content creation and dissemination codes.

Ukraine currently lacks other mechanisms for removing gender-based violence content, and has no consolidated legislation for internet content regulation, despite declaring this a state policy priority in its 2021 Information Security Strategy. There is also no regulation of online platform activities, although draft legislation analogous to the EU Digital Services Act is being developed by the Ministry of Digital Transformation. On a practical level, the Ministry has taken a number of actions to protect children from harmful content and online violence, but these efforts lack a specific gender focus and have not yet been implemented. Therefore, much of the regulatory burden will need to be incorporated into a broader framework.

To harmonise Ukrainian legislation with EU and Council of Europe standards in countering cyberbullying, revenge porn, and gender-based violence, the following steps are recommended:

- Improve legislation on criminal and administrative liability for cyberbullying and cyberviolence,
- Support the development of co-regulatory codes in the media sector addressing cyberbullying, revenge porn, and gender-based online violence,
- Implement the right to be forgotten with application to cases of cyberbullying, revenge porn, and gender-based online violence,
- Ensure that regulation of content-sharing platforms includes provisions requiring the removal of content related to cyberbullying, revenge porn, and gender-based violence through content assessment systems and user requests, and prohibit platforms from institutional tolerance of such content at the level of policies and content management system design,
- Create legal mechanisms for restricting access to content involving cyberbullying, revenge porn, and gender-based violence by court or independent regulator decisions, ensuring due process and recognising the role of internet intermediaries in content hosting,
- Conduct training for civil servants on identifying and appropriately responding to cases of cyberbullying, revenge porn, and gender-based online violence, to build an effective monitoring system in these areas,
- Increase resources for law enforcement departments responsible for registering and investigating violations in these areas, train personnel on investigative techniques and victim communication, and involve relevant civil society organisations,
- Develop an effective communication strategy to raise awareness about hotlines and legal assistance for victims of cyberbullying, revenge porn, and gender-based online violence,
- Establish a system of support and rehabilitation for victims of such violations.

3.3. Surveillance

3.3.1. Establishing and Upholding Human Rights Safeguards in the Application of Surveillance Measures

Ukraine is actively engaged in the use of surveillance technologies (often powered by artificial intelligence), yet still lacks a unified legal framework in this area. Currently, references to the use of such technologies are provided in separate sectoral laws that define the discretionary powers of authorised law enforcement bodies. Meanwhile, the general safeguards for data subjects who may be subject to surveillance are limited to the requirements of the Law of Ukraine "On Personal Data Protection."

In Ukraine, surveillance measures are primarily justified by national security and public order concerns - and thus, only authorised entities are permitted to use such technologies. The Law of Ukraine "On the National Police" allows the police to use "photo and video equipment, including equipment that operates automatically," as well as "specialised software for analytical processing of photo and video information" (Article 40(1)(1, 5)). In this case, law enforcement agencies are not subject to any restrictions other than the requirement to use surveillance for clearly defined purposes. According to the Criminal Procedure Code, investigators or prosecutors may access pre-trial investigation information systems containing data collected from technical devices, including photo and video surveillance cameras operating in public places (Article 300). Additionally, the Code authorises law enforcement agencies to conduct covert investigative actions (e.g. audio and video monitoring of persons, seizure and examination of correspondence), but only in cases of suspected serious or particularly serious crimes and when the intended purpose cannot be achieved by other means (Articles 260, 262). Under the Law of Ukraine "On Operational and Investigative Activities," authorised bodies may conduct video and audio surveillance of individuals, extract information from electronic communication networks, and monitor individuals, but only for the purpose of achieving legitimate objectives explicitly listed in the law (Article 8(1)(9, 11)). Similarly, under the Law of Ukraine "On Counterintelligence Activities," the Security Service of Ukraine (SSU) and its units are authorised to conduct surveillance, but only in the interest of national security (Article 7(2)(2)).

Currently, regulation in this area is fragmented and marked by vague formulations, which raises several issues. One of them is the excessive scope of discretion: while the laws specify the functions of law enforcement agencies, they do not include any indicators for limiting their powers in certain situations or clear grounds for when surveillance measures may be used. This problem is especially acute given the lack of an effective oversight mechanism - Ukrainian law currently does not provide for an institutionally independent body to monitor compliance with surveillance legislation. Some laws, such as the Law "On Operational and Investigative Activities," allow for the use of surveillance only with prior judicial authorisation, which in practice often becomes a mere formality.

Finally, the law does not provide minimum safeguards for data subjects who are subjected to surveillance. Notification of a person about being placed under surveillance occurs only in the context of criminal investigations, excluding warnings about audio or video monitoring in other situations (e.g. in public places). Even then, the individual is deprived of the opportunity to challenge such actions. This is also due to the lack of judicial review of the legality of the measures taken, despite the fact that initial authorisation is issued by a court.

The absence of legal safeguards is also reflected in recent legislative initiatives submitted to parliament. One such initiative is draft law No. 11228-1, which proposes amendments

to the Law "On Counterintelligence Activities" granting the SSU new powers to carry out special operations in cyberspace. The draft law provides the SSU with effectively unlimited access to personal data stored in state databases, without establishing safeguards for data subjects or preventing potential abuse. The draft is currently awaiting its second reading in the Verkhovna Rada's Committee on Law Enforcement.

Furthermore, the lack of legal regulation in the surveillance sphere became especially evident following the scandal involving the surveillance of journalists of Bihus.info - surveillance cameras had been secretly installed in hotel rooms used by the journalists, and later, videos were published online alleging the journalists' use of illicit substances. Subsequent investigations revealed that illegal surveillance had been conducted over the course of a year.

To harmonise Ukrainian legislation with the standards of the EU, the Council of Europe, and relevant UN recommendations, it is necessary to:

- Develop unified rules for the general legislative mechanism governing the use of surveillance tools,
- Supplement articles of the Criminal Procedure Code related to covert investigative actions with provisions establishing legitimate aims and grounds for the use of surveillance measures,
- Amend the relevant sectoral laws governing authorised bodies with surveillance powers by clearly defining the scope of their discretion, main tasks and functions, as well as establishing "red lines" as safeguards against abuse,
- Establish a set of rights and guarantees for data subjects who are placed under surveillance, including mandatory notification after surveillance has taken place (where necessary to prevent crime), information about their rights (including the right to know what data was collected or to access their personal data), and the right to judicial appeal of surveillance measures,
- Establish an effective oversight mechanism in the field of mass surveillance by creating an institutionally independent body to monitor surveillance practices, from the issuance of court authorisations to the handling and storage of collected data.

3.3.2. Restrictions on Mass Surveillance

As noted in the previous section, Ukraine does not have a unified legal framework for regulating surveillance mechanisms. Nevertheless, the state frequently resorts to mass surveillance tools to maintain public order at the local level. Since 2019, within the framework of the Safe City programme, 4,000 surveillance cameras have been installed in Kyiv, some of which are equipped with facial recognition technology. Facial recognition is a biometric technology that identifies or verifies an individual based on their digital image. Unlike conventional surveillance systems, these technologies are more intrusive and therefore subject to stricter regulation due to their enhanced interference with the privacy of data subjects. Currently, around 50,000 surveillance cameras are in operation across Ukraine, which may be integrated into a unified system - an initiative initially planned for early 2024. Notably, attempts to introduce regulatory tools envisaged granting municipal authorities the power to use surveillance tools. However, the relevant Law of Ukraine "On Local Self-Government in Ukraine" suggests no indicators or references to such functions, and no corresponding amendments have been made. There are also no procurement-related requirements - neither technical specifications nor restrictions on how such tenders should be announced.

At present, mass surveillance systems in Ukraine are used de facto without any limitations at either the legislative or by-laws levels. The minimum safeguards and the functions of authorised bodies provided under the Laws "On Personal Data Protection" and "On the National Police" (where applicable) are neither sufficient nor effective to ensure adequate privacy protection for data subjects.

Nevertheless, Ukraine continues to implement surveillance initiatives, despite not only the relatively low level of personal data protection but also the technical incompatibility of its systems with European standards. In 2021, the government announced the creation and development of the Safe Country software and hardware complex – an initiative aimed, in particular, at enhancing public safety, ensuring road traffic safety, and reducing the risk of terrorist acts. Under this programme, the state later received equipment and software worth UAH 197 million to support its implementation. This equipment includes facial recognition systems, behavioural analytics, investigation analytics, and information and security management systems – tools that were installed on most of the surveillance cameras deployed under the Safe City programme. However, in 2023, an investigation by Schemes revealed that thousands of surveillance cameras operating on Ukrainian streets were running Russian-made TRASSIR software, which meant that nearly all collected data were transmitted to servers controlled by the aggressor state. This situation not only highlights the serious technical vulnerabilities of the surveillance systems in use, but also underscores the urgent need to develop clear regulatory requirements to ensure the security of personal data within Ukrainian information systems.

Draft law No. 11031, aimed at establishing a unified system for monitoring public safety, represents a formal attempt to regulate the use of surveillance tools. Developed to support public order, the draft seeks to standardise the rules for surveillance and regulate a unified video surveillance platform in Ukraine. However, in its initial version, the draft already conflicts with several international standards and requires revision in light of the following issues: encroachment on privacy, excessively broad discretion for state and municipal authorities, lack of enforcement oversight, risks of data capture, and technical flaws within the surveillance infrastructure.

Additionally, the well-known draft law No. 8153 on personal data protection includes a separate Article 10 on video surveillance. According to the draft, state surveillance in public places may only be conducted "for the purpose of preventing, detecting, or recording offences and ensuring public safety and order." It also requires mandatory prior notification about such surveillance measures and that the collected data be processed only in ways compatible with the purposes for which they were initially gathered. In this context, Article 8 of the draft law also outlines the processing of personal data related to criminal liability, offences, criminal proceedings, and convictions. However, this article remains largely declarative and does not incorporate the key provisions of EU Directive 2016/680: it does not provide a list of offences that may justify surveillance, nor does it distinguish between categories of persons under surveillance (e.g. suspects, victims, etc.).

To harmonise Ukrainian legislation with EU, Council of Europe, and relevant UN standards, it is recommended to:

- Develop legislation on video surveillance that incorporates international human rights standards and EU regulation,
- Introduce a legal definition of "mass surveillance," including surveillance using intrusive technologies (such as facial recognition), and regulate the functioning of facial recognition systems, a clear list of grounds for their use, and rules for the further processing of biometric data,

- Distinguish between conventional surveillance and AI-powered surveillance, "high-risk" and "low-risk" systems (following the example of the EU Artificial Intelligence Act), as well as biometric and non-biometric surveillance,
- Develop a personal data processing mechanism for law enforcement purposes based on the model of EU Directive 2016/680,
- Provide additional safeguards for data subjects when surveillance involves intrusive technologies (e.g. limits on the retention period for biometric data or mandatory data deletion once surveillance objectives have been met and the data are no longer relevant).

3.3.3. Restrictions on the Use of Spyware

The effective Law of Ukraine "On Personal Data Protection" has no specific provisions regarding the possibility and conditions for using surveillance tools. As previously mentioned, there is also a legal issue with the effectiveness of the supervisory authority and its ability to properly monitor the activities of security agencies and verify the legal grounds for the use of spyware. At the same time, the Law of Ukraine "On the Security Service of Ukraine" broadly defines the powers of the SSU in Article 24. For instance, the authority "to conduct counterintelligence activities aimed at preventing, detecting, stopping and exposing any forms of intelligence and subversive activities against Ukraine" may include the use of malicious or spyware technologies. Oversight of the SSU's activities is exercised by the President of Ukraine, who has the power to issue directives and orders to the SSU and thus cannot act as an independent oversight body. The Law of Ukraine "On Counterintelligence Activities" authorises relevant agencies to conduct surveillance, but the procedures are regulated by the Law "On Operational and Investigative Activities" and require a judge's authorisation in cases involving highly intrusive measures such as video surveillance or interception of electronic communications.

The Law "On the National Police" does not list specific measures, but refers to the aforementioned law on operational activities and is based on the requirements of the Criminal Procedure Code of Ukraine. The Code includes several provisions that allow for the collection of information, but all such measures must be authorised by an investigating judge. Therefore, appropriate judicial oversight is ensured in the case of police activity, unlike the lack of similar safeguards and guarantees in legislation regulating security agencies (such as the SSU and counterintelligence bodies).

General changes are proposed in draft law No. 8153, which aims to replace the current data protection law and harmonise national standards with the GDPR. However, since the GDPR does not provide detailed regulation on surveillance technologies, the draft remains brief on this topic. Article 17 states that the use of special software or surveillance technologies (contextually understood to include spyware) is prohibited except where the data subject has given consent, the tracking is necessary for the functioning of applications or mobile programs, or the processing is needed to prevent fraud or provide a service to the data subject. Clearly, this article applies to the private sector. At the same time, the draft contains no clarifications regarding such measures in the context of law enforcement activity, leaving legal safeguards inadequate. Likewise, Article 31-2, which protects the secrecy of private communication, includes no such clarifications. Draft law No. 6177 on the establishment of the National Commission on Personal Data Protection and Access to Public Information grants the supervisory body authority to oversee data processing by other state agencies. More detail on this is provided in the section on the effectiveness and independence of the personal data protection regulator.

Additionally, debates have been ongoing around draft law No. 11228-1, aimed at regulating the response to intelligence and subversive activities by foreign special services. Among other provisions, it seeks to grant the SSU direct and automated access to systems and databases administered by state and municipal bodies. The draft significantly expands the existing discretion of security agencies without introducing amendments to sectoral legislation, granting them unrestricted access to personal data even in the absence of legitimate grounds. The draft is currently awaiting a second reading in Parliament, but even its revised version still requires substantial improvement. The draft has been repeatedly criticised by civil society organisations, primarily due to the overly broad discretion it proposes.

Ukrainian practice in the use of spyware and surveillance tools over the past few years has been limited. Given that the country has been engaged in full-scale war for three years, most efforts have focused on countering Russian aggression. One of the key internal initiatives includes projects by the Bureau of Economic Security involving the use of tools to monitor financial and economic activity and forecast risks in the economic sphere. It remains unclear whether these projects foresee intrusion into individuals' devices (e.g., officials managing public funds). Nevertheless, the risk of excessive interference remains, while there are no legislative safeguards, including privacy guarantees for individuals subject to such monitoring.

In contrast, the use of spyware and malicious software by Russian actors has been more varied and significantly more dangerous to Ukrainians. DSLU has published several studies documenting Russian cyberattacks - for example, phishing schemes involving malware-laden files. In 2023, the State Service for Special Communications also reported the automatic detection of approximately 1.5 million malware files. Among the most common were SmokeLoader, Agent Tesla, Snake Keylogger, Remcos, and Formbook. There have also been repeated attempts to impersonate government institutions, including the SSU, to gain access to users' devices and install spyware. International researchers also confirm the scale of such attacks, which target not only government institutions and enterprises but also private individuals, including Ukrainian media outlets, journalists, civil society organisations, and businesses.

In addition to strengthening general legislative and practical safeguards in the area of surveillance, the following steps are recommended to harmonise Ukrainian legislation with EU, Council of Europe, and UN standards:

- Strengthen national legislation on surveillance by including provisions that prohibit the use of malicious software with non-specific purposes and the capacity for indiscriminate data collection from users' devices,
- Establish independent oversight of the use of malicious and spyware technologies by security agencies,
- Develop protocols for processing and documenting evidence obtained through the use of surveillance software, and legally regulate the status of such evidence,
- Develop digital security training programmes, particularly for employees of government bodies and critical infrastructure enterprises, to prevent Russian cyberattacks involving malicious software,
- Introduce legal and practical mechanisms for the protection of whistle-blowers reporting abuses,
- Develop legislative regulation for dual-use technologies, including those involving cyber surveillance measures, and create by-laws on developer authorisation and licensing systems for the import/export of such technologies.

3.4. Supervisory Authority and Measures for the Protection of the Right to Respect for Private Life

3.4.1. Independence and Effectiveness of the Supervisory Authority in the Field of Personal Data Protection

The Law of Ukraine "On Personal Data Protection" states that oversight of compliance with personal data protection legislation is exercised by the courts and the Commissioner within the limits of their powers. At present, the Commissioner essentially performs the functions of a supervisory authority in line with the GDPR, albeit partially and without meeting all the requirements for such an authority.

To assess the current legal framework in terms of compliance with the guarantees of independence and effectiveness of the supervisory authority on personal data, as required by the GDPR, it is necessary to analyse the provisions of the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" and the Law of Ukraine "On Personal Data Protection".

The Law "On the Ukrainian Parliament Commissioner for Human Rights," particularly Articles 4-9, sets out the key guarantees of the Commissioner's independence. These include the term of office and grounds for dismissal, clear rules on conflict of interest and incompatibility with the Commissioner's position. It is also worth noting the institutional separation of the Commissioner from the general system of public authorities and the existence of only necessary oversight of their activities (Articles 4, 9, 18). However, the appointment procedure is entirely controlled by the Verkhovna Rada of Ukraine: candidates are nominated by Members of Parliament, and the vote is held by secret ballot. This does not comply with the GDPR's requirements for an independent appointment and dismissal process for supervisory authorities.

The dismissal of the Commissioner in 2022 was widely criticised by human rights defenders due to violations of statutory guarantees and amendments made to the Law "On the Legal Regime of Martial Law" (Article 12(4)), which allow the Verkhovna Rada to dismiss officials appointed by Parliament through a vote of no confidence. Such matters are considered immediately in plenary sessions without the procedures stipulated in the special laws defining the legal status of these officials.

The Commissioner has the necessary powers to review complaints related to personal data protection, make decisions based on such reviews, conduct necessary inspections, access any information required to ensure compliance with data protection laws, issue mandatory instructions to prevent or eliminate violations, draw up administrative offence protocols, and submit them to court as provided by law. However, the law does not regulate the procedural aspects of complaint review or the procedural rights of complainants.

Another issue concerns the enforcement measures the Commissioner can apply. Direct impact on violators is critical to stop and prevent future breaches. Although sanctions are not explicitly required under Convention 108+, the GDPR lists them among the minimum essential powers of an effective supervisory authority. The current law allows for measures to prevent or remedy violations (Article 23(1)(5)), but it does not provide for sanctions per se - for example, fines can only be imposed through the courts.

In contrast, draft law No. 6177 proposes establishing a new supervisory body - the National Commission on Personal Data Protection and Access to Public Information (hereinafter - the National Commission). Together with draft law No. 8153, which was adopted in its first reading by the Verkhovna Rada of Ukraine on 20 November 2024, these bills aim to enhance and complement the current legislation.

In its opinion on draft law No. 8153 (considering draft law No. 6177), the Council of Europe mainly noted ambiguous wording in certain provisions. Among the key recommendations: to ensure legal certainty and effective sanctions, clarify what "other measures" may be applied by the supervisory authority (i.e., beyond fines) (Article 58(2)); supplement Article 59 with specific factors for determining fines (e.g., nature, severity, and duration of the violation, its consequences, any actions taken to comply with the law or mitigate harm); extend the statute of limitations for imposing sanctions to ensure effective intervention by the supervisory authority (Article 60); grant sanctioning powers to the supervisory authority for violations of specific provisions of the Law "On Electronic Communications" (as defined in item 5.6 of the Transitional and Final Provisions - particularly regarding the secrecy of private communication); and jointly review and analyse draft laws No. 8153 and No. 6177 for their compliance with the GDPR and Convention 108+.

Draft law No. 6177 generally implements the GDPR's requirements regarding the independence and effectiveness of a supervisory authority. However, questions remain about whether sufficient financial resources will be allocated to ensure the quality performance of its functions. Another issue, common to all newly established regulatory bodies, concerns the legal status of the National Commission. European standards require that the data protection supervisory authority be independent from other state bodies. Draft law No. 6177 proposes establishing the National Commission as a central executive authority with special status. Despite the declared independence, the procedure for creating the Commission and appointing its members indicates significant influence by the Cabinet of Ministers of Ukraine, which does not provide sufficient institutional independence. Human rights organisations and experts have noted several other issues with draft law No. 6177, highlighting the need for substantial revision before adoption.

To harmonise Ukrainian legislation with EU and Council of Europe requirements, it is recommended to:

- Ensure a thorough and inclusive review and revision process for draft laws No. 6177 and No. 8153 to create and implement an effective and independent personal data protection supervisory system,
- Clearly distinguish between the functions of the Commissioner and the new supervisory body in the field of privacy rights protection.

3.4.2. Effective Remedies

The effective Law of Ukraine "On Personal Data Protection" sets forth several articles that provide mechanisms for challenging the actions of data controllers and processors. Article 18 allows individuals to appeal a denial of access to personal data to the Commissioner. Article 22 states that overall oversight of compliance with the Law is carried out by the Commissioner and the courts, while Article 28 notes that violators shall be held liable as provided by law. However, the Law does not establish a clear procedure for appeals or for imposing liability. For example, Article 23 lists among the Commissioner's powers the ability to receive complaints regarding violations, conduct inspections, and forward administrative offence protocols to the court. The Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" establishes no additional duties or interpretations regarding how complaints should be considered. At the same time, it does provide for the possibility of judicial appeals against the decisions or inaction of the Commissioner.

Article 182 of the Criminal Code of Ukraine establishes liability for the unlawful processing or alteration of confidential information about a person, except in cases covered by other

articles of the Code. It also provides for enhanced liability when such actions result in significant harm to legally protected rights, freedoms, or interests of the person, or when the offence is committed repeatedly. It is important to note that this article does not use the terminology of personal data protection legislation but instead relies on the broader and more ambiguous term "confidential information." In practice, there have already been incidents that likely violated Article 182, as well as complaints submitted to the Commissioner. However, there is currently a lack of sufficient case law and guidance from the Supreme Court regarding the application of this article.

Article 188-39 of the Code of Ukraine on Administrative Offences also outlines a list of prohibited practices in the field of personal data protection that result in administrative fines. These offences currently include:

- Failure to notify or delayed notification of the Commissioner regarding the processing of personal data or changes to reportable information, or the provision of incomplete or inaccurate information,
- Failure to comply with instructions issued by the Commissioner or authorised staff to prevent or eliminate violations of personal data protection legislation,
- Failure to follow personal data protection procedures that results in unlawful access or a violation of data subject rights,
- Repeat offences (subject to higher penalties).

The enforcement of these provisions is inconsistent. For example, complaints to the Commissioner regarding violations of Article 188-39 often result in appeals against the Commissioner's inaction and findings that the time taken to review complaints is excessive and the Commissioner's response inadequate. In other cases, courts recognise violations by local authorities but impose only minimal fines (UAH 5,100). Similar fines are issued to private entities that violate the law and fail to comply with the Commissioner's orders to correct the breach. In many instances, the fine is merely symbolic and does not prevent businesses from continuing unlawful data processing practices. Courts rarely provide proper justification for the level of sanctions imposed, and there is no unified set of criteria for determining the amount of the fine.

Draft law No. 8153 proposes amendments to the legislation, with Chapter X outlining a liability mechanism for violations in the field of personal data protection. Article 58 explicitly states that being held administratively or criminally liable does not deprive individuals whose rights have been violated of the right to claim compensation for material and moral damages. Article 59 indicates an increase in fines for data protection violations. However, the minimum sanctions remain too low: while the GDPR allows for fines of up to 2% of a company's annual turnover, Draft Law No. 8153 sets fines at only 0.05% to 0.1%. For many businesses, these sums are negligible. Moreover, Article 59 does not include any criteria for assessing fines, which fails to comply with Article 83 of the GDPR.

Draft law No. 6177 proposes to regulate the activities of the National Commission for the Protection of Personal Data and Access to Public Information — effectively creating a supervisory authority in this field. A key innovation, compared to the current system, is the expansion of the powers of the supervisory body. Article 4(4) grants the Commission the power to hold accountable those who violate the Law of Ukraine "On Personal Data Protection." Article 22 states that any individual or organisation may submit a complaint to the Commission, which must then initiate proceedings. The result of such proceedings may be the imposition of a fine by the Commission. Article 40 allows decisions of the supervisory authority to be appealed in court.

To harmonise Ukrainian legislation with the requirements of the EU, the Council of Europe, and relevant UN documents, the following steps are recommended:

- Amend Article 182 of the Criminal Code of Ukraine to align its terminology with the broader body of personal data protection legislation and introduce appropriate penalties for violations of data processing rules that result in serious harm to individuals,
- Authorise the new supervisory body for personal data protection to impose administrative fines for violations, with the option for judicial appeal,
- Establish legal requirements for determining the amount of a fine based on the severity of the offence and accompanying factors that influence the consequences, in accordance with Article 83 of the GDPR,
- Ensure that any reform of liability for violations of personal data protection legislation includes mechanisms for awarding moral compensation to individuals harmed by unlawful activity.

3.5. Restrictions on the Right to Respect for Private Life During Martial Law

3.5.1. Protection of Personal Data During Wartime

On 24 February 2022, the President of Ukraine signed a decree introducing martial law in the country. According to this decree, during the period of the legal regime of martial law, constitutional rights and freedoms may be restricted, including the secrecy of correspondence and communications, and the right to personal and family life. Since its initial introduction, martial law has been extended several times - under the most recent changes, it will remain in effect until 9 May 2025.

Back in 2015, in response to the occupation of Donetsk and Luhansk oblasts by the aggressor state, Ukraine formally derogated from certain obligations under the International Covenant on Civil and Political Rights and the Convention for the Protection of Human Rights and Fundamental Freedoms. After the full-scale invasion in 2022, Ukraine notified the Council of Europe of a renewed derogation from certain Convention obligations. In spring 2024, the scope of the derogation was revised and reduced, reflecting Ukraine's readiness to resume its obligations and guarantee citizens' rights and freedoms.

According to Article 25 of the Law of Ukraine "On Personal Data Protection," the restriction of rights may occur in the interests of national security, economic well-being, or the protection of the rights and freedoms of data subjects or others. This provision is broadly worded and does not include a specific mechanism for the limitation of rights in the field of data protection - such mechanisms are laid out in separate special laws. The Law of Ukraine "On the Legal Regime of Martial Law" does not directly address personal data, but does provide for interference with privacy and control over communications in the context of measures associated with martial law. According to Article 8 of this law, military command and authorised bodies may inspect personal belongings, official premises, and citizens' homes. They may also regulate the operation of electronic communication providers and prohibit the transmission of information via computer networks. Similar measures are set out in Article 18 of the Law of Ukraine "On the Legal Regime of a State of Emergency."

The mechanism for implementing relevant measures during martial law is established by subordinate legislation - currently, this is governed by a Cabinet of Ministers Order dated 24 February 2022. This Order includes an Action Plan detailing the measures set out in the special law, defines deadlines for their implementation, and assigns responsibility to specific agencies.

The current legal framework for the implementation of martial law is functional and based on lawful grounds. However, its implementation at the legislative level has not only intensified intrusions into privacy, but also significantly expanded the powers of state authorities through legislative amendments justified by the need to protect public and national security.

In March 2022, amendments were made to Article 25 of the Law of Ukraine "On the National Police," authorising the police to maintain registers and databases containing information about suspected criminals, accused persons, defendants, individuals wanted by law enforcement, and others. Notably, these databases also include biometric data (such as facial images), which the police are obliged to collect from individuals. Additionally, Article 615 of the Criminal Procedure Code was amended to authorise prosecutors to grant temporary access to information held by individuals or data controllers without the need for a judge's authorisation. In the same month, other amendments to the Code affected citizens' privacy: for example, when conducting a search of a person's home or property, investigators were granted access to computer systems and mobile terminals and permitted to record their data even without explicit authorisation, provided the information might be relevant to a criminal investigation. The law also introduced Article 245-1, which allows investigators and prosecutors to retrieve data from technical devices capable of photo, film, or video recording - including those operating automatically in publicly accessible areas. Since this Article does not limit the scope of data that may be collected, it is presumed that law enforcement agencies may access biometric data. A key issue with these provisions is the lack of clarity on the distinction between restrictions applicable during martial law and those in peacetime, and the absence of a mechanism indicating when the extended discretionary powers will cease upon the end of martial law.

In 2024, further amendments were made to laws governing military service and registration, namely the Law of Ukraine "On Military Duty and Military Service" and the Law of Ukraine "On Mobilisation Preparation and Mobilisation." Since these laws previously did not refer to "personal data" or "confidential data", Parliament adopted new legislation regulating the collection and processing of personal data of military personnel and reservists.

As part of this update, Ukraine introduced a new national register called Oberih, work on which had begun after the adoption of the Law of Ukraine "On the Unified State Register of Conscripts, Persons Liable for Military Service and Reservists" in 2017. Under this law, only authorised bodies may access the register and must ensure the protection of data from unauthorised access or misuse. The personal and service data entered into the register are classified as confidential (Article 6(2)). Article 7 contains an extensive list of personal data included in the register, while Article 14(3) includes a non-exhaustive list of public bodies that possess relevant data and supply it for register updates. During the legislative approval stage, the Main Scientific and Expert Department of the Verkhovna Rada Secretariat raised concerns that data collected for legitimate purposes could be processed by other public authorities for unrelated objectives, thereby enabling the processing of an undefined scope of data for undefined purposes - in clear violation of the core principles of the GDPR.

Subsequently, Ukraine launched the Reserv+ application - a digital cabinet for conscripts, persons liable for military service, and reservists - allowing citizens subject to military registration to voluntarily register and update their data. Information from the Oberih

register is automatically imported into the app. Upon installation, users must log in via BankID, confirm their personal data, and create a password or set up FaceID or fingerprint login. Users have criticised the app for technical malfunctions: login errors, incorrect or outdated data, etc. Experts have also raised concerns about its security infrastructure, since no official information has been published regarding the app's protection or data security measures.

To harmonise Ukrainian legislation with the requirements of the EU, the Council of Europe, and relevant UN recommendations, the following steps are recommended:

- When expanding the powers of public authorities in sectoral laws, include a clear clause that limits the applicability of such provisions to the period of martial law only,
- Conduct regular reviews of wartime measures to assess their necessity and proportionality,
- Increase transparency regarding user access to military registration data by providing information about data controllers, the volume and categories of personal data processed, and other relevant details.

3.5.2. Use of Surveillance Technologies During Wartime

Ukraine's engagement with digital technologies is evident in its deployment of advanced tools on the battlefield, including surveillance systems equipped with artificial intelligence).

Since the beginning of the full-scale invasion, Ukraine has actively used Clearview AI, an American facial recognition system. The system has been employed to locate missing persons, debunk false social media posts, enhance security at checkpoints (by identifying individuals at roadblocks), identify deceased soldiers, and detect Russian spies. While Clearview has proven effective in locating and identifying individuals, its use is accompanied by numerous privacy violations and the application of intrusive technologies that conflict with European standards. As a result, the company has faced several lawsuits and complaints from regulatory authorities in France, Austria, Italy, Greece, and the United Kingdom. Clearview has been criticised for the unlawful collection of personal data, improper processing of biometric data, and a lack of transparency regarding the system's technical principles.

Alongside Clearview, Ukraine has also used FindClone, a similarly purposed application that identifies faces using photographs. The app has primarily been used to identify Russian soldiers, as the system searches not only social media platforms (such as VKontakte and Facebook) but also publicly available images that may have been accidentally uploaded by third parties. It is important to note that both Clearview and FindClone are considered high-risk systems whose use is prohibited under the EU Artificial Intelligence Act, directly contradicting European standards.

Another controversial issue concerns the functioning of the unified video surveillance system under the Safe City programme. As mentioned in Section 3.3.2, thousands of surveillance cameras were operating on Russian software TRASSIR, and the data collected was stored on servers in Moscow belonging to companies with ties to the FSB. Later, Ukraine switched to Chinese-made cameras and software (Hikvision and Dahua), with assurances that a "closed network prevents data from being transmitted to the manufacturer's servers." However, these security measures proved insufficient. On 2 January 2024, the aggressor state launched a massive attack on Kyiv and the surrounding region. The SSU later confirmed that Russian intelligence had hacked

cameras running on outdated software, which had been streaming footage of targeted critical infrastructure. According to the SSU, since the start of the full-scale war, more than 10,000 IP cameras have been disabled to prevent the aggressor state from using them to coordinate missile strikes. Given that thousands of other surveillance cameras remain vulnerable to cyberattacks by the aggressor state, the issue of securing Ukraine's video surveillance infrastructure remains unresolved.

These practical problems are especially significant when considered alongside the complete absence of legal regulation of surveillance in Ukraine. Despite the ongoing use of intrusive technologies, no legal provisions have been introduced to regulate how such systems operate, the grounds for their use, the government bodies with access to the systems, or the safeguards against abuse.

Nevertheless, to mitigate privacy risks and prevent unauthorised access to protected data, Ukraine has begun to develop domestic tools to safeguard national security. For example, the Innovation Centre of the Ministry of Defence of Ukraine has developed the AI-powered platform *Avengers*, which helps the defence forces detect 12,000 enemy units weekly using video data. In addition, since July 2023, Ukraine has launched the Brave1 Defence Technology Cluster to support the development of AI-based technologies for wartime applications. One product of this initiative is Mantis Analytics, an AI platform that monitors and analyses the information space, identifies threats (such as disinformation or fake news), and responds to them. Mantis processes thousands of posts and gigabytes of media and social media data in real time, mapping the information on an interactive dashboard. This data supports more effective counteraction against Russian propaganda and disinformation.

Among the key issues Ukraine faces when using the above technologies during wartime are the lack of legislative regulation of these systems and the absence of an exit strategy for their use after martial law is lifted. There are no subordinate acts or specific guidelines for many of these tools. This gap is due both to the rapid development of digital technologies, which far outpaces current legislation, and to the absence of clear European benchmarks, as national defence falls outside the scope of EU regulatory frameworks. The area is left to the discretion of individual states, underscoring the urgent need for a proper legal framework.

To harmonise Ukrainian legislation with EU and Council of Europe standards, the following steps are recommended:

- Clarify, at the by-laws level, the types and scope of additional measures and technologies permitted for use solely during martial law,
- Clarify, at the by-laws level, the intrusive technologies (such as automated decision-making systems or AI-powered systems) that may be used by government bodies, and specify that such digital tools may be used only during martial law,
- Establish a framework for cooperation between law enforcement agencies and companies like Clearview AI, listing the purposes for which the system is used, the functions Clearview must perform, and restrictions on its use with due regard for the privacy of data subjects,
- Develop legislative exit strategies for phasing out the use of surveillance technologies after martial law is lifted.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON HUMAN RIGHTS IN THE DIGITAL ENVIRONMENT

Ukraine is actively investing in building an enabling legal and technological framework to develop and launch AI-driven projects. A regulatory sandbox is already in place to test socially valuable AI initiatives, an AI Center of Excellence has been launched, and a White Paper on AI regulation in Ukraine has been published. These initiatives mark an important first step in moving AI into the legal domain. In parallel, the Ministry of Digital Transformation is developing sector-specific soft-law recommendations - non-binding documents that set out key standards for the design and use of AI systems across fields such as media, advertising, education, and intellectual property.

However, meaningful AI regulation is impossible without comprehensive legislation that clearly defines the rights and obligations of key actors - system developers and providers, users, auditors, and others. It is also essential to establish, or expand the powers of, an oversight body that can independently, professionally, and effectively monitor compliance with these legal standards.

This work is needed both to keep pace with the sector's rapid development in Ukraine and to support the country's European integration. One of Ukraine's medium-term goals is to build national mechanisms that reflect the key elements of the EU's Artificial Intelligence Act (AI Act). Public discussion and concrete proposals to initiate this process are expected in the near future.

4.1. General Principles

4.1.1. Core Principles for AI Regulation

Ukraine's path toward AI regulation began with the adoption of the Concept for the Development of Artificial Intelligence, which identified priority sectors for technological advancement but effectively postponed legal regulation of the field. The Concept was introduced long before the EU AI Act was drafted, and at the time, Ukraine had no legal standards in this area. In 2023, the Ministry of Digital Transformation published a Roadmap for AI Regulation, outlining a brief plan through 2027. A more detailed version followed in the form of the White Paper on AI Regulation, which proposes a bottom-up regulatory approach - from soft-law measures to binding legal standards. While the White Paper does not impose mandatory rules, it does recommend aligning future Ukrainian legislation with the EU AI Act, which the country will need to adopt as part of EU integration.

The implementation of this plan began with the development of self-regulatory initiatives and recommendations for responsible AI use in various sectors. A key milestone was the signing of the Declaration on AI Self-Regulation, which outlines basic commitments for signatory companies, including the principle of transparency - a core element of the EU AI Act. The Ministry of Digital Transformation has also led a multi-stakeholder process to create sectoral recommendations on responsible AI use in media, advertising and marketing, personal data protection, education, and intellectual property. More detailed guidance for developers is forthcoming and is expected to reflect obligations tied to a system's risk level, in line with the EU approach. To support consistent terminology, experts have developed a Glossary of AI Terms that combines both legal and technical definitions and is intended to harmonize language in policymaking and practice.

In December 2024, the Ministry of Digital Transformation unveiled its vision for AI development in Ukraine. One of the key initiatives is the AI Center of Excellence - a hub

to foster partnerships, support development, and bring together regulatory and private initiatives in one space.

Effective AI regulation is now a priority for several reasons. First, Ukraine intends to ratify the Council of Europe Framework Convention on AI, Human Rights, Democracy and the Rule of Law. Since the Convention includes obligations to conduct risk assessments and uphold other standards, Ukraine must establish a legal framework that defines what qualifies as an AI system and who is responsible for risk assessments. Second, many AI systems are already being used in the public sector, making it critical to ensure these technologies undergo proper scrutiny. To do this, Ukraine needs both a basic legal framework for AI systems and a risk-based approach similar to the EU model. Other standards, including transparency, are also essential to enable independent evaluation of public sector AI.

To align Ukrainian legislation with the EU, the Council of Europe, and UN guidance, it is recommended to:

- Develop legislation introducing a risk-based approach to AI regulation and set out requirements for all actors involved throughout an AI system's life cycle,
- Establish baseline cybersecurity requirements for high-risk AI systems,
- Draft secondary legislation on AI system standardisation and compliance assessment procedures.

4.1.2. Human Rights Impact Assessment and Risk Management

A full legislative framework for assessing the impact of AI on human rights can only be introduced once comprehensive regulation is in place. The White Paper on AI Regulation outlines several tools to support this process, including a regulatory sandbox, human rights impact assessment methodology, voluntary codes of conduct, and general and sector-specific recommendations. The Ministry of Digital Transformation of Ukraine has also issued a series of recommendations on the responsible use of AI in fields such as media, advertising and marketing, personal data protection, education, and intellectual property - all of which can be used as a foundation for assessing compliance with human rights standards.

One important step in Ukraine's regulatory roadmap is the ratification of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. This Convention defines minimum standards for the responsible use of AI - with human rights impact assessment among the key requirements. The HUDERIA methodology, developed as one of the tools to support implementation of the Convention, can be used to meet these obligations and promote responsible, secure use of AI systems across different sectors. Since Ukraine will also need to align its national legislation with the EU Artificial Intelligence Act, it is clear that more stringent obligations will be introduced for the private sector. Ratifying the Convention should therefore explicitly extend its scope to private entities, helping Ukrainian businesses prepare for stricter EU standards and improve the quality of their AI technologies.

Ukraine was one of five countries involved in piloting the HUDERIA methodology - that is, some businesses are already loosely familiar with its approach. For example, the law firm Juscutum has delivered webinars on adapting and applying HUDERIA in practice. In addition, once draft law No. 8153 on personal data protection is adopted, a key element of human rights impact assessment - data protection impact assessment - will become mandatory for all relevant actors.

To harmonise Ukrainian legislation with the standards of the EU and the Council of Europe, it is recommended to amend national law to include:

- A requirement to conduct human rights impact assessments for high-risk AI systems before they are deployed,
- A requirement to assess risks throughout the entire life cycle of high-risk AI systems,
- Secondary legislation that sets out relevant impact assessment and risk assessment methodologies, developed with input from civil society, academia, and other stakeholders,
- Unified reporting forms for public and private actors to demonstrate implementation of such methodologies.

4.1.3. Expert Human Oversight of AI Systems

At present, Ukraine has no legal requirement for expert human oversight of high-risk AI systems, as AI remains largely unregulated. However, Article 8(13) of the Law of Ukraine "On Personal Data Protection" includes a provision requiring safeguards against fully automated decision-making that has legal consequences for individuals. In practice, this means providers must offer alternative ways to access services and ensure that AI decisions can be reviewed by a human. The Ministry of Digital Transformation's sector-specific recommendations for AI use in media, advertising and marketing, personal data protection, education, and intellectual property highlight the need for expert human oversight of AI systems. Tools for introducing such oversight are also set out in the White Paper on AI Regulation, including the use of regulatory sandboxes and proposals to establish a supervisory body. In addition, the principle of human oversight is reflected in the Declaration on AI Self-Regulation, signed by key representatives of Ukraine's AI industry - which served as a foundation for developing voluntary codes of conduct.

To align national legislation with EU, Council of Europe, and UN standards, it is recommended to amend Ukrainian law to:

- Introduce mandatory human oversight for high-risk AI systems, including standards for how such oversight should take place,
- Adopt secondary legislation setting out procedures for supervising high-risk AI systems, including templates for reporting and oversight protocols,
- Adopt secondary legislation governing the oversight of AI systems developed and used in the public sector (by state institutions, local governments, municipal and state-owned enterprises), including clear requirements for the qualifications of oversight personnel.

4.1.4. Codes of Practice and Codes of Conduct

Codes of practice - documents that interpret legal requirements and explain how they should be applied depending on the domain or type of AI system - can only be developed once a comprehensive regulatory framework for AI is in place. However, the development and adoption of codes of conduct - which outline additional voluntary commitments that AI providers undertake beyond legal requirements - are already envisioned in Ukraine's White Paper on AI Regulation. The first step was the signing of the Declaration on AI Self-Regulation, joined by representatives of Ukraine's AI industry. This Declaration lays the groundwork for developing voluntary codes of conduct in various sectors. In mid-December 2024, several tech companies signed the first such Code, which sets out

fundamental principles for working with AI systems. Fourteen companies have signed the document so far, but it remains open to other industry members. Additionally, codes of conduct can be developed through co-regulation mechanisms foreseen by the Law of Ukraine "On Media," including in relation to the use of AI in media and advertising.

To harmonise Ukrainian legislation with EU and Council of Europe standards, the national law should be updated to:

- Introduce provisions enabling co-regulation and self-regulation mechanisms for AI, as well as thematic areas to be covered by documents developed under such mechanisms,
- Ensure that both codes of conduct and codes of practice are developed with input from all relevant stakeholders, including civil society and academia,
- Require that industry actors honour the voluntary commitments they adopt, and consider (non-)compliance with such commitments when imposing penalties for AI-related violations.

4.1.5. Regulatory Sandboxes and Real-World Testing

In March 2023, Ukraine's Ministry of Digital Transformation announced the launch of its first regulatory sandbox. This initiative is intended to allow AI, Web3, blockchain, and other innovative projects to be tested in a real-world setting, enabling businesses to refine their models, better understand applicable regulations, and attract investment. Plans for the sandbox were confirmed in both the AI Regulatory Roadmap and the White Paper on AI Regulation, which suggests adopting the sandbox model outlined in the EU AI Act - a step that would facilitate both EU integration and the adaptation of Ukrainian businesses to EU requirements. Given resource limitations, participation in the sandbox is expected to be limited to AI systems with medium or high human rights impact. Another selection criterion will be the project's social significance. Priority will be given to small and medium-sized enterprises and startups - in line with Article 58 of the EU AI Act. In late October 2024, the Ukrainian government adopted a Resolution on the Regulatory Sandbox, establishing the procedure for the pilot programme. According to the official summary, the sandbox will operate as follows:

- Companies apply via the Innovation Development Fund's web portal by submitting basic information,
- An administrator reviews the application,
- If eligibility criteria are met, applicants can submit a detailed description of their product,
- A team of experts prepares a testing plan in collaboration with the company,
- Testing is then conducted by a range of specialists.

The EU AI Act allows national governments some flexibility in how Articles 57-58 are implemented, and the sandbox model proposed by the Ministry of Digital Transformation aligns with these provisions. However, final selection criteria must be non-discriminatory, which will be a key issue for moving this initiative forward.

Currently, the main challenge is the absence of a supervisory body to oversee compliance with rules and procedures within the sandbox. It is also important to note that Articles 57 and 59 of the EU AI Act establish a special regime for processing personal data within regulatory sandboxes. Therefore, if Ukraine aims to align with EU standards, amendments

will also be required to the Law of Ukraine "On Personal Data Protection." Otherwise, processing personal data in the sandbox will pose significant legal difficulties - requiring either repeated consent from individuals or a strong legitimate interest justification.

To align national legislation with EU, Council of Europe, and UN recommendations, it is recommended to:

- Introduce the concept of a regulatory sandbox into national law,
- Develop regulations, guidelines, and other secondary legislation governing access to the sandbox (including equal access guarantees), as well as rules for participation, withdrawal, reporting, and oversight,
- Create tools and methodologies to assess risks and legal compliance of AI systems within the sandbox,
- Establish legal requirements for real-world testing of AI systems, and authorise a supervisory body to oversee such activities.

4.2. Institutions in the AI Sector

4.2.1. Notifying Authority

Ukraine currently lacks AI-specific regulation, and as a result, there are no requirements for appointing designated notifying authorities. While the creation of an AI regulatory body is mentioned in Ukraine's White Paper on AI Regulation, this refers more to market surveillance authorities (covered in section 5.2.2 of this document), rather than notifying bodies. Under the EU AI Act, notifying authorities are responsible for developing and applying procedures to assess, designate, and notify conformity assessment bodies and monitor their activities. These bodies are non-governmental entities that independently assess AI systems for compliance with legal standards - essentially acting as third-party auditors.

Since the AI sector remains largely unregulated, no formal certification requirements exist for conformity assessment bodies. However, it is likely that this responsibility will fall to the National Accreditation Agency of Ukraine, whose core mandate is to certify that organisations and institutions are competent to carry out evaluations in line with legal requirements.

At the same time, since the activities of the National Accreditation Agency are regulated by a Regulation issued by the Ministry of Economy of Ukraine, concerns may arise regarding compliance with the principles of independence and impartiality in how the agency is designed. Therefore, any future changes should address not only the expansion of the agency's powers to include the AI sector, but also the procedure for its formation. It is important to emphasise that such powers must not be assigned to a market surveillance authority.

To align Ukrainian legislation with EU standards, the national framework should be amended to:

- Expand the mandate of the National Accreditation Agency of Ukraine,
- Introduce changes to how the agency is formed and ensure safeguards for its independence,
- Adopt secondary legislation establishing procedures for accrediting bodies responsible for assessing AI systems for compliance with national law.

4.2.2. Market Surveillance

The need to appoint a dedicated market surveillance authority in the field of AI is set in Ukraine's White Paper on AI Regulation. However, the document does not provide specific proposals on which institution should be assigned this mandate or how a new regulator should be created.

Across the EU, regulatory approaches vary depending on national legal systems and the presence of existing institutions with thematically related mandates. For example, Ireland has established nine commissions responsible for monitoring compliance with different parts of the EU AI Act. Each commission oversees a specific area of EU legislation, such as data protection, media, human rights, or the environment. Ireland's approach has become a precedent for national AI regulation among EU countries. In contrast, France has chosen to amend existing legislation by expanding the mandates of already-established oversight bodies in specific sectors, thereby enabling them to enforce EU AI Act requirements without creating new regulators.

At present, most coordination and regulatory functions in Ukraine are handled at the ministerial level. For instance, the Resolution on the Regulatory Sandbox, adopted in October 2024, designates the Ministry of Digital Transformation as the coordinator of the pilot programme. While this may be appropriate for issues like test environments or national policy development, the resolution of disputes and contentious issues should fall under the mandate of an independent regulator rather than central executive bodies. As the number of AI projects in Ukraine grows, the creation of a market surveillance authority – or the expansion of powers of an existing regulator – is becoming increasingly urgent.

Establishing a new institution would require significant financial and administrative resources, which could make this option more challenging for Ukraine in the short term. However, broader EU integration efforts also call for transformation of Ukraine's system of public institutions beyond the AI domain. This includes the appointment of a Digital Services Coordinator under the implementation of the EU Digital Services Act, as well as the establishment of a national data protection authority.

One possible option is to expand the mandate of the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum, and Postal Services (NCEC), which already possesses technical expertise and oversees the electronic communications sector. The downside to this option is that the NCEC is not specifically focused on human rights, which is central to the mandate of a market surveillance authority under the EU AI Act. On the other hand, the National Council of Television and Radio Broadcasting of Ukraine (National Broadcasting Council), whose powers were expanded under the Law of Ukraine "On Media," already deals with online technologies and platforms and frequently encounters AI-related issues in its work on freedom of expression. However, this regulator is already under heavy workload. Given that no institutional changes can be made before martial law ends, assigning it an entirely new area of responsibility is controversial. Moreover, Ukraine is planning to establish a separate oversight body for data protection and access to public information. However, much will depend on the final version of its mandate and how the institution is formed, as the current draft law remains imperfect – as discussed in sections 3.4.1 and 3.4.2 of this report. In short, no ideal solution exists. Any decision on which body should be entrusted with oversight of the AI sector must take into account all relevant advantages and risks.

Finally, specialised functions may be assigned to sectoral regulators. For example, oversight of competition in AI markets could naturally fall under the jurisdiction of the

Antimonopoly Committee of Ukraine (AMCU). Therefore, even if a new oversight authority is created to monitor compliance with specific AI requirements, updates to sectoral legislation will still be needed to avoid duplication of responsibilities and to clearly define the mandates of competent authorities. These legislative updates will be necessary regardless of whether a new regulator is created or an existing one is assigned additional responsibilities.

To harmonise Ukrainian legislation with EU requirements, the following steps should be taken:

- Determine the optimal model for a market surveillance authority and either create a new body or assign this mandate to an existing regulator, ensuring a strong focus on human rights,
- Ensure that all powers which should fall under the competence of an independent regulator are transferred from central executive bodies currently exercising them on a temporary basis,
- Update national legislation with secondary legal acts regulating the procedure for reporting violations to supervisory authorities.

4.2.3. Remedies

At present, Ukraine does not have dedicated procedures for appealing human rights violations linked to the use of AI technologies - whether through supervisory bodies, the courts, or relevant regulatory authorities. Individuals can rely on the general right to submit proposals, complaints, and petitions under the Law of Ukraine "On Citizens' Appeals." This law enables people to file complaints against government agencies that develop or use AI systems capable of infringing on human rights. In principle, this includes technologies such as facial recognition-equipped surveillance systems, e-governance tools like "State in a Smartphone," and other AI technologies used in the public sector. It also allows appeals to any business, institution, or organisation operating in Ukraine, which includes domestic AI developers. Things become more complicated with foreign companies - if they have no representation in Ukraine, alternative avenues must be found to restore violated rights.

Article 212-3 of Ukraine's Code of Administrative Offences imposes liability for unlawful refusal to accept or review appeals submitted under the Law on Citizens' Appeals. However, there is no precedent for using this article to challenge incomplete responses or a lack of response from AI developers. This may suggest that appeals are being handled properly, or that claimants are simply not using this article to bring complaints before the Ukrainian Parliament Commissioner for Human Rights (Commissioner) or in court.

Additionally, liability may arise under sectoral legislation - for instance, the Law of Ukraine "On Personal Data Protection," which includes general provisions that apply to data protection in all sectors, including AI. The Law of Ukraine "On Copyright and Related Rights" is also relevant, as it regulates objects created by computer programs and protects them under a *sui generis* regime. Violations of anti-discrimination laws may also apply. However, most such cases are likely to be handled by the Commissioner or the courts - outside the jurisdiction of AI regulators. The only exception is the media sector: the Law of Ukraine "On Media" authorises the National Broadcasting Council to investigate incidents of bias and hate speech in the media, which could include AI-generated media content.

Still, none of the existing mechanisms are tailored to address the unique legal challenges of AI systems or to hold developers or users accountable for violations in this domain. Nor

do they guarantee victims access to the information needed to understand how these systems work - a prerequisite for filing effective complaints or lawsuits.

To bring Ukrainian legislation in line with EU standards, the following updates are needed:

- Empower supervisory bodies to handle AI-related complaints through non-judicial procedures (as is already done in the media sector),
- Adopt secondary legislation detailing the procedures for submitting complaints in cases of violations,
- Adopt secondary legislation requiring that users be informed of violations and establishing appropriate response mechanisms,
- Establish legal requirements for determining the amount of penalties based on the severity of the violation and other relevant factors that affect its consequences.

4.3. Content and AI

4.3.1. Labelling Content Requirements

Currently, there are no legal requirements in Ukraine to label AI-modified content. The Ministry of Digital Transformation has issued a series of recommendations on the responsible use of AI systems. Some of these - particularly those relating to media, advertising and marketing communications, and intellectual property - contain direct labelling requirements. The media recommendations, for example, emphasise the need to proactively inform audiences when AI systems are used to generate or modify content. They explicitly call for labelling to help distinguish authentic content from AI-generated material. Developing tools for labelling AI-modified content is also listed among the actions in Ukraine's White Paper on AI Regulation. This document recommends voluntary labelling by AI developers to ensure compliance with current and future legal requirements in both Ukraine and the EU.

Transparency is also a principle of the Code of Conduct adopted as part of Ukraine's emerging AI self-regulation framework. Since media is the area where labelling concerns are most relevant, the Journalism Ethics Commission has issued the Guidelines on AI use in media, which stress the importance of clearly marking AI-generated content and identifying cases where such use is inappropriate or potentially harmful.

In practice, some public institutions have already begun using labelling for AI-generated content. For example, the Ministry of Foreign Affairs' Victoria AI project - a digital consular assistant, which includes warnings and labels to indicate that content is artificially generated. However, AI-generated content is not consistently labelled across all government communications. In the private sector, the situation is mixed: media outlets have on multiple occasions unintentionally published unlabeled AI-generated content or failed to verify it properly. Because there are no legal consequences for such lapses, some outlets continue to share AI-modified material without labels, even after facing public backlash.

To align national legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Impose labelling requirements on AI developers for AI-modified content,
- Adopt secondary legislation specifying procedures for labelling - including format, method, and requirements based on content type, actor, and risk level of the AI system,

- Introduce mandatory labelling rules for users of AI systems, and define liability for certain categories of actors (e.g. media outlets or advertisers) in the event of non-compliance.

4.3.2. Countering Disinformation

The Law of Ukraine "On Information" defines accuracy and integrity of information as key principles of information relations. However, it does not include any specific measures to prevent or penalise disinformation. Similarly, the Law of Ukraine "On Media" relies on general prohibitions: both Article 36 and Article 119 restrict the dissemination of illegal appeals and content related to Russian aggression, without assessing its factual accuracy. The only vaguely relevant provision can be found in Article 302 of the Civil Code of Ukraine, which obliges individuals to disseminate only accurate information. However, this applies strictly to defamation claims regarding honour, dignity, and business reputation, and is unlikely to be used in cases involving public interest, where an individual claimant might not be recognised as having legal standing.

The Ministry of Digital Transformation has issued a series of recommendations on the responsible use of AI systems. Several of these - particularly those addressing media, advertising and marketing communications - directly or indirectly address the spread of false content. For instance, the media recommendations stress the need to proactively inform audiences when AI systems are used to generate or modify content. They also warn against sharing AI-generated content intended to deceive, spread disinformation, or circulate illegal material. Media outlets are encouraged to carefully consider the context in which they publish such content - for example, AI-generated images should not be used when reporting on sensitive topics such as war, politics, or social issues.

While in many European countries concerns about AI-generated content and disinformation are closely tied to electoral processes, in Ukraine the most serious risks are linked to Russian information warfare. Deepfakes of Zelenskyi, Zaluzhnyi, Syrskyi, Klitschko, and others have been widely circulated. Coordinated inauthentic behaviour campaigns are being run on platforms such as Meta. Similarly, images of Ukrainian TV hosts and popular bloggers have been used on TikTok to spread disinformation about sensitive topics like military mobilisation. Since platform operations and user activity on platforms are not currently regulated in Ukraine, the only available tools to counter such threats are media literacy initiatives and horizontal cooperation with platforms - whether led by public authorities or civil society organisations.

Since March 2021, Ukraine has had a Centre for Countering Disinformation under the National Security and Defence Council. The Centre is tasked with identifying and preventing information threats to national security and interests. Another body - the Centre for Strategic Communications and Information Security under the Ministry of Culture and Information Policy - also tracks harmful narratives in the information space and coordinates government responses. The Ministry additionally runs an educational initiative called Filter, which focuses primarily on promoting media literacy. Much of the work done by these institutions and projects is devoted to countering disinformation, particularly disinformation related to Russia's aggression. Monitoring of military-related narratives is also carried out by Brave1, which hosts a dedicated platform - Mantis Analytics - to track harmful messages and their distribution channels. Importantly, this project uses AI tools to verify information and analyse large datasets.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Introduce clear provisions defining the respective roles of the Centre for Countering Disinformation and the Centre for Strategic Communications and Information Security, including for monitoring AI-generated disinformation and coordinating with key stakeholders,
- Enact legal prohibitions on the use of AI systems that manipulate human cognition or deceive individuals into making atypical decisions, including through deepfakes,
- Establish requirements for public authorities to promote co- and self-regulatory mechanisms aimed at countering disinformation and enhancing digital and media literacy.

4.3.3. Requirements for Content Governance Systems

Effective Ukrainian legislation does not include any rules or standards for content prioritisation, recommendation, or moderation systems used by online platforms. While the Law of Ukraine "On Information" sets out a general obligation to ensure equal access to information and affirms principles of information pluralism and freedom of expression, these provisions are overly broad. As such, their application to technical platforms remains unclear and open to interpretation. The Law of Ukraine "On Media" limits its scope to video-sharing platforms. Article 25 of the law does not impose specific obligations related to recommendation systems for such providers, instead requiring only that platforms publish clear and transparent terms of use. At the same time, these platforms are explicitly prohibited from collecting and processing children's personal data for commercial purposes.

Existing legislative initiatives also do not offer any clear approach to regulating content recommendation systems. For example, draft law No. 11115, which primarily targets regulation of Telegram, does not include any proposals on how to regulate content management systems and falls short of European standards in this area. It focuses on penalising platforms for failing to remove specific content items, rather than requiring them to take systemic measures. No other legislative initiatives that comprehensively regulate online platform providers have been registered in Parliament so far, although discussions are ongoing about the need for a Ukrainian equivalent to the EU Digital Services Act.

Meanwhile, the Ministry of Digital Transformation of Ukraine has issued several recommendations on the responsible use of AI systems in the media, intellectual property, and advertising and marketing communication sectors. All three documents emphasise that content personalisation systems should be transparent and grounded in principles of pluralism, integrity of information, and respect for personal data. They also stress that information should be truthful and reliable, and that users should have the right to customise advertising and commercial communications, as well as the way content is presented to them. However, none of the documents explicitly prohibits systems designed to manipulate user behaviour.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Ban AI systems that use subliminal techniques or are intentionally manipulative or deceptive in ways that influence human behaviour, including manipulative content recommendation systems,

- Establish requirements for information-sharing platforms regarding the transparency and functioning of their recommendation systems, and prohibit the use of such systems for manipulative or deceptive purposes,
- Ban advertising that uses children's personal data for commercial purposes across all types of online intermediaries, for example by amending the Law of Ukraine "On Personal Data Protection,"
- Introduce a legal obligation for platforms to provide users with tools to customise their content feeds,
- Amend legislation to define the responsibilities of device manufacturers and providers of user interfaces in relation to the deployment of AI technologies.

4.4. AI and Privacy

4.4.1. Rules on Data Collection for AI Development

Effective Ukrainian legislation lacks proper regulation on the collection of training data for testing and validating AI products. The primary legal reference for AI developers is the Law of Ukraine "On Personal Data Protection," which sets out general safeguards but does not address the specifics of automated data collection or machine learning algorithms. The law outlines the general legal grounds for processing personal data and prohibits the collection of biometric data, except in several legitimate cases - including when the data have been "clearly made public by the data subject" (Article 7(2)(8)).

In terms of access to data protected by copyright, the Law of Ukraine "On Copyright and Related Rights" classifies databases (data compilations) as copyright-protected works if their selection or arrangement is the result of intellectual effort. However, the law does not provide a mechanism for authorising access to or collection of such data. Article 33 of the same law grants a *sui generis* right to certain non-original works generated by computer programs. In this context, synthetic data created by AI algorithms may fall under this category, as they are not the product of human creativity. The rights to such data belong to the developer of the AI system, not to the author of the original input, which in practice allows developers to use generated data for training machine models. However, these rights are limited when third parties seek to reuse the data (Article 33(8)). In such cases, it is essential to follow the principle of fair use - a key European standard for working with data.

Ukrainian law also permits developers to use data in the public domain. Article 10-1 of the Law of Ukraine "On Access to Public Information" states that public information in the form of open data may be freely used and shared. This includes copying, publishing, and using data (including for commercial purposes), provided that the source of the information is cited (Article 10-1(2)). Cabinet of Ministers Resolution No. 835 defines the set of open datasets that must be published, as well as the public entities responsible for managing that information.

There have been no attempts to regulate AI testing procedures at the level of draft laws. Draft law No. 8153 on personal data protection, which aims to harmonise Ukrainian legislation with EU standards, does highlight issues related to automated decision-making, but only marginally touches on AI. The regulation of biometric data in the draft remains quite strict, although developers could potentially rely on provisions allowing the processing of biometric data "for archival purposes in the public interest, scientific or historical research, or statistical purposes" (Article 7). In this case, the draft law would allow for non-commercial data collection for AI training.

Attempts to regulate AI data collection can, however, be observed in national policy. The White Paper on AI Regulation, issued by the Ministry of Digital Transformation, outlines plans to create a regulatory sandbox to support the supervised development and testing of AI products. In March 2023, the Ministry announced the launch of a regulatory sandbox for AI developers. One year later, the government adopted Resolution No. 1238 to introduce this tool in support of Ukrainian startups in AI and blockchain. According to the Resolution, companies planning to launch high-tech products can use the sandbox to conduct research before full-scale deployment. While the resolution does not specify what kind of data may be used to train AI systems, it refers to the concept of a "distributed database," implying a decentralised and synchronised data storage system.

Additional guidance is provided in recommendations issued by the Ministry of Digital Transformation, which were developed in partnership with legal and technical experts. These documents interpret existing legislation and advise on responsible and ethical use of AI. For example, the Recommendations on AI and intellectual property affirm the legitimate use of *sui generis* rights under the following conditions: (1) obtaining permission to use the object, such as via a licensing agreement; (2) implementing mechanisms to protect rights, such as removing protected objects from the AI system; and (3) encouraging the use of open data for AI training. The Recommendations on AI and human rights emphasise the protection of personal data that may be collected during system development. They also encourage developers to anonymise data where necessary and to carry out risk assessments when designing AI systems.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- In the updated Law of Ukraine "On Personal Data Protection," introduce mechanisms for data exchange for the purposes of AI training and validation (modelled on the EU Data Act and EU Data Governance Act), specifically:
    - Require explicit user consent for the collection and processing of biometric data, and ensure users are informed in advance about how their data will be used, as mandatory conditions for data collection by AI developers,
    - Establish a mechanism allowing data subjects to request deletion of training data after the AI system has been trained,
- Develop ethical standards for data use in AI training, which may include anonymisation or data licensing,
- Establish publicly managed datasets (based on prior consent from data subjects and content authors) to provide open training data for AI developers,
- Allow AI developers to reuse non-open government-held data (as foreseen in the EU Data Governance Act), by defining categories of such data, mechanisms for their anonymisation or modification prior to use, and ensuring the protection of intellectual property and personal data.

4.4.2. Protection Against Automated Decision-Making

Ukrainian legislation recognises the right to protection against automated decision-making. For instance, Article 8(13) of the Law of Ukraine "On Personal Data Protection" includes this right among those granted to data subjects. However, the law does not provide any further detail on this right, nor does it include exceptions similar to those outlined in the EU GDPR, such as explicit consent or the conclusion of a contract. Paragraph 12 of the same article also guarantees the right to know the mechanism behind

automated data processing, but the wording is vague. It is unclear whether this includes the right to receive an explanation in each individual case or simply access general information about how the system operates. This lack of clarity is particularly problematic in the AI context, where developers need to understand the extent of their obligations towards data subjects.

Draft law No. 8153 - a full revision of the personal data protection law designed to align Ukraine's legal framework with EU standards - proposes changes to address these issues. For example, Articles 18 and 19 of the draft law would strengthen the right to information by requiring that individuals be notified of "the existence of automated decision-making mechanisms, including profiling, and relevant information about the algorithms/logic used in these mechanisms, as well as the significance and foreseeable consequences of such processing." This provision reflects a blend of requirements from both the EU AI Act and the GDPR. Additionally, the draft includes a separate Article 25 devoted to protection against automated decision-making, which mirrors Article 22 of the GDPR.

Although case law on automated data processing and decision-making remains limited, it does exist. A notable example is Case No. 127/13877/19, which involved Ukrposhta's automated processing of personal data. The plaintiffs challenged the company's practice of pre-filling invoices and requiring mobile phone numbers for deliveries, citing reliance on an automated computer system. The court ruled that under the Article 8(13) of the Law of Ukraine "On Personal Data Protection," individuals have the right to receive services without automated data processing. The court concluded that denying this option constitutes a violation of the law. While this case provides an illustrative precedent, it remains an exception. In many instances, automated data processing occurs without offering individuals a human alternative.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Introduce exceptions to the right to protection against automated decision-making in national law, mirroring Article 22 of the GDPR,
- Explicitly establish the right to receive an explanation for decisions made by automated systems in each individual case (in addition to the right to be informed of how such systems operate),
- Develop effective programmes for media, digital, and AI literacy,
- Require the personal data protection regulator to review current practices involving automated data processing that result in decisions significantly affecting individuals, to assess their legality and ensure that the right to protection is fully upheld.

4.4.3. Biometric Identification Systems

The use of biometric identification systems in Ukraine is growing rapidly - from biometric passports to facial recognition technologies. Currently, these systems are primarily employed for security purposes and the provision of public services.

One of the most well-known platforms in this area is Diia - a digital government portal that offers online public services, supports businesses, and facilitates the IT sector. Diia includes a mobile application that enables access to citizens' electronic documents and data from state registries. Log-in is performed via FaceID, and facial recognition is also used to enable electronic signature functionality. Electronic documents are widely used

across Ukraine: biometric passports were introduced in 2015, including biometric data such as fingerprints. Online banking apps are also highly popular, many of which allow login through biometric authentication. The BankID system, in its turn, can be used to access Diia and similar services.

At the beginning of the full-scale invasion, Ukraine made active use of Clearview AI and FindClone - foreign facial recognition systems used to identify deceased soldiers from the aggressor state. In addition, the Regulation on the National Biometric Verification and Identification System operates in Ukraine for citizens of Ukraine, foreign nationals, and stateless persons. The system monitors individuals entering and leaving the country, as well as their compliance with the rules for staying on Ukrainian territory. The Regulation includes a list of authorities authorised to access biometric data. However, assessing the system's compliance with GDPR requirements is difficult due to the broad and vague wording of its provisions. According to paragraph 4, "the processing of personal data within the national system, including their storage, shall be carried out in compliance with the Law of Ukraine 'On Personal Data Protection.'" At the same time, the Regulation does not specify what guarantees are in place to ensure that data subjects are properly informed of their rights in relation to such processing.

Biometric identification systems are also in use at the local level. For example, under the Safe City initiative, many Ukrainian municipalities have installed surveillance cameras equipped with facial recognition software. These systems serve legitimate goals such as identifying wanted individuals, documenting public order violations, and monitoring public spaces. With a dedicated analytics module, the system can simultaneously process 450 streams and recognise up to 1,100 faces per second. The data are stored in databases of wanted individuals. Oversight of such intrusive systems is currently handled by local governments, as in Kyiv City Regulation on its Comprehensive Video Surveillance System. A draft law - draft law No. 11031 - proposes to create a unified video monitoring system and standardise the use of surveillance cameras. However, its current version allows for the collection of biometric data in a way that violates fundamental privacy rights. Under the draft law, identification is based on biometric data and additional information such as date of birth/death, place of birth, gender, and citizenship - a profiling practice that, under EU law, requires strict adherence to personal data protection principles and strong justification for such privacy intrusions. The draft does not provide an adequate rationale for collecting such extensive data, which is at odds with GDPR requirements.

Draft law No. 8153 on personal data protection (Article 7) sets general rules for the processing of sensitive data - including biometric data - and outlines conditions for its lawful processing. Article 9 of the draft specifically regulates processing of biometric data by public authorities, listing all permitted scenarios. Article 11 covers the processing of personal data derived from audio, video, or photographic recordings of public events.

One of the key problems with Ukraine's use of biometric identification systems is that the comprehensive legal regulation is lacking. There are currently no unified standards that can guide both data subjects and authorised entities. Regulation exists only at the sub-legal level, resulting in fragmented rules, legal gaps, and misalignment with EU standards. While the Law of Ukraine "On Personal Data Protection" does offer some guarantees, they fall short of the clear, robust protections provided under EU law for the collection, processing, and storage of biometric data.

Therefore, the privacy of individuals whose biometric data are collected faces real risks - both technical (e.g. unauthorised access, data leaks, or system flaws) and ethical (e.g. use of data without consent, or discrimination based on biometric features).

To align Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Enact legislation defining clear rules for the use of biometric identification systems by state authorities, including legal grounds, conditions, authorised entities, and limitations, consistent with the EU AI Act,
- Prohibit the use of biometric categorisation systems under national law,
- Strengthen provisions in the Law of Ukraine "On Personal Data Protection" regarding the processing and storage of biometric data by introducing additional safeguards for data subjects, including:
  - A mechanism allowing individuals to request the deletion of their biometric data once the processing purpose has been fulfilled or where processing is unlawful,
  - Requirement to store biometric data in encrypted form as a security measure,
  - Limited access to biometric data granted only to specifically authorised personnel,
  - A mechanism enabling individuals to challenge unlawful processing of their biometric data.

4.4.4. Privacy by Design and Privacy by Default

Ukrainian legislation currently does not include references to the concepts of privacy by design or privacy by default. These are expected to be introduced by draft law No. 8153, which replicates Article 25 of the General Data Protection Regulation (GDPR) in its Article 29. However, until the law is adopted, there are no requirements for enhanced privacy safeguards in the design of technical systems. At the same time, the Ministry of Digital Transformation has issued several recommendations on the responsible use of AI systems in media, advertising and marketing communications, data protection, education, and intellectual property. Each document stresses the importance of integrating privacy safeguards during the development and use of AI systems, while the dedicated privacy guidance outlines ways in which these concepts can be incorporated into the AI development process.

Additionally, in mid-December 2024, a group of technology companies signed a Code of Conduct - a self-regulatory instrument for AI that defines key principles for responsible AI development and is expected to form the basis for a future AI self-regulatory body. One of its principles is the obligation to protect user privacy throughout the AI system lifecycle.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN recommendations, the following steps should be taken:

- Introduce privacy by design and privacy by default principles into the Law of Ukraine "On Personal Data Protection,"
- Adopt secondary legislation detailing the implementation of these principles in the development of AI systems,
- Conduct a privacy audit of government digital platforms (e.g. Diia, Mriia, Reserv+).

4.5. AI and the Prohibition of Discrimination

4.5.1. Balance in Datasets

Ukrainian anti-discrimination legislation is general in nature. The Law of Ukraine "On Principles of Prevention and Combating Discrimination in Ukraine" prohibits all forms of discriminatory treatment on any grounds. While this extends in principle to developers, providers, and users of AI systems, the law does not specify how these provisions apply to such technologies, what measures should be taken at various stages, what form they should take, or who is responsible for enforcement. Other equality-related laws – including the Law "On Ensuring Equal Rights and Opportunities for Women and Men," the Law "On the Fundamentals of Social Protection of Persons with Disabilities in Ukraine," the Law "On the Rights and Freedoms of Internally Displaced Persons," the Law "On Combating the Spread of Diseases Caused by the Human Immunodeficiency Virus (HIV) and Legal and Social Protection of People Living with HIV," and the Criminal Code of Ukraine – likewise do not address how anti-discrimination norms apply to AI or emerging technologies. At the same time, as discussed in the previous section, the data protection framework does contain specific provisions on sensitive data.

Ukraine's White Paper on AI Regulation highlights the need to adopt anti-discrimination safeguards as part of efforts to build a responsible AI environment. However, it does not offer concrete proposals on how datasets should be constructed. Some potential to improve dataset fairness exists through initiatives such as regulatory sandboxes, which allow developers to test their systems. In addition, recommendations on responsible AI use in media, advertising and marketing communications, data protection, education, and intellectual property sectors all underline the importance of equality in the design and deployment of AI. In 2025, detailed recommendations for AI developers are expected, likely reflecting the requirements of Article 10 of the EU AI Act.

Given the growing use of AI systems in the public sector, it is especially important to ensure that training datasets are balanced and that information on which data were used for development and testing is made publicly available for review by independent experts.

To align Ukrainian legislation with EU, Council of Europe, and UN standards, the following actions are recommended:

- Establish legal requirements to prevent discrimination and ensure equality at all stages of the AI system lifecycle,
- Enshrine legal standards for datasets used in training, testing, and validating AI systems, including rules on the use of sensitive data,
- Develop a methodology for auditing datasets for potential bias or legal violations,
- Introduce mechanisms to restore violated rights and ensure equality in the AI sector, including out-of-court remedies,
- Conduct an audit of datasets that have been and are currently used in the training, testing, and operation of public sector AI systems,
- Develop a benchmark dataset for training, testing, and validating AI systems intended for use in the public sector.

4.5.2. Predictive Analytics Systems

The effective Ukrainian legislation contains neither prohibitions on the use of certain types of predictive AI systems nor any framework governing their use in the judicial or law enforcement sectors. For instance, Article 314-1 of the Criminal Procedure Code of Ukraine, which addresses the content of pre-trial reports prepared by probation officers, does not reference automated systems or set any standards for their use. Similarly, laws regulating the police, anti-corruption agencies, the Security Service, and counterintelligence bodies do not provide specific mandates related to predictive analytics. No relevant regulation exists at the level of secondary legislation issued by ministries or government agencies.

In practice, the Ministry of Justice of Ukraine has piloted the use of Kassandra, an AI-based tool designed to assess a person's risk of reoffending based on a 97-question survey, with results to be integrated into pre-trial reports. Back in 2020, Justice Minister Denys Maliuska stated that in a few years, after sufficient machine learning, Kassandra would be able to analyse not only answers to simple questions but also "all other available data about an offender." No updated information about the system's effectiveness is currently available, which may indicate either that the project has not progressed to its next stage, where AI analyses broader datasets, or that the system is being used without public disclosure. Ukrainian civil society groups and human rights advocates have expressed serious concern about Kassandra, warning that inaccurate outcomes could lead to severe consequences. No secondary legislation has been adopted to regulate the use of Kassandra or any similar system.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Prohibit AI systems that evaluate or classify individuals based on their social behaviour or known, assumed, or predicted personal characteristics where such evaluation causes harmful effects, as well as AI systems that assess or predict criminal behaviour solely based on profiling or personality assessments (with exceptions as outlined below),
- Introduce legislation to regulate the use of predictive analytics in law enforcement and judicial processes, including safeguards such as prohibiting their use in relation to individuals without reasonable suspicion of criminal activity,
- Develop secondary legislation that establishes technical and legal standards for predictive analytics systems, rules for their use, and mechanisms of accountability for violations.

4.5.3. Feedback and Complaints Instruments

Ukrainian legislation does not currently regulate the activities of AI system developers or online platform providers, and therefore does not set requirements for feedback or complaint mechanisms. The existing Law of Ukraine "On Consumer Rights Protection" is not adapted to the functioning of online services, including those that use AI systems. As a result, it does not contain provisions on internal complaint-handling procedures or related obligations. The new version of the Law "On Consumer Rights Protection," which will enter into force after martial law ends, includes Article 39, which clearly establishes the consumer's right to have their complaint reviewed by the business entity allegedly responsible for the violation. The law also mandates timely and reasoned responses to complaints. However, the applicability of these provisions to AI system users is unclear. Similarly, it remains questionable whether Article 39, as currently formulated, is suitable

for regulating online platform providers or developers of AI systems. As such, additional rules need to be introduced into sector-specific legislation.

Meanwhile, several recommendations from the Ministry of Digital Transformation on the responsible use of AI (covering media, advertising and marketing communications, data protection, education, and intellectual property) emphasise the importance of enabling user feedback for AI systems. The White Paper on AI Regulation also proposes developing standardised tools and mechanisms to improve communication between AI providers or developers and users regarding system errors or malfunctions.

To harmonise Ukrainian legislation with EU, Council of Europe, and UN standards, the following steps should be taken:

- Include in legislation on online platforms the requirement to establish complaint portals that also cover the use of AI systems,
- Introduce requirements for feedback and complaint portals into AI sectoral regulations,
- Establish the right to appeal the inaction of AI system developers or providers to supervisory authorities.

THE RIGHT TO FREE ELECTIONS: POLITICAL ADVERTISING IN THE DIGITAL ENVIRONMENT

At present, Ukraine is not adequately prepared at the legislative level for the growing role of online political advertising. The existing regulation is fragmented and outdated, and there is no comprehensive approach to the issue. These problematic aspects were highlighted in reports by the ODIHR Limited Election Observation Mission during the 2020 local elections. Some interlocutors noted that "political parties and candidates often preferred advertising on social media to circumvent campaign finance requirements, as online political advertising was not regulated by law." One of the recommendations by the Limited Mission was that "electoral legislation and the regulatory framework for the media should include specific provisions on financial reporting for political advertising on social networks and online media." To this end, the observers emphasised that the law should define political campaigning as also including campaigning via social media.

The use of online political advertising during the electoral process is governed by the general provisions of Chapter VIII of the Election Code, which regulates pre-election campaigning. According to Article 51(1) of the Code, campaigning may be conducted through "publication in print and audiovisual (electronic) mass media of political advertising, speeches, interviews, features, video films, audio and video clips, and other publications and announcements." At the same time, Article 51(4) states that campaigning must be funded from the electoral funds of candidates, parties or their organisations. This means that spending on online campaigning should be reflected in the financial reports of electoral funds.

Under the Article 54(5) of the Code, hidden advertising and materials that are not properly labelled are prohibited in pre-election campaigning. However, the lack of a clear definition of "hidden campaigning" complicates the prevention of such violations in the online environment. Furthermore, Article 52 provides a general rule that campaigning must end at 24:00 on the Friday before election day. While Article 55 sets out rules for the use of electronic media, these apply to linear audiovisual media such as television and radio. The Code does not include special provisions for Internet-based campaigning.

In March 2021, a working group was established under the Parliamentary Committee on State Power, Local Self-Government, Regional Development and Urban Planning to address these gaps. The group included representatives of civil society organisations, media experts, business, and Members of Parliament. One of its tasks was to align media rules in the electoral process with the draft law "On Media." On 30 August 2022, the Verkhovna Rada adopted the Law of Ukraine "On Media" in the first reading. Despite public calls, provisions on campaigning in the Election Code were removed during the second reading. At the same time, amendments to the Law "On the All-Ukrainian Referendum" were adopted.

In order for these provisions to be incorporated into legislation, draft law No. 8310 "On Amendments to the Election Code of Ukraine" was registered on 27 December 2022. This document proposes a number of innovations concerning the regulation of online campaigning and campaigning on shared platforms, including:

- Placement of campaign materials only on the basis of contracts with the electoral fund,
- Provision of information on placement terms and copies of contracts upon request by the NAPC, CEC, or National Broadcasting Council,

- Mandatory labelling of online campaign materials,
- Liability for distributors of banner advertising,
- Cooperation between the National Broadcasting Council and shared platform providers to ensure compliance,
- An obligation for Internet and platform users to comply with the requirements and restrictions for pre-election campaigning.

However, implementing these provisions may prove difficult. For example, in order to enter into a contract, the media outlet must be registered in Ukraine, but such registration is voluntary (Article 63 of the Law "On Media"). Payment for online campaigning from electoral funds is also complicated due to banking restrictions. During the 2020 elections, such services were paid for by individuals, which enabled circumvention of the law. The draft law does not provide for effective monitoring mechanisms or sanctions for violations.

It should also be noted that under the draft law, labelling requirements apply only during the electoral process, while political advertising outside of election periods remains unregulated. This highlights a conceptual problem in Ukrainian legislation, namely the absence of a clear definition of "political advertising." The Election Code only governs pre-election campaigning during election periods, whereas materials that qualify as campaigning in the inter-election period are not regulated at all. Moreover, lawmakers use the terms "pre-election campaigning" and "political advertising" interchangeably, which creates confusion and allows for circumvention of campaign finance and campaigning rules.

Regarding the financing of online political advertising, according to the Election Code, the electoral fund limit for a presidential candidate or a political party in parliamentary elections is 90,000 times the minimum monthly wage. At the same time, the electoral fund limit for each MP candidate on a regional party list is capped at 4,000 times the minimum monthly wage. These limits, however, are not adapted to the digital environment and do not take into account the operational models specific to online platforms.

It should also be clarified that Ukrainian legislation does not include specific regulation of political advertising targeting online. Indirectly, such regulation is provided by the framework Law "On Personal Data Protection." According to Article 11 of this Law, the key precondition for processing personal data is the data subject's consent. A similar approach is reflected in the Law of Ukraine "On Electronic Commerce," Article 10 of which stipulates that "commercial electronic messages may be distributed only based on the recipient's consent." At the same time, commercial electronic messages may be sent without consent only if the recipient has the opportunity to opt out of further messages.

In practice, users often give consent to the processing of personal data without having full and accessible information about how it will be used. This leads to the problem of a loss of control over personal information, even though, under Article 8 of the Law "On Personal Data Protection," the data subject has the right to withdraw consent at any time. Furthermore, the Law "On Electronic Commerce" applies to "commercial electronic messages," which are defined as messages aimed at directly or indirectly promoting goods, services, or the business reputation of a person engaged in economic or professional activity. Therefore, these provisions do not apply to online political advertising during the inter-election period or to pre-election campaigning materials on the Internet.

Therefore, to harmonise Ukrainian legislation with the requirements of the EU, the Council of Europe, and relevant UN-level recommendations, it is important to introduce comprehensive amendments to the Law of Ukraine "On Advertising" well in advance

of the first post-war elections, or to adopt a separate Law "On Political Advertising." This legislation should bring the regulation of political advertising in line with Regulation (EU) 2024/900 and include provisions on the production, placement, and financing of political advertising not only during elections but also in the inter-election period.

In addition, such a legislative act should:

- Guarantee a proper level of transparency in online political advertising, including by providing information about the advertisers on the platforms where the advertising is displayed. It should also introduce labelling requirements for online political advertising to allow citizens to clearly and unequivocally distinguish political content from other types of advertising, identify its sponsors, understand whether targeting tools were used, and - if such advertising forms part of election or referendum campaigning - determine which electoral or referendum process it relates to,
- Impose obligations on political advertising providers to store online political advertising archives for a sufficient period in a machine-readable format, ensuring proper analysis of materials by public institutions and researchers. In the future, the creation of a national online political advertising repository should also be considered,
- Require platforms to regularly report the total amount of income received, in whole or in part, in exchange for online political advertising services,
- Oblige platforms and websites hosting online political advertising to have mechanisms allowing individuals or legal entities to report instances where specific political advertisements infringe human rights and freedoms or contravene the Constitution of Ukraine or other laws,
- Ensure, through co-regulation mechanisms, that online platforms provide access to political advertising in a fair and non-discriminatory manner and apply equal pricing for equal services to all users,
- Provide competent public authorities with the ability to request any necessary information from providers of online political advertising. Such information must be complete, accurate, reliable, and presented in a clear, coherent, consolidated, and understandable format,
- Establish clear regulations on targeting in online political advertising,
- Introduce appropriate sanctions for violations in the field of online political advertising.

The Final and Transitional Provisions of this Law should also foresee amendments to the Election Code to ensure harmonisation - particularly with regard to limiting campaign spending on online pre-election campaigning.

Digital
Security Lab
Ukraine

INTERNATIONAL
RENAISSANCE
FOUNDATION