Vita Volodovska,
Head of Digital Rights GS
of the NGO Digital Security Lab

Maksym Dvorovyi,
Lawyer at the NGO Digital Security Lab

Digital Security Lab

INTERNET FREEDOM REPORT 2020

RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS ON THE INTERNET

with the support of:
the American Bar Association's Rule of Law Initiative
(ABA ROLI) in Ukraine

AMERICANBARASSOCIATION
Rule of Law Initiative

SECTION 1. Favorable environment for the Internet Freedom

1.1. Legislative basis

The development and spread of the Internet have created unprecedented tools for citizens to realize their rights and freedoms, including the opportunity to freely express their views and thoughts to a wide audience and to have prompt access to any online resources. At the same time, threats related to the abuse of such rights, the spread of hate speech and unlawful violation of privacy have also increased.

In resolution 38/2018 [1] the Human Rights Council guided by the Charter of the United Nations "**affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights**."

The Council of Europe, in its documents and the decisions of the European Court of Human Rights (European Court of Justice), supports the position concerning the obligations of Member States to ensure to everyone within their jurisdiction the rights and fundamental freedoms outlined in the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as the "European Convention"), including rights of Internet users. In the case of Ahmet Yildirim v. Turkey [2] the European Court of Justice stated that "**the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest**."

According to international obligations, State authorities have an obligation not only to refrain from impeding the realization of human rights but also must to create the necessary conditions in this regard. In the case of the Editorial Board of Pravoye Delo and Shtekel v Ukraine [3] the European Court of Human Rights stated that Article 10 of the European Convention places positive obligations on States to set an appropriate regulatory framework to effectively protect internet-based freedom of expression. The right to respect for privacy and other fundamental rights has a similar obligation to establish an appropriate legal framework for the protection and promotion of these rights.

---

[1] *The Human Rights Council A/HRC/38/L.10/Rev.1 "The promotion, protection and enjoyment of human rights on the Internet", 4 July 2018: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1.*

[2] *Ahmet Yildirim and Others v Turkey App no 3111/10 (ECtHR,18 December 2012): http://hudoc.echr.coe.int/eng?i=001-115705.*

[3] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine (Application No. 33014/05): https://zakon.rada.gov.ua/laws/show/974_807*

Current national legislation contains virtually no special legal provisions to protect the digital rights of citizens. Most rights and freedoms related to the Internet are subject to the general rules of constitutional, civil, criminal and administrative law. At the same time, the specificities of the realization of human rights online are not always adequately taken into account in administrative and judicial practice.

1.2. Development of regulation

International standards require that Internet laws and other regulatory instruments be evaluated at the drafting stage for their possible impact on human rights and fundamental freedoms.

The Law of Ukraine "On the Rules of Procedures of the Verkhovna Rada of Ukraine" [4], which regulates the legislative procedure, does not explicitly provide for obligatory evaluation of the impact of Draft Laws submitted to the Parliament on human rights. At the same time, the Rules contain several procedural mechanisms that allow for its implementation. Thus, Article 91 establishes the need to justify in an explanatory note to the Draft Law the legal and other consequences of the application of the law after its adoption. The Regulation also requires mandatory expertise on the compliance of draft legislation with Ukraine's international legal obligations in the area of European integration, which today covers, inter alia, the protection of personal data, electronic communications and audio-visual media services. Article 103 of the Regulations provides that a Draft Law must be registered and placed on the agenda of the session in preparation for the first reading for a scientific examination, and in preparation for all subsequent readings: to conduct a legal expert assessment in the relevant subdivisions of the Verkhovna Rada Administration.

However, the lack of a separate focus on human rights in legislative work has led to the adoption of laws containing serious threats of violations and a reduction of human rights online. The lack of a formalized role of the Commissioner for Human Rights in the law-making process does not help the situation.

Thus, according to the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights" [5] the Ombudsman exercises parliamentary control over the observance of human and civil rights and freedoms under the Constitution and protects the rights of everyone in the territory of Ukraine and within its jurisdiction on an equal basis. The Ombudsman's powers include the right to make proposals, in accordance with established procedures, to improve Ukrainian legislation on the protection of human and civil rights and freedoms. The Standing Orders of the Verkhovna Rada grant the Ombudsman the guaranteed right to address a plenary meeting to consider issues relating to his powers. However, the current legislation does not contain any obligation to receive or provide the findings of the Ombudsman in draft human rights legislation.

[4] *Law of Ukraine "On the Rules of Procedures of the Verkhovna Rada of Ukraine": https://zakon.rada.gov.ua/laws/show/1861-17*

[5] *Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights": https://zakon.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80#Text*

The principles of inclusiveness and transparency are another important standard in the development of Internet legislation.

Current legislation makes mandatory the publication of both draft bills and Cabinet of Ministers acts of major public importance and defining the rights and obligations of citizens of Ukraine, and draft acts of other authorities. At the same time, the legislation does not prescribe regulated procedures for involving various stakeholders in the development of relevant regulations.

Thus, Article 50 of the Law of Ukraine "On the Cabinet of Ministers of Ukraine" [6] stipulates that people's deputies of Ukraine, scientists and other specialists with their consent may be involved in the preparation of draft acts of the Cabinet of Ministers of Ukraine. The Law of Ukraine "On Committees of the Verkhovna Rada of Ukraine" [7] also gives parliamentary committees the right to establish working groups and appoint their leaders from among the committee members for the preparation of draft acts of the Verkhovna Rada of Ukraine discussed at committee meetings, draft decisions, recommendations and conclusions of committees and to include in such a working group, in addition to the members of the committee, other people's deputies of Ukraine, as well as employees of research institutes and educational establishments, authors of draft legislation and other specialists with their consent.

The legislation does not describe the selection procedures for such working groups, does not guarantee access to all interested parties, and does not contain an obligation to consider proposals for bills/laws that are introduced by citizens. The only exception is the drafting of regulatory acts relating to economic activities. Article 9 of the Law of Ukraine "On the Principles of Regulatory Policy in Economic Activity" [8] describes in detail the procedure of discussion of such draft acts, in particular establishing that each draft regulatory Act must be published for the purpose of receiving comments and suggestions from natural and legal persons and their associations. At the same time, the period within which comments and proposals are accepted is set by the drafter of the regulatory Act and may not be less than one month; and all comments and proposals on the draft regulatory act and the corresponding analysis of its impact, received within a specified time period, are subject to mandatory review by the drafter. The developer of the draft regulatory act must take into consideration, in whole or in part, the comments and suggestions received or justify the rejection.

A similar approach should be adopted with regard to other acts of the executive authorities or other state bodies having an impact on the realization of human rights and freedoms.

[6] *Law of Ukraine "On the Cabinet of Ministers of Ukraine" https://zakon.rada.gov.ua/laws/show/794-18#n408*

[7] *Law of Ukraine "On Committees of the Verkhovna Rada of Ukraine": https://zakon.rada.gov.ua/laws/show/116/95-%E2%F0#Text*

[8] *Law of Ukraine "On the Principles of Regulatory Policy in Economic Activities": https://zakon.rada.gov.ua/laws/show/1160-15*

1.3. Regulatory body

In accordance with international standards, any public body with competence over Internet governance should operate independently of political and commercial influence, transparently and respectfully, to protect and promote Internet Freedom.

Ukraine does not have a single regulatory body for Internet governance. Currently, the Ministry of Digital Transformation (MDT) and the National Commission for the State Regulation of Communications and Informatization (NCSRCI) are the key state bodies in this area.

Under Regulation on the Ministry of Digital Transformation [9] the MDT is responsible for formulating and implementing public policies in the areas of digitization, digital development, digital economy, digital innovations and technologies, e-government and e-democracy, development of the information society model, informatization; in the area of electronic document management; in the area of digital skills and the digital rights of citizens; in the areas of open data, development of national electronic information resources and interoperability, development of broadband Internet and telecommunications infrastructure, e-commerce; in the area of providing of electronic administrative services; in the area of trusted services for digital identification; in the area of IT industry development.

The main tasks of NCSRCI are state regulation and supervision in the area of telecommunications, informatization and usage of radio-frequency resources. The NCSRCI exercises supervision (control) over compliance by market entities: with the legislation on telecommunications, information and postal communications; licensing requirements, special conditions specified in the relevant licenses and rules in the field of telecommunications; indicators of the quality of telecommunications and information services; routing of traffic on telecommunication and information networks, etc.

On December 16, 2020, the Verkhovna Rada of Ukraine adopted the Draft Law "On Electronic Communication" [10] partly accommodating the President's reservations [11]. The new Law, which will enter into force on 1 January 2022, consolidates several innovations that improve digital rights in Ukraine. In particular, the law announced the right to Internet access as universal service and the possibility to communicate anonymously, as well as updated anti-spam standards.

---

[9] *Regulation on the Ministry of Digital Transformation: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919?fbclid=IwAR3ypNvjs8fjr9ZpbqvAfEVlyR4680zuCWUX4m2WgQpjS8Kl1s3HmK7wEXs*

[10] *Draft Law "On Electronic Communication": https://zakon.rada.gov.ua/laws/show/1089-IX*

[11] *Digital Security Lab: The president vetoed the Law "On Electronic Communication": https://dslua.org/publications/prezydent-vetuvav-zakon-pro-elektronni-komunikatsii/*

At the same time, a full-fledged reform of the regulation of electronic communications will not be possible without the reform of the NCSRCI, which is currently not in line with the requirements of independence and efficiency. To fulfillobligations under the Association Agreement between the European Union and Ukraine and in the European Union foreign policy initiative “Eastern Partnership”, the people’s deputies of the Parliamentary Committee on Digital Transformation drafted and introduced in the Verkhovna Rada the Draft Law No. 4066 “On the National Commission for State Regulation in the Fields of Electronic Communications, Radio Frequency Spectrum and Postal Service of Ukraine” [12].

The Draft Law seeks to introduce the transparent and competitive procedures of appointment of members of the communications regulator; to ensure the independence of the communications services regulator for its competent and fair decisions, openness and transparency of the state regulatory process, according to the provisions of the Constitution of Ukraine and the decisions taken by the Constitutional Court of Ukraine on the procedure for the establishment of the regulatory bodies for communications services and the appointment of their members and describing their place in the system of authorities in Ukraine.

1.4. Effective remedies of protection

The Constitution of Ukraine guarantees everyone the right to appeal against the court decisions, acts or omissions of state or local authorities and officials; and the right to appeal to the Human Rights Commissioner of the Verkhovna Rada for the protection of their rights. However, the effectiveness of these mechanisms is not always realized.

Thus, according to Article 15 of the Law of Ukraine "On the Ukrainian Parliament Commissioner for Human Rights", in case of violation of human rights and freedoms, the Ombudsman submits to the relevant state bodies and local self-government bodies, citizens' associations, enterprises, institutions and organizations irrespective of the form of ownership, their officials and employees, requiring to take appropriate measures within one month to eliminate the violations identified. An administrative fine of UAH 1,700 to UAH 3,400 is imposed for non-compliance with the Commissioner’s legal requirements. However, the procedure for administrative prosecution is rather complicated and often makes it impossible to bring the culprit to justice in a timely manner.

To strengthen the institution of the Ombudsman, in April 2020 in the Verkhovna Rada, a Draft Law No. 3312 “On the introduction of amendments to some legislative acts of Ukraine concerning the Ukrainian Parliament Commissioner for Human Rights” [13] was registered. Among the novelties of the Draft Lawis a clear complaints procedure and procedure of the Ombudsman’s proactive response to violations of human rights and fundamental freedoms: requirements for complaints to the Ombudsman; grounds for a refusal to commence proceedings; definition of an abuse

[12] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=69864*

[13] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68542*

of the right to appeal to the Commissioner; timing of proceeding. In addition, to enhance the effectiveness of the Commissioner's work, it is assumed that, following the outcome of the proceedings opened on the basis of an individual complaint, the Commissioner or the representative of the Commissioner may issue an order to eliminate the violation of rights and freedoms, which is mandatory. For failure to comply with the Commissioner's order, the latter may question the disciplinary responsibility of the official responsible.

The Draft Law had been criticized on a number of proposed provisions, but the necessity to strengthen the Ombudsman's office was supported by both the authors of the legislative initiative and representatives of civil society and international organizations [14].

The importance of such a non-judicial instrument for the protection of human rights is particularly relevant, given the length of judicial proceedings in those cases when it examines complaints against the decisions of the authorities regarding the violation of citizens' digital rights. Judicial recourse against digital rights violations is often accompanied by legal and financial barriers, and the adjudication of cases can take months or even years. The effectiveness of and barriers to judicial protection of freedom of speech and privacy are discussed in the following chapters.

1.5. Protection against cybercrime

Ukraine ratified the Budapest Convention (The Convention on Cybercrime of the Council of Europe) [15] in 2005. This document lays down a number of requirements of national law, criminalizes several acts, as well as requirements of criminal procedural law, which should ensure the effective investigation of crimes [16]. The norms of substantive criminal law have been implemented in the Criminal Code of Ukraine, where section XVI of the Special Chapter deals with crimes in the use of computers, systems and computer networks, and contains a number of Articles in other chapters [17]. The National Police of Ukraine has a Cyber-Police Department, which implements the state policy in this area [18].

The rules of criminal procedure reflected in the Budapest Convention have not been fully implemented in the national legislation. In particular, the possibility of using electronic evidence in criminal proceedings has not yet been introduced.

[14] Draft Law was withdrawn in February 2021. A new Draft Law No. 5019 "On Amending Certain Legislative Acts of Ukraine to Improve the Legal Basis for the Work of the Ukrainian Parliament Commissioner for Human Rights" was registered as a substitute: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71010

[15] Law of Ukraine "On the Ratification of the Convention on Cybercrime": https://zakon.rada.gov.ua/laws/show/2824-15

[16] Convention on Cybercrime: https://zakon.rada.gov.ua/laws/show/994_575

[17] Criminal Code of Ukraine: https://zakon.rada.gov.ua/rada/show/2341-14

[18] The website of the Cyber Police Department of the National Police of Ukraine: https://cyberpolice.gov.ua/

On 1 September 2020, Draft Laws No. 4003 [19] and No. 4004 [20]. were submitted to the Verkhovna Rada. Although it could supplement Ukrainian legislation with some positive novelties, such as the introduction of a criminal procedure security measure as time-limited storage of information, as well as the introduction into Ukrainian legislation of the concept of "electronic evidence", they contain several human rights risks.

Thus, the provision on access by law enforcement officials to the information stored in electronic information systems (for example, information stored in a smartphone or personal computer) which is not subject to a search permit, if the investigator or prosecutor decides that there are reasonable grounds to believe that the stored information is relevant to establishing the circumstances of the criminal proceedings, it confers unlimited discretion to law enforcement officials and has not provided any mechanism to protect individuals against violation of their right to privacy of correspondence. It is also proposed that providers should take a number of obligations to preserve information in telecommunications systems, in particular on traffic flows in a volume sufficient to identify the subscriber and determine the source of the traffic and its route within 12 months, as well as the temporary storage requirements for criminal proceedings. Such information would generally be ordered by a prosecutor or investigator and would create the risk of access to any information on a personal communication without proper judicial safeguards [21]. These bills are on the agenda of the Verkhovna Rada but have not yet been adopted.

1.6. Digital literacy

The development of digital education has been identified as one of the priorities of the Ministry of Digital Transformation (MDT) activities. The Ministry has set a goal to attract 6 million Ukrainian to Digital Skills Development programs until 2024.

For that purpose, in 2020 the MDT created 1,500,000 offline hubs of digital education in different cities of Ukraine, as well as launched the Digital Literacy Platform "Diia: Digital Education" [22] where digital literacy can be taught. In 2020, the portal launched 40 educational "serials", which watched more than 400 thousand Ukrainians. These include courses on basic digital skills, media literacy, cyberbullying, online security, personal data protection and access to public information, as well as courses on enterprise development using online tools.

[19] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770*

[20] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771*

[21] *Statement of the Coalition for Free Internet: https://dslua.org/publications/paket-zakonoproektiv-shchodo-protydii-kiberzlochynnosti-ta-posylennia-sanktsiynoho-mekhanizmu-vid-1-veresnia-2020-roku-mistyt-zahrozy-dlia-tsyfrovykh-prav-zaiava-koalitsii-za-vilnyy-internet/*

[22] *https://osvita.diia.gov.ua/*

The Ministry of Digital Transformation also launched the first national digital literacy test. As of the end of November 2020, the test was passed by more than 50,000 Ukrainians. More than 34,500 Ukrainians answered all 90 questions of the national test and received a certificate of digital literacy (69% of those who started the test) [23t].

At the same time, the launching of digital skills and media literacy programs into the school curriculum is not yet systematic.

RECOMMENDATIONS TO SECTION 1:

THE VERKHOVNA RADA OF UKRAINE:

— to strengthen the role of the Ukrainian Parliament Commissioner for Human Rights to exercise parliamentary control over the observance of human rights and freedoms in legislative initiatives submitted to the Parliament or the Cabinet of Ministers; and to strengthen the powers to respond to violations in the field of the realization of digital human rights and freedoms, while guaranteeing the independence of the Ombudsman institution.

UKRAINIAN PARLIAMENT COMMISSIONER FOR HUMAN RIGHTS:

— to develop and implement a system for monitoring and evaluating the state of digital human rights.

THE VERKHOVNA RADA OF UKRAINE AND THE CABINET OF MINISTERS OF UKRAINE:

— to ensure a process of inclusive stakeholders participation in the preparation and processing of legal and regulatory acts affecting human rights and freedoms in the online environment, by introducing better practices for publicizing draft normative acts, collecting and processing proposals from the public, informing about the results of the consideration of such proposals, etc.

VERKHOVNA RADA OF UKRAINE, VERKHOVNA RADA COMMITTEE ON DIGITAL TRANSFORMATION:

— to finalize the Draft Law No. 4066 "On the National Commission for State Regulation in the Fields of Electronic Communications, Radio Frequency Spectrum and Provision of Postal Services of Ukraine" and launch the process of reform of the National Commission for State Regulation of Communications and IT (NCSRCI), establishing guarantees of independence, transparency, competence and effectiveness of electronic communications oversight.

[23] The first 50,000 Ukrainians take the Digital Literacy Test: https://thedigital.gov.ua/news/pershi-50000-ukraintsiv-pochali-skladati-natsionalniy-test-na-tsifrovu-gramotnist-tsifrogram

THE MINISTRY OF DIGITAL TRANSFORMATION OF UKRAINE AND THE MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE:

— to develop and consistently introduce programs for the development of digital skills in the mainstream school system.

THE VERKHOVNA RADA COMMITTEE OF UKRAINE ON LAW ENFORCEMENT:

— to finalize the Draft Law No. 4003 "On Introducing Amendments to the Criminal Procedure Code of Ukraine and the Code of Administrative Offences of Ukraine on Enhancing the Effectiveness of Counteracting Cyberattacks" and Draft Law No. 4004 "On Amending the Criminal Procedure Code of Ukraine on Enhancing the Effectiveness of the Fight against Cybercrime and Use of Electronic Evidence" before the adoption of the Draft Laws in the second reading and in general, in order to eliminate human rights risks.

SECTION 2. Freedom of expression

2.1. Access to the Internet

There is a broad debate about whether to recognize the right of access to the Internet as a human right and whether it should be called "the right to Internet access". The right to Internet access is enshrined at the legislative level in several countries, from Estonia to France to Costa Rica, and the need to enshrine it is stated in several documents of UN, OSCE and Council of Europe [24]. Recommendation CM/Rec (2014) 6 on a Guide to human rights for Internet users states that Internet access should be provided without discrimination and at an affordable price, and States should make reasonable efforts to facilitate access to the Internet in rural and geographically remote areas, are on a low income and/or have special needs or disabilities. However, access to the Internet may be restricted solely by court decisions [25].

2.1.1. General level of Internet access

The right to Internet access is not yet enshrined in Ukrainian legislation. On December 16, 2020, the Verkhovna Rada of Ukraine, after taking into account the proposals of the President of Ukraine, adopted the Draft Law of Ukraine "On Electronic Communication", which adds affordable broadband access to the Internet in a fixed location to the list of universal communication services [26]. This is primarily an obligation of the central executive power authority in the sector of electronic communications and radio frequency resources to ensure access to a wide range of services from social media and messengers to Internet banking and video communications. This obligation will be enshrined in Ukrainian legislation from 1 January 2022.

The infrastructure for Internet access in Ukraine should be analyzed from several aspects, both affordability and physical accessibility, that is, coverage on the population and territory.

In terms of affordability, **Ukraine is considered to be one of the countries with the cheapest Internet access in the world**. According to cable.co.uk, in 2019 Ukraine was in 5th place in the world in terms of the average cost of mobile data with an average price of $ 0.46 for 1 GB [27]. According to Pikodi, in 2019 Ukraine had the cheapest home fiber optic Internet and one of the cheapest opportunities to connect to the Gigabit-speed Internet: the average price of such connection was 6.19 $ per month [28].

---

[24] *Maksym Dvorovyi. Will we talk about the right to the Internet in Ukraine: https://detector.media/infospace/article/172446/2019-11-15-chy-budemo-my-govoryty-pro-pravo-na-internet-v-ukraini/*

[25] *Recommendation CM/Rec (2014) 6: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5b31*

[26] *Law of Ukraine "On Electronic Communications": https://zakon.rada.gov.ua/laws/show/1089-IX*

[27] *Worldwide mobile data pricing: https://www.cable.co.uk/mobiles/worldwide-data-pricing/*

[28] *Picodi. Price Rankings by Country of Internet: https://www.picodi.com/ua/mozhna-deshevshe/sravnenie-tsen-na-internet-v-mire*

With an average monthly income of UAH 10,887.46 in October 2020 [29] (approximately 388 USD at the NBU exchange rate) [30], such prices can be considered as available to the general population.

The situation is somewhat worse concerning to Internet coverage of the territory and population of Ukraine. Targeted measurements of broadband Internet coverage have not been made until recently, as emphasized by Mykhailo Fedorov, the Head of the Ministry of Digital Transformation of Ukraine that was established in 2019 [31]. In an interview in November 2019, he pointed to data of NCSRCI on the coverage of 62% of Ukraine's territory by high-speed Internet and pointed to the goal of covering 90-100% of territory by the end of 2022 [32]. This goal was envisaged as one of the 2020 goals of the Ministry [33]. The draft National Strategy for the Development of Broadband Internet Access, prepared by the MDT, contains information on the coverage of 85 % of the population of Ukraine with quality broadband Internet as of May 2020 [34]. The Head of the Ministry himself acknowledges that, as of the end of July 2020, more than 17,000 settlements are not covered by networks of any operator, and therefore more than 4 million Ukrainians live in villages without fixed wireless Internet, while 1.55 million Ukrainians live in geographically remote areas where the cost of Internet exceeds 150% of the average market cost [35].

The Ministry of Digital Transformation published an interactive map of the connection of settlements to fiber-optic networks, and one can see that such Internet connection is common only around major cities, as well as in western regions, in Kyiv and Cherkasy regions [36].

---

[29] *Pension Fund of Ukraine. Average wages for 2020: https://www.pfu.gov.ua/2121350-pokaznyk-serednoyi-zarobitnoyi-platy-za-2020-rik/*

[30] *National Bank of Ukraine, official hryvnia exchange rate against foreign currencies on 11.12.2020: https://bank.gov.ua/ua/markets/exchangerates?date=11.12.2020&period=daily*

[31] *Mykhailo Fedorov. More than 5.5 million Ukrainians cannot get quality fixed internet: https://www.pravda.com.ua/columns/2020/07/30/7261199/*

[32] *Minister spoke about the level of coverage of Ukraine by the Internet: https://www.radiosvoboda.org/a/news-pokryttia-internetom/30289573.html*

[33] *Work plan of the Ministry of Digital Transformation of Ukraine for 2020 рік: https://thedigital.gov.ua/storage/uploads/files/page/ministry/%D0%9F%D0%BB%D0%B0%D0%BD_%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B8_%D0%9C%D1%96%D0%BD%D1%86%D0%B8%D1%84%D1%80%D0%B8_%D0%BD%D0%B0_2020_%D1%80%D1%96%D0%BA.pdf*

[34] *Ministry of Digital Transformation of Ukraine. The draft National Strategy for the Development of Broadband Internet Access: https://drive.google.com/file/d/1X9xlLClpTaXwcOjRdK9l5Mw2cAlZryuQ/view*

[35] *Mykhailo Fedorov. More than 5.5 million Ukrainians cannot get quality fixed internet: https://www.pravda.com.ua/columns/2020/07/30/7261199/*

[36] *Ministry of Digital Transformation of Ukraine and Digital Transformation Committee. The interactive map of the connection of settlements to fiber-optic networks: https://thedigital.gov.ua/fiber*

The data on the fiber-optic networks coverage is also available on the Unified state web portal of open data [37]. In the testing mode, the Ministry has launched the broadband.gov.ua site [38], which is considered as a government multifunctional platform for informing on the development of broadband Internet access, including coverage information [39].

It is worth mentioning that in September 2020, the Government obliged the NCSRCI to publish in open data mode such data as "Information about Internet coverage, technology, speed and number of users in each locality, provided by telecommunication operators and providers within the framework of the response to NCSRCI requests" [40]. By the end of 2020, this data set had not been released on the Unified state web portal of open data [41].

Regarding mobile Internet coverage, the three main mobile operators (Vodafone, Kyivstar and Lifecell) that provide 4G LTE mobile Internet services publish their own data on network coverage [42]. According to Kyivstar network representatives, their 4G network as of November 2020 is available for 85% of the population of Ukraine [43]. The coverage process intensified in 2020 with the release of frequencies due to a decree of the President of Ukraine in July 2019 [44]. The Deployment of 5G networking infrastructure is envisaged by the normative acts of the President of Ukraine [45], and the Cabinet of Ministers of Ukraine [46], and tendering procedures for allocation of broadcasting frequencies to deploy the network are planned for December 2021.

---

[37] *Unified state web portal of open data. The coverage of settlements by fiber-optic networks: https://data.gov.ua/dataset/788580dd-e3ae-45b4-a93b-f7f3e8a3f80d*

[38] *https://broadband.gov.ua/*

[39] *Ministry of Digital Transformation of Ukraine. The draft National Strategy for the Development of Broadband Internet Access: https://drive.google.com/file/d/1X9xlLClpTaXwcOjRdK9l5Mw2cAlZryuQ/view*

[40] *Resolution of the Cabinet of Ministers of Ukraine No. 870 "On Amendments to Annex to the Regulations on Data Sets to be Disclosed in the Form of Open Data", 23.09. 2020: https://zakon.rada.gov.ua/laws/show/870-2020-%D0%BF#n8*

[41] *Unified state web portal of open data, the National Commission for State Regulation of Communications and IT: https://data.gov.ua/organization/natsionalna-komisiia-shcho-zdiisniuie-derzhavne-rehuliuvannia-u-sferi-zviazku-ta-informatyzatsi*

[42] *Vodafone network coverage: https://www.vodafone.ua/services/network/coverage-map.*
Kyivstar network coverage: https://kyivstar.ua/uk/mm/mobile-internet/karta-pokrytiya-3g.
Lifecell network coverage: https://www.lifecell.ua/uk/mobilnij-internet/pokrittya/

[43] *Mykhailo Fedorov: 5.4 million Ukrainians got 4G coverage from July to November 2020: https://www.kmu.gov.ua/news/mihajlo-fedorov-54-mln-ukrayinciv-otrimali-krashchu-yakist-pokrittya-4g-z-lipnya-po-listopad-2020-roku*

[44] *Decree of the President of Ukraine No. 497, 8.08.2019 "On Some Measures on Improvement of Access to Mobile Internet: https://www.president.gov.ua/documents/4972019-27953*

[45] *Decree of the President of Ukraine No. 242/19, 17.05. 2019 "On providing conditions for the implementation of the mobile communication system of the fifth generation": https://www.president.gov.ua/documents/2422019-26881*

[46] *Order of the Cabinet of Ministers of Ukraine No. 1409-r, 11.11. 2020: https://zakon.rada.gov.ua/laws/show/1409-2020-%D1%80*

2.1.2. Special measures for Internet access

Ukraine does not have reliable access to the Internet through special points in public service and educational institutions. Mykhailo Fedorov declares the existence of a digital divide between urban and rural residents and recognizes this as a problem; he also reported that 40 % of schools, 92 % of libraries and 37 % of hospitals, mostly located in villages and small towns, are not connected to quality fiber optical Internet. In the context of a pandemic, this poses challenges for distance learning and telemedicine [47]. In the Ministry of Digital Transformation's Action Plan for 2020, one of the stated goals was to connect 90% of schools to fixed broadband Internet of good quality, as well as obtaining up-to-date data and gradually connecting all medical institutions and social infrastructure to broadband Internet [48].

The draft of the National Broadband Strategy, which defines in more detail the solutions to the problems of connecting social infrastructure to broadband networks, was discussed publicly in 2020 and is awaiting approval. The MDT plans that by the end of 2023 95 % of social infrastructure facilities will be provided with at least 100 Mbps Internet, with the possibility of upgrading to 1 Gbit Internet without the purchase of additional modules. It is proposed to connect social infrastructure facilities in three stages: by the end of 2021, 55 % of facilities must be connected, and 80 % of the rural population should be able to access broadband Internet by the end of 2022; by the end of 2022 those rates should change to 75 % and 95 % respectively; and by the end of 2023 the same rates should rose to 95 % and 99 %. The draft Strategy intends to allocate more than UAH 55,000,000 [49]. At the same time, in 2021 only UAN 500,000,000 have been allocated from the State budget to local budgets for the implementation of measures aimed at increasing access to broadband Internet in rural areas, instead of UAN 3,000,000,000,000 listed in the draft Strategy [50]. This could boost the Ministry's efforts, and there is a possibility of change in dates of mentioned in the draft Strategy because it has not yet been approved.

The Government also intends to take steps to improve the situation and fulfil its positive obligations in providing Internet for vulnerable populations. The draft Strategy proposes the introduction of Internet accessibility activities for persons with disabilities.

[47] *Mykhailo Fedorov: More than 5.5 million Ukrainians cannot get quality fixed internet: https://www.pravda.com.ua/columns/2020/07/30/7261199/*

[48] *Work plan of the Ministry of Digital Transformation of Ukraine for 2020: https://thedigital.gov.ua/storage/uploads/files/page/ministry/%D0%9F%D0%BB%D0%B0%D0%BD_%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B8_%D0%9C%D1%96%D0%BD%D1%86%D0%B8%D1%84%D1%80%D0%B8_%D0%BD%D0%B0_2020_%D1%80%D1%96%D0%BA.pdf*

[49] *Ministry of Digital Transformation of Ukraine. The draft National Strategy for the Development of Broadband Internet Access: https://drive.google.com/file/d/1X9xlLClpTaXwcOjRdK9l5Mw2cAlZryuQ/view*

[50] *Law of Ukraine "On the State Budget of Ukraine for 2021": https://zakon.rada.gov.ua/laws/show/1082-IX*

In terms of affordability, the MDT believes that the cost of Internet services amounting to 5-6 % of the monthly pension is excessive, and postulates plans to offer budgetary aid in the amount of approximately UAH 240,000,000 to provide Internet access to such populations [51]. According to the draft Action Plan for the Implementation of the Strategy, by the end of 2023 persons with disabilities are to be provided with equipment for Internet access, by the end of 2021 – with access to websites of public authorities, and by the end of 2022 – with Internet access software that would facilitate the Internet access to this population [52].

The Law of Ukraine "On Electronic Communication" provides the normative basis for the implementation of such specific measures of Internet access [53]. As of 1 January 2022, the legislation will introduce mechanisms that will make it possible to implement the provisions of the Strategy mentioned above. The Law is implementing the monitoring of the cost of Internet access to universal services. As a result, vulnerable populations will be able to receive targeted assistance to access quality Internet if the cost of such connection is too high for them.

The State also takes responsibility to ensure universal services in a certain territory if such services are unavailable or not commercially available. In such a case, the Ministry of Digital Transformation holds a tender (public procurement) for providing a certain area with broadband Internet services. If the winner of the tender is not identified or no supplier has participated, the regulator must identify one or more suppliers that should provide access to the Internet. The supplier has a right to refuse merely on account of State arrears. The deployment of such networks is also subject to reimbursement from the State budget. The Cabinet of Ministers of Ukraine will establish the procedure for obtaining it.

2.1.3. Legality of restrictions on Internet access

Ukraine does not have a regulation in force that clearly provides for the possibility of Internet facilities cut off but contains norms that allow suggesting the application of such a measure.

The Law of Ukraine "On the Legal Regime of the State of Emergency" provides the possibility of applying special rules on the use of communications and the transmission of information via computer networks during the state of emergency declared as a result of terrorist attacks, ethnic and sectarian conflicts, civil disorders or the restoration of the constitutional order. These measures may be introduced by a decree of the President of Ukraine for a period of up to 30 days, subject to further approval by the Verkhovna Rada of Ukraine.

---

[51] Ministry of Digital Transformation of Ukraine. The draft National Strategy for the Development of Broadband Internet Access: https://drive.google.com/file/d/1X9xlLClpTaXwcOjRdK9l5Mw2cAlZryuQ/view

[52] Ministry of Digital Transformation of Ukraine. The draft plan of measures to implement the National Strategy for the Development of Broadband Internet Access: https://drive.google.com/file/d/1S9JEEHBnTtY7aSwcS0y1b9OOdDrQPSQy/view

[53] Law of Ukraine "On Electronic Communication": https://zakon.rada.gov.ua/laws/show/1089-IX

This period may be extended by no more than 30 days under the same approval procedure and must be communicated to the international community through the Secretary-General of the United Nations in accordance with the International Covenant on Civil and Political Rights [54].

The Law of Ukraine "On the Legal Regime of Martial Law" also stipulates that in case of its introduction in the respective territories, the military command and the military administrations may prohibit the transmission of information through computer networks. The international community must be informed of these activities in a manner similar to that of the restriction imposed by the state of emergency [55]. It is worth remembering that, despite the wide margin of discretion of the State to suspend human rights in the event that a state of emergency or martial law is declared, and that digital rights are not among those which derogation is prohibited, both under international law and under the Constitution of Ukraine [56], Such restrictions are permitted only to the extent strictly required by the exigencies, providing that such measures are not inconsistent with other obligations under international law [57].

Also, the Law of Ukraine "On Telecommunications" provides that such restrictions, except the state of emergency or martial law, may be imposed directly by providers in times of emergency in order to alert and provide telecommunications services to emergency response workers, with the approval of NCSRCI [58].

The Draft Law of Ukraine "On Electronic Communication", adopted on December 16, 2020, envisages the introduction of changes to the text of the Law of Ukraine "On Combating Terrorism". According to the draft, from 1 January 2022, in the area of anti-terrorist operation conducting, the providing of electronic communication services may be temporarily restricted in accordance with the procedure established by the Cabinet of Ministers. The law also reinforces the possibility for providers to restrict Internet access services in response to emergency situations and martial law declared [59].

There are no mechanisms for judicial control or appeal against decisions Internet access restricting in response to martial law or a state of emergency. The practice of using existing norms to restrict Internet access on the territory of Ukraine was not recorded in 2020. At the same time, any application must be strictly consistent with the three pillars of human rights and, above all, must be proportional.

---

[54] *Law of Ukraine "On the Legal Regime of Martial Law": https://zakon.rada.gov.ua/laws/show/1550-14*

[55] *Law of Ukraine "On the Legal Regime of Martial Law": https://zakon.rada.gov.ua/laws/show/389-19*

[56] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

[57] *Convention for the Protection of Human Rights and Fundamental Freedoms: https://zakon.rada.gov.ua/laws/show/995_004*

[58] *Law of Ukraine "On Telecommunications": https://zakon.rada.gov.ua/laws/show/1280-15*

[59] *Draft Law of Ukraine "On Electronic Communication": https://zakon.rada.gov.ua/laws/show/1089-IX*

As for restricted Internet access in prisons, the Criminal Executive Code of Ukraine states the right for Internet for persons deprived of liberty, under the supervision of the administration, during their free time, at their own expense or at the expense of other persons by E-wallet. Persons deprived of liberty are allowed to set up and use an e-mail box under the supervision of the administration; due to individual risks of such persons, the administration has the right to avail themselves of contents of incoming and outgoing communications [60].

The procedure for providing access to the Internet for persons deprived of liberty details these provisions and provides the establishment of Internet classrooms or isolated workplaces, and, in some cases, providing such services in cells. Internet access is available upon application to the administration and in accordance with the schedule of the Internet class. Information on the right of imprisoned persons to use the Internet is recorded in a special register, as are their use of IP telephony and video communication [61]. It is assumed that, during Internet access, imprisoned persons are allowed to visit a certain list of sites determined by the administration of the institution and approved by the above-mentioned procedure. Imprisoned persons may have access to the websites of state and local government bodies, international organizations, creative, educational, sports, cultural, legal, and reference websites, as well as those of registered media; upon the request of the imprisoned person, the administration may provide access to other sites [62]. At the same time, in accordance with the Code, it is prohibited to visit social media websites, websites with inappropriate content that promotes cruelty, violence, explicit or pornographic information and images; or to visit sites that may have a negative impact on the mental condition of the imprisoned person; to register on any other site, except authorized and for the purpose of creating an e-mail account or collecting data [63].

It is important to recall that the procedure mentioned above provides protection of the confidentiality of the correspondence of an imprisoned person if such correspondence is conducted with the Ukrainian Parliament Commissioner for Human Rights and the European Court of Human Rights, courts, other relevant international organizations the member of which is Ukraine, authorized persons of such international organizations, the prosecutor, the defense counsel who exercises his or her powers. This contrasts with the need to register the logins and passwords of the e-mail accounts of imprisoned persons, provided by the Procedure [64].

---

[60] *Criminal Executive Code of Ukraine: https://zakon.rada.gov.ua/laws/show/1129-15*

[61] *The procedure for providing access to the Internet for persons deprived of liberty, approved by the Order of the Ministry of Justice of Ukraine No. 1280/31148, October 20, 2017: https://zakon.rada.gov.ua/laws/show/z1280-17*

[62] *Ibidem: https://zakon.rada.gov.ua/laws/show/z1280-17*

[63] *Criminal Executive Code of Ukraine: https://zakon.rada.gov.ua/laws/show/1129-15*

[64] *The procedure for providing access to the Internet for persons deprived of liberty, approved by the Order of the Ministry of Justice of Ukraine No. 1280/31148, October 20, 2017: https://zakon.rada.gov.ua/laws/show/z1280-17*

There is no restriction on the right to Internet access in places of deprivation of liberty. This means that if the imprisoned person has the means to access the network and adheres to all the conditions mentioned above, the prison administration may not restrict him in this right. Given this, the legislation does not provide for a special appeal procedure for additional restrictions, so that any decision, act, or omission concerning the right of Internet access in places of deprivation of liberty is subject of the administrative judiciary in a general order [65].

2.2. Freedom of thought, the right to receive and impart information

The case-law of the European Court of Human Rights shows that Article 10 of the Convention protects not only the content of information but also the process of its dissemination since any restriction interferes with the right to receive and impart information [66]. Given this, it is important to remember that blocking websites, IP addresses, ports, network protocols, and access to individual services (such as social networks) is an extreme measure that can only be justified if such a measure is prescribed by law, necessary for the protection of human rights or other legitimate interests, considered as a proportionate measure, and when the less intrusive alternative is unavailable and that minimum guarantees of due process should be ensured [67].

2.2.1. Internet resources blocking

Ukrainian legislation contains three mechanisms for Internet resources blocking. The Law of Ukraine "On Telecommunications" prescribes the obligation of telecommunication providers to restrict access of their subscribers to resources through which child pornography is distributed by a court order [68]. This mechanism can be considered legitimate, necessary and proportionate, given the threat posed by the dissemination of such content, and the fact that this mechanism is judicial is positive. However, this norm would become void as of 1 January 2022 after entry into force of the Law of Ukraine "On Electronic Communication".

The second mechanism was enshrined in the legislation in August 2020, after the adoption of the Law of Ukraine "On State Regulation of Activities on Organization and Conduct of Gambling" [69]. According to its provisions, a person who organizes or provides access to a gambling website without the necessary license obliged to restrict such access within three days after the request of the Gambling and Lottery Regulatory Commission.

[65] *Code of Administrative Proceedings of Ukraine: https://zakon.rada.gov.ua/laws/show/2747-15*

[66] *Ahmet Yildirim and Others v Turkey App no 3111/10 (ECtHR,18 December 2012): http://hudoc.echr.coe.int/eng?i=001-115705*

[67] *OSCE Representative on Freedom of the Media. Joint declaration on freedom of expression and "fake news", disinformation and propaganda. 3 March 2017: https://www.osce.org/files/f/documents/6/8/302796.pdf*

[68] *Law of Ukraine "On Telecommunications": https://zakon.rada.gov.ua/laws/show/1280-15*

[69] *Law of Ukraine "On State Regulation of Activities on Organization and Conduct of Gambling": https://zakon.rada.gov.ua/laws/show/768-IX*

A similar obligation to restrict access to a website or webpage is imposed on the hosting service provider, whose facilities contain the website or part thereof, which provides access to gambling without a license. The procedure for restricting access to such websites, as provided by law, with regard to the prohibition of carrying out activities without a license, may be permissible despite the extrajudicial character of the procedure, as it does not require website content evaluation and enforce blocking to comply with formal grounds. At the same time, the discretion given to the Commission for the establishment of the referral and claims procedures, mentioned above, is a problem, as it does not contain sufficient safeguards against abuse [70]. An appropriate blocking procedure has not yet been developed by the Commission.

The third mechanism is provided by the Law of Ukraine "On Copyright and Related Rights" [71]. It can only be applied if it is not possible to restrict access to an illegal content, and therefore the hosting service provider should restrict access to the website containing the material that violates the copyright. The mechanism, like the entire procedure for restricting access to such content, is extrajudicial.

Attempts to enshrine more mechanisms for blocking Internet resources in Ukrainian legislation were made in 2020. A number of provisions are proposed by the Draft Law "On Online Media" No. 2693-d, which is under consideration in the Verkhovna Rada of Ukraine and is a revised version of the Draft Law, introduced in 2019 [72]. The Draft Law provides such a sanction as the prohibition of online media distribution on the territory of Ukraine. It can only be applied solely by a court decision issued on the request by the National Council and only if online media has committed three or two gross violations during the year. It is also possible to ban the distribution of online media on the territory of Ukraine in the event of a gross violation by an entity in the sphere of online media, which could not be identified and which did not comply with the relevant order of the National Council.

The Draft Law also specifies the procedure of court order prohibiting the distribution of online media. For example, if the domain name of an online media website is registered in the UA. or УКР domain, and the resources for its hosting are provided by a host in Ukraine then, by the court order, the restriction of access to such resource should be provided by the registrar and the hosting service provider, and not by the telecommunications providers that provide Internet access.

The Draft Law on Mass Media also provides for the possibility of the National Council to apply to the court for a ban on the distribution of foreign audio-visual media services (for example, Netflix) on the territory of Ukraine, if such proliferation threatens the information security of Ukraine.

[70] Digital Security Lab: A new mechanism for restricting access to websites has appeared in Ukraine: https://dslua.org/publications/v-ukraini-z-iavyvsia-novyy-mekhanizm-obmezhennia-dostupu-do-saytiv/

[71] Law of Ukraine "On Copyright and Related Rights: https://zakon.rada.gov.ua/laws/show/3792-12

[72] Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353

Such a limitation shall apply only during the period of armed aggression and shall apply only to entities registered in the Aggressor State, or co-owned by natural persons, residents of the Aggressor State, or its legal persons, or whose media services are directed entirely or predominantly at the Aggressor State. The prohibition of the distribution of foreign audio-visual media service on the territory of Ukraine is implemented, inter alia, through the obligation of telecommunication service providers (operators) to restrict the access of users to the corresponding services.

Another Draft Law worth mentioning in this context is the Draft Law No.3196-d on amending the Law of Ukraine "On the Security Service of Ukraine" on improving the organizational and legal basis of the activities of the Security Service of Ukraine, which essentially constitutes a new version of the mentioned-above Law [73]. According to the provisions of this Draft Law, the Security Service is empowered **"to restrict access to certain (identified) information resources (services) in order to prevent a terrorist act or the commission of intelligence and subversive activities to the detriment of Ukraine, to prevent information attacks against Ukraine aimed at undermining the constitutional order, violating the sovereignty and territorial integrity of Ukraine and aggravating the socio-political and socio-economic situation, those used to organize, prepare, commit, finance, facilitate or cover up unauthorized interference in the activities of critical information infrastructure, using technical facilities, installed by operators, providers of telecommunication services and other business entities"**. While it is proposed that such blocking should take place by court order, the introduction of this procedure contains a number of risks due to the vagueness of the defined categories of illegal content and the guarantees of due process of law [74]. To date, Draft Laws No. 2693-d and No. 3196-d are pending in the Verkhovna Rada of Ukraine but have not been rejected, which creates a risk of their further adoption and implementation.

At the same time, website blocking was also applied on the basis of legal norms that do not allow the possibility of blocking. Thus, the Law of Ukraine "On Sanctions", which does not contain any provisions on the out-of-court blocking procedure that would oblige providers to restrict access to content, has repeatedly been criticized for not meeting the criteria of predictability and proportionality [75].

[73] *Draft Law: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243*

[74] *Digital Security Lab: Websites blocking, mass surveillance, elections with candidates filtering, or New powers of the SSU: https://dslua.org/publications/blokuvannia-saytiv-masove-stezhennia-filtruvannia-kandydativ-na-vyborakh-abo-novi-povnovazhennia-sbu/*

[75] *Digital Security Lab: Civil society organizations call on the President of Ukraine and NSDC to ensure legality and transparency in the application of sanctions against Internet resources: https://dslua.org/publications/hromads-ki-orhanizatsii-zaklykaiut-prezydenta-ukrainy-ta-rnbo-zabezpechyty-zakonnist-ta-prozorist-pry-zastosuvanni-sanktsiy-do-internet-resursiv/*

Another way of blocking Internet resources was invented by the courts and provides "intellectual property rights seizure that arises from users of the Internet when using websites". It also does not meet the criteria of predictability of the law and is not based on any existing norm of law [76].

Despite widespread criticism of the use of these mechanisms to block Internet resources, this practice continued in 2020. In particular, on May 15, 2020, sanctions against Russian social networks Mail.ru, Vkontakte, and Odnoklassniki were extended for 3 years, and for on 1 year – against Yandex [77]. Other Russian websites remain blocked by similar presidential decrees in 2018 [78] and 2019 [79].

Also in 2020, the practice of using the seizure of intellectual property rights as a measure of de facto blocking continued [80]. According to the data, published by the NCSRCI for operators and providers, four such decisions were made in 2020 [81]. At the same time, it is worth mentioning that the courts at the appellate level ruled that those practices were unlawful [82]. In particular, the Kyiv Court of Appeal, in its decision of 18 November 2020 on case 757/45 636/20-k, in which a provider challenged the event, stated that **"the seizure of intellectual property rights arising from the use of web resources by Internet users, is not provided by a specified norm of the Criminal Procedure Code of Ukraine"** [83]. One of the media resources whose website was blocked in 2019, Enigma, has submitted an application to the European Court of Human Rights, registered by a court in Strasbourg in July 2020 [84].

---

[76] The court's decision to block 17 sites hampers Ukrainian and international law – NGO Digital Security Lab: https://medium.com/@cyberlabukraine/%D1%83%D1%85%D0%B2%D0%B0%D0%BB%D0%B0-%D1%81%D1%83%D0%B4%D1%83-%D0%BF%D1%80%D0%BE-%D0%B1%D0%BB%D0%BE%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-19-%D1%81%D0%B0%D0%B9%D1%82%D1%96%D0%B2-%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%B5%D1%87%D0%B8%D1%82%D1%8C-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D0%BC%D1%83-%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D0%B4%D0%B0%D0%B2%D1%81%D1%82%D0%B2%D1%83-%D1%96-%D0%BC%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%BE%D0%BC%D1%83-%D0%BF%D1%80%D0%B0%D0%B2%D1%83-c19b111745ae

[77] Decree of the President of Ukraine No. 184/2020, 19.03. 2019 "On the decision of the National Security and Defense Council of Ukraine of March 19, 2019 "On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)": https://www.president.gov.ua/documents/1842020-33629

[78] Decree of the President of Ukraine No. 126/2018, 14.05. 2018 "On the decision of the National Security and Defense Council of Ukraine of May 2, 2018 "On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)": https://www.president.gov.ua/documents/1262018-24150

[79] Decree of the President of Ukraine No. 184/2020, 19.03. 2019 "On the decision of the National Security and Defense Council of Ukraine of March 19, 2019 "On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)": https://www.president.gov.ua/documents/822019-26290

[80] Decision of the Dnipro District Court of Kyiv on 30 January 2020 on the case No. 755/1439/16-к: https://reyestr.court.gov.ua/Review/87263489

[81] News. National Commission for the State Regulation of Communications and Informatization: https://nkrzi.gov.ua/index.php?r=site/index&pg=99&language=uk

[82] Decision of the Kyiv Court of Appeal on 10 September 2020 on the case No. 757/3623/20-к: https://reyestr.court.gov.ua/Review/91552942

[83] Decision of the Kyiv Court of Appeal on 18 November 2020 on the case No. 757/45636/20-к: https://reyestr.court.gov.ua/Review/93299672

[84] Human Rights Platform, 16.08.2020: https://www.facebook.com/ppl.org.ua/posts/865518630605983/

In Ukrainian practice of previous years, we may recall the attempts of the Security Service of Ukraine to request the Internet Association of Ukraine in order to restrict access to certain sites on the territory of Ukraine [85], as well as the work of the Working Group under the Ministry of Information Policy on compiling a list of websites containing information that has the characteristics of proliferation prohibited by the norms of Ukrainian law [86]. The latter was conducted by unclear criteria [87]; neither the Security Service of Ukraine nor the Ministry of Information Policy has any legislative authority to conduct such activities. Information from open sources indicates that this was not the case in 2020.

2.2.2. Blocking, filtering and take-down of digital content

At the same time, with the practice of Internet resources blocking, which is contrary to recognized human rights standards, Ukraine almost lacks mechanisms for blocking, filtering and take down of digital content. Also, unlike the blocking of Internet resources, there are no known instances of content being blocked, filtered or removed directly, and the mentioned-above Draft Law on media proposed the principle of technological neutrality in order to prohibit the advantage of one user over another, depending on the data to be provided, the content and the amount of data to be transferred, the end-user or on other grounds [88].

The only norm in the legislation is provided in Article 52-1 of the already mentioned Law of Ukraine "On Copyright and Related Rights" [89]. It only excludes access to illegal content and in an out-of-court procedure: a person who believes that his or her copyright has been infringed requires removing such content, and only in the absence of a response from the website owner applies to the hosting provider. There are 48 hours allowed for the removal of content unless the owner of the website can prove that he or she has the right to distribute the content. The procedure also provides the possibility of restoring access to content that is blocked. In general, this procedure is appropriate and complies with international human rights standards.

---

[85] *The SSU asks to block websites that promote the war (document). Livyj Bereg 4.08.2014: https://lb.ua/society/2014/08/04/275122_sbu_prosit_zablokirovat_sayti.html*

[86] *Ministry of Information Policy: a list of websites containing information that has the characteristics of proliferation prohibited by the norms of Ukrainian law: http://mip.gov.ua/documents/116.html*

[87] *The court denied the Coalition for Free Internet disclosing the criteria for the "illegality" of the websites. Dostup do pravdy, 17.10.2019: https://dostup.pravda.com.ua/news/publications/sud-vidmovyv-koalitsii-za-vilnyi-internet-u-rozkrytti-kryteriiv-nezakonnosti-saitiv-vid-mininformpolityky*

[88] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

[89] *Law of Ukraine "On Copyright and Related Rights": https://zakon.rada.gov.ua/laws/show/3792-12*

At the governmental level, a draft National Strategy for the Protection of Children in the Digital Environment until 2025 was discussed in 2020 [90]. It provides the introduction of filtering of content and Internet services at educational institutions and for the children's recreation centers in 2021-2024. A proposal to take into account the need for proportionality of such measures already in the text of the Strategy for Risk Reduction [91] had been rejected at the stage of public discussion, but could still be implemented. The draft strategy also introduces a regime for the removal and blocking of content that containing sexual exploitation and child abuse, whereby Internet service providers are obliged to remove such materials immediately after detection (if the web service placed within the territory of Ukraine), or, by a court decision, to block access to the Internet resource on the territory of Ukraine; and the law enforcement agencies of Ukraine should apply to representatives of the law enforcement agencies of the country, where such material is hosted, for its removal at the source. Such a mechanism could meet the standards of freedom of expression if adopted. However, as of the end of 2020, the draft strategy had not been adopted, so these provisions were not implemented and did not begin to be put into practice by the Ministry of Digital Transformation of Ukraine.

2.2.3. The right to appeal

Under the Constitution, everyone is guaranteed the right to appeal in court against the decisions, acts, or omissions of state or local authorities, their officials or employees [92]. The procedure for such an appeal is regulated by the Code of Administrative Proceeding of Ukraine, so that appeals against the blocking of Internet resources by decision or with the participation of a body of public authority may be lodged through the administrative court [93].

The situation with regard to appeals against blocking that has no basis in national legislation is more difficult. In the case of blocking, which takes place in the context of criminal and legal proceedings, the right of appeal must be exercised by the suspect, the accused, and third parties; cassation is not foreseen [94]. These third parties are service providers whose appeals overturned some blockages in 2020 [95].

[90] *Ministry of Digital Transformation: the message on public discussion of the draft National Strategy for the Protection of Children in the Digital Environment until 2025: https://thedigital.gov.ua/regulations/povidomlennya-pro-provedennya-publichnogo-gromadskogo-obgovorennya-proyektu-rozporyadzhennya-kabinetu-ministriv-ukrayini-pro-shvalennya-nacionalnoyi-strategiyi-z-zahistu-ditej-u-cifrovomu-seredovishi-na-period-do-2025-roku*

[91] *Digital Security Lab. The Protection of Children in the Digital Environment: what is strategized by the MDT: https://dslua.org/publications/zakhyst-ditey-u-tsyfrovomu-seredovyshchi-shcho-nastratehuvalo-mintsyfry/*

[92] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

[93] *Code of Administrative Procedure of Ukraine: https://zakon.rada.gov.ua/laws/show/2747-15*

[94] *Code of Criminal Procedure of Ukraine: https://zakon.rada.gov.ua/laws/show/4651-17*

[95] *Decision of the Kyiv Court of Appeal on 18 November 2020 on the case No. 757/45636/20-к: https://reyestr.court.gov.ua/Review/93299672*

On appeal of restrictions imposed in accordance with the Law of Ukraine "On Sanctions", its norms do not provide any possibility of appeal of the court decision [96]. At the same time, since sanctions are imposed by a decree of the President of Ukraine, an appeal may be lodged directly against the decree. Court practice is not uniform when it comes to users' possibility to appeal against blocking: the Supreme Court in the case on the legality of blocking social networks Vkontakte and Odnoklasniki stated that "rights and legitimate interests of users are not violated by Decree of the President of Ukraine No. 133 / 2017 from 15.05.201" [97]. In a later decision on the legality of the blocking of Yandex services, the Grand Chamber of the Supreme Court was not so categorical and recognized that "sanctions imposed by the Decree restrict the right of access, in particular, to certain Internet resources, and may be considered as interference with the freedom to receive and impart information and ideas without interference by public authorities and regardless of borders, guaranteed by Article 10 of the Convention". This may be an implicit recognition of the users' right to appeal blockages in accordance with the jurisprudence of the European Court of Human Rights in the Ahmet Yildirim v. Turkey case [98].

Despite the formal mechanisms to appeal against blocking, their effectiveness and the extent to which they can be considered effective remedies within the meaning of Article 13 of the European Convention on Human Rights remain questionable [99]. One reason may be a ground for blocking, as issues related to national security are often considered by the courts without proper analysis of the legal positions of the parties and have an inappropriate motivation. It is worth mentioning the general context of mistrust of the courts caused by corruption risks [100], including the District Administrative Court of Kyiv, which is competent to hear most cases of appeal against acts of the state authorities, located in the city of Kyiv [101].

2.2.4. Transparency of restrictions

The issue of transparency of restrictions on Internet content in Ukraine is controversial. On the one hand, the existing mechanisms for blocking Internet resources and removing content, which could be described as legitimate, do not contain clear requirements for informing the public about the blocking of resources. The court decision is notified to the parties to the case and published in the Unified State Register of Court Decisions [102]. However, there is no unified catalog of blocked websites.

[96] *Law of Ukraine "On Sanction": https://zakon.rada.gov.ua/laws/show/1644-18*

[97] *Decision of the Supreme Court on 13 April 2018 on the case No. 800/198/17: https://reyestr.court.gov.ua/Review/73397535*

[98] *Ahmet Yildirim and Others v. Turkey App no 3111/10 (ECHR,18 December 2012): http://hudoc.echr.coe.int/eng?i=001-115705*

[99] *Convention for the Protection of Human Rights and Fundamental Freedoms: https://zakon.rada.gov.ua/laws/show/995_004*

[100] *76% of Ukrainians do not trust courts. ZMINA. 21.02.2020: https://zmina.info/news/76-ukrayinczіv-ne-doviryut-sudovij-systemi/*

[101] *Centre of Policy and Legal Reform. Reorganization of the Administrative Court of Kyiv as a matter of national security of Ukraine: https://pravo.org.ua/ua/news/judiciary/20874581-reorganizatsiya-administrativnogo-sudu-kieva--pitannya-natsionalnoyi-bezpeki-ukrayini*

[102] *Law of Ukraine "On Access to Court Decisions": https://zakon.rada.gov.ua/laws/show/3262-15*

If we consider other actions to block Internet resources, such as the sanctions and the use of criminal procedure mechanisms, the transparency of these restrictions is beyond doubt. Presidential decrees imposing sanctions were duly published on the official website [103]. NCSRCI has also published on its website the resume parts of court decisions on the seizure of intellectual property rights arising from the use of web resources by Internet users, in which the possibility of appealing against them has been noted [104].

Various transparency practices are introduced by Internet service providers. On the example of blocking of the Enigma website it can be seen that different providers provided different information on the main webpage – from notification "no connection to the site" to information about website blocking by the court decision and links to the above-mentioned presidential decrees [105]. The current legislation does not contain uniform requirements for such a message.

2.3. Freedom of online media

2.3.1. Freedom of activity

Online media in Ukraine does not have to obtain a special permit or license to carry out its activities online or blogging (except business registration if necessary).

The Draft Law of Ukraine No. 2693-d "On Media" proposes to introduce voluntary registration of online media as media subjects and to regulate their status [106].

According to the Draft Law, the features of online media are regular dissemination of information, using website or webpage on the platforms of general access to information (for example, YouTube channel) with individualized name, and editorial control.

[103] *Decree of the President of Ukraine No. 184/2020, 14.05. 2020 "On the decision of the National Security and Defense Council of Ukraine of May 14, 2020 "On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)" : https://www.president.gov.ua/documents/1842020-33629; the Decree of the President of Ukraine No. 126/2018, 14.05. 2018 "On the decision of the National Security and Defense Council of Ukraine of May 2, 2018 "On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)": https://www.president.gov.ua/documents/1262018-24150; the Decree of the President of Ukraine No. 184/2020, 19.03. 2019 "On the decision of the National Security and Defense Council of Ukraine of March 19, 2019 "On the application, abolition and amendment of personal special economic and other restrictive measures (sanctions)": https://www.president.gov.ua/documents/822019-26290.*

[104] *National Commission for the State Regulation of Communications and Informatization: To the attention of telecommunication operators and providers!: https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2000&language=uk; National Commission for the State Regulation of Communications and Informatization: To the attention of telecommunication operators and providers: https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1935&language=uk; National Commission for the State Regulation of Communications and Informatization: To the attention of telecommunication operators and providers! The information on the decision of the investigative judge of Pechersky District Court in Kyiv: https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1903&language=uk*

[105] *Unprecedented attacks on freedom of speech in Ukraine. Dozens of sites blocked. Enigma, 30.07. 2019: https://enigma.ua/articles/bezpretsedentniy-nastup-na-svobodu-slova-v-ukraini-zablokovano-desyatki-nezalezhnikh-saytiv*

[106] *Draft law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

TThis definition partly reflects the approach of the Council of Europe stated in Recommendation CM / Rec (2011) 7 on the new definition of media [107], but requires further clarification. According to the Draft Law, detailed criteria and procedures for classifying a resource as an online media must be developed by the regulatory body, that is, directly by representatives of the media and the National Council.

Online media registration can offer certain advantages to media actors and their journalists. In particular, Draft Law No. 2693-d provides that only registered media may receive state support, as well as enter in contracts on covering the activities of state and local authorities. Journalists of registered media are guaranteed accreditation with the authorities (it is prohibited to refuse the accreditation). In addition, registered online media are given the right to participate in the development of protection mechanisms, which includes not only participation in the development of rules and codes, but also additional guarantees in the cases of possible violations of the law – they can request expertise from the regulatory body.

At the same time, the lack of online media registration cannot be an obstacle to their activities.

2.3.2. Guarantees of journalistic activity.

The European Court of Human Rights, in its judgment in the Editorial Board of Pravoye Delo and Shtekel v. Ukraine [108] case as early as 2011, drew attention to the lack of adequate safeguards in national legislation for journalists who use information from the Internet resources (§ 66). In particular, the ECHR noted that Ukrainian legislation, in particular, the Law of Ukraine "On Print Media (Press) in Ukraine", grants journalists' immunity from civil liability for the reproduction of information published in the press. However, according to the position of national courts, such immunity of journalists does not extend to the reproduction of material from Internet sources that are not registered in accordance with the Law of Ukraine "On Print Media (Press) in Ukraine". In this connection, the ECHR noted that at that time there were no national regulations on the state registration of Internet publications and, as the Government claimed, the Law of Ukraine "On Print Media (Press) in Ukraine" and other normative acts, did not contain any provisions on the status of Internet publications or on the use of information obtained from the Internet.

[107] *Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media: https://www.osce.org/files/f/documents/1/f/101403.pdf*

[108] *Case of Editorial Board of Pravoye Delo and Shtekel v. Ukraine (Application No. 33014/05): https://zakon.rada.gov.ua/laws/show/974_807*

The ECHR stated that the Internet, as an information and communication tool, is very different from the print media, especially with regard to the ability to preserve and transmit information. A digital network serving billions of users worldwide is not and potentially will not be subject to the same regulation and controls. The risk of undermining the exercise of human rights and freedoms, in particular the right to respect for private life, posed by information and communication on the Internet, is clearly higher than that of the press. Thus, the approaches that govern the reproduction of print media information and Internet information may differ. The latter undoubtedly should be adjusted to the technology involved in order to protect and promote these rights and freedoms. However, taking into account the role played by the Internet in the professional activities of the media and its importance for the general exercise of the right to freedom of expression, the ECHR noted, that the lack of a sufficient legislative basis at the national level, which would allow journalists to use information obtained from the Internet without fear of sanctions, seriously prevents the press from playing its role as a "watchdog of the society".

In the view of the ECHR, the total exclusion of such information from the scope of application of the legislative guarantees of the freedom of journalists may in itself give rise to interference with the freedom of the press guaranteed by Article 10 of the Convention.

National legislation has not changed significantly since the ECHR decision. Most of the guarantees of journalism activity are still governed by the legislation on print and audiovisual media.

At the same time, a number of guarantees of freedom of speech are contained in the Law of Ukraine “On Information” and extend to any person exercising the right to information [109]. This applies in particular to the right of access and dissemination of information with restricted access, if such information is of public interest, exemption from liability for value judgments, etc. Moreover, the status of a journalist may be confirmed not only by a press card issued by the media concerned but also by a press credential issued by a professional or artistic union of journalists. In general, however, the application of audiovisual and print media safeguards to online media remains problematic.

The Draft Law No. 2693-d “On Media”, registered in July 2020, proposes to improve and bring into line with European standards the grounds for exempting journalists from liability for disseminating inaccurate or illegal information if they act in good faith and in accordance with ethical standards [110]. Such standards would apply to all types of media.

[109] *Law of Ukraine “On Information”: https://zakon.rada.gov.ua/laws/show/2657-12*

[110] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

2.3.3. Editorial independence

The Constitution of Ukraine and national legislation prohibit censorship and interference in the editorial policy of the media [111]. At the same time, journalists and media editorial staff are often subjected to pressure from individual current and former state officials.

In 2020, such pressure often took the form of lawsuits against the editorial offices of, inter alia, investigative journalism programs requiring the denial or removal of information and compensation of moral damages. In November 2020, human rights organizations issued a statement on threats to freedom of expression due to inconsistency of national jurisprudence with international human rights standards [112].

Human rights defenders have noted an increase in court decisions according to which investigative journalists are obliged to confute the information on evidence of investigative journalism. For example, in the cases against the team of journalists of the program "Our Money with Denys Bihus" on the claims of the subjects of their investigations – Sergii Semochko [113] and the Gladkowski family [114] — the court ordered to confute "value judgments' grounded on the testimony of witnesses and official documents, contrary to the practice of the European Court of Human Rights. The Court also prohibits [115] releasing the names of individuals involved in high-profile corruption-related criminal cases, despite the explicit provision of public interest law that prevails in such cases.

The statement also mentions the extrajudicial practice of websites and web resources blocking, in particular cases against the Enigma, informator.news, The Correspondent website and others and "the seizure of intellectual property rights by Internet users using web resources" [116].

---

[111] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

[112] *A number of court decisions threaten freedom of expression, human rights defenders say. The Institute of Mass Information, 19. 11. 2020: https://imi.org.ua/news/nyzka-sudovyh-rishen-nesut-zagrozu-svobodi-slova-pravozahysnyky-i36306*

[113] *Semochko could not explain either Russian passports or multimillion-dollar property - but he won the lawsuit, renouncing his relatives. Bihus.info, 12.11.2020: https://bihus.info/semochko-ne-zmig-sprostuvaty-ani-rosijski-pasporty-ani-bagatomiljonne-majno-ale-vygrav-sud-vidrikshys-vid-rodyny/*

[114] *Scandal with Gladkovsky and Ukroboronprom: the court called the investigation untrue. BBC, 8.07.2020: https://www.bbc.com/ukrainian/features-53341299*

[115] *Martynenko and Trukhanov Nameless: The Supreme Court opposes the dissemination of the names of individuals involved in high-profile cases. Anti-Corruption Action Center, 13.11.2019: https://antac.org.ua/news/bezimenni-martynenky-ta-trukhanovy-verkhovnyy-sud-proty-poshyrennia-imen-fihurantiv-rezonansnykh-sprav/*

[116] *The Court of Appeal upheld the blocking of 17 Ukrainian websites, which human rights defenders called unlawful. ZMINA, 25.11.2019: https://bihus.info/semochko-ne-zmig-sprostuvaty-ani-rosijski-pasporty-ani-bagatomiljonne-majno-ale-vygrav-sud-vidrikshys-vid-rodyny/*

The court does not explain what content on these web resources directly infringes "intellectual property rights", what property is involved and how it is linked with Internet users. This practice creates a situation of legal uncertainty, in which journalists are threatened with serious legal action, regardless of the legality of the information they disseminate and compliance with the law and professional ethics.

2.3.4. Protection against threats and pressure

Ukrainian media and journalists are often victims of cyberattacks and online threats. The investigation of such cases is largely protracted and ineffective, creating a climate of impunity and contributing to further violations.

The Institute of Mass Information recorded nine publicly reported cybercrimes in 2020. The most common were DDoS attacks (7) [117]. Cyberattacks have tested both regional and national media – RIA Melitopol, Politerno (Ternopil), Chetwerta wlada (Rivne) and Liga.net [118], as well as The Voice of the Carpathians (Zakarpatska Oblast) [119] and others.

Online and investigative journalists themselves are also often the targets of cyberattacks. The monitoring of cybersecurity incidents faced by Ukrainian journalists and social activists, carried out by the NGO Digital Security Lab, revealed more than 40 cyber attacks from January to June 2020 [120]. The most common types are phishing (33.3% of all cases), password resetting (16.6%), password reuse (13.3%), and text messages intercepting (6.6%) [121].

It should be noted that according to an anonymous poll [122], conducted by the Institute of Mass Information in 2020, 88 % of Ukrainian media workers faced Internet pressure and 87 % of those who have come across cyberbullying link it with their professional activities.

---

[117] *Iryna Zemlyana. Cybergross: How journalists are persecuted on the Internet. The Mass Media Institute, 25.02.2021: https://imi.org.ua/monitorings/kiberzhest-yak-zhurnalistiv-peresliduyut-v-interneti-i37803*

[118] *Freedom of speech barometer for October 2020. The Mass Media Institute: https://imi.org.ua/monitorings/barometr-svobody-slova-za-zhovten-2020-roku-i36006*

[119] *Zakarpattia information website was the target of DoS attack. The Mass Media Institute, 16.11.2020: https://imi.org.ua/news/zakarpatskyj-informatsijnyj-sajt-zaznav-ddos-ataky-i36222*

[120] *Digital Security Lab. Digital threats to civic activists and journalists: https://dslua.org/publications/tsyfrovi-zahrozy-dlia-hromads-kykh-aktyvistiv-ta-zhurnalistiv-cherven-2020/*

[121] *Mass Media Institute. The most common digital attacks on journalists in 2020: https://imi.org.ua/monitorings/najposhyrenishi-tsyfrovi-ataky-na-zhurnalistiv-u-2020-i36844*

[122] *The vast majority of Ukrainian journalists have experienced cyberbullying – IMI research: https://imi.org.ua/news/perevazhna-bil-shist-ukrains-kykh-zhurnalistiv-stykalysia-z-kiberbulinhom-doslidzhennia-imi-i29180*

Threats and cyberbullying most often took the form of bullying on social networks [123], and the dissemination of offensive and sexist comments [124].

In October 2020, journalist Lyubov Velychko made a public appeal to the National Police about the threats she had begun to receive following an investigation into illegal casinos linked to the company of the wife of the Deputy Chief of Investigation Department of the National Police, which was published in online media [125]. In November 2020, a lawsuit was also filed against the journalist for protection of honor, dignity and business reputation, demanding refutation of incorrect information and 1 million hryvnias compensation of moral damages [126]. Previously, on the threat to the journalist Lyubov Velychko, which she started to receive after the release of his investigation into Russian Telegram channels, published in the online edition of Texty, a criminal proceeding was opened, on which the investigation is continuing [127].

At the same time, according to the data of the Institute of Mass Information, in 2020 only nine criminal proceedings on the indictment were transferred to the courts: six under Article 171 of the Criminal Code of Ukraine ("Obstruction of the legal professional activity of journalists") and three under Article 345-1 CCU ("Threat or violence against a journalist"). According to the register of court decisions, in 2020, Ukrainian courts had handed down only four sentences for obstruction: three convictions and one acquittal. However, only one verdict related to events that occurred in 2020, all the others related to previous years. There only two verdicts in the register of court decisions are under Article 345-1 of the Criminal Code. However, none of these sentences relate to the events of 2020 [128].

[123] *In Zaporizhia, a journalist gets bullied on Facebook for news of the coronavirus. The Mass Media Institute, 10. 11. 2020: https://imi.org.ua/news/u-zaporizhzhi-zhurnalista-tskuyut-u-fejsbutsi-za-novyny-pro-koronavirus-i36114*

[124] *The reporter of 061.ua became an object of cyberbullying. The Mass Media Institute, 30.10. 2020: https://imi.org.ua/news/zhurnalistka-sajtu-061-ua-stala-ob-yektom-kiberbulingu-i35959*

[125] *Journalist Lyubov Velychko reported receiving threats after investigating illegal casinos. The Mass Media Institute, 28.10.2020: https://imi.org.ua/news/zhurnalistka-lyubov-velychko-povidomyla-shho-otrymuye-pogrozy-pislya-rozsliduvannya-pro-nelegalni-i35903*

[126] *The court set 9 February as the date for the hearing of the 1 million claim of Alyona Shevtsova against the journalist Velychko. The Mass Media Institute, 23.12.2020: https://imi.org.ua/news/sud-pryznachyv-na-9-lyutogo-rozglyad-spravy-za-pozovom-alony-shevtsovoyi-na-1-mln-proty-i36839*

[127] *Ministry of Internal Affairs reported that they were looking for a person who threatened the journalist Lyubov Velychko. The Mass Media Institute, 28.09.2020: https://imi.org.ua/news/u-mvs-povidomyly-shho-shukayut-osobu-yaka-pogrozhuvala-zhurnalisttsi-lyubovi-velychko-i35202*

[128] *Ali Safarov. Threats and violence against journalists: what punishment is given to the attackers. 5.11.2020: https://imi.org.ua/monitorings/pogrozy-i-nasyllya-shhodo-zhurnalistiv-yake-pokarannya-otrymuyut-napadnyky-i36038*

2.4. Legality, legitimacy and the need for restrictions in a democratic society

2.4.1. General principles of restrictions

Article 34 of the Constitution guarantees everyone the right to freedom of thought and speech, the freedom to express his or her views and beliefs and the right to collect, store, use and disseminate information by oral, written, or other means at his discretion [129]. These safeguards apply to both the exercise of freedom of speech in the physical world and the online environment.

The exercise of freedom of expression may, however, be restricted by law for the protection of national security, territorial integrity or public order, to prevent disorder or crime, to protect public health, the reputation or rights of others, to prevent the disclosure of information received in confidence, or to ensure the credibility and impartiality of justice.

The Constitution does not refer directly to the test of the necessity of such a restriction in a democratic society. However, such a requirement is mandatory under the Law of Ukraine "On the Implementation of Judgments and the Practice of the European Court of Human Rights", Article 17 of which defines that the courts obliged to apply the Convention for the Protection of Human Rights and Fundamental Freedoms and the practice of the ECHR as a source of law [130].

Current legislation does not specifically prohibit the exercise of freedom of expression online. The acquisition and dissemination of information on the Internet may be subject to general restrictions aimed to protect national security, the rights of others and other legitimate interests defined by the Constitution of Ukraine.

2.4.2. Freedom of expression and protection of national security, territorial integrity, public safety, prevention of disclosure of confidential information

Protection of national security, territorial integrity, public safety, as well as the prevention of disorder or crime is legitimate aims of restricting freedom of speech under the requirements of Article 10 of the European Convention on Human Rights [131] and Article 34 of the Constitution of Ukraine [132]. At the same time, it is worth mentioning that current Ukrainian legislation contains no specific rules concerning restrictions on the dissemination of information for the various entities exercising their right to freedom of expression online.

[129] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

[130] *Law of Ukraine "On the Implementation of Judgments and the Practice of the European Court of Human Rights": https://zakon.rada.gov.ua/laws/show/3477-15*

[131] *The Convention for the Protection of Human Rights and Fundamental Freedoms: https://zakon.rada.gov.ua/laws/show/995_004*

[132] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

General rule of the Law of Ukraine "On Information", containing the prohibition of spreading calls for overthrowing the constitutional order, violation of the territorial integrity of Ukraine, propaganda of war, violence, cruelty, incitement to inter-ethnic, racial, religious hatred, the commission of terrorist acts and attacks on human rights and freedoms [133], do not contain accountability mechanisms for such violations, although the Law reflects the state's obligation to protect the public interest. The same is true of the Law of Ukraine "On Information Agencies" [134], which, considering the absence of regulation of online media in Ukraine, applies to a significant number of online media registered as information agencies, though there no implementation mechanisms as well.

In such circumstances, attention is drawn to the provisions of the Criminal Code of Ukraine [135], that may be applied to persons who disseminate certain information, in particular through the Internet. The relevant rules and sanctions for violations are:

- **Art 109.** Public appeals to violent change or overthrow of the constitutional order of take-over of government, and also dissemination of materials with any appeals to commit any such actions, – shall be punishable by restraint of liberty for a term up to three years, or imprisonment for the same term. Any such action, if committed by means of mass media, – shall be punishable by restraint of liberty for a term up to five years, or imprisonment for the same term;
- **Art 110.** Willful actions committed to change the territorial boundaries or national borders of Ukraine in violation of the order provided for in the Constitution of Ukraine (254к/96-ВР), and also public appeals or distribution of materials with appeals to commit any such actions, – shall be punishable by restraint of liberty for a term up to three years, or imprisonment for the same term. Any such actions, if they caused the killing of people or any other grave consequences, – shall be punishable by imprisonment for a term of seven to twelve years;
- **Art 161.** Willful actions inciting national, racial or religious enmity and hatred, the humiliation of national honor and dignity, or the insult of citizens' feelings in respect to their religious convictions, and also any direct or indirect restriction of rights, or granting direct or indirect privileges to citizens based on race, the color of skin, political, religious and other convictions, sex, ethnic and social origin, property status, place of residence, linguistic or other characteristics, – shall be punishable by restraint of liberty for a term up to five years. The same actions accompanied with violence, – shall be punishable by imprisonment for a term of seven years; if they have serious consequences, – shall be punishable by imprisonment for a term up to 8 years);
- **Art 258-2.** Public incitement to commit a terrorist act, – shall be punishable by restraint of liberty for a term up to three years or deprivation of liberty for the same term. The same actions committed with the use of the media, – shall be punishable by restraint of liberty for a term up to four years, or imprisonment for a term up to five years;
- **Art 295.** Public calls to riotous damage, arson, destruction of property, taking control of buildings or constructions, forceful eviction of citizens, where these actions pose a threat to the public order, – shall be punishable by restraint of liberty for a term up to three years;

[133] *Law of Ukraine "On Information": https://zakon.rada.gov.ua/laws/show/2657-12*

[134] *Law of Ukraine "On Information Agencies": https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80*

[135] *Criminal Code of Ukraine: https://zakon.rada.gov.ua/rada/show/2341-14*

- **Article 436** Public calls to an aggressive war or an armed conflict, – shall be punishable by imprisonment for a term up to three years;
- **Art 436-1** Public use of symbols of communist and national socialist (Nazi) totalitarian regimes, – shall be punishable by imprisonment for a term up to five years. The same actions committed with the use of the media, – shall be punishable by restraint of liberty for a term up to four years, or imprisonment for a term up to ten years;
- **Art 442** Public calls to genocide, – shall be punishable by imprisonment for a term up to five years.

Most of these rules are clearly formulated and contain adequate sanctions, given the importance of the interest protected by the State through the application of these rules. An exception is the provision of Article 436-1 of the Criminal Code: in 2015, in its opinion, the Venice Commission acknowledged the redundancy of sanctions for expression of opinion that does not lead to violence [136]. Attempts to adopt this rule to the principles of proportionality have not been implemented by the previous Parliament [137]. The proportionality of the sanctions should, however, be determined on a case-by-case basis.

In 2020, according to the analysis of the Unified State Register of Court Decisions, 41 sentences were handed down under the above-mentioned Articles on the dissemination of information on the Internet. Of these, two were acquittals and only two were sentenced to imprisonment, one in absentia. This means that only one person was directly prosecuted. The reason for this was a public call on Facebook for the capture of the Chuhuiv City Council, other local councils, as well as encouragement to unite with the Russian Federation, for which the person was sentenced to one year of imprisonment [138]. In the light of the case-law of the European Court of Human Rights, namely the Smajic v. Bosnia and Herzegovina case [139], such punishment could be considered proportionate.

From a statistical point of view, it can be concluded that, in general, the application of the relevant provisions of the Criminal Code does not create excessive restrictions for free discussions in the digital space. Although the absence of those who are punished for abusing the right to freedom of expression on the Internet is a positive factor, we should be addressing the negative trends in the case law under the relevant criminal law rules first outlined in the 2019 Human Rights Platform study [140].

[136] *Venice Commission. Joint Interim Opinion on the Law of Ukraine on the condemnation of the communist and national socialist (Nazi) regimes, and prohibition of propaganda of their symbols. 18 December 2015: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)041-e*

[137] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59178*

[138] *Decision of Derhachivskyi District Court of the Kharkiv Region of 18 June 2020 in the case No. 619/946/20: https://opendatabot.ua/court/89903668-9661b19343cfe620a3e58db3cec17b78*

[139] *Smajic v. Bosnia and Herzegovina (dec) App no 48657/17 (ECtHR, 16 January 2018): http://hudoc.echr.coe.int/eng?i=001-180956*

[140] *Opryshko L., Volodovska V., Dvorovyi M. M. Freedom of expression on the Internet: legislative initiatives and practice in criminal cases in Ukraine in 2014 - 2018: https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf*

The Article of the CCU	The number of convictions (here and hereinafter – the totality of crimes)	The number of plea agreements	The number of other cases of release from serving a sentence	The number of imprisonments	The verdicts of acquittal
109	14 (4)	12 (4)	1	1	-
110	24 (4)	17 (3)	7 (1)	-	2
161	1 (1)	1 (1)	-	-	-
258-2	-	-	-	-	-
295	-	-	-	-	-
436	2 (1)	-	1 (1)	1 (in absentia)	-
436-1	3 (1)	2	1 (1)	-	-
442	-	-	-	-	-

In particular, courts still refuse to analyze the statements that are the subject of consideration, often grounding their arguments on duplicating the conclusions of experts. A good example of the opposite approach is the decision of the Oktiabrski District Court in Poltava of August 7, 2020, where the analysis of the content of the comments led to the acquittal because "statements incriminated to PERSON_1 do not contain factual data, but are personal judgments and opinions expressed satirically, using linguistic means, concerning events taking place in his home state, of which this person is a citizen" [141].

Courts also do not analyze the extent to which the content for which a person is prosecuted has affected other network users who have had the chance to view it. In contrast to the cited study, in none of the analyzed sentences did the courts pay attention to the number of friends or subscribers in a particular social network, nor did they distinguish whether it was an original post or a repost. It is worth recalling that, according to the case-law of the European Court of Human Rights in Savva Terentyev v. Russia, **"thus the potential impact of a statement released online with a small readership is certainly not the same as that of a statement published on mainstream or highly visited web pages"** [142]. Such a situation with the inadequate motivation of court decisions, although not disproportionate, significantly limits the scope for appeals and does not meet the standards of the right to a fair trial guaranteed at the international legal and constitutional levels.

[141] *Decision of the Oktiabrskyi District Court of Poltava of 7 August 2020 in the case No. 554/1848/19: https://opendatabot.ua/court/90823974-c169b42f8e0543b35d612ce3782c77cd*

[142] *Savva Terentyev v. Russia App no 10692/09 (ECtHR, 28 August 2018): http://hudoc.echr.coe.int/eng?i=001-185307*

Finally, it is worth noting another aspect of the ambiguity of the application of these rules of criminal law. Articles 109 and 110 of the Criminal Code contain such an aggravating circumstance as the use of the media, which increases the potential punishment for spreading calls for a violent change or overthrow of the constitutional order or change the national borders of Ukraine. Some courts have argued that such a medium is the "audiovisual (electronic) mass medium – the World Wide Web." A clear example of the heterogeneity of this circumstance' interpretation is the decision of the Khmelnytskyi City District Court of Khmelnytskyi region, in which the person was prosecuted for two Facebook posts under Articles 109 and 110 of the Criminal Code: under Article 109 his actions were qualified with aggravating circumstances, under Article 110 – no [143]. Even though a plea agreement was approved, and therefore such a qualification had no actual impact on the convict, such an interpretation is potentially dangerous. It is worth recalling that the Internet is only a platform through which individuals exercise their right to freedom of expression, and therefore the dissemination of certain expressions through it can not be a basis for the application of stricter measures of responsibility.

During 2020, the People's Deputies of Ukraine also made few attempts to incorporate in law formulations of some offenses that would be aimed against the territorial integrity and national security – from the denial of the Holodomor and the genocide of Crimean Tatars [144] to public denial of occupation of Ukraine [145]. However, none of the bills were passed, and as of February 2021, they were withdrawn from consideration. Among the bills that can be adopted is the Draft Law on Amendments to Certain Legislative Acts of Ukraine on Prevention of Heroization of War Criminals and Legalization of Nazism (No. 2797) [146], which aims to detail the provisions of decommunization laws and extend them to Holocaust denial, but without changes of excessive sanctions. The Draft Law on Bringing the Provisions of Article 161 of the Criminal Code of Ukraine on Ensuring Equality of Citizens (No. 3111) [147] into line with the Constitution of Ukraine expands the list of grounds for incitement to hatred for which one can be prosecuted. Both bills generally comply with international human rights standards, given the prohibitions under Article 20 of the ICCPR [148] and the case-law of the European Court of Human Rights on Holocaust denial, which is not protected by the Convention [149].

---

[143] *Decision of the Khmelnytskyi City District Court of the Khmelnytskyi Region of November 6, 2020 in the case No. 686/22028/20: https://opendatabot.ua/court/92761683-b96a746f7c50c9b44cbfc950fb13722c*

[144] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69917*

[145] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69919*

[146] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=67974*

[147] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=68214*

[148] *ICPPR: https://zakon.rada.gov.ua/laws/show/995_043*

[149] *Williamson v Germany (dec) App no 64496/17 (ECtHR, 8 January 2019): http://hudoc.echr.coe.int/eng?i=001-189777*

It is worth mentioning the Draft Law on media, which contains a number of categories of prohibited content, which will apply to online media [150]. Failure to do so may result in a fine of between 1 and 5 the minimum wage, as well as a distribution ban. Among the new categories of content prohibited for distribution online, it is worth noting "unreliable materials on armed aggression and actions of the aggressor state (occupying state), its officials, persons and organizations controlled by the aggressor state (occupying state) if this results in incitement to hostility or hatred, or calls for a forcible change of territorial integrity or constitutional order."

As for interfering with the freedom of expression to prevent the dissemination of confidential information, prosecution for disseminating state secrets protected by law is foreseen by the Criminal Code of Ukraine and creates an opportunity for potentially illegal actions by those who want to silence critics on the pretext of state secret' protection. Thus, Article 232 of the Criminal Code ensures liability for disclosure of trade or banking secrets in the amount of up to 3 000 non-taxable minimum income, and Article 328 ensures liability for disclosure of state secrets (imprisonment for up to 5 years, and if disclosure caused serious consequences – up to 8 years) [151].

However, according to the Unified State Register of Court Decisions, no verdict was passed on the dissemination of such information on the Internet during 2020. The lack of interference with the freedom of expression on the Internet, based on the need to protect confidential information outside the context of denials of access to public information, is also recorded by the monitoring of violations of digital rights conducted by the Human Rights Platform [152].

2.4.3. Freedom of expression and protection of health or morals

Ukrainian legislation as a whole does not impose excessive restrictions on freedom of expression that would be in the interests of health or morals. At the same time, the application of existing restrictions in some cases may be contrary to the democratic society's principles of proportionality and necessity.

The Law of Ukraine "On Protection of Public Morality" [153] provides quite broad categories of content, the production and distribution of which is prohibited. In particular, these are products that:

- ***has a pornographic nature;***
- ***promotes war, national and religious enmity, violent change of the constitutional order or territorial integrity of Ukraine;***
- ***promotes fascism and neo-fascism;***

[150] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

[151] *Criminal Code of Ukraine: https://zakon.rada.gov.ua/rada/show/2341-14*

[152] *Human Rights Platform. Monitoring of Digital Rights: https://www.ppl.org.ua/monitoring/monitoring-cifrovix-prav*

[153] *Law of Ukraine "On Protection of Public Morality": https://zakon.rada.gov.ua/laws/show/1296-15*

- ***humiliates or insults a nation or individual on national grounds;***
- ***promotes blasphemy or disrespect for national and religious shrines;***
- ***humiliates the person, bullying of people with disabilities and mental disorders, the elderly;***
- ***promotes ignorance, disrespect for parents;***
- ***promotes drug addiction, substance abuse, alcoholism, smoking and other bad habits.***

At the same time, the law does not establish legal liability for disseminating such information online, except in the case of criminal offenses, in particular, child pornography.

In 2020, the protection of children's rights in the online environment has become one of the priorities of policy development by the Ministry of Digital Transformation of Ukraine. The Ministry developed a draft National Strategy for the Protection of Children in the Digital Environment until 2025 [154]. The Draft Law was publicly discussed but was not accepted by the government. At the same time, it became the basis for further work of the Ministry in early 2021 [155]. In general, the strategy provided a qualitative presentation of the issues related to the fight against sexual exploitation and child abuse online. However, there were comments regarding the out-of-court restriction of access to such content, as well as the lack of public involvement in the development of responsibility standards in this field [156].

In October 2020, the Ministry of Education and Science presented a glossary of terms on online security, which explained a number of terms in the field of child protection online (deepfake, victim-blaming, porn revenge, etc.) [157]. In continuation, the Ministry, with the help of partner organizations, conducted several studies on the criminalization of porn revenge [158] which may become the basis for the criminalization of such activities in the future.

---

[154] *Ministry of Digital Transformation. The MDT initiated public discussion of the draft National Strategy for the Protection of Children in the Digital Environment until 2025: https://thedigital.gov.ua/news/mintsifra-zaproshue-do-gromadskogo-obgovorennya-kontseptsii-ta-planu-zakhodiv-z-rozvitku-tsifrovikh-prav-ditey*

[155] *Ministry of Digital Transformation. The MDT invites to public discussion on conception and measures plan on development of children' digital rights: https://thedigital.gov.ua/news/mintsifra-zaproshue-do-gromadskogo-obgovorennya-kontseptsii-ta-planu-zakhodiv-z-rozvitku-tsifrovikh-prav-ditey*

[156] *Digital Security Lab. The Protection of Children in the Digital Environment: what is strategized by the MDT: https://dslua.org/publications/zakhyst-ditey-u-tsyfrovomu-seredovyshchi-shcho-nastratehuvalo-mintsyfry/*

[157] *Ministry of Digital Transformation. From deepfake to phishing. The MDT is launching an educational campaign to interpret the online security terms: https://dslua.org/publications/zakhyst-ditey-u-tsyfrovomu-seredovyshchi-shcho-nastratehuvalo-mintsyfry/*

[158] *Dvorovyi Maksym. Responsibility for porn revenge: international experience, the approach of technological companies and Ukrainian realities. The Digital Security Lab: https://dslua.org/publications/zakhyst-ditey-u-tsyfrovomu-seredovyshchi-shcho-nastratehuvalo-mintsyfry/*

In 2020, the Verkhovna Rada of Ukraine adopted in the first reading the Draft Law No. 3055 "On Amendments to Certain Legislative Acts of Ukraine Concerning the Implementation of the Council of Europe Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)" [159]. The Draft Law proposed to criminalize a number of actions related to sexual exploitation and violence online, including online child harassment, involvement of a child in acts of sexual nature and publicity of such acts, and so on [160].

In 2020, in connection with the spread of Covid-19 in Ukraine and the introduction of quarantine measures, the issue of finding a balance between the interests of freedom of expression and health care became relevant, in particular in connection with the publication on social networks of false information and theories conspiracies about the origin of the virus, morbidity statistics, treatments, etc. This, in turn, has led to an unprecedented number of cases of Internet users being held administratively liable for spreading false rumors that may cause panic among the population or public order violations (Article 173-1 of the Code of Ukraine on Administrative Offenses) [161].

Thus, in 2020, the Unified State Register of Court Decisions included more than 3,700 rulings in cases of spreading false rumors, the vast majority of which related to cases of dissemination of information online, in particular on the social network Facebook. Although the sanction for violation is insignificant – the commission may result in a fine of UAH 170 to 255 or correctional labor for up to one month with deduction of 20% of earnings – the practice of prosecuting for disseminating information through the Internet (in particular, on social networks), is of concern.

The analysis of the NGO "Human Rights Platform" [162] showed the inconsistency of court practice in such cases that may lead to unjustified restrictions on freedom of expression online. Human rights activists, in particular, noted such problems as insufficient court investigation of the case circumstances, inadequate assessment of the evidence of the falsity of the information disseminated, and the existence of a potential possibility of panic or disturbance of public order as a result of its dissemination; use of SSU' letters as evidence of a person's guilt; unequal assessment of the same circumstances by different courts, which ultimately leads to radically opposite conclusions and decisions in identical situations; finding a person guilty of committing an offense on the basis of improper or insufficient evidence; non-application of the standards of Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, etc.

[159] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68122*

[160] *Law was adopted on February 18, 2021: https://zakon.rada.gov.ua/laws/show/1256-IX#Text*

[161] *Code of Ukraine on Administrative Offenses: https://zakon.rada.gov.ua/rada/show/80731-10*

[162] *Jurisprudence on the dissemination of information on the Internet: trends and challenges in law enforcement/Burmahin O.O., Opryshko L.B. – Kyiv: NGO Human Rights Platform, 2020*

2.4.4. Freedom of expression and protection of the reputation or rights of others

Ukrainian legislation does not provide criminal liability for defamation. Initiatives, aimed at returning the criminalization of defamation, are submitted to the parliament from time to time [163], but in 2020 such bills were not registered.

In case of dissemination of unreliable information about a person or insulting judgments, a person may apply to the court to protect his or her honor, dignity or business reputation in civil proceedings, and entrepreneurs, in case of encroachment on their business reputation, – also in the manner prescribed by the Commercial Code of Ukraine.

To ensure the correct and unified application of legislation governing the protection of dignity and honor of individuals, as well as the business reputation of individuals and legal entities, in 2009, the Plenum of the Supreme Court of Ukraine has formulated clarifications that generally meet the requirements of the Convention on Human Rights and the Fundamental Freedoms and case law of the European Court of Human Rights [164]. However, the resolution does not take into account the specifics of disseminating information on the Internet.

An analysis of case law on the protection of honor, dignity and business reputation conducted by the NGO "Human Rights Platform" revealed a number of problems that arise in the application of the law by courts and can lead to unjustified restrictions on freedom of expression in the online environment.

In particular, the experts noted the spread of the practice of simultaneous application of the requirements for the refutation of untrue information and its removal. The lack of proper justification for both the combination of these methods and the proportionality of the use of such a remedy as removal, in general, is a matter of concern, as the removal of the entire publication may be excessive and lead to censorship [165].

[163] *Coalition for Free Internet requests the deputies to withdraw the draft law on the criminalization of defamationt: https://detector.media/infospace/article/142739/2018-11-21-koalitsiya-za-vilnyy-internet-prosyt-nardepiv-vidklykaty-zakonoproekt-pro-kryminalizatsiyu-naklepu/*

[164] *Order of the Plenum of the Supreme Court of Ukraine No. 1 on 27 February, 2009, "On jurisprudence on the protection of the honor and dignity of natural persons and the business reputation of natural and legal persons": https://zakon.rada.gov.ua/laws/show/v_001700-09*

[165] *Jurisprudence on the dissemination of information on the Internet: trends and challenges in law enforcement/Burmahin O.O., Opryshko L.B. – Kyiv: NGO Human Rights Platform, 2020. P. 25-26.*

Another controversial approach is the obligation of the defendant to publish the text of the court decision [166]. In some cases, this leads to the fact that rebuttal significantly exceeds relevant controversial information. In addition, the obligation to publish a photocopy of the court decision may lead to forced violation of the legal requirements on the protection of confidential personal information by the defendant, as the text of the court decision may contain personal data of the parties.

Another dangerous court approach is the obligation to publish the text of the rebuttal by placing it between the title and the first paragraph of the disputed publication. Experts concluded that this leads to unjustified interference with copyright – the court actually makes changes to the publication, distorting it, and thus violates the personal intangible rights of the author to preserve the integrity of the work, guaranteed by Article 14 of the Law of Ukraine "On Copyright and Related Rights" and other international legal acts [167].

It is also worth noting that the current civil legislation sets a reduced statute of limitations of one year for claims to refute untrue information published in the media. At the same time, the Civil Code of Ukraine does not contain any restrictions on filing claims for non-pecuniary damage caused by the dissemination of such information, which can be used by unscrupulous plaintiffs.

Filing lawsuits to protect honor, dignity and business reputation remains an instrument of pressure on journalists by current and former high-ranking officials [168].

Given the identified conflicts and shortcomings in court practice, it is appropriate to review the current legislation to more clearly regulate the protection of honor, dignity and reputation, while maintaining a balance on freedom of expression on the Internet. Some attempts in this direction were made in the Draft Law “On Media” № 2693-d, which was registered in the Verkhovna Rada of Ukraine on July 2, 2020, and is currently pending [169].

[166] *Jurisprudence on the dissemination of information on the Internet: trends and challenges in law enforcement /Burmahin O.O., Opryshko L.B. – Kyiv: NGO Human Rights Platform, 2020. P. 30*

[167] *Ibidem, p. 29*

[168] *See 2.3.3*

[169] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

In particular, the document proposes to regulate the procedure for consideration of applications for the right to reply or refute, in case of dissemination of untrue information about the person in the online media. The text of the rebuttal or reply shall be disseminated in the online media in a manner as close as possible to the dissemination of the information in respect of which the request for rebuttal or exercise of the right of reply was received (to the same extent, on the same web page or in the same section of the website, etc.). If the text of the rebuttal or reply cannot be placed on the same web page as the original publication, the online media entity should provide cross-references between the relevant publications and place a message next to the original text stating that the information in that publication has been refuted or has become the subject of the right of reply. The online media entity is obliged to review the application and notify the applicant of its decision immediately, but not later than five working days from the date of receipt of the application.

At the same time, the Draft Law defines several grounds on which the online media can reasonably refuse to disseminate refutations and replies. For example, if the information disseminated is an evaluative judgment or there is sufficient evidence that the information disseminated is true, it sufficiently and accurately reflects the facts in question; if the disseminated information is a literal reproduction of public speeches or messages, public information of state or local bodies, their officials and employees; if the disseminated information is a literal reproduction of materials distributed by other registered media or media for which there is no mandatory registration requirement; if there is information about the persons exercising editorial control, their location and current contacts or regarding such information; if the information disseminated contains a minor factual error which does not prejudice the rights and legitimate interests of the applicant.

To protect the rights of others, the Criminal Code of Ukraine provides liability for inciting national, racial, or religious hostility and hatred, humiliating national honor and dignity, or insulting the feelings of citizens due to their religious beliefs, as well as directly or indirectly restricting rights or establishing direct or indirect privileges of citizens on the grounds of race, political, religious and other beliefs, sex, disability, ethnic and social origin, property status, place of residence, language or other characteristics (Article 161 of the Criminal Code). Such actions may be punishable by up to three years' imprisonment and, in the case of serious consequences, it may be punished by imprisonment for a term up to eight years [170].

Criminal liability is also provided for violation of the secrecy of correspondence, telephone conversations, telegraph or other correspondence transmitted by means of communication or computer (Article 163 of the Criminal Code). Imprisonment for up to seven years may be applied if such actions are committed against statesmen or public figures, journalists, or if special means have been used to secretly remove information.

[170] *Criminal Code of Ukraine: https://zakon.rada.gov.ua/rada/show/2341-14*

The Criminal Code of Ukraine also provides criminal liability for the illegal collection, storage, use, destruction, dissemination of confidential personal information. If such actions have caused significant violence of the rights, freedoms and interests of the person protected by law, it may be punished by imprisonment for a term of up to five years.

However, the legal action under these Articles is solitary. Thus, in 2020, only 8 sentences were handed down, only one of which concerned the assessment and balancing of freedom of expression in the online environment and the protection of the rights of others. The Korostyshivskyi District Court of Zhytomyr Oblast found the person guilty of spreading discriminatory statements, as well as disseminating online posts calling for a violent change and overthrow of the constitutional order, and the seizure of state power [171]. At the same time, the prosecutor's office qualified the latter as committed repeatedly, with the use of the media (part three of Article 109 of the Criminal Code). As the court approved a plea agreement between the prosecutor and the accused, there is no assessment of whether those statements threaten legitimate interests and if the application of a 3-year prison sentence with a 1-year probationary period is necessary for a democratic society.

It is worth noting that in 2020 there has been a new dangerous court practice, which may lead to increased pressure on journalists due to abuse by those involved in their investigations and disclosing personal data of journalists and editorial staff.

Thus, in November 2019, Andrii Portnov [172] a former deputy and official of the Presidential Office of Viktor Yanukovych, posted in his Telegram channel personal data of drivers (passport data, home address, car numbers, etc.) of the film crew of the investigative journalism project "Schemes" in response to the journalistic investigation into Portnov's influence and possible links to the current government. The lawyers of the editorial office filed civil lawsuits in court demanding to stop the dissemination of personal data of drivers of the "Schemes" program. In August 2020, the car of Borys Mazur, one of the drivers of "Schemes", was set on fire.

On August 31, the judge of Kyiv's Pechersk District Court Svitlana Volkova has dismissed the privacy claim filed by Borys Mazur. Thus, his request to oblige former Deputy Chief of Staff Andrii Portnov to revoke his personal data from the public domain has been rejected. In addition to dismissing the lawsuit, the judge also decided to order 52,500 hryvnias of lawyers' fees of Portnov from Borys Mazur. In December 2020, this decision was upheld by the Kyiv City Court of Appeal [173].

[171] *Decision of the Korostyshivskyi District Court of Zhytomyr Oblast on 11 June 2020 in the case No. 935/1251/20: https://reyestr.court.gov.ua/Review/89742100*

[172] *Police investigate Portnov's reports about the Radio Svoboda journalists. Ukrainska Pravda, 7.11. 2019: https://www.pravda.com.ua/news/2019/11/7/7231236/*

[173] *Court of Appeal sided with Portnov, who disclosed the personal data of members of the "Schemes", editorial staff. Radio Svoboda, 14.12.2020: https://www.radiosvoboda.org/a/news-schemes-portnov-apeliatsiya/31000535.html*

The danger of this court decision is that the court recognized the admissibility of the dissemination of confidential personal data of any person, despite the requirements of the Constitution and laws of Ukraine. In addition, the obligation to reimburse a significant amount of the ex-official's legal protection costs can in practice have a "cooling effect" and lead to censorship, as it creates serious obstacles for journalists to go to court to protect their rights. At the time of writing, a cassation appeal was filed with the Supreme Court [174].

2.4.5. Freedom of expression and maintenance of the authority and impartiality of the court

Ukrainian legislation generally complies with European standards on grounds for restricting freedom of expression in the interests of protecting the authority and impartiality of the court. Article 6 of the Law of Ukraine "On the Judiciary and the Status of Judges" [175] stipulates that interference with the administration of justice, pressure on the court or judges, contempt of court or judges, collection, storage, use and dissemination of information in oral, in writing or any other way in order to discredit the court or to influence the impartiality of the court, appeals to non-enforcement of court decisions are prohibited and result in liability provided by law. The Criminal Code of Ukraine provides criminal liability only if the interference in the activities of a judge is carried out to prevent him or her from performing his official duties or to obtain an unjust decision.

Thus, the law does not threaten public debate over high-profile court cases and the functioning of the judiciary as such and is not used to prosecute critics of the court.

At the same time, it should be noted that the openness of the judiciary is an important element of the right of citizens to receive socially necessary information. Given this, Ukrainian legislation obliges the State Judicial Administration of Ukraine, the High Qualifications Commission of Judges of Ukraine and the High Council of Justice to publish public information in the field of justice and the judiciary in an open data format, ie in a format that allows its automated electronic processing and free access to it, as well as its further use for any purpose. According to the Resolution of the Cabinet of Ministers of Ukraine No. 835 of October 21, 2015, with the following amendments [176] the relevant bodies must publish data sets that are mandatory for all and specified for each body.

---

[174] *Defenders of the "Schemes"' employee applied to the Supreme Court. Radio Svoboda, 15.01.2020: https://www.radiosvoboda.org/a/new-schemes-portnov-verkhovny-sud/31047463.html*

[175] *Law of Ukraine "On the Judiciary and the Status of Judges": https://zakon.rada.gov.ua/laws/show/1402-19*

[176] *Resolution of the Cabinet of Ministers of Ukraine No. 835 of October 21, 2015 "About approval of the Regulations on data sets which are subject to promulgation in the form of open data": https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF*

At the same time, according to the analytical report of the DEJURE Foundation [177] only the State Judicial Administration somehow published all specified data sets, while the High Qualifications Commission of Judges, in violation of the statutory deadline, did not publish its own decisions and the Register of Declarations in Family Connections and Integrity, and the High Council of Justice did not publish its own decisions, as well as any other set of mandatory information in an open data format, except for reports on requests for information.

In the context of the ongoing judicial reform in Ukraine, the openness of the judiciary is an important condition for citizens to receive reliable and objective information about the administration of justice and to build public confidence in judges. In view of this, the full realization of the rights of citizens to freedom of expression requires proper compliance by courts and other bodies in the field of justice with the requirements for access to public information.

[177] *Khymchuk A. V. The open data of judiciary: analytical report. — Kyiv, 2020. — P. 22.: https://dejure.foundation/library/vidkryti-dani-sudovoi-vlady*

RECOMMENDATIONS TO SECTION 2:

2.1. Internet connection

THE CABINET OF MINISTERS OF UKRAINE AND THE MINISTRY OF DIGITAL TRANSFORMATION:

— to ensure the development and adoption of bylaws to implement the provisions of the new Law "On Electronic Communications" to ensure access to the Internet, including vulnerable populations, since its entry into force;

THE CABINET OF MINISTERS OF UKRAINE:

— to ensure the adoption of the National Strategy for the Development of Broadband Internet Access and the beginning of the implementation of its provisions, in particular regarding tenders for the deployment of the 5G network;

NATIONAL COMMISSION FOR STATE REGULATION OF COMMUNICATIONS AND INFORMATIZATION:

— to publish open data on the coverage of the territory of Ukraine by Internet access

THE MINISTRY OF JUSTICE OF UKRAINE:

— to agree on the Procedure for providing imprisoned persons with access to the global network with guarantees of secrecy of correspondence between imprisoned persons and their defenders.

2.2. Freedom of thought, the right to receive and disseminate information

SUBJECTS OF THE LEGISLATIVE INITIATIVE:

– to refrain from developing legislative initiatives that would create threats of extrajudicial blocking of access to Internet resources if the content, on the basis of which it is proposed to block the resource, is not obviously illegal (child pornography, etc.);

– to propose amendments to the Law of Ukraine "On Sanctions", which would harmonize the practice of their application to Internet resources with the requirements of legal certainty;

– when developing legislative initiatives aimed at restricting harmful content on the Internet, take into account the case-law of the European Court of Human Rights, providing a separate assessment of the need to restrict access to content and the Internet in general, and focusing on the need to block illegal content;

– to provide legal guarantees for the effective consideration of cases of blocking Internet resources and restricting access to content by a court decision;

COMMITTEE OF THE VERKHOVNA RADA OF UKRAINE ON HUMANITARIAN AND INFORMATION POLICY:

— to finalize the provisions of the Draft Law of Ukraine "On Media" No. 2693-d before adopting them as a basis and in general on restricting access to online media taking into account the case-law of the European Court of Human Rights;

COMMITTEE OF THE VERKHOVNA RADA OF UKRAINE ON NATIONAL SECURITY, DEFENSE AND INTELLIGENCE:

— to finalize the Draft Law On Amendments to the Law of Ukraine "On the Security Service of Ukraine" to improve the organizational and legal framework of the Security Service of Ukraine No. 3196-d and bring requirements for possible restrictions on access to websites that threaten the interests of national security, in line with European standards;

MINISTRY OF DIGITAL TRANSFORMATION :

— to take into account international standards and the case-law of the European Court of Human Rights on restricting access to content on the Internet when developing and implementing initiatives in the field of child protection in the online environment;

THE PRESIDENT OF UKRAINE, THE NATIONAL SECURITY AND DEFENSE COUNCIL OF UKRAINE :

— to bring the decrees of the President of Ukraine and the practice of sanctions in line with the Constitution and international obligations of Ukraine, in particular, the practice of restricting access to information resources specified by decrees of the President of Ukraine;

THE SUPREME COURT:

— to generalize the case law on the seizure of intellectual property rights that arise from using websites by Internet users, to restrict access to Internet resources, and to provide appropriate explanations to the courts on the consideration of such applications, taking into account the systematic interpretation of national legislation and practice of the European Court of Human Rights.

2.3. Freedom of online media [178]

COMMITTEE OF THE VERKHOVNA RADA OF UKRAINE ON HUMANITARIAN AND INFORMATION POLICY:

— to finalize the Draft Law of Ukraine "On Media" № 2693-d regarding the determination of the legal status of online media and online media journalists, to guarantee voluntary registration of online media and eliminate excessive restrictions on content and other requirements for journalistic activities, extending guarantees of freedom of journalistic activity to online media journalists;

VERKHOVNA RADA COMMITTEE ON FREEDOM OF SPEECH:

— with the participation of interested bodies of the Verkhovna Rada of Ukraine and civil society institutions to ensure the preparation and consideration of legislative initiatives aimed at improving the protection of legitimate professional activities of journalists and other media participants, as well as strengthening criminal liability for offenses against journalists;

[178] *Several number of recommendations on the protection of journalists' activities in Ukraine were formulated on the results of the parliamentary hearings on the topic "Safety of journalists' activities in Ukraine: status, challenges and responses". It is worth emphasizing the importance of implementing these recommendations: https://zakon.rada.gov.ua/laws/show/456-IX#Text*

OFFICE OF THE PROSECUTOR GENERAL:

– to strengthen control on compliance with the law during the pre-trial investigation in the form of procedural guidance for the pre-trial investigation of crimes committed against journalists, media workers and others persons, exercising their rights for freedom of expression; on adding information on criminal offenses into the Unified Register of Pre-trial Investigations in a timely manner; on correctness of legal qualification, completeness (thoroughness) of pre-trial investigation, including investigation of motives and presence or absence of connection between illegal act and creation of obstacles to realization of right to freedom of speech; on terms of pre-trial investigation and ensuring the rights of victims during the pre-trial investigation;

– to include in the obligatory program of training, retraining (advanced training) of prosecutors and investigators a special course on protection of professional activity of journalists and other media participants, effective investigation of crimes committed against such persons, taking into account European human rights standards, and ensure its further implementation;

THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE,
THE OFFICE OF THE PROSECUTOR GENERAL AND / OR THE STATE BUREAU OF INVESTIGATION:

– to agree on methodological recommendations for the investigation of crimes against freedom of speech;

– to ensure the publication of quarterly reports on the results of the investigation of crimes committed against journalists;

– during the investigation of crimes committed against journalists, other media workers, as well as other persons in connection with their exercise of the right to freedom of speech, to ensure timely entry of information on such criminal offenses in the Unified Register of Pre-trial Investigations, proper legal qualification of such acts, completeness (thoroughness) of pre-trial investigation, including investigation of the motives of the crime and presence or absence of a connection between the illegal act and creating obstacles to the exercise of the right to freedom of speech, observance of reasonable pre-trial investigation and ensuring the rights of victims during pre-trial investigation.

2.4. Legality, legitimacy and the necessity of restrictions in a democratic society

SUBJECTS OF THE LEGISLATIVE INITIATIVE:

– to ensure the observance of international human rights standards in the development and consideration of any legislative (and other regulatory) initiatives aimed at restricting or stopping the dissemination of information that threatens the interests of national security. In particular, to formulate categories of prohibited content in order to avoid abuses of prosecution for violation and unjustified interference with the freedom of expression;

– to review the rules of criminal law and decriminalize or exclude imprisonment for certain types of statements that do not contain calls for violence, such as the use of certain symbols as propaganda for totalitarian regimes. Only actions that pose a real threat to society should entail criminal liability, which should be proportional to the crime committed. Nonviolent acts of freedom of expression should not be punishable by imprisonment;

THE CABINET OF MINISTERS OF UKRAINE:

— to adopt an updated concept or strategy for the protection of children in the online environment and ensure its implementation, while respecting the guarantees of freedom of expression;

THE SUPREME COURT:

– to ensure the unification of case law in cases of administrative violations under Article 173-1 of the Code of Administrative Offenses on the dissemination of rumors, in particular on the proper assessment of the content of publications, the context of its dissemination and purpose, assessment of the evidence base for inaccuracy of information violation of public order), as well as the application of the case law of the European Court of Human Rights in order to establish a balance between the right of a person to disseminate information and the protection of the legitimate interests of health or public order;

– to update the clarification on the application of legislation in the field of protection of honor, dignity and business reputation, paying attention to the peculiarities of the application of civil legislation in order to protect personal non-property rights in the online environment;

– to promote the unification of jurisprudence in criminal proceedings for disseminating information that threatens national security interests on the Internet and its compliance with international standards in the field of freedom of expression, in particular through proper analysis of the content, its context and purpose of the disseminated publication, careful assessment of the relevance and admissibility of evidence, ensuring the proportionality of the sentence, etc.;

THE STATE JUDICIAL ADMINISTRATION OF UKRAINE,
THE HIGH QUALIFICATIONS COMMISSION OF UKRAINE,
THE HIGH COUNCIL OF JUSTICE:

– to disclose public information in the form of open data in full and in timely manner, in accordance with the list defined by law, to ensure proper openness and transparency of the judiciary in Ukraine.

SECTION 3.
Freedom of peaceful assembly and association

3.1. Freedom to use online platforms

Freedom of peaceful assembly and association and the use of Internet platforms to exercise this right are guaranteed by the Constitution of Ukraine and its Articles 34, 36 and 39 [179]. These rights, however, provide only general limitations. Since the Constitution had been adopted in 1996, when the development of the Internet in Ukraine had just begun, it is difficult to expect that the Constitution would have enshrined detailed provisions on digital rights. The chapter on human rights has not been amended since then.

The Constitution lays down a notification procedure for peaceful assemblies: in order to meet, citizens must notify the executive or local authorities in advance. At least until the end of the Dignity Revolution there was a practice of applying the already Soviet legislation, which provided a procedure for authorizing the holding of such meetings [180].

In 2013, the European Court of Human Rights, however, had recognized the application of the relevant norms as contrary to Article 11 of the European Convention on Human Rights [181], and, in 2016, the Constitutional Court had ruled them unconstitutional [182]. A specific law on regulating the freedom of peaceful assembly has not been adopted in Ukraine.

3.2. Restrictions on freedom of assembly and association on the Internet.

There is no application of the direct constitutional provision on the necessity to notify about peaceful measures to restrict this right in Ukraine. Furthermore, such restriction may be applied only by court order in accordance with the law and only in the interests of national security and public order, to prevent disorder or crime, to protect public health or the rights and freedoms of others [183].

---

[179] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

[180] *Decree of the Presidium of the Supreme Soviet of the USSR "On the procedure for organizing and conducting meetings, street marches and demonstrations in the USSR": https://zakon.rada.gov.ua/laws/show/v9306400-88*

[181] *Case of Verentsov v. Ukraine (No. 20372/11): https://zakon.rada.gov.ua/laws/show/974_945*

[182] *Decision of the Constitutional Court of Ukraine Np. 6-rp / 2016 in the case on the constitutional petition of the Ukrainian Parliament Commissioner for Human Rights on the constitutionality of the provisions of part five of Article 21 Law of Ukraine "On Freedom of Conscience and Religious Organizations" (the reasons for notification on public worship, religious rites, ceremonies and processions), September 8, 2016: https://zakon.rada.gov.ua/laws/show/v006p710-16*

[183] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

However, there are no other laws that restrict this right. There are also no specific actions provided for blocking of Internet platforms in the context of the right to freedom of assembly, as described in section 2.2 of this report. While it is true that the unlawful blocking Russian social networks has a direct negative impact on the exercise by Ukrainian Internet users of the right to freedom of association on the appropriate platforms.

There is also no attempt to legislate regulation in this field. The only Draft Law to regulate the freedom of peaceful assembly was submitted by the People's Deputies as early as August 2019 – and the Draft Law has withdrawn a week later [184]. However, it did not contain any threats to the exercise of this right on the Internet.

Special mention should be made of restrictions on freedom of assembly imposed by Internet platforms, which apply this restriction to public groups that violate community standards. In the Ukrainian context, it is worth mentioning the removal of several public groups on Facebook in February 2020 due to their spread of misinformation about the war in Eastern Ukraine [185]. Such a measure should be considered appropriate and proportionate.

RECOMMENDATIONS TO SECTION 3:

LAW ENFORCEMENT AGENCIES:

— do not apply existing legislation to restrict freedom of peaceful assembly and association on the Internet;

THE SUBJECTS OF THE LEGISLATIVE INITIATIVE:

— to refrain from legislative initiatives that would make it possible to restrict freedom of peaceful assembly and association on the Internet, including by blocking online platforms, as well as criminalizing access to restricted resources.

[184] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66509*

[185] *Anna Zhurba. Facebook has blocked the accounts the Intelligence Agency used to disseminate misinformation about the war in Eastern Ukraine. Zahid.net, 12.02.2020: https://zaxid.net/facebook_zablokuvav_akaunti_yakimi_rozvidka_rosiyi_poshiryuvala_dezinformatsiyu_pro_ukrayinu_n1497610*

SECTION 4. The right to respect for private and family life

4.1. Protection of personal data

The Law of Ukraine "On Protection of Personal Data" [186] entered into force on 1 January 2011. This Law systematized approaches to the definition and key principles of the processing of personal data in Ukraine for the first time and was intended to bring national legislation in line with the requirements of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [187], Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [188] Directive 97/66 / EC of the European Parliament [189] and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [190].

The current version of the Law implements the key requirements and principles for the processing of personal data defined by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. At the same time, the Convention itself was substantially modernized in May 2018 in accordance with Protocol CM (2018) 2 [191]. Ukraine has not yet acceded to the Protocol but has committed bringing personal data protection legislation in line with EU requirements. Thus, according to paragraph 11 of the Action Plan on Implementation of the Association Agreement with the EU, approved by Resolution of the Cabinet of Ministers of Ukraine No.1106 of 25 October 2017 [192], provides updating of legislation on the protection of personal data to bring it in line with the General Regulations on Data Protection, entered into force on 25 May 2018 [193].

Work on the updated version of the Law of Ukraine "On Personal Data Protection" began in 2018 and continued in 2020. A working group on the reforming of legislation on personal data was established jointly by the Verkhovna Rada Committee on Digital Transformation and the Verkhovna Rada Committee on Human Rights, de-occupation and reintegration of temporarily occupied territories in the Donetsk, Luhansk regions and the Autonomous Republic of Crimea, the city of Sevastopol, national minorities and interethnic relations.

[186] *Law of Ukraine "On Protection of Personal Data" : https://zakon.rada.gov.ua/laws/show/2297-17*

[187] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data: https://zakon.rada.gov.ua/laws/show/994_326*

[188] *Directive 95/46/EC: https://zakon.rada.gov.ua/laws/show/994_242*

[189] *Directive 97/66/EC : https://zakon.rada.gov.ua/laws/show/994_243*

[190] *Explanatory Note to the Draft Law "On the protection of personal data": http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2273&skl=7*

[191] *Protocol CM (2018)2: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108*

[192] *Resolution of the Cabinet of Ministers of Ukraine "About agreement performance about association between Ukraine, on the one hand, and the European Union, European Atomic Energy Community and their state members, on the other hand: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF*

[193] *General Data Protection Regulation://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf*

The working group is composed of People's Deputies and their assistants, representatives of the Ministry of Digital Transformation of Ukraine, representatives of the Secretariat of the Ukrainian Parliament Commissioner for Human Rights, experts of international organizations, lawyers, civil society representatives.

In November 2020, Nataša Pirc Musar and Dijana Šinkūnienė, experts of the project "European Union and the Council of Europe working together to strengthen the Ombudsperson's capacity to protect human rights" presented the legal review of the Draft Law of Ukraine "On Personal Data Protection". They indicated the necessity to include in the bill, inter alia: to set up the obligation for the state institutions to include into the pieces of legislation regulating personal data processing the purpose of the processing at stake and, as the case may be, other related information; to foresee procedure of the data protection impact assessment in the course of adoption of the legal act; to lay down the main principles relating to personal data processing by public authorities; to foresee provisions of the establishment of the independent supervisory authority with regard to proper enforcement of the data protection legislation. The experts paid special attention to the necessity of update provisions on processing of personal data for journalistic or creative activities [194].

4.1.2. Principles of personal data processing

The Law of Ukraine "On the Protection of Personal Data" [195] defines the key principles of the processing of personal data, which meet the requirements of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data but has not yet specified these requirements in the light of the latest amendments proposed by the Protocol to the Convention [196].

According to Article 6 of the Law of Ukraine "On the Protection of Personal Data", processing of personal data must be carried out for specific and legitimate purposes defined by the consent of the subject of personal data or based on the law. Consent, however, must conform to such principles as voluntariness, unambiguity, and awareness.

In case of changing a purpose of processing personal data to a new purpose which is incompatible with the previous one, for further processing of the data, the holder of the personal data must obtain the consent of the subject of the personal data for processing his or her data following the modified purpose, unless otherwise provided by law.

---

[194] *KExpert consultation on the new Draft Law on personal data protection: https://www.coe.int/uk/web/kyiv/-/new-draft-law-of-ukraine-on-personal-data-protection-expert-consultations-with-support-of-join-eu-and-coe-project*

[195] *Law of Ukraine "On the Protection of Personal Data": https://zakon.rada.gov.ua/laws/show/2297-17*
про Україну. Zaxid.net. 12 лютого 2020 року: https://zaxid.net/facebook_zablokuvav_akaunti_yakimi_rozvidka_rosiyi_poshiryuvala_dezinformatsiyu_pro_ukrayinu_n1497610

[196] *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e*

Personal data should be accurate, reliable and updated as necessary, with a defined purpose for processing them, and the composition and content of personal data should be appropriate and adequate with respect to a defined purpose for its processing.

Article 24 of the Law of Ukraine "On the Protection of Personal Data" provides the obligation of those who process personal data to ensure the protection of that data from accidental loss or destruction, from illegal processing, including unlawful destruction or access to personal data.

At the same time, in practice, the processing of personal data often violates these principles, not only by private actors but also by public authorities.

Thus, according to the Annual Report of the Commissioner of the Verkhovna Rada on the status of protection of human and civil rights and freedoms in Ukraine in 2020, the Commissioner received almost 1,500 complaints, concerning the violation of the human right to privacy and family life in the performance of debt collection activities for monetary obligations of individuals (debt collection activities). Most of the violations identified related specifically to the uncertain legal basis for processing the personal data of subjects and the improper processing of the personal data of third (contact) individuals, as well as the failure to inform the subject of his or her rights, the failure to provide information on the information owner, the purpose of the processing and content of the personal data collected, and their transmission to third parties [197].

In October 2020, the Parliament registered Draft Law No. 4241 "On Amending Certain Legislative Acts of Ukraine to Protect Debtors in Settlement of Overdue Debts" [198], which should regulate the rules of work of collectors, in particular, the procedure for registration of the collecting company, the requirements for ethical conduct with debtors, the forms and procedure of communication, the exhaustive list of personal data for processing, supervision of debt collection activities, sanctions for violations [199].

The Commissioner for Human Rights also drew attention in her report to the illegal dissemination of personal data authorized by state bodies, as well as to the practice of improperly obtaining consent for the processing of personal data from a person which results in artificial obstacles to the exercise of human rights under the Constitution (education, work, health, etc.).

Separate legislative initiatives introduced in Parliament in 2020 also contradicted principles of personal data processing. For example, on October 26, 2020, Draft Law No. 4265 "On State Registration of Human Genomic Information" was registered [200].

[197] *Annual report of the Commissioner for Human Rights on the state of observance and protection of human and civil rights and freedoms in Ukraine for 2020: https://ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf*

[198] *Draft Law: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70219*

[199] *The Law was adopted on 19 March 2021.*

[200] *Draft Law: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70249*

The Draft Law envisages the creation of the Human Genome Information Database, which will be held by the Ministry of Internal Affairs of Ukraine and administered by the State Research and Expert Forensic Centre of the Ministry of Internal Affairs of Ukraine. The purpose of state registration of genomic information is to prevent criminal offenses; identity of perpetrators of criminal offenses; search for missing persons; identification of unidentified bodies (remains) or of an individual who, due to his health or age, cannot identify himself.

At the same time, the Draft Law does not define the proper procedure for processing personal data in accordance with the fundamental principles defined by the law [201]. ПIt is assumed that the procedure for processing genomic information and maintaining the database will be established by the Cabinet of Ministers of Ukraine [202], whereas, taking into account the sensitive nature of genomic information, the manner in which such personal data are collected, used and protected should be defined at the legislative level, without leaving the broad borders for discretion. The law does not define clearly whether biological materials should be collected and when, as well as the procedure for their collection that would guarantee an appropriate level of protection. Finally, a number of state-run institutions, penal institutions and specialized medical institutions will have access to the "keys" and biological material that will enable the data from this database to be interpreted, which creates significant risks of information leakage, and the concentration of data collection, storage and management access to such data in the Ministry of Internal Affairs of Ukraine create significant risks of corruption [203].

The Draft Law No. 3196-d on Amendments to the Law of Ukraine "On the Security Service of Ukraine" [204], to improve the organizational and legal framework of the Security Service of Ukraine, adopted on first reading in January 2021, proposes the SSU to be given unrestricted access to any personal data of citizens, in particular those stored not only in public registers but also in private databases and collected through video surveillance systems. At the same time, the SSU may create its own databases and data banks, information arrays, information and telecommunication systems, and keep special operational records. There are no requirements or details on how personal information can be entered and stored in such databases. In this way, the Security Service will have unrestricted access to huge amounts of personal data, regardless of whether there are grounds for conducting counterintelligence, search and other activities against such persons that fall within the competence of the SSU.

[201] *What is wrong with Draft Law No.4265 on the processing of genomic information? The Digital Security Lab:* https://dslua.org/publications/shcho-ne-tak-z-obrobkoiu-henomnoi-informatsii-v-zakonoproekti-4265/

[203] *Conclusion of Central Scientific Experts Office:* https://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=70249&pf35401=538372

[204] *Draft Law:* https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243

It is proposed that the procedure for access by the Security Service to state personal databases should be approved by decrees of the President of Ukraine and decrees of the Cabinet of Ministers of Ukraine. This approach is contrary to the requirements of the Law "On the Protection of Personal Data", which stipulates that such procedure should be regulated by current legislation and conform to the principles of legality, proportionality, minimization, accountability of data processing and others. The conditions and manner of transmission of such information should be regulated by law [205].

Ukrainian legislation does not provide any special restrictions or requirements on the implementation of "profiling" – automatic processing of personal data to collect and use information about a person for the identification purpose, analysis and prediction of her preferences, behavior, and attitudes.

At the same time, the Concept for the Development of Artificial Intelligence [206], approved by the Cabinet of Ministers of Ukraine on December 2, 2020, among the basic principles for the development and use of artificial intelligence technology, aimed to ensure that the activities and algorithms of artificial intelligence solutions meet the requirements of personal data protection legislation, and respect for the constitutional right of everyone to the privacy of private and family life regarding the processing of personal data [207].

4.1.3. Rights of individuals in connection with the processing of their data

The Law of Ukraine "On the Protection of Personal Data" guarantees every individual a number of rights regarding the implementation of automated processing of his or personal data, in particular:

1) to know the sources of the collection, the location of their personal data, the purpose of their processing, the location or residence of the holder of personal data, or to order authorized individuals to obtain this information, except as provided by law;

2) to receive information on the conditions for access to personal data, including information on third parties to whom their personal data are transmitted;

3) the right of access to personal data;

4) to receive a reply on whether his or her personal data are being processed, as well as to receive the content of such personal data, not later than 30 days after the date of receiving of such request, except in the cases provided for by law;

[205] *New powers of SSU. The Digital Security Lab: https://dslua.org/publications/blokuvannia-saytiv-masove-stezhennia-filtruvannia-kandydativ-na-vyborakh-abo-novi-povnovazhennia-sbu/*

[206] *Order of the Cabinet of Ministers of Ukraine on 2 December 2020 No. 1556-R "On approvement of the Concept for the Development of Artificial Intelligence in Ukraine": https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text*

[207] *The Government approved the Concept for the Development of Artificial Intelligence taking into account the proposals of the Digital Security Lab: https://dslua.org/publications/uriad-zatverdyv-kontseptsiiu-rozvytku-shtuchnoho-intelektu-v-ukraini-z-urakhuvanniam-propozytsiy-tsyfrolaby/*

5) to submit a reasoned request to the holder of personal data with an objection to the processing of his or her personal data;

6) to make a substantiated request for the alteration or removing of personal data by any holder of personal data if the data are being processed illegally or unreliable;

7) to protect their personal data from illegal processing and accidental loss, removing or damage due to willful concealment, failure to provide or untimely provision thereof, and to protect personal data from the processing, which is unreliable or detrimental to the honor, dignity and business reputation of an individual;

8) to complain to the Commissioner or the courts regarding the processing of their personal data;

9) to apply legal remedies in cases of violation of the legislation on the protection of personal data;

10) to enter restrictions on the right to process their personal data when giving consent;

11) to withdraw consent to the processing of personal data;

12) to know the mechanism for automatic processing of personal data;

13) to protect against automatic processing of personal data that has legal consequences for an individual.

At the same time, in practice, the legal rights of the holder of personal data do not always guarantee their full realization. The State must also provide effective remedies for human rights violations. As of today, a person whose personal non-property rights have been violated may file a complaint to the Human Rights Commissioner, courts or the police, in case of illegal collection, storage, use, removing or dissemination of confidential information about a person (Article 182 of the Criminal Code of Ukraine). However, none of these measures guarantee effective protection of the right violated. Thus, the Office of the Human Rights Commissioner does not have sufficient resources to deal effectively with all complaints received, and judicial and criminal investigations may take several months or even more than a year. Nevertheless, the establishment of a separate specialized body to monitor compliance with the law and the rights of citizens to protect personal data remains a pressing issue.

The case-law is particularly noteworthy, indicating the existence of systemic violations related to the abusive access to public registers and databases containing personal data.

Thus, in 2020, 6 criminal convictions were handed down [208] for unauthorized dissemination of information with restricted access stored in automated systems of the State Fiscal Service of Ukraine and the State Border Service of Ukraine (Articles 361-2 and 362 of the Criminal Code of Ukraine). Thus, the legislator should consider enhanced mechanisms to protect against possible abuses in the processing of personal data in public registries.

The fight against the illegal sale of personal data of citizens, which is becoming widespread in Telegram [209], requires the development of systematic approaches, both to strengthen the security requirements of state and commercial databases and to develop methods of investigation of such illegal activities. The lack of effective state measures to prevent the illegal dissemination of personal data on the Myrotvorets [210]. website is of particular concern. In 2020, this website added the journalist of the investigation project "Our money with Denys Bihus" to its database of "people who pose a threat to the Ukrainian state and society, committed crimes against the fundamentals of national security" for the episode on theft in the defense industry [211].

It is worth noting that the rights of personal data holders are not absolute and may be subject to limitations imposed by law. Ukrainian legislation, in particular, properly balances the requirements for the protection of personal data with the requirements for access to public information and freedom of speech.

Thus, Article 5 of the Law of Ukraine "On the Protection of Personal Data" stipulates that the personal data of an individual authorized to perform the functions of the state or local government or official are not confidential information. Personal data mentioned in the declaration of a person authorized to perform the functions of the state or local government, in accordance with the Law of Ukraine "On Prevention of Corruption" are not considered to be restricted information, except the information on the registration number of the tax payer's card or series and the passport number, the unique entry number in the Unified State Demographic Register, the place of residence, the date of birth, the location of the objects which are mentioned in the declaration (except for the region and the locality), the bank account numbers [212]. The law also provides a number of other cases in which personal data may be disseminated without the consent of the person if this is a matter of public interest that prevails over possible harm caused by the disclosure.

---

[208] See for example:
the verdict in the case No. 641/3658/20: https://reyestr.court.gov.ua/Review/93639586;
the verdict in the case No. 686/6670/20: https://reyestr.court.gov.ua/Review/88730915;
the verdict in the case No. 711/870/20: https://reyestr.court.gov.ua/Review/88115992;
the verdict in the case No. 344/8068/20: https://reyestr.court.gov.ua/Review/93809770

[209] MediaSapiens. A Telegram bot is selling the personal data of Ukrainians. The SSU has started investigation: https://ms.detector.media/kiberbezpeka/post/24656/2020-05-12-telegram-bot-prodaie-osobysti-dani-ukraintsiv-sbu-rozpochala-rozsliduvannya/

[210] https://myrotvorets.center/

[211] Bihus was added to a database of Myrotvorets. The Institute of Mass Information: https://imi.org.ua/news/bigusa-vnesly-v-bazu-myrotvortsya-i34627

[21] Law of Ukraine "On Prevention of Corruption": https://zakon.rada.gov.ua/laws/show/1700-18

4.1.4. Supervisory body

One of the key elements of an effective mechanism for the protection of personal data is the operation of an independent supervisory body in the field of personal data and the creation of effective mechanisms to protect the rights of personal data owners.

In Ukraine, there is no system of protection that fully complies with international standards for this purpose. Under Article 22 of the Law of Ukraine "On the Protection of Personal Data", the Ukrainian Parliament Commissioner for Human Rights (Ombudsman) supervises the monitoring of compliance with the legislation on the protection of personal data within the limits of the powers provided by the law. Citizens may also file a complaint about a violation of their right of access to personal data directly in court.

According to the report of the Ukrainian Parliament Commissioner for Human Rights, in 2020 the Commissioner received 2,031 complaints about violations of human rights to the protection of personal data, almost twice as many as in 2019 (1,061). An analysis of the communications received by the Commissioner shows that the majority (almost 1,500) of them concerning violations of the human right to privacy and family life in the course of collection of individual debt (debt collection activities). The reports received also related to the illegal dissemination of personal data via the Internet, messengers and social networks, violation of the right to protection of personal data when using electronic services. With a view to exercising parliamentary control over the observance of the right to personal data protection, 67 inspections have been carried out on enterprises, institutions and organizations, state and local authorities, holders and / or managers of personal data; 62 proceedings have been instituted by the Commissioner, and 9 reports on administrative offenses under Article188-39, paragraph 4, of the Code of Administrative Offences have been drawn up and submitted to the courts [213].

Even though the Ombudsman is empowered to verification on compliance with the legislation on the protection of personal data and may issue mandatory requirements (regulations) to prevent or eliminate violations of the legislation on the protection of personal data, including the alteration, deletion or removing of personal data, allow or prohibit their disclosure to a third person, the Commissioner's mandate is limited to parliamentary control, as provided for in the Constitution of Ukraine.

[213] *Annual report of the Commissioner for Human Rights on the state of observance and protection of human and civil rights and freedoms in Ukraine for 2020: https://ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf*

As noted by the current Commissioner, part of the powers to be exercised by the supervisory authority under Article 58 of the EU General Data Protection Regulations (in particular, investigations and administrative fines) are not fully in line with the constitutional and legal status of the Ukrainian Parliament Commissioner for Human Rights, who, under Article 101 of the Constitution, exercises "parliamentary control over observance of constitutional rights and freedoms of man and the citizen". Based on the above, the Commissioner supports the necessity for a separate supervisory body in the field of personal data protection and access to public information. According to the EU General Regulation on Data Protection, in establishing the supervisory body, it is important to ensure a high degree of its independence at the legislative and constitutional level. It is possible to avoid any possibility of influencing the decisions of the supervisory authority, as well as any suspicion of bias only through the creation of a new body outside the executive branch [214].

To date, no proposals have been submitted for the establishment of a new body to supervise the implementation of personal data legislation. Among the models that can be considered, there is the establishment of a separate state body outside all the branches of state power in Ukraine; the establishment of a separate central executive body or the granting of control powers to different state bodies [215]. In any case, the key criteria of the independence of such an institution must be met.

4.1.5. Restriction

As a general rule, Ukrainian legislation provides that any interference in a person's right to respect for private and family life must be provided for by law, pursue a legitimate aim and be necessary for a democratic society. At the same time, recent legislative changes and some legislative initiatives introduced raise concerns about deviations from such standards.

The State does not prohibit anonymity, pseudonymization, the secrecy of private communications or the use of encryption technologies. The restriction of anonymity is generally applied under criminal procedural law.

[214] *On the establishment of a supervisory body in the field of personal data protection and access to public information: https://www.ombudsman.gov.ua/ua/all-news/pr/shhodo-stvorennya-naglyadovogo-organu-u-sfer%d1%96-zaxistu-personalnix-danix-ta-dostupu-do-publ%d1%96chno%d1%97-%d1%96nformacz%d1%96%d1%97/*

[215] *Volodymyr Venher, Oleh Zayarnyi. Legal analysis of basic models for State supervisory institutionalizing in the field of personal data and access to public information in Ukraine, 2020.: https://rm.coe.int/legal-analysis-data-ua/16809ee077*

At the same time, at the beginning of 2020, the Ministry of Culture, Youth and Sport of Ukraine initiated discussions on the Draft Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Ensuring National Information Security and Right to Access Reliable Information" which, inter alia, imposed mandatory public disclosure of the identity of all media disseminators, contrary to international principles on anonymity [216]. The document was sharply criticized by the public and international organizations [217], and the Ministry took no steps to promote it further or to submit it to Parliament.

In the spring of 2020, due to the spread of the Covid-19 on the territory of Ukraine, issues of personal data protection became particularly relevant in the context of the introduction of epidemic control measures. On April 13, 2020, the Verkhovna Rada adopted the Law of Ukraine On Amendments to the Law of Ukraine "On Protection of the Population from Infectious Diseases" for on Prevention of Coronavirus Disease (COVID-19)" [218]. Among the novelties is the authorization for the period of quarantine to counteract the spread of coronavirus disease, to process data on the state of health, place of hospitalization or self-isolation, surname, first name, patronymic, date of birth, place of residence, work (studies) without patient's consent.

The adopted Law is contrary to general requirements and principles in the field of protection of personal data. Although there is an obvious legitimate interest in restricting individual rights in order to protect citizens' health, the Law does not provide adequate legal certainty, in particular, does not defines which public authorities are authorized to process personal data without the consent of the person and to what extent. The Law does not provide any safeguards against possible abusive use of particularly sensitive information on a person's state of health. At the same time, the range of persons involved in anti-epidemic measures is extremely wide. It is therefore not justified to authorize them to have access to all the above information [219].

The Digital Security Lab also analyzed compliance with the principles of personal data processing when introducing the application "Vdoma" ("Act at Home"), created by the Ministry of Digital Transformation to monitor citizens' compliance with quarantine restrictions [220].

---

[216] *Digital Security Lab. Legal analysis of the Draft Law on misinformation: https://dslua.org/publications/yurydychnyy-analiz-zakonoproektu-pro-dezinformatsiiu/*

[217] *https://detector.media/community/article/174120/2020-01-22-efj-vystupyla-proty-regulyuvannya-diyalnosti-zhurnalistiv-z-boku-ukrainskoi-vlady/*

[218] *Law of Ukraine "On Protection of the Population from Infectious Diseases" for on Prevention of Coronavirus Disease (COVID-19)" https://zakon.rada.gov.ua/laws/show/555-IX*

[219] *Ibidem: https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antyvirusnym-zakonom/*

[220] *Digital Security Lab. The Cabinet of Ministers has explained the application "Dii vdoma"' terms of use: https://dslua.org/publications/kabmin-detalizuvav-umovy-zastosuvannia-diy-vdoma/*

Although the installation of the application is voluntary, the exchange of information in the system between the Ministry of Health, the Ministry of Internal Affairs, and the Ministry of Digital Transformation is not carried out in the manner prescribed by law but grounded on the separate agreements between mentioned ministries. This does not ensure adequate transparency as to whom and to what extent neither given the access to the personal data of persons with or suspected of Covid-19 nor does it guarantee sufficient discretion on the use of such data by the authorities.

The "experimental" project on verification of data of public registries is also causing serious concern about the interference of the authorities in the right to information privacy of a person and possible profiling. Thus, on December 4, 2019, the Cabinet of Ministers of Ukraine approved Resolution No.1078 "On the implementation of the pilot project of verification of data on natural persons processed in some national electronic information resources" [221].

In accordance with the Resolution, data on natural persons processed in the State Registry of Civil Status Acts, the State Register of Natural Tax Payers, the Register of Insured Persons of the State Register of Mandatory State Social Insurance, the Unified State Electronic Database on Education, as well as the Register of E-health Patients, are subject to verification. This verification must be carried out by transmitting certain categories of data from the relevant registers to the Ministry of Internal Affairs, which must match the various registers through its own information system. The Ministry of Finance, with a view to verifying data on individuals, processed in national electronic information resources, must provide the Ministry of Internal Affairs with the relevant software and technical solutions for establishing the analytical platform of electronic verification and monitoring.

It should be noted that validation of national registry data is not the only purpose of such "verification". This information will be used to complete the Single State Demographic Register. Under paragraph 5 of Regulation No. 1078, the Ministry of Internal Affairs and the State Migration Service must verify the data obtained with the data of the Unified State Demographic Register and complete the Unified State Demographic Register with data on the verified physical person, simultaneous creating a temporary number of the unique entry number in the register. And according to paragraph 6 of the Regulation, the Ministry of Internal Affairs should introduce an electronic service for the identification of individuals through the unified information system of the Ministry of Internal Affairs with a view to bring information from other national electronic information resources in accordance with a single identifier.

[221] *Resolution No. 1078: https://www.kmu.gov.ua/npas/pro-realizaciyu-eksperimentalnogo-p-a1078*

According to the timetable and stages of the pilot project defined in Annex 2 of the Regulation, already at the end of May 2020 the Ministry of Digital Transformation, which ensures coordination of the verification process, together with the Ministry of Internal Affairs, was required to prepare a report on the results of the verification of the reliability, its relevance, completeness and avoiding of data redundancy, and to submit proposals for "ensuring an integrated and unified approach to the legal and organizational framework for the operation of national electronic information resources". However, in 2020, the Ministry of Internal Affairs has still not made public the methodology for such verification, which nevertheless does not prevent the Ministry from receiving data from the administrators of the relevant registers.

Of course, validation of information in public registers is important. At the same time, in view of the scope of the verification and the fact that this function is entrusted to a law enforcement body, the verification procedure must have a clear legal basis, to meet the requirements of the legislation on the protection of personal data, to be transparent and implemented with all necessary security measures. However, the verification mechanism proposed by Regulation No.1078 is in direct contravention of the current legislation of Ukraine, which defines a different procedure for processing and verifying personal data in the registers [222]. Thus, the verification procedure requires immediate harmonization with the requirements of the current legislation.

4.2. Surveillance

Surveillance activities carried out by state authorities should meet the requirements of Article 8 of the European Convention, in particular the principles of legality, legitimacy and necessity in a democratic society, and shall be subject to effective, independent and impartial monitoring.

To date, Ukrainian legislation does not provide sufficient safeguards to ensure respect for the right to privacy, including the privacy of electronic communications, in an online environment. Lack of legally defined procedures for the interception of electronic communications, weak and formal human rights monitoring of such activities, as well as combined functions of the Security Service of Ukraine in the field of national security and the investigation of criminal offences creates unlimited discretion for such bodies and may lead to uncontrolled interference in citizens' right to privacy.

4.2.2. Requirements for legislation in the field of surveillance

In accordance with the standards of the European Convention, surveillance measures must be carried out under the law, which is accessible, clear, precise, and foreseeable. The law contains safeguards for the exercise of discretion by public authorities and thus defines with sufficient clarity and precision. The law must contain safeguards for the exercise of discretion by public authorities and thus defines with sufficient clarity and precision:

[222] *"Digital State" and Personal Data: Compliance with the Law on Personal Data Protection in Digital Data Initiatives: https://internetfreedom.org.ua/ua/zakhody/158-aba-roli-ta-laboratoriia-tsyfrovoi-bezpeky-provely-ekspertne-obhovorennia-tsyfrova-derzhava-ta-personalni-dani-dotrymannia-zakonodavstva-pro-zakhyst-personalnykh-danykh-v-initsiatyvakh-didzhytalizatsii*

– the nature of offenses which may give rise to surveillance measures;

– the competent authorities that carry out surveillance measures, the scope of any discretion conferred on such authorities and the manner of its exercise having regard to the legitimate aim of the measure in question;

– the categories of individuals liable to be subjected to surveillance measures;

– the limitation for carrying out surveillance measures;

– the procedures for examining, using and storing data obtained from surveillance measures;

– the precautions to be taken when communicating data acquired through surveillance measures to other parties and the measures applicable during the communication to ensure data security;

– the circumstances for the destruction and erasure of data obtained from surveillance measures;

– the bodies responsible for overseeing surveillance measures [223].

The Ukrainian Code of Criminal Procedure incorporates most of these elements. At the same time, the use of surveillance measures in intelligence, counterintelligence and other activities related to national security issues is not accompanied by sufficient safeguards against excessive interference with personal privacy.

The Law of Ukraine "On Intelligence" [224], which was adopted on September 17, 2020, gives the intelligence agencies the power to carry out, in respect of persons, places or things which are located on the territory of Ukraine, separate intelligence activities, consisting of the removal of information from telecommunications networks by selecting and recording the content of the relevant information or data transmitted or received by the person and the retrieval of information from electronic information systems by means of a search, the selection and recording of relevant information or data contained in an electronic information system or its part thereof without the knowledge of its holder or owner, and the localization of the storage medium, by selecting and recording information or data about the location and / or using such means(device) without disclosing the content transmitted or received by the individual.

The Law provides that such intelligence activities shall be conducted on the condition that they are directly related to intelligence activities outside Ukraine or aimed at obtaining intelligence information, with a source of origin outside Ukraine and solely based on a court decision. At the same time, the intelligence agencies have considerable discretion in determining the grounds for the application of such measures. In addition, intelligence activities may be conducted prior to a court decision but no longer than 72 hours after a person' identification.

[223] *Recommendation CM/Rec(2016)5 on Internet Freedom: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016806415d8*

[224] *Law of Ukraine "On Intelligence": https://zakon.rada.gov.ua/laws/show/912-20*

The Law stipulates that the period of validity of an order for the application of appropriate surveillance measures may not exceed six months, but does not contain any other requirements concerning the storage, use or disposal of the data obtained.

Moreover, the removal of information from the transport networks of telecommunications operators providing mobile and / or fixed communications services should be ensured by "system of technical means, used by all intelligence bodies under conditions of autonomous access to information in the manner determined by the legislation". The current legislation has not regulated the appropriate procedure for autonomous access to information. Moreover, the mere possibility of direct access to telecommunications networks by security agencies creates serious obstacles to adequate and effective human rights oversight in the conduct of intelligence activities.

At the same time, it is proposed to give even broader powers to the Security Service of Ukraine in carrying out counterintelligence measures. The corresponding Draft Law No. 3196-d "On Amendments to the Law of Ukraine "On the Security Service of Ukraine "on Improvement of the Organizational and Legal Basis of the Security Service of Ukraine" [225] provides that SSU may receive from telecommunications operators and providers technological and other information about the networks functioning, including with restricted access, under conditions determined by the holder of this information and the authorized sub-unit of the Security Service of Ukraine. The removal of information from telecommunications networks, as well as the search, access, selection and recording of data contained in electronic information networks (systems) or parts thereof to which access is restricted by its owner, the owner, holder or user of a logical protection system, may be subject only to a court order, except in urgent cases; delay may lead to the destruction of evidence necessary for counterintelligence activities or to the impossibility of obtaining it. In this case, the officials of the SSU may make a decision independently, but within 24 hours it must be submitted to the court for approval. If the court refuses to give such permission, the information obtained must be destroyed.

At the same time, the extension of the surveillance powers of the SSU is not accompanied by corresponding safeguards against human rights abuses and violations. In contrast to the regulation of criminal disclosure procedures, the application of surveillance measures does not provide clear grounds, categories and rights of the subjects to whom such measures are applied. For example, the Draft Law significantly broadens the scope of counterintelligence activities and makes subversive activities one of its objectives, defined quite broadly as "influence on public relations that is no threat to state security and / or increases the risks of state security". The lack of clarity in the exercise of surveillance powers in counterintelligence operations also fails to take into account the strengthened safeguards for the secrecy of communications for certain categories of individuals, such as lawyers, journalists, doctors and others.

[225] *Draft Law: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243*

Furthermore, although the new provisions do not provide direct access to electronic communication networks by SSU, compared to the previous version of the Law, pointing out the necessity to assist providers in organizing and conducting counterintelligence measures, it is proposed to supplement the Law of Ukraine "On Telecommunications" [226] by the certain requirement: "the technical means for the extraction of information from the communication channels and other technical means for the tacit receipt of information for the performance of operational and counterintelligence activities by the relevant bodies must comply with the standards and technical regulations developed by the state body authorized by law". Thus, the technical conditions for access to electronic communications will be determined solely by the SSU, and the possibility of automatic remote access to interception of communications is not excluded by the Draft Law.

4.2.3. Authorization and supervision in the field of monitoring

As a general rule, surveillance measures must be approved by the court, which authorizes their use by order. Judicial supervision meets the requirements of independence and impartiality of the "arbitrator". However, effective surveillance oversight also requires sufficient powers by relevant monitoring bodies.

The Court, which exercises oversight, must have at its disposal all information necessary for the exercise of its powers, regardless of the degree of secrecy, must carefully evaluate the conformity of surveillance activities with human rights principles, must have the power to revoke or terminate surveillance measures, which deemed illegal and require the removal of any information resulting from such activities.

In view of these standards, judicial oversight of the observance of human rights in the application of surveillance measures in Ukraine needs to be strengthened.

First of all, it should be noted that it is very difficult to evaluate whether the courts carefully assess and balance the interests of national security or of countering a criminal offense with the interests of respecting a person's privacy, as the relevant court decisions are not usually publicly available, as it will be discussed in subsection 4.2.5.

No statistical information is available on the number of applications to the courts for permission to apply such measures and the level of their "success" – the number of refusals and the number of permits granted.

Ukrainian courts did not have the power, on their own initiative, to revoke or suspend surveillance measures if there were indications of their unlawfulness. The law also does not regulate the procedure for considering the abolition of such measures. In general, the procedure of court oversight is now virtually formal and does not guarantee effective protection against undue interference with a person's privacy.

[226] *Law of Ukraine "On Telecommunications": https://zakon.rada.gov.ua/laws/show/1280-15*

It should also be noted that the existing procedure does not protect against offense by Security Service personnel of their access to private communications. Thus, in 2020, at least two convictions [227] were handed down by the courts in cases involving the illegal sale of subscriber telephone data, which were obtained by means of special technology, designed for the covert removal of information by SSU employees within the framework of "counterintelligence inspection".

4.2.4. Security guarantees

Council of Europe standards stipulates that surveillance measures should not include the use of methods that weaken encryption systems or the integrity of communications infrastructures, such as built-in vulnerabilities and so-called backdoors.

Ukrainian legislation does not contain requirements for the use of such instruments.

At the same time, the Law of Ukraine "On Telecommunications" stipulates that telecommunications operators are obliged, for their own means, to install on their telecommunication networks the technical means, necessary for operational and investigative measures hold by authorized bodies, and to ensure the functioning of this equipment and, within the limits of its powers, to facilitate the conduct of investigative and operational activities and to prevent the disclosure of organizational and tactical methods of such measures.

The Law of Ukraine "On Intelligence" determines that such a system of technical means must provide the possibility of autonomous access to information in the manner defined by the law.

The Law of Ukraine "On Electronic Communication" [228], which was adopted to replace the Law of Ukraine "On Telecommunications" and will enter into force in 2022, provides that the removal of information from the electronic networks of electronic communication service providers should be ensured by a unified system of technical means, used by all legally authorized bodies, with autonomous access to information in a manner, defined by the Law. At the same time, the provider of electronic communication services and / or networks should allow the technical means to be connected at a point for such access in an electronic communication network, defined by the electronic communication network and / or service provider.

However, there is no statutory procedure for the use of such equipment. That is to say, the safeguards necessary to protect the secrecy of communications from arbitrary interference are not currently provided by law. For this reason, the installation of equipment with technical specifications that allow direct access by law enforcement officials will allow uncontrolled intervention in electronic communications.

---

[227] *See verdicts in cases No. 755/2110/20: https://reyestr.court.gov.ua/Review/91885873 та у справі № 755/1730/20: https://reyestr.court.gov.ua/Review/88100538*

[228] *Law of Ukraine "On Electronic Communication": https://zakon.rada.gov.ua/laws/show/1089-IX*

The Draft Law No. 3196-d on Amendments to the Law of Ukraine "On Security Service of Ukraine" proposes to endow SSU with power to install equipment for the receiving of information from transport and telecommunications networks and control technical means for private transmission of information. This approach effectively precludes independent monitoring of the installing of such equipment and may also result in classification of general information on the functionality of the equipment installed: for example, whether technical means will allow interfering with the integrity of electronic communications, blocking or otherwise preventing users from accessing certain web resources, etc.

4.2.5. Access to information

Ukrainian legislation does not guarantee an appropriate level of transparency in the implementation of surveillance measures. The Law of Ukraine "On Access to Public Information" provides the general duty of all subjects of authority to publish and provide public information in response to requests, and allows to restrict access to information, if the following requirements are met together (three-component test):

1) solely in the interests of national security, territorial integrity or public order, to prevent disorder or a criminal offense, for the protection of public health, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence or ensuring the credibility and impartiality of justice;

2) disclosure of information may be prejudicial to those interests;

3) the harm of making such information public shall prevail over the public interest in obtaining it [229].

Despite this, access to information on the activities of law enforcement and security agencies remains very limited. Public reports published by state authorities do not even contain statistical information on the application of surveillance measures.

The Law of Ukraine "On Intelligence" introduces a new kind of classified information – intelligence secret, that shall be applied to information and data received or created by the intelligence bodies of Ukraine, the disclosure of which "could be expected to hamper the intelligence agency functioning", and access to which is restricted under this Law in the interests of the national security of Ukraine. Article 46 of this Law stipulates that information relating to the intelligence secrecy shall not be made public and shall not be made available to inquiries under the Law of Ukraine "On Access to Public Information", as well as to other inquiries, except where otherwise expressly provided by law. To ensure citizens' access to information on the activities of the intelligence agencies, certain information or data relating to intelligence secrets may be transmitted or published by the decision of the head of the intelligence agency.

[229] *Law of Ukraine "On Access to Public Information": https://zakon.rada.gov.ua/laws/show/2939-17*

Thus, the Law "On Intelligence" actually allowed restricting access to information about the activities of the intelligence bodies at the discretion of its head, regardless of compliance with the requirements of the "three-component test", which contradicts the requirements of the Constitution of Ukraine and the Convention. Human rights organizations had even appealed to the President of Ukraine to review the Draft Law. [230].

Such an approach is proposed in the Draft Law of Ukraine No. 3196-d "On the Security Service of Ukraine". The Head of the SSU or authorized officers may be granted the right to refuse to provide information about the activities of the SSU if they "reasonably" consider that such disclosure will create threats to "their own security and the security of operational activities", regardless of the possibility to cause damage and the existence of an overwhelming public interest in the publicity.

Particular attention should be paid to the possibility of an individual being informed of the use of surveillance measures against him or her.

Under the Law of Ukraine "On Access to Court Decisions" [231] general access to the court orders to conduct secret investigative (search) activities, or on refusal to grant a request for the conduct of secret investigation (search) activities, is allowed one year after such court decision was entered in the Unified State Register of Court Decisions. However, the information in the register is anonymized and it is not possible to identify the person against whom the measures have been taken. The Law also provides that, in cases specified by this Law, a court decision granting or denying permission to conduct an intelligence action, in camera, is neither published nor disclosed.

The Law "On Intelligence" provides that the intelligence body shall provide information on the restriction of the rights, freedoms and legitimate interests of an individual only after the conclusion of the intelligence activities to which the restriction was related, and provided that the provision of this information does not pose a threat to the national security of Ukraine.

The Draft Law "On amending the Law of Ukraine No. 3196-d "On the Security Service of Ukraine" stipulates that court decisions court orders to conduct counterintelligence measures or to refuse such measures, will be not listed in the Unified State Register of Court Decisions, and the relevant information must be kept under the law on the protection of state secrets. Although such a requirement may be justified in the time of counter-intelligence activities, once they are completed, the status of the documents must be reviewed and access to such information must be open in accordance with the provisions of the Law of Ukraine "On Access to Public Information".

[230] *Statement: https://imi.org.ua/news/gromadyanske-suspilstvo-prosyt-zelenskogo-vetuvaty-zakon-pro-rozvidku-i35254*

[231] *Law of Ukraine "On Access to Court Decisions": https://zakon.rada.gov.ua/laws/show/3262-15*

The Draft Law also gives rise to conflicts, proposing, on the one hand, to limit, without alternative, the right of an individual to receive information on the transmission of his or her personal data at the request of intelligence and counterintelligence bodies, and providing changes in the Law on "On Access to Public Information" for which such restriction should apply until a decision is taken on the results of the mentioned activity or events.

Only the Criminal Procedure Code of Ukraine specifically regulates a manner in which the person whose constitutional rights have been temporarily restricted in the course of secret investigative (search) action, as well as the suspect and his or her defense counsel, must be notified of such restriction in writing by the procurator or, at his or her request, by the investigator. The specific time of a notification is determined by the existence or absence of threats to the purpose of the pre-trial investigation, public safety, the life or health of individuals involved in the conduct of secret investigative (search) action. The relevant report on the fact and results of the tacit investigative (search) action must be made within 12 months of the cessation of such action, but no later than the submission of an indictment to the court (Article 253 of the Code of Criminal Procedure) [232].

[232] *Code of Criminal Procedure of Ukraine: https://zakon.rada.gov.ua/laws/show/4651-17*

RECOMMENDATIONS FOR SECTION 4:

4.1. Protection of personal data

THE VERKHOVNA RADA OF UKRAINE,
THE VERKHOVNA RADA COMMITTEE ON HUMAN RIGHTS,
THE VERKHOVNA RADA COMMITTEE ON DIGITAL TRANSFORMATION,
AND UKRAINIAN PARLIAMENT COMMISSIONER FOR HUMAN RIGHTS:

– to harmonize national legislation with the requirements of the updated Convention and the EU General Regulation on Data Protection and ensure the establishment of an independent supervisory body for the protection of personal data with sufficient resources to effectively carry out its mandate;

TO THE PRESIDENT OF UKRAINE, THE CABINET OF MINISTERS OF UKRAINE AND THE VERKHOVNA RADA OF UKRAINE:

– to sign and ratify the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.223), which strengthen regulations on personal data protection in the Member States of the Council of Europe and opened for signature on October 10, 2018;

THE VERKHOVNA RADA OF UKRAINE, THE COMMITTEE OF THE VERKHOVNA RADA FOR DIGITAL TRANSFORMATION AND THE CABINET OF MINISTERS OF UKRAINE:

– to improve the regulation and operation of state registers and databases by introducing appropriate regulative, technical and organizational measures to ensure data security and transparent rules on access to such information;

THE CABINET OF MINISTERS OF UKRAINE,
THE MINISTRY OF DIGITAL TRANSFORMATION:

– to take measures to bring the processing of personal data of citizens, linked with the counteracting of Covid-19, in accordance with national legislation and international standards, in particular:

  – to restrict the access of authorities involved in epidemic control measures to only those categories of personal data that are essential for the exercise of their powers as defined by law. This will make it possible to bring the existing system in line with Article 6 of the Law "On the Protection of Personal Data": the content of personal data should be appropriate, adequate but not excessive concerning a purpose of their processing;

– to ensure transparent procedure of the processing of personal data in the framework of the interaction between the Ministry of Health, the Ministry of Digital Information, and the Ministry of Internal Affairs. In particular, the Ministry of Digital Information should be obliged to publish the protocols regulating the list of information transmitted in the context of information exchange with the Ministry of Internal Affairs and the procedure for such information-sharing on quarantine. In addition, it should ensure the preparation and publication of consolidated reports on the information received from the Ministry of Health and on the manner in which these data have been used, as well as on the number and grounds of requests for information from the Ministry of Internal Affairs and the results of their processing;

– to make public information about the results of using "Vdoma" ("Act at Home") for the whole period of quarantine restrictions;

– to ensure transparency in the preparation of acts regulating the procedure for the anonymization and destruction of collected personal data after the completion of quarantine activities, etc.;

THE CABINET OF MINISTERS OF UKRAINE:

– to take measures to bring its acts and acts of the central executive authorities into line with the requirements of current legislation in the field of personal data protection; in particular with regard to compliance with the principles of processing personal data in the collection, use and verification of data from public registers, as well as access to information from such registers in the process of providing administrative services online;

THE MINISTRY OF DIGITAL TRANSFORMATION:

– to ensure transparency and accountability at all stages of the implementation of digital initiatives, to evaluate compliance with the principles of reliability, confidentiality, security of data, and the proportionality of the amount of data used to proposes of its processing using digital identification tools;

THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE,
THE OFFICE OF THE PROCURATOR:

General, and the Security Service of Ukraine – to develop and agree on methodological recommendations for the investigation of cases, related to the illegal dissemination of personal data on the Internet and regularly

4.2. Surveillance

THE VERKHOVNA RADA OF UKRAINE AND OTHER PARTICIPANTS IN THE LEGISLATIVE INITIATIVE:

– to guarantee that all legislative initiatives involving interference in private life by state bodies, in particular concerning the secrecy of electronic communications, will be subject to open and broad discussion (including with human rights defenders) to ensure that they are consistent with international standards of legality, legitimacy, proportionality, reasonableness and justifiability of limitations;

THE VERKHOVNA RADA OF UKRAINE:

– to draft and adopt a law regulating the requirements for intercepting a person's electronic communications, meeting the requirements of predictability, transparency, proportionality and reasonableness of such measures, containing safeguards to limit the discretionary power of the authorities by establishing the categories of persons who may be subject to monitoring, the procedure for carrying out the actions, the time limit for the activities, the procedure for analyzing, using and storing the data obtained, conditions for the transfer of data to others or data destruction, requirements for the safety of technical arrangements for surveillance, etc.;

THE VERKHOVNA RADA OF UKRAINE, THE VERKHOVNA RADA COMMITTEE ON NATIONAL SECURITY, DEFENCE AND INTELLIGENCE:

– to finalize the Draft Law No. 3196 On Amendments to the Law of Ukraine "On the Security Service of Ukraine" to improve the organizational and legal framework of the Security Service of Ukraine and to bring the requirements for access to personal data and surveillance measures in line with the requirements of the Convention for the Protection of Human Rights and Fundamental Freedoms and the practice of the European Court of Human Rights.

THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE, THE OFFICE OF THE PROSECUTOR GENERAL, THE SECURITY SERVICE OF UKRAINE:

– to ensure the quarterly publication of statistical information on the number and types of surveillance measures that were applied to citizens of Ukraine during the relevant period;

– to comply with the requirements of the Law of Ukraine "On Access to Public Information" when restricting access to information concerning their activities.

SECTION 5. Respect for human rights in the activities of Internet intermediaries

5.1. General requirements

5.1.1. State policy in the area of Internet intermediaries

The issue of regulating the activities of Internet intermediaries has become quite acute in Ukraine with the beginning of aggression by the Russian Federation in 2014, after which social networks became another arena of struggle. At the same time, the area of such Internet intermediaries' activities remained unregulated. There were only regulations on the activities of telecommunications providers (including the Internet) in the Law of Ukraine "On Telecommunications", but they were concerned with the technical aspects of their licensing activities [233]. Regulation of other Internet intermediaries categories was not provided. It can be because none of the main global intermediaries, including social media and video-sharing platforms has not Ukrainian origin. It means that any application of regulatory mechanisms by the state will face issues of jurisdiction over such intermediaries and jurisdictional conflicts. Also, despite such a trend for applying the application of national law to foreign intermediaries, in particular in Germany after the adoption of NetzDG [234]. An additional factor is also the general trend of unregulated Internet development in Ukraine, which has both positive and negative features [235].

The only rule, that concerned the content of information transmitted by networks of intermediaries, was in Article 39 of the Law "On Telecommunications" and provided the obligation of telecommunications providers, based on a court decision, to restrict the access of their subscribers to the resources through which child pornography was distributed. As mentioned above, such a technical regulation will be replaced from January 1, 2022, with the entry into force of the Law of Ukraine "On Electronic Communications".

In general, it can be argued that Ukraine imposes on the Internet intermediaries a minimum amount of obligations to respect human rights in their own activities and the intervention of such intermediaries in their activities under the influence of the state. The most significant opposition in the area of human rights and technical regulation is the obligation of Internet Providers to install technical means at their own expense through which law enforcement agencies will be able to carry out operational and investigative measures.

[233] *Law of Ukraine "On Telecommunications": https://zakon.rada.gov.ua/laws/show/1280-15*

[234] *Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG): https://germanlawarchive.iuscomp.org/?p=1245*

[235] *Human rights online: Agenda for Ukraine / Vita Volodovska, Maksym Dvorovyi – Kyiv: NGO "Digital Security Laboratory", 2019. – p.56.: https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_UKR.pdf*

Legislative acts aimed at modifying the relevant provision at the Law "On Telecommunications" are constantly on the agenda of the Parliament. The last of them is a Draft Law on amendments to the Criminal Procedure Code of Ukraine to increase the effectiveness of the fight against cybercrime and the use of electronic evidence (No. 4004) [236]. The corresponding obligation to install content monitoring and filtering equipment on one's own and at one's own expense is contrary to the requirements of E-Commerce Directives [237]. Another aspect of regulating the activities of the intermediaries is the requirements to restrict access to the content on the network and block sites.

An example of hybrid regulation of Internet intermediaries that do not fall under the category of audiovisual media services and video sharing platforms is provided by the Draft Law on Media [238]. The National Council of Ukraine on Television and Radio Broadcasting may obtain the right to conclude memorandums according to the project terminology, platforms for joint access to information, which may provide for the provision of information requirements and restrictions, which is distributed on the platform of shared access to information and accessibility on the territory of Ukraine. They can also form mechanisms of co-regulation and cooperation in the area of resistance to the spread of misinformation and ensuring transparency of financing election campaigns on different social platforms and compliance with other requirements of the legislative election of Ukraine by users.

This legislative act will also regulate such a category of intermediaries as video-sharing platforms, by the requirements of the EU Audiovisual Media Services Directive, as well as custom audiovisual media services (an example of such a service is Netflix), regulation of which will be more equated to audiovisual media [239]. It provides the following responsibilities of platforms under the jurisdiction of Ukraine and subject to registration in Ukraine. They are generally appropriate to the provisions of the Directive:

1) to place the terms of use of the video-sharing platform service on such platform and to acquaint the users of the platform with such conditions;

2) to provide the conditions of using the service of the video access sharing platform a ban on the dissemination of information that violates the requirements of the Law, as well as the requirements of copyright and related rights legislation;

---

[236] *Legislative act card: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771*

[237] *C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Judgment of the Court (Third Chamber) of 24 November 2011: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN*

[238] *Legislative act card: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

[239] *Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02010L0013-20181218&from=EN*

3) to verify the user's age before gaining access to information, which may hurt the physical, moral or mental development of children, and also ensure the possibility of establishing parental control systems to protect children from such information;

4) to provide users with an effective mechanism for forwarding requests of information or materials distributed on the video-sharing platform, as well as the smooth operation of an effective mechanism for responding to requests, notifying the user of the consideration of his requests and the mechanism for appealing the actions of the provider of the video-sharing platform;

5) to provide the conditions of using the video-sharing platform service the procedure for exercising the right to reply or refute inaccurate information and to inform users about the fact and content of refutation or response in descriptive information to the relevant user video, as well as by notifying users before accessing the program.

It is worth mentioning another legislative initiative – the Draft Law of Ukraine on amendments to the Tax Code of Ukraine to abolish the taxation of income received by non-residents in the form of payment for the production and/or distribution of advertising and improving the procedure for value-added tax (VAT) on transactions for the supply of electronic services by non-residents to individuals (No. 4184) [240]. According to its provisions, providers of electronic services will pay VAT in the amount of 20% of paid services provided in the customs territory of Ukraine. The tax will be indirect, so its value will be included in the price of services provided. Those e-service providers that will provide them over UAH 1 million will have to register as VAT payers.

5.1.2. Obligations of Internet intermediaries to respect human rights

Due to the legislative problems, which are described above, Ukraine cannot require the world's largest intermediaries, such as Youtube, Facebook, Twitter and others, to respect human rights in their activities and cannot force them to ensure the observance of the relevant rights. That is why this area is in exclusive regulation by these intermediaries. Human rights violations have been repeatedly remarked by various international organizations, in particular, the Council of Europe [241] and the Special Rapporteurs on Freedom of Expression, the OSCE and other organizations [242]. In particular, all the above-mentioned organizations in 2019 in their "Joint Declaration on Challenges to Freedom of Expression in the Next Decade" (Joint Declaration) stressed the need for companies to implement the UN Guiding Principles on Business and Human Rights [243], with further state oversight of such implementation.

---

[240] *Legislative act card: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70112*

[241] *Recommendation of the Committee of Ministers CM / Rec (2018) to 2 Member States on the roles and responsibilities of Internet intermediaries: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808c6192*

[242] *OSCE Representative on Freedom of the Media. Joint Declaration on Challenges to Freedom of Expression in the Next Decade: https://www.osce.org/files/f/documents/9/c/425282.pdf*

[242] *UN Guiding Principles on Business and Human Rights: https://www.osce.org/files/f/documents/9/c/425282.pdf*

This document points that the state should provide the next steps in its legislation: the obligation of enterprises to respect human rights in their activities; to provide guidance on this matter. In conflict-affected areas, relevant to Ukraine, the state should help enterprises identify and prevent the risks of their activities for human rights, and deny any assistance to businesses that involve serious human rights violations. At the same time, enterprises must avoid any harmful impact on human rights, guaranteed by the International Draft Law of Human Rights, and eliminate harmful effects where they arise from their activities. This document also encourages every business to have a human rights policy and to conduct due diligence on human rights. Both states and businesses must also provide an appropriate and effective mechanism for compensating for human rights violations.

As mentioned above, the Draft Law on Media creates a legal basis to require respect for human rights from one of the intermediaries categories – video-sharing platforms, an example of which is YouTube [244]. If such a platform is registered in Ukraine, it should ensure the establishment of several mechanisms to respond to content and human rights violations with such content. If such mechanisms are not established, the appropriate platforms will face a fine of 10 to 50 minimum wages on the day of the violation.

5.2. Transparency and accountability

5.2.1. Obligations of the state

As was mentioned above, there were no legally-established mechanisms for appeals from law enforcement and other government authorities to intermediaries for removing the content in Ukraine at the end of 2020. Because of this, there are no legal requirements for the publication of information on such appeals. That is why we should not expect transparency of the relevant measures if they are implemented. At the same time, measures to block illegal sites are implemented quite transparently and with appropriate publication on the site of the National Commission for State Regulation of Communications and IT (NCSRCI) and in the Unified State Register of Court Decisions.

In some cases, the authorities publish information about their own appeal to intermediaries. Thus, on October 9, 2020, the Security Service of Ukraine announced its own appeal to "Google LLC" and "Apple Inc" about distribution on their services "Play Market" and "App Store" mobile applications which are blocked in Ukraine [245]. Also, it was heard information about Facebook contacts with law enforcement agencies during a series of public discussions.

Despite the first attempts to regulate the activities of Internet intermediaries in Ukraine by the Draft Law on Media, the legislature decided not to include transparency obligations in it. Therefore, even if the project is adopted soon, publishing information on human rights restrictions will be their voluntary practice, and non-disclosure of such information will not entail any sanctions.

[244] *Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

[245] *The Security Service of Ukraine has initiated the blocking of banned Russian applications on the electronic platforms of Google and Apple: https://www.facebook.com/SecurSerUkraine/posts/2833103260252994/*

5.2.2. Obligations of the Internet intermediaries

Transparency of Internet intermediaries can be considered in several aspects. Firstly, they need to publish their usage rules and content management policies so that they are understandable to users. Secondly, they must provide relevant information on the use of algorithms and automated data processing methods during their activities. Thirdly, they should publish transparency reports that include information on interactions with government agencies to provide information about users and deleting content, and also implementing its own policies to limit the dissemination of certain categories of information [246].

Regarding the first aspect, the largest intermediaries, such as Facebook [247], Instagram as a separate service of Facebook [248], Google [249] and Youtube as a separate service of Google [250], have translations of their own terms of use in Ukrainian. Facebook has also translated a number of policies, including community standards that govern content [251]. They are also translated on Instagram [252]. On Twitter, the terms and conditions are only in English or Russian; at the same time, there is an available translation of Twitter rules into Ukrainian [253]. Almost all policies of Google services are translated into Ukrainian. Tiktok, on the other hand, has no translation of the user agreement and no policies into Ukrainian [254].

Transparency of Internet intermediary algorithms is a cornerstone for understanding how relevant sites and companies affect our consciousness. At the same time, such algorithms are often protected as objects of copyright, and therefore intermediaries are reluctant to disclose their own secrets.

Transparency of Internet intermediary algorithms is a cornerstone for understanding how relevant sites and companies affect our consciousness. At the same time, such algorithms are often protected as objects of copyright, and therefore intermediaries are reluctant to disclose their own secrets. Google's search algorithm is transparent, in which the company has provided a list of factors that affect the searching of materials [255].

[246] *Recommendation of the Committee of Ministers CM / Rec (2018) to 2 Member States on the roles and responsibilities of Internet intermediaries : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808c6192*

[247] *Facebook Terms of Service: https://www.facebook.com/legal/terms*

[248] *Instagram Terms of Use: https://help.instagram.com/581066165581870*

[249] *Google Terms of Service: https://policies.google.com/terms?hl=uk*

[250] *Youtube Rules and Security Terms: https://www.youtube.com/intl/uk/about/policies/#community-guidelines*

[251] *Facebook Community Standards: https://www.facebook.com/communitystandards/*

[252] *Instagram Community Guidelines: https://www.facebook.com/help/instagram/477434105621119/*

[253] *Twitter Rules: https://help.twitter.com/uk/rules-and-policies/twitter-rules*

[254] *Tiktok User Agreement: https://www.tiktok.com/legal/terms-of-use?lang=ru-RU*

[255] *Google. How do search algorithms work: https://www.google.com/search/howsearchworks/algorithms/*

Twitter provides clear information about the formation of its own feed [256]. In 2020, Tiktok also provided some information in his official blog based on which the video is formed [257]. As for Youtube, there is a Google Article where they explain the use of links networks to rank content online [258]. However, according to researchers, network algorithms have changed since then [259].

The advantage is that all the above-mentioned platforms regularly and properly publish transparency reports twice a year. At the time of the analysis, reports for this study were published only for the first 6 months of 2020. According to them, we can say that Ukraine did not send any inquiries to Tiktok during this period [260], while Twitter was subject to one legal requirement to remove content (without specifying whether from an individual or the state), but it was not satisfied [261]. Twitter did not receive any requests from government agencies for information during the reporting period [262].

Facebook received 52 requests from Ukraine for information about 163 users, of which in 58% of cases provided some information. It was also received 9 requests for retention of the information [263]. Facebook deleted one post due to a private notification of defamation from Ukraine [264].

Google received 29 requests to disclose information about 46 accounts. During the first half of 2020, Google also received 2 requests for retention of the information. Their transparency report also specifically states that 1 request was received through official diplomatic channels during this period. In particular, through international legal aid mechanisms [265].

---

[256] *About your Twitter timeline: https://help.twitter.com/en/using-twitter/twitter-timeline*

[257] *How TikTok recommends videos #ForYou: https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you*

[258] *Paul Covington. Jay Adams. Emre Sargin. Deep Neural Networks for YouTube Recommendations: https://static.googleusercontent.com/media/research.google.com/uk//pubs/archive/45530.pdf*

[259] *Paige Cooper. How Does the YouTube Algorithm Work? A Guide to Getting More Views. Hootsuite. 18 August 2020: https://blog.hootsuite.com/how-the-youtube-algorithm-works/*

[260] *TikTok Transparency Report 2020 H1: https://www.tiktok.com/safety/resources/transparency-report-2020-1?lang=en*

[261] *Twitter Transparency — Removal Requests, January-June 2020: https://transparency.twitter.com/en/reports/removal-requests.html#2020-jan-jun*

[262] *Twitter Transparency — Information Requests, January-June 2020: https://transparency.twitter.com/en/reports/information-requests.html#2020-jan-jun*

[263] *Facebook Transparency — Requests Ukraine: https://transparency.facebook.com/government-data-requests/country/UA*

[264] *Facebook Transparency — Content Restrictions Ukraine: https://transparency.facebook.com/content-restrictions/country/UA*

[265] *Google. Global requests for personal data of users. Ukraine: https://transparencyreport.google.com/user-data/overview?user_data_produced=authority:UA;series:compliance&lu=dlr_requests&user_requests_report_period=series:requests,accounts;authority:UA;time:Y2020H1&legal_process_breakdown=expanded:0&dlr_requests=authority:UA;time*

Google has a separate report on government requests to remove content. According to them, during this period, 45 requests for 242 items were received from Ukraine. According to these appeals, 230 concerned defamation and only 5 concerned national security issues. According to the court's decision, it was applied a limit of 222 elements. Only 55 items were removed for legal reasons, it is about 22.7% of the total number of appeals. Google even provides one example of such queries, which the company did not satisfy: "We have received a request from the former chief prosecutor of Kyiv based on a court ruling to remove an Article stating that he and a colleague demanded money from businessmen in exchange for closing criminal cases [266].

Google separately publishes quarterly reports on the removal of content that does not comply with the rules of the Youtube community [267]. With its help, you can find out how many videos and for what reasons were deleted in the Ukrainian segment, although most videos disappear due to the auto-detection procedure. A similar quarterly report, without detailing by country, but with explanations of quarterly trends, is published by Facebook [268], and semi-annual – by Twitter [269]. Tiktok also publishes data on the implementation of its own content policies [270].

In the context of transparency, the transparency of political advertising should be emphasized. In 2020, local elections were held in Ukraine, where some mediators were involved in the election campaigns of candidates. Facebook uses its advertising

library to track relevant expenses [271]. According to NGO "Opora", more than 90,000 political advertisements were published on the platform during the local election campaign [272]. The relevant Google transparency policy has not applied to Ukraine yet [273], while Twitter banned the distribution of political advertising on the platform in 2019.

---

[266] *Google. Requests for removing content from government agencies. Ukraine: https://transparencyreport.google.com/government-removals/by-country/UA?hl=uk&country_item_amount=group_by:requestors;period:Y2020H1;authority:UA&lu=country_item_amount&country_request_amount=group_by:totals;period:Y2020H1;authority:UA&country_request_explore=period:Y2020H1;authority:UA*

[267] *YouTube. YouTube Community Compliance Monitoring: https://transparencyreport.google.com/youtube-policy/removals?videos_by_country=period:Y2020Q4;region:&lu=content_by_flag&content_by_flag=period:Y2020Q4;exclude_automated:human_only*

[268] *Facebook Community Standards Enforcement Report: https://transparency.facebook.com/community-standards-enforcement*

[269] *Twitter Transparency — Rules Enforcement, January — June 2020: https://transparency.twitter.com/en/reports/rules-enforcement.html#2020-jan-jun*

[270] *TikTok Transparency Report 2020 H1: https://www.tiktok.com/safety/resources/transparency-report-2020-1?lang=en*

[271] *Facebook Ad Library: https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=UA*

[272] *Political advertising on Google: : https://transparencyreport.google.com/political-ads/home*

[273] *Twitter. Political content policy: https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html*

5.3. Protection of the right to freedom of expression

5.3.1. State obligations

The issue of content blocking in Ukraine has already been described in sections 2.2.1 and 2.2.2 of this report. It can be confirmed that there are mechanisms in Ukrainian law to block websites and restricting access to content generally corresponds to the three-part human rights restriction test. At the same time, several mechanisms used in practice, in particular the use of the Law of Ukraine "On Sanctions" and the seizure of intellectual property rights that arise from Internet users when using websites, have no basis in law and violate the requirements for predictability of such restrictions by law. Also, Ukrainian legislation does not contain clear definitions of which content categories are prohibited for distribution on the network.

After the passing of the Law of Ukraine "On Electronic Commerce" [274]. in 2015 and subsequent amendments to it in 2017, the issue of intermediaries' immunity has become more regulated. The provisions of this law were intended to implement the provisions of the EU Directive on e-commerce [275]. Its provisions stipulate that hosting service providers (including social networks) are released from liability for the content they post. If they do not have information about illegal activities and content or about the circumstances that give rise to the obvious illegal nature of such activities ("actual knowledge") or after receiving information about such activities and content, they act quickly enough to remove or restrict access to such content ("expeditious removal"). These provisions are prescribed in the fourth part of Article 9 of the Law "On Electronic Commerce". In addition, the adopted Law of Ukraine "On Electronic Communications" directly refers to these provisions in the context of references to the responsibility of providers of electronic communications services for the content of the transmitted information. However, there is no case law on the application of this norm during 2020 in the Unified State Register of Court Decisions, which may indicate the generally proper application of this norm. The absence of litigation can be considered appropriate notification of the lawful nature of information and access to information.

At the same time, Ukrainian law does not prohibit intermediaries from establishing a general obligation to control the content to which they provide access. This obligation is provided by Article 15 of the above-mentioned EU Directive on e-commerce and serves as an additional guarantee for the protection of platforms [276].

---

[274] *Law of Ukraine "On Electronic Communications": https://zakon.rada.gov.ua/laws/show/1089-IX*

[275] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN*

[276] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN*

The current legislation only in general distinguishes the difference between categories of intermediaries and different degrees of their responsibility in Article 9 of the Law "On E-Commerce", which provides for the difference between: "an intermediary information service provider that provides intermediate (temporary) storage of information provided by the recipient of the service, with the sole purpose of improving the further transmission of information to other recipients of the service at their request" ("Caching" in the terminology of Article 13 of the Directive) and "a provider of intermediate services in the information field, providing services of permanent storage of information at the request of the recipient of hosting services" ("Hosting" in the terminology of Article 14 of the Directive) [277]. The activities of "mere conduit" are regulated by the Law "On Telecommunications" and the Law "On Electronic Communications", that will replace it from 2022. As was mentioned above, the Draft Law on Media establishes additional distinctions and different ways of regulation for such categories of intermediaries as video-sharing platforms, information sharing platforms and custom audiovisual media services [278].

5.3.2. Obligations of Internet intermediaries

Internet platforms have their own extensive policies to restrict access to illegal content. They are published on platforms. This is part of the terms of use of the services of certain intermediaries, and their implementation is ensured by a set of human and automated resources. The operating of these resources must be provided by the intermediary. At the same time, the question is how these policies and their implementation meet the requirements of the protection of human rights, UN Guiding Principles on Human Rights and Business and the International Covenant on the Protection of Human Rights, respectively.

In 2018, the international organization "Article 19" analyzed the internal policies of the largest intermediaries (Facebook, Youtube, Twitter, and Google) regarding their compliance with the standards of protection of human rights and freedom of expression [279]. According to its experts, the categories of content marked as prohibited in internal policies are too broad in all areas, from language hostility and terrorist content to privacy-infringing content and fake news. It was incomprehensible to experts the use of algorithm mechanisms and artificial intelligence to the counteraction of harmful content.

[277] *Law of Ukraine "On Electronic Commerce": https://zakon.rada.gov.ua/laws/show/675-19*

[278] *Legislative act card: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

[279] *Article 19. Side-stepping rights: Regulating speech by contract. Policy brief: https://www.Article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf*

The experts of "Article 19" also stressed that sanctions for violating users' own policies often remain unclear. That is why it is unclear what response measure and how it will be applied to a particular violation committed by the user. At the same time, "Article 19" concluded that, in a broad sense, the standards applied by Facebook, Youtube and Twitter are in line with international standards in the field of intermediary protection.

Youtube has a number of policies governing content types, starting from child safety to fake information about Covid-19 [280]. As of 2020, they had the clearest system of sanctions: for the first violation, the author of the channel received a warning, for the second – a strike. During the strike, the author of the channel loses a number of rights on the platform during one week, in particular, the right to download new videos. The second strike is issued to the author of the channel if he commits again a violation within 90 days after receiving the first strike; then the ban on downloading content will last for two weeks. If the situation is repeated for the third time, the channel will be deleted. Each strike is removed from the channel after 90 days from the date of its imposition [281].

Facebook's community standards explain the various categories of banned content in detail and try to explain to users what not to post. At the same time, sanctions for violating the requirements of the content are uncertain. Thus, Facebook notes that the consequences for violating the community standards will vary depending on the degree of the violation: someone can be warned for the first violation; in some cases Facebook can restrict the right to post, and even to deactivate the profile [282]. The measures that Instagram will apply to users in case of violation are also uncertain [283].

Twitter describes a number of factors that it will take into account when imposing sanctions on violators. These factors are: to whom the content or behavior is directed; whether the complaint was posted by a person that was affected by the content or by a third party; what is the history of the person who broken up the rules; what is the brutality of the violation and how the content can serve as a topic of legitimate public interest. At the same time, the procedure for applying sanctions is unclear: Twitter may first point out to the user the illegality of his post and then ask him to delete this post before creating the next content. Further violations may result in a temporary suspension of the ability to post tweets or verification of account ownership. Deletion of an account is an exceptional measure [284].

---

[280] *Youtube Community Guidelines: https://www.youtube.com/howyoutubeworks/policies/community-guidelines/#community-guidelines*

[281] *Youtube Community Guidelines strike basics: https://support.google.com/youtube/answer/2802032*

[282] *Facebook Community Standards: https://www.facebook.com/communitystandards/*

[283] *Instagram Community Guidelines: https://www.facebook.com/help/instagram/477434105621119/*

[284] *Twitter. Our approach to policy development and enforcement philosophy: https://help.twitter.com/en/rules-and-policies/enforcement-philosophy*

TikTok's community standards are generally less detailed in terms of definitions of illegal content than those that have been on the market longer. The provisions on the application of sanctions for their violation are also vague. It is indicated that for certain types of violations, the account can be suspended or banned. In particular, for repeated and gross violations, such as calls for hostility or brutal extremism [285].

In the Ukrainian context, we can mention the mass blocking of Ukrainian Facebook users in 2015 [286] and 2018 [287], when they were blocked for various statements, mostly related to the aggression of the Russian Federation against Ukraine. At the time, Facebook attributed this to a violation of community standards but did not provide detailed arguments regarding the blocking cases. In 2020, there was no such practice of blocking users in Ukraine. However, we can mention the case of deleting a network of accounts observed in coordinated inauthentic behavior during the elections 2019 and associated with the advertising agency "Postmen". It was totally deleted 65 accounts and 32 Facebook pages and 5 Instagram accounts. They have spent almost $ 2 million on advertising in above mentioned social networks [288].

5.4. Privacy protection and data protection

5.4.1. Obligations of the state

Although the main Internet intermediaries do not apply directly under the jurisdiction of Ukraine, the state must take all appropriate measures to guarantee the rights of personal citizens' data when using social networks or other platforms.

First of all, such measures should include the establishment of a clear legal framework on the principles of personal data processing (legality, fairness, transparency, purpose limitation, data minimization, accuracy, data protection, including integrity and confidentiality) and guarantees of observance of the rights of these subjects in Ukraine in full compliance with Convention 108, taking into account the latest changes [289].

In addition, national legislation should properly regulate the grounds and procedure for public authorities to contact Internet intermediaries to provide access to information about users. Any inquiry or request of public authorities to Internet intermediaries to provide access, collection or interception of personal data of their users, including the purposes of criminal proceedings, or any other measures contrary to the right to privacy which has been provided by law, have to carry out to achieve a legitimate aim and be proportionate and reasonable.

---

[285] *Tiktok Community Guidelines: https://www.tiktok.com/community-guidelines*

[286] *Alexander Savitsky, Anna Bednova. Why are famous Ukrainians blocked on Facebook? Deutsche Welle. March 23, 2015: https://www.dw.com/uk/чому-у-facebook-блокують-відомих-українців/a-18468517*

[287] *Yuriy Lapayev. Ban in one gate. Why are Ukrainians blocked on Facebook? Ukrainian week. April 21, 2018: https://tyzhden.ua/Society/212651*

[288] *Nathaniel Gleicher. Removing Coordinated Inauthentic Behavior: https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/*

[289] *See Section 4.1.*

Currently, national regulation of surveillance measures (access to personal communications or other information about users) establishes the procedure for obtaining information from telecommunications operators, while the requirements and procedure for accessing international Internet intermediaries are not defined actually.

5.4.2. Obligations of Internet intermediaries

Internet intermediaries are required to comply with the requirements for the lawful processing of users' data. In particular, obtain the informed consent of users to the use of their personal data, which includes information about the purposes and scope of data processing, user rights, etc. Internet intermediaries should give users the right to revoke their consent and delete their personal data. Compliance with these requirements mostly depends on the intermediaries' transparency requirements which were mentioned above. International Internet intermediaries such as Facebook, Google and Twitter generally comply with the requirements for proper processing and protection of personal data in Ukraine, in particular, because of the extension of EU data protection regulations to them. However, user's tracking and profiling are not completely transparent.

In 2020, Ukrainian government agencies repeatedly appealed to the most popular Internet platforms to obtain information about users.

Thus, in the first half of 2020, Facebook received 52 requests from Ukraine to obtain information about 163 participants. In almost 58% of cases, Facebook provided some information. According to these requests, 9 were based on legal requirements, the rest were emergency. Thus, it means that they were concerned about cases involving a potential threat to the child or the risk of death or serious bodily injury to any person [290]. Google received 29 requests to disclose information about 46 accounts. 21 of them related to emergencies, and 8 were based on other legal requirements. In 38% of cases, some data were provided, and never upon legal requirement [291].

Transparency reports suggest that, as a general rule, intermediaries do not disclose personal data in response to any request, and assess its compliance with the law, may refuse to provide data or require clarification of too wide a range of requirements. However, the reports do not contain sufficient information to assess the principles of legitimacy and necessity in a democratic society when considering such requests. For example, generalized data on the grounds for requests, their justification, reasons for refusal of providing information, etc.

---

[290] *Facebook Transparency — Requests Ukraine: https://transparency.facebook.com/government-data-requests/country/UA*

[291] *Google. Global requests for personal data of users. Ukraine: https://transparencyreport.google.com/user-data/overview?user_data_produced=authority:UA;series:compliance&lu=dlr_requests&user_requests_report_period=series:requests,accounts;authority:UA;time:Y2020H1&legal_process_breakdown=expanded:0&dlr_requests=authority:UA;time*

5.5. Access to effective remedies of legal protection

5.5.1. Obligations of the state

Without the right access to effective remedies of legal protection, the state's obligation to protect human rights on the Internet is incomplete, as users will not be able to appeal to the illegal actions of intermediaries. In the regulation triangle "state-user-mediator", it is the state dispute resolution mechanisms that should put an end to the settlement of the relationship between the user and the mediator.

It should remind that in the Ukrainian context, the right to a fair trial is guaranteed by the Constitution of Ukraine [292] and further decisions of the Constitutional Court of Ukraine: the court cannot refuse justice if a citizen of Ukraine, a foreigner or a stateless person consider that their rights and freedoms have been violated, obstacles to their realization are created or other violations of rights and freedoms occur [293]. Theoretically, it means that any dispute that arises because of the actions of intermediaries against users in Ukraine should be considered by Ukrainian courts. Since this lawsuit will concern the protection of consumer rights, according to the requirements of the Civil Procedure Code, they may be filed at the residence registered place of consumers [294] Therefore, potential lawsuits against technology giants, such as illegal removal of content, can be considered by courts of general jurisdiction. However, there are serious problems with the overall legitimacy of judicial settlement of disputes: 78% of the state's population generally does not trust the courts in Ukraine [295].

The Draft Law "On Media" proposes to establish a commitment for such a category of intermediaries as a video-sharing platform to create an effective mechanism for sending requests for information or materials disseminated on the platform. It is necessary to ensure the efficiency of such a mechanism, as well as the uninterrupted operation of an effective mechanism for responding to appeals, notifying the user about the consideration of his appeals and the mechanism for appealing the actions of the provider of such a platform [296].

---

[292] *Constitution of Ukraine: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80*

[293] *Judgment of the Constitutional Court of Ukraine № 9-zp of December 25, 1997, in the case on the constitutional appeal of citizens Protsenko Raisa Mykolayivna, Yaroshenko Polina Petrovna and other citizens on the official interpretation of Articles 55, 64, 124 of the Constitution of Ukraine (case on appeals of Zhovti Vody residents): https://zakon.rada.gov.ua/laws/show/v009p710-97*

[294] *Civil Procedure Code of Ukraine: https://zakon.rada.gov.ua/laws/show/1618-15*

[295] *Razumkov Center. Report on the results of the study "Attitudes of Ukrainian citizens to the judiciary." 2020: https://rm.coe.int/zvitsud2020/1680a0c2d7*

[296] *The Draft Law: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

If this legislative act is adopted, the platforms under Ukraine's jurisdiction will have to create an appropriate mechanism under the threat of application sanctions.

Ukraine is actively moving towards the use of media literacy tools to promote human rights measures on the Internet. In 2020, the Ministry of Digital Transformation of Ukraine started several educational serials related to digital rights [297]. Thanks to the above-mentioned serials users can learn how to protect their personal data, the safety of children on the Internet and social networks.

5.5.2. Obligations of the Internet intermediaries

Most intermediaries have created a variety of dispute resolution and reporting mechanisms on their platforms. Using these mechanisms, the user can report to the network the spread of certain hostilities or terrorist content, and the Internet intermediary can respond to violations by itself. At the same time, according to "Article 19", the relevant mechanisms of Facebook, Youtube, Twitter and Google lack guarantees of a fair trial. In addition, they often do not explain the reasons for deleting users' content, they do not provide an opportunity to express their own position on the disputed content of the participant as well as they did not create mechanisms for appealing the decision made by the intermediary [298] (except for Twitter, where you can appeal your account suspension) [299]. Similarly, intermediaries do not specify the timing of the decision on the contested content. That is why in some cases, decisions about the pages that have been reported can take years.

Internet intermediaries additionally protect themselves with jurisdictional provisions in their own rules for using the services. Only Facebook provides that consumers can sue the company for interpretation the rules of use of their services at the place of residence [300]. Twitter's users should contact San Francisco, the USA if they want to protect their rights [301], and what about Tiktok users, they should contact an arbitration tribunal in Singapore [302]. Google and Youtube are considering disputes in California unless applicable local law impedes the resolution of such disputes in a California court [303].

---

[297] *Action. Digital education. Educational serials: https://osvita.diia.gov.ua/courses*

[298] *Article 19. Side-stepping rights: Regulating speech by contract. Policy brief: https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf*

[299] *Twitter Help Center. Appeal an account suspension or locked account: https://help.twitter.com/forms/general*

[300] *Умови надання послуг Facebook: https://www.facebook.com/terms.php*

[301] *Twitter Terms of Service: https://twitter.com/en/tos#update*

[302] *TikTok Terms of Service: https://www.tiktok.com/legal/terms-of-use?lang=en#terms-row*

[303] *Google Terms of Service: https://policies.google.com/terms?hl=uk*

As of 2020, the strike appeal mechanism has also appeared on Youtube [304] and TikTok, which during the study in 2018 has not gained much popularity yet [305]. However, the biggest achievement in respecting the right to access effective remedies in 2020 among Internet intermediaries was the launch of the Facebook Oversight Board [306]. This expert authority will be authorized to review the decisions of moderators and algorithms of Facebook and Instagram on restricting access to content, involving content authors, independent experts and collecting comments from third parties. The decision will be made by a majority of the experts who are members of the body. The decision will contain motivation and recommendations for future modifications of Facebook's content policies [307]. The publication of the first decisions is expected at the beginning of 2021 and will take place on the Facebook Oversight Board website.

[304] *Youtube. Appeal Community Guidelines Actions: https://support.google.com/youtube/answer/185111?hl=en*

[305] *TikTok. Account Safety: https://support.tiktok.com/en/safety-hc/account-and-user-safety/account-safety*

[306] *The Oversight Board is now accepting cases. October 2020: https://www.oversightboard.com/news/833880990682078-the-oversight-board-is-now-accepting-cases/*

[307] *Oversight Board Charter: https://www.oversightboard.com/governance/*

RECOMMENDATIONS FOR THE SECTION 5:

5.1. General requirements

OBJECTS OF LEGISLATIVE INITIATIVE:

– to develop legislative initiatives aimed at regulating Internet intermediaries to take into account their diversity and need, apply various regulatory measures, as well as properly apply the rules for establishing jurisdiction over Internet intermediaries;

SUBJECTS OF LEGISLATIVE INITIATIVE:

– to provide in the current legislation the obligation of private companies to respect human rights and create their domestic policies based on international standards in this area.

5.2. Transparency and accountability

SUBJECTS OF LEGISLATIVE INITIATIVE:

– to provide in the legislation for the obligation to publish statistics of law enforcement agencies' appeals to the largest Internet intermediaries with requests to remove content, pages or resources, or with requests for access of personal data;

LAW ENFORCEMENT AGENCIES:
(NATIONAL POLICE, SECURITY SERVICE OF UKRAINE):

– to publish statistics of appeals to the largest Internet intermediaries with requirements to delete this or the other content, page or resource;

INTERNET INTERMEDIARIES:

– to disclose more information about their own algorithms and their application to the content.

5.3. Protection of expression freedom

INTERNET INTERMEDIARIES:

– to provide more clarity on the mechanism for imposing sanctions for violations of community standards so that users can regulate more clearly their own behavior.

5.4. Privacy and data protection

LAW ENFORCEMENT AGENCIES (NATIONAL POLICE, SECURITY SERVICE OF UKRAINE):

– to publish statistics of appeals to the largest Internet intermediaries with requirements to provide access to information about their users;

INTERNET INTERMEDIARIES:

– to publish generalized information on the consideration of requests of state authorities about the access to information about their users, which, besides statistical data, will include information about the grounds for denying such requests, types of violations in connection with which the relevant requests for access were submitted.

5.5. Access to effective remedies of legislative protection

SUBJECTS OF THE LEGISLATIVE INITIATIVE:

– to provide mechanisms for effective protection of the rights of consumers of provided services by Internet intermediaries, in particular by obliging such intermediaries to establish effective protection mechanisms on the platforms;

INTERNET INTERMEDIARIES:

– to establish mechanisms for appealing content decisions on their own platforms.

CONTENTS

PROLOGUE

The world and Ukrainian trend of the 2010-s is full digitization. With the Internet access and devices whereby one can benefit the World Wide Web services becoming more affordable, online threats have increased. Where there are threats to civilians, the State very often and very quickly emerges and seeks to eliminate those threats. However, very often such attempts end up in their opposite and result in the violation of digital rights.

The Internet, as an environment for the realization of human rights, is also unclassified: in addition to the relationship between the State and the user, the role of such actors as Internet intermediaries is important. They may also violate human rights in their activities by unlawfully transmitting personal data to third parties, blocking users' access to websites, or not removing content containing a language of hostility. However, they are often beyond the reach of the State, because they are not under its jurisdiction.

This report was created to initiate a tradition to hold an annual complex analysis of the state of regulation of the triangle system "State – User – Internet Intermediary" in Ukraine. We have tried to outline the current regulation of legal relations arising from Internet use in Ukrainian as a starting point for further research, as well as to describe the main trends of such regulation during 2020. To that end, we have analyzed draft legislative and governmental initiatives published during the year, adopted acts as well as case laws, and formulated recommendations to the responsible authorities, with the hope of implementing at least some of them in 2021.

The conclusion of our analysis is encouraging: despite the continuation of illegal practices of websites blocking, legislative spam with new proposed categories of illegal Internet content, as well as some major acts, aiming at comprehensively regulating certain issues (in the sphere of media, in the activities of the intelligence services, in the sphere of electronic communications, etc.), which contain threats to human rights, in 2020 a significant deterioration of the situation was avoided. Despite this, the risks remain, and we can only hope that the 2021 report will not have to analyze the negative impact of bills that would have become laws.

Contacts:
Yaropolk Brynykh
yaropolk.brynykh@abaroli.org
+38-063-241-20-87