Digital Security Lab
FreeNet Ukraine Coalition

DIGITAL RIGHTS AGENGA FOR UKRAINE

The document has been developed as part of the Digital Rights Agenda for Ukraine project funded by the United States Agency for International Development (USAID) through Counterpart International

September 2019

Digital Rights Agenda for Ukraine / Vita Volodovska, Maksym Dvorovyi — Kyiv: NGO Digital Security Lab Ukraine, 2019. — 56 p. This publication was prepared and published as part of the Digital Rights Agenda for Ukraine project funded by the United States Agency for International Development (USAID) through Counterpart International. The views expressed in this publication reflect the views of the authors and do not necessarily reflect those of USAID and Counterpart International.

Kyiv, 2019

Contents

DIGITAL RIGHTS ARE HUMAN RIGHTS

As its primary commitment, the Government shall promote and guarantee human rights and freedoms. This principle underlies democracy and is proclaimed in Article 3 of the Ukrainian Constitution. The same Article states that human rights and freedoms, and assertion thereof, should determine the content and directions of Government's acts.

Development and expansion of the Internet have brought about unprecedented tools for communities to enjoy their rights and freedoms, including opportunities of free expression of their opinions and thoughts before a wider public, and prompt access to any information available online. At the same time, the threats related to abuse of such rights, spreading of hate speeches and unlawful interference with the right of privacy, have increased.

In its recent Resolution 38/2018[1], the Human Rights Council emphasized, once again, that *'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 of the International Covenant on Civil and Political Rights'.*

The Council of Europe, in its documents and in the judgements of the European Court of Human Rights ("the European Court"), held that Member States should guarantee to everyone within their jurisdictions the rights and fundamental freedoms provided for in the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter also referred to as "the European Convention"), including those in the area of Internet. In the Case of *Ahmet Yildirim v. Turkey*[2], the European Court reported 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'*.

The term 'digital rights' is quite often used with reference to online human rights; however, such use is not justified in theory. As a matter of fact, freedom of speech or privacy has been long included into the list of fundamental human rights in a number of international acts — the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention for the Protection of Human Rights and Fundamental Freedoms — and shall be

---

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 CASE OF AHMET YILDIRIM AND OTHERS v. TURKEY no. 3111/10, 18 December 2012: http://hudoc.echr.coe.int/eng?i=001-115705

protected irrespective of the way or areas of their exercise. The right to freedom of expression is still a right, whether information is communicated verbally, in a newspaper, or at a website. At the same time, emergence of such potential 'digital right' as the right to Internet access, and the definition of 'the right to be forgotten' (the right to demand removal of the information in respect of a person from search engine results) are quite new[3].

From a practical perspective, the 'digital rights' concept should be treated as a conventional category covering the specificity of fundamental human rights exercising and protection on the Internet (in particular, online freedom of expression and online privacy right), rather than as a separate group of human rights. Considering the crucial role of the Internet in the modern world, defining such category helps better systemize and study the needs of protection of online human rights, with separate protections of such rights being currently scattered in various guidelines, resolutions and other acts of international institutions.

Although the majority of Internet related rights and freedoms are already covered by the protections provided for in the currently effective international acts, such protections are rather minimum ones, whereas more substantial guarantees require time to develop in case law, in particular, in judgements of international courts. As a consequence, implementation and protection of online rights and freedoms presently require close attention of national authorities, legislative support of online human rights protections and applying of the relevant principles in administrative and judicial practices.

This Agenda sets forth recommendations with respect to the implementation, improvement and enhancement of guaranteed protections of online human rights and freedoms. In particular, this document includes suggestions concerning safeguards for the right of Internet access, freedom of expression, privacy and personal data protection rights, and outlines the current challenges of Government's involvement in ensuring the respect of human rights by private corporations.

It is also equally important to emphasize separate general recommendations aimed at contributing to better awareness of authorities and communities in respect of online human rights enjoyment.

[3] This right was first clearly distinguished in the Case of Google Spain v AEPD and Mario Costeja González heard by the European Court of Justice in 2014.

General recommendations on the enhanced protection of online human rights:

1. Presently, no systemic monitoring and analysis of online human rights enforcement is in place in Ukraine. *The Human Rights Commissioner of the Verkhovna Rada of Ukraine*, as the official in charge of the Parliament's control of respecting of constitutional human rights and freedoms and civil rights, is recommended to develop and implement the system of monitoring and assessment of digital human rights enforcement.
2. *The Verkhovna Rada of Ukraine*, in particular, the Parliament's *Committee for Humanitarian and Information Policy, Committee for Digital Transformation and other committees* in charge of the information, information safety and information technologies governmental policies, are recommended to start dialogue with experts and human rights advocates in respect of legislative and other initiatives aimed at regulating of public relations in the Internet through launching of a task force or holding of working meetings to prevent infringements of human rights in the course of development and implementation of such initiative, and to make a clear and balanced concept of regulating of the relations appertaining to information dissemination in the Internet.
3. *The Cabinet of Ministers of Ukraine (the Ministry of Justice, the Ministry of Internal Affairs, etc.)* is recommended to develop and include into the education programs of public officers and law enforcement officials certain issues of information technologies development and enforcement of online human rights.
4. *The National School of Judges of Ukraine* is recommended to integrate and include trainings related to information technologies development and enforcement of online human rights into the programs of judge qualification obtaining.
5. *The Ukrainian Ministry of Education and Science* is recommended to develop and ensure integration into school curricula of the mandatory components of Internet and media competencies; and ensure inclusion of the relevant components into teacher training and skill improvement programs.

RIGHT TO INTERNET ACCESS

Internet access is an integral part of enjoyment of human rights and freedoms and involvement in decision making processes of governmental regulation. The right to Internet access has not been yet officially recognized worldwide as a human right, although international institutions systematically emphasize the crucial role of the Internet in a democratic society. Availability of Internet access is seen as the factor that contributes to enjoyment of other human rights and freedoms, in particular, online freedom of expression.

In 2003, the Committee of Ministers of the Council of Europe stated, in the Declaration on freedoms of communication on the Internet, that member states of the Council of Europe should foster and encourage access for all to Internet services on a non-discriminatory basis at an affordable price[4]. In 2014, in Recommendation CM/Rec (2014)6, it was also emphasized that people who rely on the Internet for their activities have a legitimate expectation that Internet services are accessible, secure, reliable and provided without discrimination[5]

On July 10, 2019, the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, published the annual *Joint Declaration on Challenges to Freedom of Expression in the Next Decade.* It was the twentieth joint declaration of international institutions' representatives and the first one directly calling states to consider Internet access as a human right, since the ability to be online is a must in enjoyment of freedom of expression. The document asserts that exercising freedom of expression requires a digital infrastructure that is robust, universal and regulated in a way that maintains it as a free, accessible and open space for all stakeholders[6].

It's worth mentioning that the 'right of Internet access' already finds its legal implementation in certain states. For instance, in Brazil, a special act adopted

---

4 Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5.

5 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies): https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f3d.

6 Joint Declaration on Challenges to Freedom of Expression in the Next Decade: https://www.osce.org/representative-on-freedom-of-media/425282?fbclid=IwAR2IkGPrxvjhlShXZrJJX_sQa2yoKTiXlprzIi6ZPDCuIeyijAWL9AQERaA.

in 2014 — *The Internet Bill of Rights*[7] — proclaims that ensuring Internet access for all is the purpose of such governance. In 2009, the Constitutional Council of France also admitted Internet access as a fundamental human right, stating that the provisions in respect of possible automatic and extrajudicial Internet disconnection for persons committing offences, as suggested in the French Act of Internet Intellectual Property Rights Protection, should be cancelled[8]. In Greece, the right to Internet access, formulated as the right to participate in the Information Society and access to electronically transmitted information, is provided for in the Constitution[9].

The right of Internet access, as the right for everyone to freely use the safe and open Internet, shall cover two aspects:

The first aspect is that governments should be prohibited from unjustified restriction of Internet access, in particular, Internet denial and disconnection all over the country or in certain regions thereof. Blocking of Internet access for certain persons may be justified by valid and sufficient reasons only. For instance, the European Court of Human Rights, in the Case of *Kalda v Estonia* concerning the denial of prisoner's access to a number of official websites containing electronic versions of statutory acts, court judgements and awards of the European Court of Human Rights, held that imprisonment inevitably results in prisoner's restricted communication with the outside world. At the same time, although Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms does not impose the obligation to provide access to the Internet or to specific Internet sites for prisoners, the Estonian law, in general, permits prisoners' access to certain websites containing law related information from specially secured computers. Therefore, interference with the rights of the Applicant took place. Such interference was found to constitute an infringement of Article 10 of the Convention, since the domestic courts undertook no detailed analysis as to the security risks emerging from the Applicant's use of the relevant websites. Noticeably, in paragraph 52 of its Judgement, the European Court emphasized that '*Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to attain universal access to the Internet and to overcome the digital divide*'[10].

---

7 Law no. 12.965 of April 23, 2014. Learn more about the Law at https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf

8 Decision n° 2009-580 of June 10th 2009: https://edri.org/edri-gramnumber7-123-strikes-censured-council-constitutional/

9 Constitution of Greece (in English): https://www.wipo.int/edocs/lexdocs/laws/en/gr/gr220en.pdf

10 CASE OF KALDA v. ESTONIA, no. 17429/10, 19 January 2016

The second aspect of this right calls upon governments to take all reasonable efforts to ensure the best access of their communities to the Internet, for instance, to develop and implement a specific and efficient policy to make the Internet commonly accessible, open and provided at an affordable price for all community groups. Specific forms of contribution may cover low-income communities and disabled people. In addition, full enjoyment of this right by communities is also conditional upon access to technology information and digital competencies — the ability to get knowledge and skills from the Internet use in satisfying of their needs.

The right to Internet access shall be based on several significant principles:

- *Inclusiveness and non-discrimination.* Access to the Internet should be provided at a reasonable price and on a non-discriminative basis. Interactions on the Internet should be free from any discrimination based on sex, race, skin color, language, religion or belief, political or other convictions, nationality or social background, belonging to a national minority, material condition, origin or any other status, including, in particular, ethnicity, age or sexual orientation. The government should also contribute to promotion of online cultural and language diversity, and ensure technical abilities of Internet access for vulnerable communities, for instance, through the support of public access points (such as libraries, training centres, schools, etc.).
- *Internet neutrality*. All users shall have the ability to freely choose the computer system, applications, software, etc. Internet architecture, communication systems and formats shall be based on public standards that ensure interoperability, inclusiveness and equal abilities — free information exchange.
- *Internet safety*. The government shall guarantee Internet safety. At the same time, it should be noted that technical standards related to the Internet infrastructure shall not be applied for censorship or unlawful supervision. Technical features that enable security agencies' remote access to the equipment (for example, as it is implemented in Russia and was suggested in Ukraine[11]) are inconsistent with the democratic values.
- *Service quality*. Guaranteed Internet access shall be consistent with the level of modern technology development and dissemination.

[11] Legal Analysis of the Draft Law 'On Amending Certain Laws of Ukraine on Countering Threats to National Security in Information Sector', Registration No. 6688: https://www.ppl.org.ua/yuridichnij-analiz-vid-koalici%D1%97-za-vilnij-internet-proektu-zakonu-6688.html

Presently, the Ukrainian legislation does not provide for the right of Internet access. The Ukrainian Act of Telecommunication sets forth the list of generally accessible telecommunication services; however, it includes only universal access to general fixed-line network connections, local telephone communication, emergency calls, inquiry services and public pay-phone communications. Simultaneously, Ukraine is gradually developing communication access technologies and expects the 5G technology release in 2020[12], despite the fact that a significant part of Ukraine is not yet covered by 3G and 4G communication technologies[13]. The Government is taking separate deregulation measures to enhance the broadband Internet coverage[14], and has allotted UAH 1 billion to ensure Internet access at schools[15]. However, no well-targeted measures to enhance Internet access are currently implemented. Nevertheless, according to numerous studies, the Ukrainian Internet service is still one of the cheapest in the world[16].

[12] Presidential Decree No.222 / 2019 «On the provision of conditions for the implementation of the fifth generation mobile communication system": https://www.president.gov.ua/documents/2422019-26881

[13] https://www.mobua.net/maps/?pos=48,31,6

[14] The government has simplified access to telecommunications networks for businesses: https://www.kmu.gov.ua/ua/news/u-ramkah-deregulyacijnogo-zasidannya-uryad-sprostiv-dostup-do-telekomunikacijnih-merezh-dlya-biznesu-ta-pravila-pracevlashtuvannya-inozemciv

[15] The Government allocated 1 billion UAH on internetization and computerization of Ukrainian schools https://mon.gov.ua/ua/news/uryad-spryamuvav-1-mlrd-grn-na-internetizaciyu-ta-kompyuterizaciyu-ukrayinskih-shkil-liliya-grinevich

[16] Ukraine has world's cheapest broadband internet: https://emerging-europe.com/news/ukraine-has-worlds-cheapest-broadband-internet/; https://www.kyivpost.com/technology/ukraines-mobile-internet-one-of-worlds-cheapest.html.

Recommendations on Internet access:

1. *The Verkhovna Rada of Ukraine*, in particular, the Parliament's *Committee for Humanitarian and Information Policy, Committee for Digital Transformation,* and *the Ukrainian Cabinet of Ministers* are recommended to give consideration to the issue of possible and required integration into the laws of the right and guarantees of Internet access in Ukraine;
2. *The Ukrainian Cabinet of Ministers (the Ministry of Digital Transformation of Ukraine)* is recommended to ensure the independent analysis of users' access to the Internet in Ukraine, in particular, the Internet coverage level and connection speed;
3. *The Verkhovna Rada of Ukraine (the Committee for Digital Transformation*) and *the Ukrainian Cabinet of Ministers (the Ministry of Digital Transformation of Ukraine)* are recommended to procure favorable conditions for development of the Internet access infrastructure, including through the simplified regulation of the telecommunication service market, and alignment of the domestic laws with the EU laws in pursuance of the EU-Ukraine Association Agreement;
4. *The Ministry of Digital Transformation of Ukraine* is recommended to contribute to Internet access in rural areas and geographically remote localities, and develop special programs aimed at the support of Internet access for low-income communities and disabled people.
5. *The Verkhovna Rada of Ukraine and the Ukrainian Cabinet of Ministers* are recommended to avoid initiating draft laws or measures purporting obstacles or blocking of Internet access, telecommunication networks.
6. *The Ministry of Digital Transformation of Ukraine* is recommended to guarantee respect of human rights and, in particular, of the 'privacy by default' principle, in the course of implementation of new technologies, development of the "Internet of Things" (IOT), etc.

FREEDOM OF EXPRESSION ONLINE

Freedom of expression is one of the most important foundations of a democratic society and one of the key conditions for its development and self-actualization of each person. In the light of the accessibility and the possibilities of storage and transmission of large amounts of information, the Internet plays an important role in expanding of the public access to news and contributes to the dissemination of information in general. Freedom of expression includes the right to freely search, receive and disseminate information and ideas online, the scope and essence of exercising of which correspond to the similar right of free expression of opinions in an offline environment.

Public authorities must not only refrain from impeding the exercise of the human right to freedom of expression, but shall also create the necessary conditions for such exercise. The European Court of Human Rights in its judgment in the case of *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* recognized that Article 10 of the European Convention places positive obligations on states to establish the necessary legal framework to ensure the proper protection of the right to freedom of expression on the Internet.

The Coalition for the Free Internet performed an analysis of all legislative initiatives in the area of freedom of expression on the Internet that had been registered in the Verkhovna Rada of Ukraine of the previous convocation, the eighth one[17]. The analysis of the bills and the course of consideration thereof by the parliament showed the lack of efficient interaction between representatives of the government agencies, civil society, business (in particular, telecommunication providers) and media. Virtually all legislative initiatives aimed at establishing regulatory mechanisms on the Internet were developed without the proper involvement and discussion of the interests of the various groups. As a consequence, the proposed bills were often duplicated, contained ambiguous definitions and disproportionate grounds and procedure for restriction of the freedom of expression on the Internet.

A number of the analyzed legislative initiatives, in particular, were aimed at bringing back criminal liability for defamation and insult. In 2001, together with the adoption of the new Criminal Code, Ukraine decriminalized defamation in accordance with the best international standards in the field of freedom of speech, since criminalization of statements inevitably leads to suppression of discussion and self-censorship of the media. Even if journalists can prove the truthfulness of the disseminated information through an independent judicial

[17] Analytical report "Freedom of Expression on the Internet: Legislative Initiatives and Practice of Examination of Criminal Cases in Ukraine in 2014-2018.": https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

examination, the mere fact of opening criminal proceedings entails many negative consequences that can seriously affect the work of the media[18].

On the other hand, in the case of fraudulent online media, the protection of the reputation of a person or the need to identify the person who spreads illegal content may get more complicated due to the lack of information about its owner or the person responsible for the editorial policy of such online media on the relevant website, or any other information necessary to file a relevant complaint. At present, Ukrainian legislation does not establish a procedure for registration of online media and any special requirements to their activities. At the same time, a considerable part of online media is registered as news agencies and statutory guarantees of freedom of activities and regulations on liability for violations apply to their activities. Such news agencies are required, among other things, to disclose their background information: name, information on founders and owners, the surname of the duty editor or production editor and their details, the agency's address, etc. However, the current version of the law links the disclosure of such data to "product releases", what is not quite consistent with the online media activity which is ongoing by its nature. Thus, it makes sense to revise the current legislation to increase the transparency of online news agency activities.

The current Civil Code of Ukraine, in Articles 277 and 278, sets forth the general rules for the refutation of false information or stopping the dissemination of information that violates a person's personal non-property rights. At the same time, the provisions of the code do not contain any specific rules on protection against false information disseminated online. Applying the said provisions in practice, courts often resort to obliging the defendant to refute and exclude false information at the same time, that is often an excessive and unjustified measure. In view of this, there is a need to generalize and analyze the court practice in cases of protection of honor, dignity and business reputation on the Internet and to prepare appropriate recommendations for courts.

Furthermore, the practice of blocking access to individual websites based on the decision of investigating judges within the framework of measures for securing the criminal proceedings is becoming widespread. Thus, on July 23, 2019, the investigating judge of Pecherskyi District Court of Kyiv, within the framework of the criminal case No. 757/38387/19-к passed the determination to attach the intellectual property rights arising for the Internet users in the

[18] Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression on Freedom of Expression and the Administration of Justice, Commercialisation and Freedom of Expression and Criminal Defamation (2002): https:// www.osce.org/fom/99558?download=true

course of use of 19 websites (including blogs.korrespondent.net, enigma.ua, etc.) by obligating a number of large Ukrainian Internet providers to block the access to them[19]. Said determination doesn't conform[20] to requirements of the law of criminal procedure for determining the material evidence that may be attached and requirements of current law on obligations of telecommunication service providers who may block the full access to certain resources only in cases of spreading of child pornography. Instead, such court practice opens the door for extremely serious abuses and violations of the freedom of expression online and should be carefully reviewed.

The right of citizens to information also includes the right to access to public information, i.e. information held by state and local authorities. In 2015, the Law of Ukraine "On Access to Public Information" was supplemented by Article 10-1, which established the obligation of the owners to publish public information in the form of open data — in a format that allows for its automated processing by electronic means, free and no-charge access to it, as well as its further use. The Cabinet of Ministers of Ukraine also approved the relevant List of Data Sets[21], which must be published by each government body. In 2018 the State Agency for Electronic Governance launched the updated Open Data Portal[22]. At the same time, the analysis of fulfillment of legal requirements by owners shows that not all open data are duly published[23]. Furthermore, in order to fully secure the right of citizens to information, it is important that the data be regularly updated and be of good quality, in particular be published in formats that are most conducive to re-use and integration with data from other registers.

The Internet has created unprecedented opportunities for sharing information. At the same time, such access to knowledge is inevitably fraught with serious risks and threats, such as, for example, threats of violence and hate speech, as well as coordinated campaigns to spread misinformation, which generally complicates access to truly valuable information and undermines confidence in mass media.

Because of this, the right to freedom of expression online is not absolute and may be restricted. However, any regulation and legal restriction on digital rights must be developed in a transparent, open and inclusive manner, with the participation of representatives of not only government bodies but also civil

---

19 https://korrespondent.net/ukraine/4124650-pecherskyi-sud-zablokyroval-desiatky-smy-v-ynternete

20 https://hromadske.ua/posts/pecherskij-precedent-za-sho-namagayutsya-zakriti-19-veb-sajtiv-odniyeyu-uhvaloyu-sudu

21 https://zakon.rada.gov.ua/laws/show/835-2015-п - n12

22 https://data.gov.ua/

23 http://texty.org.ua/pg/article/Oximets/read/95708/Derzhorgany_zvolikajut_z_opryludnennam_naboriv_vidkrytyh_danyh

society and business. The restrictions imposed should not be interpreted too broadly and should meet the set of criteria established by the European Court of Human Rights, judgements of which are binding in Ukraine:

1. Legitimate objective of the restriction

The Constitution of Ukraine reckons among such legitimate interests in the course of restriction of freedom of expression, for example, the interests of:

- national security,
- territorial integrity or public order to prevent unrest or crime,
- public health protection,
- protection of the reputation or rights of other people,
- prevention of disclosure of information obtained as confidential,
- maintenance of authority and impartiality of the system of justice

Similar grounds are determined by the European Convention (which also adds moral protection) and the International Covenant on Civil and Political Rights.

This criterion is almost always met, because the categories are defined quite broadly. Thus, publishing of a journalistic investigation into corruption in the defense sector may be prohibited on the pretext of protection of reputation and national security. That is why it is important to consider all conditions for restrictions taken together. Most of the discussions about the legitimacy of restrictions relate precisely to the following two criteria.

2. Legality

A restriction must be prescribed by law. The law must be promulgated according to the established procedure and meet the quality requirements — be accessible, clear, understandable and predictable. In addition, a restriction must be applied by independent bodies whose powers are established by law. In a number of cases, the European Court has emphasized the importance of judicial supervision not only of the imposition of restrictions but also of their implementation. This criterion also provides for the existence of statutory remedies against excessive restrictions, such as efficient appealing against applied measures.

3. Necessity in a democratic society

The criterion of necessity includes the need to justify the “extreme necessity” of restrictive measures, that is, what constitutes a danger to legitimate purposes, if the restriction is not imposed and why such measure is necessary to achieve the legitimate purpose. Next, the proportionality of the intervention must be ensured — the restriction should be the minimum necessary to effectively protect the legitimate purpose. Therefore, it’s necessary to find a balance between the purpose and the right being restricted: blocking the entire web resource or removal of only illegal information. Finally, the state

that restricts any right must give sufficient and adequate grounds for such intervention, that is, provide reasons for its decision.

General recommendations:

1. *To the Verkhovna Rada of Ukraine and other subjects of legislative initiative* — to ensure that any initiatives aimed at restriction of the freedom to receive and disseminate information online meet international standards in the field of human rights. The grounds and procedure for restricting the freedom to disseminate and receive information on the Internet must be clearly defined by law. Such law must be accessible, predictable and contain protection against uncontrolled actions of public authorities that will ensure enforcement of the restrictions. The restriction must meet the pressing social need and be proportionate. In particular, based on a court decision, access may be restricted only to the information that is clearly and explicitly defined by law, and not to the entire information resource where it is posted. Therewith, guarantees must be provided against excessive interference, in particular through setting of time limits for the restriction, the possibility to appeal against it fairly, etc.
2. *To the Plenum of the Supreme Court* — in order to ensure the uniform application of the rules of law when deciding on cases relating to the protection of honor, dignity and business reputation online, to generalize the practice of application of the substantive and procedural laws and to prepare relevant explanations.
3. *To courts* — when deciding whether to restrict the freedom of expression online, including but not limited with regard to defamation cases, to be guided by the above criteria of legitimacy, legality and necessity, as well as to assess the following criteria: contribution of the information to the discussion of socially important issues, the degree of publicity of the person concerned, the essence of the information, the person's previous behavior, method of obtaining information and its reliability, content, form and consequences of disclosure of the information, severity of punishment (sanctions).
4. *To the Verkhovna Rada of Ukraine (Committee on Humanitarian and Information Policy)* — to initiate discussions with experts, journalists, representatives of public authorities on the expediency of regulation of the status of online media and enhancing the transparency of their activities (disclosure of information about the owners of web resources, persons responsible for the editorial

policy, contact details for filing complaints about the materials published in the publication).

5. *To the Verkhovna Rada of Ukraine and other subjects of legislative initiative* — to refrain from any attempts to return criminal liability for defamation or other statements that may infringe upon the honor and dignity of an individual. Citizens shall have the right to freely criticize public authorities and public figures. Legislative initiatives aimed at restriction of the right of citizens to discuss issues of public interest are contrary to the democratic principles of the constitutional order of Ukraine.
6. *The Human Rights Commissioner of the Verkhovna Rada of Ukraine* - to strengthen the control over timely, complete and qualitative disclosure of public information in the form of open data, as well as proper updating of such information by administrators of public information.
7. *To the Ministry of Digital Transformation of Ukraine* — to facilitate full compliance with legal requirements for the publication and updating of sets of open data of proper quality, in order to increase government accountability, develop innovation and social impact.

FREEDOM OF EXPRESSION AND NATIONAL SECURITY

The interest of protection of the national security has always been a priority for states. For them, the security-related sphere is the area of considerable discretion, since this is the way how states must duly protect the rights of their own citizens against external threats. This legitimate aim is cross-cutting for international legal instruments that guarantee the freedom of expression and is found in both Article 10 of the European Convention (together with the aim of ensuring of territorial integrity) and Article 19 of the International Covenant on Civil and Political Rights. The provisions of Article 15 of the European Convention and Article 4 of the Covenant are also worth mentioning, which provisions allow derogation from the convention rights during an emergency situation in the state where the life of the nation is threatened, but such derogation is allowed only to the extent required by the urgency of the situation. The right to freedom of expression under both documents does not belong to the rights derogation of which is prohibited — but Ukraine did not include those rights in the relevant declarations sent to the Council of Europe and the UN. Finally, Article 20 of the Covenant, which prohibits spreading of war propaganda, cannot be passed over.

Perhaps the biggest problem with the legitimate aim of ensuring the national security is the possibility of its abuse by the state to silence (or even to turn off) opposition voices in the society. In order to remedy abuses, a careful balance must be maintained between the freedom of expression and the interest of ensuring the national security. In particular, the interpretation of this interest should be sufficiently narrow.

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information prepared in 1995[24], emphasize that if the true aim of an invocation of the protection of the national security is the protection of the "prestige of the government" or the protection against disclosure of offenses, or concealment of information about activities of government agencies, or cultivation of a certain ideology, or the suppression of peaceful protests, the restrictions will be unlawful. At the same time, they also suggest that restrictions aimed at prohibiting statements that uphold non-violent changes in the policy of the government or the government itself; criticism or offensive remarks about the nation, state or its symbols, government, its institutions, or individual government officials, or a foreign nation, state or its symbols, government, its institutions or individual government officials (except cases where it may lead to violence and cruelty); objections based on religion, conscience or beliefs

[24] Johannesburg Principles on National Security, Freedom of Expression and Access to Information, UN Doc E/CN 4/1996/39 (1996): http://hrlibrary.umn.edu/instree/johannesburg.html

to military mobilization or service, a particular conflict, or the use or threat of the use of force in the resolution of international conflicts; dissemination of information on alleged violations of international standards for human rights or rules of the international humanitarian law, should also be considered unlawful.

In 2011 in the General Comment No. 34, the United Nations Human Rights Committee also emphasized[25] that treason legislation and other regulations related to protection of the national security should only be applied in strict compliance with the requirements of the three-part test for restriction of human rights, just like anti-terrorist legislation with its rules prohibiting the support of terrorist activity and its justification.

Special mention should be made of such mechanism as sanctions or counter-measures.

In 2014, the Verkhovna Rada of Ukraine adopted the Law "On Sanctions", which provided the National Security and Defense Council with the power to take decisions on the application of special economic and other restrictive measures to foreign persons and companies in order to protect national interests, national security, sovereignty and territorial integrity of Ukraine, combat terrorist activity, as well as to prevent violation of, restore violated rights, freedoms and legitimate interests of citizens of Ukraine, the society and the state. Pursuant to this law, Decrees of the President of Ukraine No. 133/2017 of May 16, 2017, No. 126/2018 of May 14, 2018, and No. 82/2019 of March 19, 2019, which put into effect relevant decisions of the NSDC, more than 200 information resources, including the popular social networks VKontakte and Odnoklassniki, have been blocked in Ukraine.

In general, sanctions are acceptable measures to respond to violations of international law that exist in the form of aggression of the Russian Federation in the territory of Ukraine and directly threaten national security interests. The Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) provide some direction on the application of sanctions in the interstate context. According to its rules, namely Articles 50-51, countermeasures should not affect the obligations to protect fundamental human rights, and should be proportionate and relevant to the harm caused, taking into account the gravity of the international offense and the weight of the restricted rights.[26]

---

[25] General comment no 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

[26] Draft Articles on Responsibility of States for Internationally Wrongful Acts, from the International Law Commissions fifty-third session in 2001, in the YBILC (2001), vol. II, part two: http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

At the same time, the practice of blocking access to the Internet resources at the international level is considered to be inconsistent with the freedom of expression. Thus, *General Comment No. 34 to the International Covenant on Civil and Political Rights* states in paragraph 43 that any restrictions of the activity of Internet resources should be content-specific, while the general ban on the activity of individual websites and systems doesn't meet the three-part test for restriction of human rights. In the abovementioned 2011 *Joint Declaration on Freedom of Expression and the Internet*[27], principle 3 (a) states that unwarranted blocking of websites, IP addresses, ports, network protocols and certain services (such as social networks) is an emergency measure that can only be justified according to international standards (essentially, the three-part test), in particular in cases of protection of minors against sexual abuse.

The European Court of Human Rights considered a number of cases relating to blocking of web-sites by Turkey: *Ahmet Yıldırım v Turkey*[28] (blocking of Google Sites domain) and *Cengiz and Others v Turkey*[29] (blocking of YouTube and Twitter). In both cases the Court found that blocking of the websites didn't meet the standards for restriction of the freedom of expression under Article 10 of the Convention, since it hadn't been provided for by the law. Thus, the international regime on protection of human rights recognizes blocking of websites only as an exceptional measure for protection of the rights of other people and national security that is acceptable only where it is based on the relevant decision of a court or other independent competent authority and only where it is clearly and explicitly provided for by law, legitimate and proportionate to the purpose.

In its analysis[30] of the Presidential Decree No. 126/2018 On the Decision of the National Security and Defense Council of Ukraine dated May 2, 2018 "On the Application and Cancellation of Personal Special Economic and Other Restrictive Measures (Sanctions)"[31] in the part of introduction of the "prohibition for the

---

27 U.N. Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression & ACHPR Special Rapporteur on Freedom of Expression and Access to Information, International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet (1 June 2011): http://www.osce.org/fom/78309?download=true

28 Ahmet Yıldırım v Turkey App no 3111/10 (ECtHR, 18 March 2013): http://hudoc.echr.coe.int/eng?i=001-115705

29 Cengiz and Others v Turkey App nos 48226/10 and 14027/11 (ECtHR, 1 December 2015): http://hudoc.echr.coe.int/eng?i=001-159188

30 Legal analysis of the Presidential Decree No. 126/2018: https://www.ppl.org.ua/wp-content/uploads/2018/06/Legal-analysis-of-the-Presidential-Decree-on-websites-ban.pdf

31 Presidential Decree No. 126/2018 On the Decision of the National Security and Defense Council of Ukraine dated May 2, 2018 "On the Application and Cancellation of Personal Special Economic and Other Restrictive Measures (Sanctions): http://www.president.gov.ua/documents/1262018-24150

Internet service providers on provision of services of access to resources/ services, including sub-domains, to the Internet users", the Coalition for the Free Internet emphasized that application of such measures is contrary to the Constitution of Ukraine and international standards.

Obligation of providers to restrict access to certain information resources based on decisions of the NSDC on sanctions does not comply with the principle of legality. Thus, Article 39 of the Law of Ukraine "On Telecommunications" determines the obligation of telecommunication operators to block access only to the resources through which child pornography is distributed and only pursuant to the relevant court decision. The Law "On Sanctions" itself does not include such measures as "prohibition for the Internet service providers on provision of services of access to resources/services, including sub-domains, to the Internet users" in the list of sanctions (although the list is not exhaustive). At the same time, according to the Law of Ukraine "On the National Security and Defense Council", the decisions of this body shall be binding only for the executive authorities.

It should also be noted that Article 3 of the Law "On Sanctions" provides that their application should be based on the principles of legality, transparency, objectivity, consistency with the purpose and efficiency. However, neither transparent criteria for determining the grounds for blocking specific information resources, nor information on the results (effectiveness) of restricting access to those resources have been made public.

However, the Criminal Code of Ukraine establishes liability for a number of crimes related to the dissemination of statements that may be subject to legal restrictions in accordance with international standards. Thus, Article 109 of the Code prohibits public calls for the violent change or the overthrow of the constitutional order or the seizure of the state power, as well as the distribution of materials calling for such actions, and Article 110 prohibits public calls for or the distribution of materials calling for changing the borders of the territory or the state border of Ukraine in violation of the procedure established by the Constitution of Ukraine. Public calls to commit a terrorist act, as well as distribution, manufacturing or storage for the purpose of dissemination of materials with such calls (Article 258-2 of the Code), and public calls for aggressive war or initiation of a military conflict (Article 436) are also prohibited. Thus, the decision to restrict access to information that threatens the national security must be based on the results of relevant criminal investigations that prove the illegality of such content. The purpose of protection of the national security can be fully achieved only when the criminal activity itself is stopped, because under the current conditions blocking of any site can always be bypassed or a new site that distributes the same content can be created quickly.

At the same time, the analysis of the court practice in criminal cases relating to the above categories of statements shows that there is no well-grounded and systematic approach to their resolution.[32]

First, courts do not carry out an independent analysis of the statements that are the subject of consideration, but confine themselves to giving the thesis on a specialist or expert's opinion on the content. Thus, the fact of committing a crime is determined not by a court, but rather by a forensic expert, who provides an assessment of the content of the disseminated message, and the role of the court is often reduced only to statement of the fact of a criminal offense and imposition of a punishment. Giving a proper justification in court decisions instead of listing the facts in the case, the evidence received and examined, the procedural aspects and citing of the rules of the law is a proper guarantee of a fair legal trial under Article 6 of the European Convention on Human Rights — and therefore, failure to comply with this guarantee significantly influences the possibility to appeal against the decision later.

Secondly, courts do not independently analyze the impact of the content on social media users. There is no analysis of the potential impact on the national security in the decisions, and courts themselves rarely seek to differentiate between the content that poses a threat to the national security and hate speech. As a consequence, posts in social networks that are very similar in content may be differently qualified, and this creates inconsistent practice.

Thirdly, in eight sentences under Article 109 of the Criminal Code, courts qualify the Internet as mass media — and this, in turn, entails a more severe sanction, since the dissemination of such calls in mass media is an aggravating circumstance. This approach is non-uniform and threatening, since violators receive additional punishment for acts, they have not committed. In addition, despite the availability of online versions of traditional media, it is difficult to qualify all websites as mass media by their nature.

Thus, the priority in the process of protection of the national security of Ukraine should be the improvement of the law enforcement and judicial practice in investigation of crimes related to dissemination of criminal statements, rather than creation of new mechanisms to block information resources, which can lead to censorship and human rights abuses.

[32] Analytical report "Freedom of Expression on the Internet: Legislative Initiatives and Practice of Examination of Criminal Cases in Ukraine in 2014-2018.": https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

Recommendations on freedom of expression and national security:

1. *To 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 applying sanctions in conformity with the Constitution and international obligations of Ukraine, in particular with regard to limiting the access of users to the information resources determined by the decrees of the President of Ukraine;
2. *To the Verkhovna Rada of Ukraine* (*Committee on Humanitarian and Information Policy)* — to revise the current legislation in the field of information and develop transparent mechanisms for content assessment for its threat to the national security instead of disproportionately banning broad categories of statements, and to establish the temporality of restrictions imposed on information dissemination in connection with the aggression of the Russian Federation and the procedure for periodic assessment of their expediency with publishing of the results of such assessment for the society.
3. *To the Verkhovna Rada of Ukraine* — to ensure that international human rights standards are complied with in the course of development and consideration of any legislative initiatives aimed at restricting or stopping the dissemination of information that threatens national security interests. In particular, the possibility of restriction of access to individual websites is only permitted as an exceptional measure in the case of distribution of child pornography or other criminal content by such websites, when such content constitutes the vast majority of the material placed on the resource. In doing so, the grounds for blocking should be clearly defined by the law, applied in accordance with the adequate legal procedure, and only if less restrictive alternative measures cannot be applied. Restrictions should be based on a court decision.
4. *To the Verkhovna Rada of Ukraine* (*Committee on Humanitarian and Information Policy*, *Committee on Environmental Management, Committee on Freedom of Speech*) — to revise the rules of criminal law and decriminalize certain types of statements that do not contain calls for violent acts, including the use of certain symbols as propaganda of totalitarian regimes (to substitute for administrative responsibility). Any legislative proposals regarding the prohibition of certain ideas or symbols

need to be open and subject to proper public consultations. The provisions of the law must be sufficiently specific and clear to enable a person, with sufficient certainty, to anticipate the lawfulness or illegality of his/her actions in advance, and to prevent arbitrary intervention of public authorities. Only actions that pose a real threat to the society should entail criminal liability which should be proportionate to the gravity of the committed crime. Non-violent displays of freedom of expression should not be punishable by imprisonment.

5. To the *Verkhovna Rada of Ukraine and the Cabinet of Ministers of Ukraine* - to promote the development and ensure the implementation of scientific researches in the field of information threats, on the basis of the results of which the state bodies will be able to develop adequate and effective measures to protect national security
6. *To the Security Service of Ukraine* — to develop and ensure the implementation of instructional guidelines on investigation of crimes in the field of the national security relating to dissemination of illegal calls and information.

FREEDOM OF EXPRESSION AND HATE SPEECH

Hate speech is one of the absolutely forbidden categories of statements that is not protected in the international and national law. At the international level (and at the level of mandatory documents), this prohibition was first enshrined in Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (in the narrower context) and in Article 20 of the International Covenant on Civil and Political Rights: "*Any statement in favor of national, racial or religious hatred, which is inciting discrimination, hatred or violence, must be prohibited by law*." As we can see, such wording does not give a clear definition of hate speech, but it does establish the requirement to provide for a prohibition on the use of certain categories of statements in the national law of states. It will be recalled that Ukraine ratified both documents as early as the USSR in 1969 and 1973 respectively, without any reservations in respect of the relevant provisions.

Despite the general nature of the terminology used in said documents, international organizations later developed a number of tests and criteria on the basis of which the existence or absence of hate speech should be assessed. The Rabat Plan of Action approved by the UN General Assembly in 2012[33] proposes a six-part test to determine the "gravity" of hate speech:

1) *the content of the statement* which must place it in a dominant socio-political situation with respect to the targeted social group as of the time of the statement;

2) *the status of the speaker*, and his / her ability to influence the audience;

3) *the presence of intent* on the part of the person to incite a specific group of persons, since negligence cannot lead to incitement as such within the terminology of Article 20 of the International Covenant*;*

4) the content and form of the statement, which are key elements for analysis;

5) the extent of the dissemination of the statement, including the analysis of the number of the audience to whom the statement was delivered, the method of its dissemination, whether the statement was public and accessible to the general public, etc.;

6) the possibility and inevitability of occurrence of consequences after the statement, which should be assessed by the state authorities in the course of analysis of a certain statement through the prism of the standard of reasonableness.

[33] UNHRC, 'Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence' (2012), http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

Only a cumulative analysis of the relevant elements can make it possible to understand whether one or another statement can be qualified as hate speech. Another test was developed by the European Court of Human Rights, which in 2015, in a key decision of the Grand Chamber on the application of Article 10 of the European Convention on Human Rights — *Perinçek v Switzerland [GC]* — which identified some other criteria for analysis, summarizing its own practice in such cases. The Court separately emphasized that it is the interrelation between various factors and not the emphasis on any of them that must be decisive.

Thus, in paragraphs 204-207 of the judgment[34] the Court specified that it took into account:

1) whether the statements were expressed against a tense political or social background;

2) whether expressions that are reasonably interpreted and considered in their immediate or wider context can be taken as a direct or indirect call for violence or as justification for violence, hatred or intolerance;

3) the manner in which the statements were made and their ability - direct or indirect - to cause harmful consequences.

The European Court of Human Rights divides cases of hate speech into two categories: those that fall under Article 17 of the Convention (abuse of rights) and are not protected under any circumstances, and those in which statements are not explicit abuse and need to be analyzed for compliance with the three part test for restrictions under paragraph 2 Article 10 of the Convention. The first category usually includes cases in which statements deny Nazism crimes, promote terrorism, anti-semitism, or call for the establishment of a totalitarian ideology.

In the context of the Internet and application of Article 17 of the Convention, consideration should be given to the judgement in the case of *Belkacem v Belgium*.[35] The applicant, the head of Sharia4Belgium (Sharia for Belgium) organization, who posted a series of videos on YouTube calling for jihad and fighting against the infidels, and made comments calling for the deaths of Belgian politicians, was sentenced to a fine and a year and a half of imprisonment for the calls for discrimination, segregation, hatred and violence against non-Muslims. His complaint to the Court regarding the violation of the rights under Article 10 of the Convention was dismissed: the European Court agreed with the findings of the national courts and confirmed that the videos in which the applicant was calling to dominate non-Muslims, to teach them

[34] Perinçek v Switzerland App no 27510/08 (ECtHR, 15 October 2015): http://hudoc.echr.coe.int/eng?i=001-158235

[35] Belkacem v Belgium App no 34367/14 (ECtHR, 27 June 2017) (dec): http://hudoc.echr.coe.int/eng?i=001-175941

a lesson and to conquer them constitute a general and violent attack against the values of tolerance, social harmony and non-discrimination, which are the foundations of the Convention. Given also the conformity of the Belgian law with European standards in this field, the Court declared the application inadmissible.

Speaking of the second category of cases in the field of digital rights, the main judgment that is worth paying attention to is the judgment in the case of *Savva Terentyev v Russia*.[36] In this case, the applicant became the victim of the first ever application of the provisions on hate speech to comments on the Internet in the history of Russia. In fact, the applicant himself commented on a blogger's LiveJournal blog post about searches in the local newspaper in the pre-election period. The comment header was the expression "*I hate the cops, for fuck's sake*"; while the comment itself read "*It would be great if in the centre of every Russian city, on the main square ... there was an oven, like at Auschwitz, in which ceremonially every day, and better yet, twice a day… — infidel cops would be burnt. … this would be the first step to cleansing society of this cop-hoodlum filth*". Russian courts justified the applicant's conviction by the fact that he definitely incited violence against such a social group as Russian police officers, and deliberately posted his comment under the blog which had more readers than his own. They also noted that his statements were particularly dangerous to the national security because they contradicted the principles of the constitutional system — and this was the reason for the punishment in the form of imprisonment with probation.

The European Court, taking into account the Perinçek test, stated that, in the context of this case, it focused on examination of the nature of the applicant's statements, the context of their publication, their potential to lead to adverse consequences, and the analysis of the motivation behind the decision of the Russian courts. The Court noted that although the comments and comparisons were quite rude, they should be considered as part of the style of the communication protected by the provisions of the Convention. Such comments of the applicant, made in the context of a public debate on the role of the police in interfering with the election process, were the sarcastic emotional reaction of the applicant to the actions which seemed to him to be an excess of powers on the part of law enforcement agencies; while the words about the ceremonial burning of the infidel cops were the provocative metaphor aimed not at cruelty to police officers but rather at demonstrating his desire to clear the police system of corruption. In addition, the police, as a part of the state apparatus, must tolerate greater criticism of themselves if such criticism does

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

not entail the inevitable risk of violence against the police apparatus - and such risk does not arise from the circumstances of the case and socio-political context of Russia of that time (2007).

The Court also laid special emphasis on the fact that the potential impact of a statement made online for a small number of readers is different from the effect of a statement published on mainstream or frequently visited web pages. However, Russian courts did not even make an attempt to establish how many users had read the comment — instead, it was the proceedings against the applicant that drew attention to this comment. Moreover, the Court also noted that Savva Terentyev had not been a popular blogger or social media user, which fact could have attracted public attention to his comment. Finally, the European Court noted that Russian courts had not made an attempt to assess the potential adverse consequences of the applicant's comment and had provided the punishment that was disproportionate. Therefore, although criminal punishment for hate speech is permissible, the relevant criminal law rules must be formulated in such a way as to prevent the excessively wide discretion of the state in accusing of committing such crimes and selective application of the relevant rules. As a consequence, the violation of Article 10 of the European Convention on Human Rights against Savva Terentyev was found — that is, the violation of his right to freedom of expression.

Thus, in addition to more general tests of the European Court of Human Rights, there are a few more key points in its practice that should be taken into account when analyzing a particular statement in the Internet for presence of hate speech:

1) the use of punishment within the framework of the criminal law for hate speech on the Internet may be acceptable;

2) at the same time, some ruder statements should be tolerated on the Internet because they are natural for communication in the network environment;

3) when analyzing Perinçek test in respect of statements on the Internet, it is necessary to determine how wide the audience of the material was and how many users saw or could have seen it;

4) the popularity of the user who posted the statement and his or her ability to influence the public will also be a significant factor.

Ukrainian law also contains a number of provisions relating to restriction of the dissemination of hate speech. First of all, it is worth mentioning Article 161 of the Criminal Code of Ukraine, which is entitled "Violation of equality of citizens depending on their race, nationality, religious beliefs, disability and other grounds" and is the closest one to the content of the prohibition of hate speech. Thus, it prohibits intentional acts aimed at inciting national, racial or religious

enmity and hatred — that, in general, is consistent with the approaches set out in Article 20 of the International Covenant on Civil and Political Rights. The punishment for committing such acts is a fine ranging from UAH 3,400 to UAH 8,500 or imprisonment for up to 5 years, with deprivation of the right to occupy certain positions for 3 years, and in the case of aggravating circumstances - up to 8 years of imprisonment. There is also Article 300 of the Criminal Code of Ukraine, which provides for the responsibility for the importation into Ukraine of works promoting the cult of violence and cruelty, racial, national or religious intolerance and discrimination, for sale or distribution, or their production, which may be punished by imprisonment for 3 years, and in the case of aggravating circumstances — imprisonment for up to 5 years.

The prohibition on such statements is also provided for by Article 28 of the Law of Ukraine "On Information" ("information may not be used for calls for violence, cruelty, incitement of interethnic, racial, religious hatred") and Article 6 of the Law of Ukraine "On Television and Radio Broadcasting" ("it is prohibited to use television and radio broadcasting organizations to incite national, racial or religious enmity or hatred").

The Law of Ukraine "On the Principles of Preventing and Combating Discrimination in Ukraine" also prohibits restricting of human rights by race, skin color, political, religious and other beliefs, gender, age, disability, ethnic and social origin, citizenship, marital status and financial situation, place of residence, language and other characteristics. At the same time, the law is quite abstract and offers no effective mechanisms to counteract hate speech.

The Draft Law on Amendment of Some Legislative Acts of Ukraine (On Harmonization of the Legislation in the Field of Preventing and Combating Discrimination with the Law of the European Union) No. 0931[37], passed by the previous parliament in its first reading as far back as 2016, is under consideration of the Verkhovna Rada of Ukraine. Among the proposals of the bill, there are amendments to Article 161 of the Criminal Code of Ukraine that propose leaving criminal liability solely for deliberate acts aimed and incitement of national, racial or religious enmity and hatred, disparagement of national honor and dignity, or violation of the feelings of citizens in connection with their religious beliefs. While it is proposed to exclude direct or indirect restriction of rights or establishment of direct or indirect privileges of citizens on the basis of race, skin color, political, religious and other beliefs, gender, disability, ethnic and social origin, financial situation, place of residence, language or other characteristics from the disposition of the Article and administrative liability by supplementing the Code of Ukraine on Administrative Offenses with Article 188[48] "Violations of the Law in the Field of Preventing and Combating Discrimination". These

[37] Draft law profile: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66561

changes, according to the authors, will ensure proportionality and adequacy of liability for violations of the law in this field and will significantly simplify the procedural mechanism of consideration of cases on facts of discrimination by courts.

This approach in general corresponds to international standards on the distinction between tough and weak hate speech. At the same time, narrowing of the signs of criminal hate speech solely to national, racial or religious grounds does not cover possible dangerous calls for hatred on the basis of ethnic or social origin, language or gender characteristics.

In addition, significant problems in the enforcement of the statutory regulations on countering hate speech also need to be resolved. Over the period from 2007 to 2018, national courts adopted 14 decisions under Article 161, in which decisions the courts assessed various manifestations of hate speech. Of these, only 3 were related to the dissemination of illegal content on the Internet.[38] The small number of cases is partly due to the qualification of actions that have the signs of incitement of hatred under other provisions of the Criminal Code, which provide for greater punitive measures for crimes against the national security.

Typical of these decisions is the lack of an attempt of the courts to analyze the content of common statements on their own, not to mention the application of the practice of the European Court of Human Rights and the Perinçek test. In most cases the courts blindly rely on the conclusions of the expert examination and do not give them their own assessment: these are both comments in groups in VKontakte and posting of graphic files. The extent of dissemination of the materials, the number of subscribers of a particular user or users of a particular group are not analyzed either; as a rule, the court finds that the content was accessible to all users of social networks, and was received as a notification by friends. In addition, most cases end in a plea agreement — and therefore convicts are not punished for their actions.

[38] Analytical report “Freedom of Expression on the Internet: Legislative Initiatives and Practice of Examination of Criminal Cases in Ukraine in 2014-2018.”: https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf

Recommendations on freedom of expression and combating hate speech:

1. *To the Verkhovna Rada of Ukraine (Committee on Environmental Management, Committee on Human Rights)* — to improve the requirements of the national legislation on combating hate speech, in particular, to draw a line between criminal and administrative liability for discriminatory statements, depending on the degree of threat thereof;
2. *To courts* — when considering cases of dissemination of hate speech, to consider the following criteria for determining the presence, degree and extent of punishment for hate speech:
   - *the content and form of the statement*, which are the key elements for analysis. Therewith the peculiarities of communication in the network environment should be taken into account, in particular its higher tolerance for rude remarks;
   - *context of the statement (for example,* whether the statement was expressed against the tense political or social background)*;*
   - *status and popularity of the speaker*, and his/her ability to influence the relevant audience;
   - *the presence of intent* on the part of the person to incite a specific group of persons;
   - *the extent of the dissemination of the statement,* including the analysis of the number of the audience to whom the statement was delivered, the method of its dissemination, whether the statement was public and accessible to the general public, etc.;
   - *the possibility and inevitability of occurrence of consequences* after the statement, which should be assessed by the state authorities in the course of analysis of a certain statement through the prism of the standard of reasonableness.
3. *To the Ministry of Internal Affairs* — to ensure the development and introduction of instructional guidelines on investigation of crimes relating to hate speech and online threats. To get experts in human rights defense involved in preparing of the guidelines.

RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

The right to respect for private and family life is a fundamental right of every individual. Article 32 of the Constitution of Ukraine stipulates that no one shall experience an intrusion into his/her private and family life, and prohibits to collect, store, use confidential information about a person without his/her consent (save for cases determined by law). At the same time, just like the freedom of expression, this right is not absolute and may be limited for reasons provided for by the Constitution and laws, in the interests of national security, economic welfare and human rights. The important elements of this right are also the guarantees of protection of a person's reputation and the right of citizens to familiarize themselves with information about them which doesn't constitute state or other secret protected by law at bodies of state power, local self-government bodies, institutions and organizations.

The European Convention in Article 8 also provides that every individual has the right to respect for his/her private and family life, his/her home and correspondence. State authorities may not interfere with the exercise of this right save for cases where the interference is carried out in accordance with law and is necessary in a democratic society in the interests of national and public security or economic welfare of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The European Court of Human Rights in its case-law interprets the content of this right quite broadly, including a wide variety of aspects of development and self-actualization of a person in relations with others and the world outside. At the same time, in the context of the exercise of human rights in an online environment, it makes sense to dwell on aspects of information and communication privacy in more detail.

The right to information privacy has appeared as a mechanism of protection against uncontrolled dissemination of facts about a person's private life and provides for the protection of a person's personal data and other confidential information about him/her against their unauthorized collection, storage or distribution. Against the backdrop of rapid development of modern information technologies that make it possible to collect, process and disseminate information about virtually any person in unlimited amounts, the protection of a person's information privacy gains particular importance. To this end, positive obligations to implement personal data protection legislation are imposed on states.

A person's communication privacy consists in the right to respect for a person's correspondence, i.e. in ensuring privacy of correspondence (including electronic one), telephone conversations of the person and other communication by any means. The European Court of Human Rights interprets the notion

of "correspondence"[39] quite broadly, evolutionarily, since communication technologies are constantly developing, and limiting the scope of protection to classical methods alone will inevitably lead to undesirable narrowing of the right to privacy itself. Communication privacy is the guarantee of confidentiality of the information exchange between individuals. It is closely related but not identical to "information privacy", since here the protection is provided not only to the content of the information transmitted by communication means, but to the person's right as such to be sure that his/her conversations will not be accessible to others, regardless of the means used by such person for communication.

Any interference with the content of communication by network operators or service providers is prohibited, unless it is done for technical reasons of recording or transmitting the message, for other legitimate reasons, or for the performance of a contract concluded with the subscriber. Therewith, the data on a person collected in such manner can only be transferred to state authorities and only if this complies with the provisions of para 2 of Art. 8 of the European Convention, in particular, the transfer of the data is provided by law and necessary in a democratic society, for example, for the protection of national security or public safety, crime prevention, protection of an individual[40]. This means, in particular, that the state should not provide law enforcement agencies with uncontrolled possibilities of direct access to private communications.

Internet users have the right to anonymity and to use aliases. However, such right is not absolute. A user's identity may be disclosed pursuant to a court decision. At the same time, the law must clearly set out the grounds for disclosing such information (e.g. criminal investigation). In particular, Article 18 of the Convention on Cybercrime (Budapest Convention)[41] provides that, on the basis of a relevant order, Internet service providers may be required to disclose information about users which "means any information, in the form of computer data or any other form, that is held by the service provider, relating to users of its services, other than traffic or content data and by which the following can be established:

a. the type of the communication service used, its technical provisions and the period of use of the service;

---

[39] Copland v. the United Kingdom (no. 62617/00), 3 April 2007

[40] Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e

[41] Convention on Cybercrime (CETS No.185): https://www.coe.int/en/web/cybercrime/the-budapest-convention

b. the identity, postal or geographic address, telephones and other access number of the service user, billing and payment information, available on the basis of the service agreement or arrangement;

c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement".

At the same time, according to Article 15 of the Budapest Convention, the application of such measures must be accompanied by adequate protection of human rights and freedoms and be proportionate and include judicial or other independent supervision, the grounds justifying the application, and restrictions on the scope and duration of such powers or procedures.

In 2015, ensuring of the right to privacy was identified as one of the strategic directions of the National Human Rights Strategy[42]. The expected results included the establishment of an effective institutional mechanism for monitoring observation of the right to privacy, in particular, activities of law enforcement agencies, and the introduction of a system that precludes the creation of excessive state databases of personal data and eliminates the possibility of unlawful interference with privacy. The Action Plan[43], developed by the Cabinet of Ministers of Ukraine for the implementation of the Strategy includes, inter alia, such measures as reviewing the grounds for operational investigative measures and covert investigative activities, determining an exhaustive list of grounds precluding any abuse of such a right, preparing recommendations on compliance with the law in the field of personal data protection during the application of video surveillance systems, assessment of legal compliance, filling, administration and protection of such personal data bases, such as the Unified State Demographic Register, Register of Patients, educational registers, and making proposals on legal settlement of revealed non-conformities, etc. However, none of the above items has been fulfilled yet.

On September 2, 2019, the Draft Law "On Law Enforcement Intelligence Operations" (No. 1229, initiated by A.A. Kozhemyakin) was registered in the Verkhovna Rada of Ukraine[44]. The proposed version of the law contains clearer provisions and safeguards in respect of restriction of human rights in connection with the conduct of law enforcement intelligence operations. At the same time, the draft law still does not fully comply with international human rights obligations. Thus, the document still defines the grounds for the use of operative investigative measures (such as "*the need for intelligence information*

---

42 Decree of the President of Ukraine on the National Human Rights Strategy: https://zakon.rada.gov.ua/laws/show/501/2015

43 National Human Rights Strategy Action Plan: https://zakon.rada.gov.ua/laws/show/1393-2015-p - n13

44 Draft law profile: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66597.

in the interests of security of the society and the state") too broadly, and also provides for the possibility of using such measures in some urgent cases, not only without a court order, but even without the consent of the prosecutor. These include monitoring of information in electronic information systems and communication channels.

The Verkhovna Rada of Ukraine of the eighth convocation registered several bills aimed at expanding the powers of law enforcement bodies in respect of access to private communications. Thus, for example, the Draft Law "On Amendments to Certain Legislative Acts of Ukraine (on Improvement of the Procedure for Pre-trial Investigation" No. 1220[45] dated December 03, 2014 provided for the obligation of telecommunication operators to install the technical means necessary for carrying out of operative-investigative measures, conducting covert investigative activities by authorized units of internal affairs and security bodies and for provision of (remote) temporary access to information, held by telecommunication operators and providers, on telecommunication, subscriber, provision of telecommunication services, including receipt of the services, their duration, content, transmission routes, etc., on their telecommunication networks at their own expense and to ensure the functioning of these technical means. Therewith, the draft law proposed to establish the possibility for investigators, in certain "urgent" cases, to obtain temporary access to such information even without prior approval of the investigating judge or court. Similar provisions were also contained in the Draft Law "On Amendments to Certain Laws of Ukraine on Enhancing the Responsibility for Offenses in the Field of Information Security and Combating Cybercrime" No. 2133a[46] and the Draft Law "On Amendments to Certain Legislative Acts of Ukraine on Countering Threats to the National Security in the Information Domain" No. 6688[47], none of which was approved even in the first reading.

However, on January 21, 2019, the Administration of the State Service of Special Communications and Information Protection of Ukraine and the Security Service of Ukraine approved a joint Order No. 25/82 "*On Approval of General Technical Requirements to Technical Means for Blocking Access to a Certain (Identified) Information Resource (Service) in Telecommunication Networks*". Therewith, the Law of Ukraine "On Telecommunications", which establishes the legal basis for activities in the field of telecommunications, defines the powers of the state in respect of management and regulation of said activities, as well as

[45] Draft law profile: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=1220&skl=9

[46] Draft law profile: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55668

[47] Draft law profile: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236

the rights, obligations and the principles of responsibility of individuals and legal entities involved in such activities or using telecommunication services, does not provide for an obligation for telecommunication operators to install any technical means to block access to a certain (identified) information resource (service) in telecommunication networks.

The danger of said Order is that the technical specifications of said equipment stipulated by it will in fact make it possible to monitor, block and modify the Internet traffic of users in real time. The order reads that the equipment must ensure, in particular, the support and processing of "VoIP voice transmission technologies (Skype, Viber, WhatsApp, BBM, SIP)"; Messenger instant message and video exchange technologies (Telegram, MS Messenger, ICQ, Jabber, etc.); social networks (Twitter, Facebook, Vkontakte, Odnoklassniki, etc.); VideoStreaming adaptive video streaming technologies (Youtube, Youtube HD, Adobe RTMP, etc.). The Security Service of Ukraine, the State Service of Special Communications and Information Protection of Ukraine, or anyone else, who will control the relevant equipment, will be able to determine, on a number of grounds, which sites the user visits, as well as what messengers and blocking bypass means he/she uses and, if desired, to block them or to slow them down substantially. Therewith, there is no real opportunity to monitor compliance with the law in the course of using such equipment, given the possibility of remote access to it by law enforcement officials[48].

In the case of *Roman Zakharov v. Russia*[49], the European Court considered the Russian law that allowed the covert interception of mobile telephone communications using similar technical means. In particular, the court noted the technical possibilities for direct access to the equipment, making it possible to ensure relevant measures. The Court acknowledged that the method of covert surveillance in Russia provides the security services and police with the technical means to circumvent the authorization procedure and intercept any communications without prior court authorization. Although the possibility of abuse by unscrupulous officials can never be completely excluded regardless of the system (see Klass and Others v. Germany), the Court considers that a system such as the Russian one that allows intelligence services and police to directly intercept the communications of every citizen without even requiring them to notify telecommunication service providers. In such a system, the risk of abuse inherent in any system of covert surveillance becomes particularly threatening.

In view of this, the legislation must provide for adequate and effective safeguards against arbitrariness. This includes, in particular, clear definition of the grounds and circumstances for the interference, clear rules for stopping

[48] https://zaborona.com/interactive/nash-onlajn-leviafan/

[49] Roman Zakharov v. Russia (no. 47143/06) 4 December 2015

the interception, storage and destruction of the information received. Authorization procedures must guarantee that covert surveillance measures are applied only when they are truly "necessary in a democratic society" (suit the purpose, proportionate, grounded). Supervision of interception must meet the independence requirements, and the supervision body must also have sufficient powers and competence to carry out effective and ongoing monitoring of compliance with the law in the course of application of surveillance measures. The legislation must also provide for the possibility of protection in the event of an inappropriate application of such measures to a person.

Currently, the Ukrainian legislation does not regulate the use of such technical means for the purpose of carrying out operative-investigative measures (equally as for blocking information resources). Thus, for now there are no guarantees necessary for protection of the secrecy of communications against arbitrary interference. This is why installation of equipment with technical characteristics that provide law enforcement agencies with direct access will create opportunities for unchecked interference with our electronic communications, and is impermissible.

Recommendations on protection of a person's communication privacy:

1. *To the Verkhovna Rada of Ukraine and other subjects of legislative initiative* - to guarantee that all legislative initiatives involving the interference with the privacy by state authorities, in particular with the secrecy of electronic communications, will be subject to open and extensive discussion, including with the participation of human rights defenders, in order to ensure that the proposed restrictions comply with international standards of legality, legitimacy, proportionality, justifiability and reasonableness of restrictions.
2. *To the Verkhovna Rada* - to review the legislation in the field of operative-investigative, counterintelligence activities and criminal proceedings in order to ensure compliance of legal provisions with predictability requirements:
    - clearly and accurately worded, publicly available legislation, which makes it possible to understand under what circumstances relevant measures of surveillance and interception of information may be applied;
    - Minimum guarantees relating to restriction of discretionary powers of the state authorities: defined nature of the offenses to which the measure may be applied, the categories of persons that may be monitored, the procedure for the conduct of such actions, the maximum duration, the

procedure for analysis, use and storage of the data received, the conditions for the transfer of the data to other subjects or their destruction

- oblige telecommunication providers to disclose information about compliance with requests by law enforcement agencies to grant access to a person's data and communications, except where disclosure of such information is expressly prohibited by procedural law and is necessary in a democratic society

3. *To the Verkhovna Rada of Ukraine* (*to the Committee of the Verkhovna Rada of Ukraine on Law Enforcement)* — to ensure open and extensive discussion of the Draft Law on Law Enforcement Intelligence Operations No. 1229 in order to eliminate threats to the right of citizens to privacy and to ensure that the draft law complies with international standards;
4. *To the Verkhovna Rada of Ukraine (Committee on Digital Transformation)* — to ensure that the legislation in the field of electronic communications is brought in line with the standards of the EU and the Council of Europe, including the Convention on Cybercrime;
5. *To the Cabinet of Ministers of Ukraine, the Human Rights Commissioner of the Verkhovna Rada* — to ensure the fulfillment of the Action Plan of the National Human Rights Strategy as it pertains to the protection of an individual's right to privacy, in particular, to introduce regular annual reporting of law enforcement bodies on the use of measures connected with interference with the secrecy of electronic communications and to obligate relevant law enforcement bodies to publish said information on their web-sites.

PERSONAL DATA PROTECTION

A separate important aspect of protection of a person's privacy is the fulfillment by the state of positive obligations relating to creation of a proper legal and institutional system for personal data protection.

The Law of Ukraine "On Personal Data Protection" was adopted in 2010 and has not undergone any significant changes since then. Therewith, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in pursuance of which it was adopted, was substantially modernized in May 2018 by the relevant Protocol CM (2018)2[50]. Ukraine has not yet acceded to the Protocol, but has assumed the obligation to bring the legislation on personal data protection in conformity with EU requirements. Thus, in accordance with clause 11 of the Action Plan for the implementation of the EU Association Agreement, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 1106 dated October 25, 2017[51], it is envisaged to improve the legislation on personal data protection in order to bring it into conformity with the General Data Protection Regulation[52], which came into effect on May 25, 2018. The relevant draft law is prepared by the Human Rights Commissioner of the Verkhovna Rada of Ukraine. At the same time, taking into account the complex of social relations that will be subject to changes in the legislation, it is necessary to ensure an open process of preparing a new version of the law, including with the participation of human rights defenders.

It is the primary duty of any state party to the European Convention to introduce legal safeguards for the individual rights, i.e. there must be a proper legal regulation of privacy relations. Notwithstanding the considerable discretion afforded to states in ensuring respect for the private and family life of an individual, the standards of the European Convention must be observed. In particular, in order to protect the information privacy of an individual, States must ensure the principles of fairness, lawfulness and proportionality in collection and processing of personal data, provide for the rights and obligations of subjects of relevant legal relations, and establish bodies to monitor compliance with said principles and protect the violated rights[53].

---

[50] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[51] Decree of the Cabinet of Ministers of Ukraine "On the Implementation of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part"https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF

[52] General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

As the European Court of Human Rights noted, any storage of personal data by state authorities is considered to be an interference with the right to respect for private life[54], therefore it must be justified by a legitimate purpose without fail. In view of this, the creation and operation of any state registers must be justified by a legitimate purpose, and the list, scope of information, its use and the procedure for access to it by third parties must be clearly regulated by law.

Thus, the Constitutional Court of Ukraine in its decision[55] dated October 11, 2018, in the case on the constitutional submission from the Human Rights Commissioner of the Verkhovna Rada of Ukraine on the conformity with the Constitution of Ukraine (constitutionality) of certain provisions of paragraph one of clause 40 of section VI "Final and Transitional Provisions" of the Budget Code of Ukraine, held unconstitutional the provisions according to which: *"in the course of exercising powers of monitoring compliance with budgetary legislation as it pertains to monitoring pensions, allowances, benefits, subsidies and other social payments, the Ministry of Finance of Ukraine has the right to receive free of charge information containing bank secrecy, personal data, and access to automated information and reference systems, registers and data banks, the holders (administrators) of which are state authorities or local self-government bodies"*.

The Constitutional Court noted that the Ministry may be granted the powers to obtain and process information containing personal data only for a legitimate purpose. However, due to the absence of any limits of discretion established by the law regarding further actions with information containing personal data, even minimal protection of the personal data subject was precluded. The disputed provisions of the Code do not provide criteria for determining the content and scope of information containing personal data, categories of persons as personal data subjects, the periods of time to which the personal data should relate, the terms, procedure and conditions of their storage, i.e. there are no clear limits of the powers of the state body and that makes it impossible for the state to be held liable for possible abuses. Thus, the court found that the stated provisions did not meet the criterion of quality of the law - they contradicted such elements of the principle of the rule of law as

---

[53] Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling: https://www.garanteprivacy.it/documents/10160/10704/Recommendation+2010+13+Profiling.pdf/42ed93be-031c-4298-bed7-ae79231c7ad5?version=1.2

[54] Leander v. Sweden (no. 9248/81), 26 March 1987

[55] Decision of the Constitutional Court of Ukraine as of 11 October 2018: http://ccu.gov.ua/docs/2406

legal certainty and prohibition of arbitrariness, and that could lead to violation of the constitutional right of everyone to privacy. It is expedient to apply the criteria analyzed by the court to the analysis of the conformity of powers of state bodies and officials to the state registers and other databases containing personal data of citizens. In addition, it should also be emphasized that state bodies are required to take effective technical and organizational measures to protect confidential information against unauthorized access.

At the same time, while there is a certain regulatory framework in respect of the protection of personal information contained in state databases, the matters of collection, storage and processing of information by video surveillance systems (smart city) remain unaddressed by the legislator, depriving citizens of their ability to effectively protect their rights. Thus, only in Kyiv there are currently more than 7 thousand security cameras and according to the data of the Kyiv City State Administration this number will keep growing[56].

[56] https://kyivcity.gov.ua/news/bezpechna_stolitsya_kiv_uviyshov_u_top-50_mist_svitu_z_naybilshim_pokrittyam_kamerami_videosposterezhennya

Recommendations on improvement of the personal data protection:

1. *To the President of Ukraine, Cabinet of Ministers of Ukraine (Ministry of Justice, Ministry of Foreign Affairs) and the Verkhovna Rada of Ukraine (Committee on Foreign Policy and Inter-Parliamentary Cooperation)* - to sign and ratify the Protocol of Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), which enhances the requirements for the protection of personal data by members of the Council of Europe, and was opened for signing on October 10, 2018.
2. *To the Verkhovna Rada of Ukraine (Committee on Ukraine's Integration into the European Union, Committee on Human Rights), Human Rights Commissioner of the Verkhovna Rada of Ukraine* - to bring the national legislation into conformity with the requirements of the updated Convention and the EU General Data Protection Regulation, in compliance with the following recommendations:

   a) Transparency and inclusivity must be ensured at all stages of drafting and review of the relevant draft law. It is also advisable to conduct an international examination of the prepared document for its compliance with the CoE and EU standards.

   b) At least the following minimum standards for personal data protection must be implemented:

   - *Legality* — combination of a clear legal basis, legitimate purpose, openness and awareness of users about the processing of personal data;
   - *Validity of the purpose of processing* — specific, legal and time-bound;
   - *Data minimization* — the scope of the collected data must be relevant, not excessive and fit for the purpose;
   - *Reliability of the information* — the information must be up-to-date and accurate, users may require to update, correct or delete the information;
   - Implementation of technical security and confidentiality measures;

   c) At least the following rights of individuals relating to processing of their data must be safeguarded:

   - The right *to access information* about one's own data and their processing and the right to *clarification of information regarding processing* of the individual's personal data;

- The right *to object to processing* of personal data, in particular when it comes to using profiling algorithms;
- The right *to request the removal* of personal information that does not comply with the principles of personal data processing;
- The right *to correction of inaccurate information*;

d) Exceptions to said principles and restrictions on the rights of individuals must be specified in the law, which must include: clear and unambiguous grounds, judicial review procedure and mechanisms for redress in the case of unlawful acts.

3. *To the Verkhovna Rada of Ukraine (Committee on Human Rights), Human Rights Commissioner of the Verkhovna Rada of Ukraine, Cabinet of Ministers of Ukraine* — to ensure the creation of an independent supervisory authority in the field of personal data protection (it may also combine the functions of supervision of compliance of the law in respect of access to public information) and to provide sufficient resources for the effective exercise of its powers. In particular, the powers of the supervisory authority should include the exercise of the ability to investigate cases of violation of legal requirements and imposition of sanctions, to initiate judicial review in case of violations of the requirements for personal data processing. The supervisory authority should also assist organizations and institutions, including private companies, in observation of the law through preparing of recommendations, giving advice, etc.
4. *To the Cabinet of Ministers of Ukraine, Human Rights Commissioner of the Verkhovna Rada of Ukraine* — to ensure the fulfillment of the Action Plan of the National Human Rights Strategy, in particular, the objectives relating to personal data protection:
   - To prepare recommendations on compliance with the law in the field of personal data protection when using video surveillance systems;
   - To assess compliance with legal requirements, filling, administration and protection of such personal data bases as the Unified State Demographic Register, the Register of Patients, educational registers, and the submission of proposals on the legal settlement of identified non-conformities;
   - To revise databases maintained by law enforcement agencies in order to bring them into compliance with the requirements of the law or cancel, etc.

HUMAN RIGHTS ONLINE AND PRIVATE COMPANIES

Today, the Universal Declaration of Human Rights, international covenants and conventions impose the duty to respect and protect human rights solely upon states. Although it is fair to say that the Declaration still calls upon everyone to respect and promote human rights.

At the same time, the number of active Facebook users monthly in 2019 is already more than 2.4 billion[57]. And the most popular Google service - YouTube - has about 2 billion users[58]. This is more than the population of any country of the world (at least according to official data). Therewith, the ability of the platforms to influence the information received and disseminated by users and the ability to collect personal data often exceed the powers of any governmental agencies, except perhaps China and several other undemocratic states.

Against this background, the question whether it is the time for major online platforms to assume the obligation to observe the high international requirements in the field of human rights and, accordingly, whether individuals can obtain an effective and efficient mechanism to lodge complaints about violations of their rights by such platforms, is quite appropriate.

In fact, the European Union has already introduced serious obligations relating to protection of personal data for large Internet corporations, and has even pointedly applied its high fines to Google (€ 50 million for breach of informed consent requirements[59]). Earlier, EU courts recognized the existence of "the right to be forgotten", which obligates to remove links to individual publications from search results.

However, these measures do not yet address other threats to human rights by large corporations — in particular, removing content and blocking users based on platform rules that often contradict international standards of free speech. This is evidenced by the analysis of the international organization Article 19, which assessed the Standards of Facebook[60], Youtube[61], and Twitter Rules[62]. In particular, there are inconsistencies not only in the use of a number of assessment categories in restriction of "illegal content", but also in the absence of effective

---

57 https://newsroom.fb.com/company-info/

58 https://variety.com/2019/digital/news/youtube-2-billion-users-tv-screen-watch-time-hours-1203204267/

59 https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

60 https://www.article19.org/resources/facebook-community-standards-analysis-against-international-standards-on-freedom-of-expression/

61 https://www.article19.org/resources/youtube-community-guidelines-analysis-against-international-standards-on-freedom-of-expression/

62 https://www.article19.org/resources/twitter-rules-analysis-against-international-standards-on-freedom-of-expression/

possibilities to appeal against the restrictions or even to get explanations on the reasons for application thereof. At the same time, it should be noted that Google, for example, publishes content removal information in response to requests from a court or a public authority in the Lumen public database[63].

Particular attention should be paid to the use of algorithms for filtering and prioritizing of the content we are reviewing. Thus, the search results we receive often depend not only on the language, but also on many other (often hidden) factors based on the information about us stored by the corporation. And while this is supposed to facilitate a quick search for exactly what we need, on the other hand it creates an "information bubble" for us, that is, on the contrary, it limits our ability to access knowledge.

The relations in the triangle "state - private companies - individuals" have remained without any attempt at regulation on the part of the international community for quite a while. That is why the issue of respect for human rights in this triangle also remains quite controversial as to the distribution of the roles between the major players. In 2011, the UN prepared and published the Guiding Principles on Business and Human Rights, also called the Ruggie Principles, after the author's name.[64] They contain certain outlines on what corporate social responsibility should be for businesses in respecting human rights. Thus, they stipulate that the state in its legislation must provide for the obligation of companies to respect human rights in their activities and provide guidance in this respect. In conflict-affected areas, the state should help companies to identify and prevent the risks posed by their activities to observation of human rights, and deny any assistance to companies that have serious human rights violations. At the same time, companies should avoid any harmful impact on human rights as guaranteed by the International Bill of Human Rights and eliminate any harmful impact where it arises from their activities. Said document also encourages every business to have a policy on observation of human rights and conduct due diligence on human rights. Furthermore, both states and businesses must ensure a proper and effective mechanism for compensation for losses caused by human rights violations on their part.

In 2019, the importance of the role of private corporations in regulation of the freedom of expression was also addressed by Special Rapporteurs on Freedom of Expression of international and regional human rights organizations. In their Joint Declaration, "Challenges to Freedom of Expression in the Next Decade",[65] they emphasized the necessity of implementation of the "Ruggie

[63] https://lumendatabase.org/

[64] https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[65] https://www.article19.org/wp-content/uploads/2019/07/Joint-Declaration-2019-Final-text.pdf

Principles" by companies with further supervision of such implementation by the state. They also called for the development of independent mechanisms for supervision, transparency and accountability with the involvement of all stakeholders, in order to revise content placement rules that are contrary to the international human rights protection standards — that is, for co-regulation in the field of content management

Recommendations on the role of the state in protection of human rights in the activities of private companies:

1. *To the Cabinet of Ministers of Ukraine, Human Rights Commissioner of the Verkhovna Rada of Ukraine* — to initiate and promote a full-fledged dialogue of public authorities with representatives of civil society and private corporations on corporate social responsibility issues;
2. *To the Verkhovna Rada of Ukraine (Committee on Humanitarian and Information Policy, Committee on Digital Transformation)* — to initiate discussions with experts, representatives of the Internet platforms and public authorities on the expediency of enshrining in law of the requirements for the transparency and accountability for the activities of the Internet companies, in particular in the areas of advertising (including political), protection of personal data, counteraction to misinformation.
3. *To the Verkhovna Rada of Ukraine (Committee on Humanitarian and Information Policy, Committee on Digital Transformation, Committee on Legal Policy, etc.), Ministry of Digital Transformation* — to develop effective legal remedies for an individual against violations of his/her fundamental rights by private companies (by improving antitrust, personal data legislation, imposing the obligation on platforms to determine effective mechanisms for lodging complaints, etc.);
4. *To the Verkhovna Rada of Ukraine (Committee on Humanitarian and Information Policy, Committee on Digital Transformation)* — to create conditions and actively promote the initiation of co-regulation mechanisms in order to secure human rights in the activities of the Internet platforms.
5. *To the Cabinet of Ministers of Ukraine, Human Rights Commissioner of the Verkhovna Rada of Ukraine* — to ensure effective communication of the government with representatives of the largest international Internet platforms on the challenges of misinformation and human rights abuses in connection with the military aggression of the Russian Federation.
6. *To the Cabinet of Ministers of Ukraine* — to implement joint programs aimed at increasing the Internet literacy of citizens, clarifying the rights of social network users in respect of their rights, protection against harmful content, etc.

RESPONSIBILITY OF THE INTERNET INTERMEDIARIES FOR ILLEGAL CONTENT

The exercise of rights on the Web would be impossible without the role of intermediaries - Internet platforms, Internet service providers, developers of the physical infrastructure of the Internet, through which access to the network is exercised. On the one hand, most of these intermediaries play a passive role and have no influence on online content. Thus, they are neither more nor less than an analog of a postman who facilitates the delivery of information from one place to another. On the other hand, with the development of technology and algorithms, a number of websites (mostly social networks and search and advertising services) began to influence content ranking, made it possible to filter it automatically and create an ecosystem that allowed it to remove malicious content. In doing so, some websites have set up their own regulatory system, which is completely independent of the state one, except for extraordinary cases of inactivity of the intermediary. All this raises the question of what the system of responsibility of intermediaries in Ukraine and the world currently is for now and how it should be modified.

Article 14 of the European Union Directive 2000/31/EC on e-commerce establishes the so-called "safe harbor" principle under which hosting providers (including, in particular, social networks, in accordance with the ECJ judgment in the case of *SABAM v Netlog*[66]) are released from liability for the content posted by them if:

1) they have no information about illegal activity and content or about the circumstances from which the apparent illegal nature of such activity results ("*actual knowledge*");

2) having received the information about such activity and content, they act promptly enough to remove such content or restrict access to it ("*expeditious removal*").

These provisions are also in line with those of the US DMCA (Digital Millenium Copyright Act). Both acts laid the groundwork for the "notice-and-takedown" regime as the primary procedure used to restrict access to harmful content on the Web. Article 15 of the E-Commerce Directive also emphasizes that states may not impose the general obligation to monitor the information transmitted through intermediaries, or to proactively search for facts or circumstances that indicate illegal content or activity. At the same time, monitoring is not prohibited in some cases.

---

[66] SABAM v. Netlog NV, Case C 360/10: http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=150383

In 2011, the Special Rapporteurs of international organizations on freedom of expression issued a Joint Declaration on Freedom of Expression and the Internet[67], where principle 1 (c) emphasized the need for the design of special regulation for the network. In respect of the intermediaries, principles 2 (a) and 2 (b) of the Declaration set forth the following:

1) no one who provides technical services for the Internet access (in particular, provision of access, search functionality, transmission or caching of information) may be held liable for the content created by others and disseminated on these platforms, as long as they do not interfere with the content or refuse to comply with a court decision to remove such content; however, consideration should be given to the possibility of extending this regime to any intermediaries;

2) intermediaries may not be forced to monitor user content and may not be obligated to restrict access to content out of court if such mechanism does not meet the standards of freedom of expression.

Thus, the Declaration summarizes the provisions of various national regimes of regulation on what constitutes "actual knowledge", adding a clearer requirement for the role of courts in deciding whether to restrict access or to remove harmful content. This requirement is the guarantee of observation of procedural rights of both intermediaries and users. In 2017, in their Joint Declaration on Freedom of Expression, "Fake News", Misinformation and Propaganda in Principle 1 (d), the guarantee of the judicial procedure was detailed and extended — and it was recommended to extend the immunity of intermediaries to all cases except the interference of such intermediaries with the content or their refusal to comply with the decision on content removal taken in accordance with the guarantees of the proper judicial procedure by an independent, impartial and authoritative supervisory body (such as a court).

The main and, to some extent, codification document in the area of liability of intermediaries is the Manila Principles on Intermediary Liability[68], developed by the world's non-governmental organizations in 2015 and aimed at summarizing the best practices for limitation of liability of intermediaries for the content on the Web. Among the main provisions on the liability of intermediaries, the following are worth mentioning:

principle I (b) — intermediaries have immunity from user-generated content where they have not interfered with the modification of such content;

---

[67] Joint declaration on freedom of expression and the Internet: https://www.osce.org/ru/fom/78310

[68] Manila Principles on Intermediary Liability: https://www.manilaprinciples.org/principles

principle I (d) — the intermediary's liability regime can never include active content monitoring requirements;

principle II (a-b) — intermediaries don't have to restrict content unless there is the relevant decision of an independent and impartial judicial agency that found that the content was illegal, and such decision must include the determination of the illegality of the content in a particular jurisdiction, describe and provide an Internet identifier for such content, analyze evidence to support the grounds for the decision, and, where applicable, indicate the periodicity of the restriction;

principle III (d) — where intermediaries use an out-of-court content restriction mechanism, they do not have to assess the content in a meaningful way — but should send reasonable complaints to the person who created the relevant content (notice-and-notice);

principle IV — any content restriction should be limited to a specific content unit, and the least restrictive technical measures should be used to restrict it, including the possibility to restrict access to the content in a specific geographic area and/or for a certain period of time with the possibility of periodic review;

principle V — laws and policies on content restriction must respect the due process including the right to be heard, the right to appeal, etc., and must take human rights into account;

principle VI (b) — the government may not use out-of-court measures to restrict content, including through the pressure to change the terms of use of intermediaries;

principle VI (d-e) — governments and intermediaries should publish transparency reports where they should provide information on all requests for content restriction and fulfillment thereof.

Currently, this document is one of the most comprehensive in respect of the liability of intermediaries and compiles the best practices to be implemented in the course of development and updating of the Internet regulation legislation.

One of the most recent ones is the Recommendation of the Committee of Ministers of the Council of Europe CM/Rec(2018)2 on the roles and responsibilities of the Internet intermediaries[69]. Already in the preamble it is emphasized that with the development of technology, the classic categorization of intermediaries into active and passive has lost its role, since one intermediary can perform different roles — both simply provide access to the information and control information through moderation and ranking. The recommendation turns upon detailing of the three-part test for restrictions in the context of

[69] Recommendation of the Committee of Ministers of the Council of Europe CM/Rec(2018)2 on the roles and responsibilities of the Internet intermediaries: https://rm.coe.int/1680790e14

intermediaries. In particular, it reaffirms the need for any legislation in this field to guarantee human rights, as well as the direction to states to publish information on requests for restriction of access to harmful content, and to intermediaries on the transparency of their content-restricting activities, both under state and private requests. Clause 1.3.2 specifies the need for obtaining a decision of a court or other independent administrative authority whose decisions are subject to judicial review in order to restrict access to the content (except for cases of the obvious unlawfulness of content or the existence of prompt removal requirements).

The prohibition to impose the obligations of overall content monitoring on intermediaries directly or indirectly is again emphasized. One of the key points of the document is paragraph 1.3.7, which again emphasizes the "*safe harbor*" regime, but suggests the co-responsibility of intermediaries if they do not restrict access to the content sufficiently quickly after receiving information about its illegality. At the same time, the receipt of notices of such potential illegality should be based on the legal analysis on the part of the public authorities and not on the part of the intermediary itself; the relevant liability regime should not encourage restrictions of access to legal content. The recommendation also calls for a differentiated approach to the liability of intermediaries.

The Recommendation also mentions content moderation by intermediaries themselves. Paragraph 2.3 of the document emphasizes the use of the least restrictive technical means in the process, the severe limitation of the scope of blocking or removal of content, as well as the communication of the reasons for taking such measures. With regard to the use of automated content identification systems, they are considered useful to limit the appearance of content that has already been restricted in access, but it is specified that these systems do not understand the context of the utterances well enough and require human oversight. When applied, the risk of too restrictive or, on the contrary, too soft regulation should be taken into account.

It can be summarized that over the recent years, the "*safe harbor*" concept has not lost its position and, in general, remains dominant in determining the regime of liability of intermediaries for the distribution of malicious content. At the same time, the standard of the necessity of obtaining "actual knowledge" of the illegality of the content through the relevant decision of a court or other independent body has taken a more definite shape. Restriction of access to content by intermediaries should be ensured through the least restrictive measures in order to secure the rights of users of such intermediaries on the Internet. At the same time, intermediaries themselves should be kept out of the need to independently assess the content for compliance with the law or international standards in the area of freedom of expression as much as possible,

and the obligation of monitoring information passing through the platform may not be imposed on them.

Another problematic concept in the area of liability of intermediaries is how prompt the restriction of access to the content should be in the event of receipt of information about its illegality. This area is at the discretion of states that are sovereign in establishing national regulatory regimes, and international standards are usually confined to common phrases regarding sufficient speed and proper amount of time for the intermediary to take decisions. There are few documents where the concept of "expeditious removal" has been developed at the transnational level. In particular, in 2016, a Code of Conduct on Countering Illegal Hate Speech Online was signed within the European Union. Signatories including Facebook, Microsoft, Twitter, Google etc. have agreed to assume the obligation to review most notices of removal of illegal hate speech within 24 hours and, if necessary, to remove such content or restrict the access to it. European Commission Recommendation C(2018)1177 on measures to effectively tackle illegal content online[70] mentions the deadline of 1 hour after receipt of the notification for removal of terrorist content.

However, at the international level, the dominant position is that the analysis of whether or not the access to the content was restricted sufficiently promptly should depend on the nature of the content in each case, which brings us to the third important category in the area of liability of intermediaries — which content is illegal. The content removal speed requirement directly depends on the harmfulness of the potential impact of the content.

In the case of Delfi AS v Estonia[71], the European Court of Human Rights considered the matter of liability of the news portal for offensive comments posted under one of the publications. The Court outlined a number of criteria that influenced its analysis and the decision that there had been no violation of freedom of expression in the case. The Court took into account the context of the comments, the measures taken by the intermediary to restrict the access to the illegal content, the liability of the actual authors of the content as an alternative to the intermediary's liability, and the consequences of the proceedings in the domestic courts for the intermediary company (payment of moral damages in the amount of EUR 320). In its analysis, the court concluded that the comments that were the subject of the case should be classified as hate speech and calls for violence and acknowledged that the comments had been removed promptly enough (on the day the complaint was received). However, since the news portal

[70] European Commission Recommendation C(2018)1177 on measures to effectively tackle illegal content online: https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[71] Delfi AS v. Estonia (no. 64569/09) 16 June 2015

had an economic interest in posting the comments, only the portal itself had the technical capability to delete comments, and given the difficulty of identification of anonymous commentators and the apparently unlawful nature of comments, which sometimes needed to be removed even without notice, the imposition of the liability on the internet portal was found to be in conformity with Article 10 of the European Convention on Human Rights.

At the same time, in 2019, the European Court of Human Rights published the judgment in the case of *Høiness v Norway*[72]. This case concerned the posting on the forum of one of the Internet portals of user comments which the applicant, a professional lawyer, interpreted as sexual harassment. Two comments were deleted immediately after receipt of the relevant notice by the editor of the Internet portal, and the third was deleted at the initiative of one of the moderators. However, the applicant initiated proceedings in the Norwegian courts for recovery of non-pecuniary damage — and lost in all instances. The European Court of Human Rights also analyzed the case in accordance with the criteria set out in its previous practice in the case of *Delfi AS v Estonia*. It noted that the site on which the comments were published, although it was a major news site created for economic gain, its forum couldn't be considered a continuation of articles on the site itself, because the discussions on it were initiated by users of the network. In addition, the comments that were the subject of the case did not constitute hate speech or incitement to violence, and were deleted either before the notification (one of the comments) or 13 minutes after the proper notification was received. In view of said fact, the Court did not find a violation of Article 8 in respect the right to respect for the applicant's privacy.

Thus, one of the key criteria is the content of user-generated content. When it comes to hate speech or incitement to violence, there are reasons to apply stricter standards, including in respect of the need to promptly remove the content from the platform provided by the intermediary.

[72] Høiness v Norway (no. 43624/14) 19 March 2019

Recommendations on the responsibilities of Internet-intermediaries:

1. *To the Verkhovna Rada of Ukraine and other subjects of legislative initiative* — to refrain from introducing legislative initiatives that are contrary to the international human rights standards and impose excessive obligations in respect of monitoring and checking of user-generated content, as well as outright liability for any comments posted by third parties, on Internet intermediaries;
2. *To courts and law enforcement bodies* — when determining whether individual Internet intermediaries are responsible for the illegal content that has been posted on their site by users, they must take into account the following criteria and principles without fail:

   ▪ intermediaries have the immunity from user-generated content in cases where they have not interfered with the modification of such content;

   ▪ the intermediary liability regime shall never include the requirements of active content monitoring;

   ▪ intermediaries don't have to restrict content unless there is the relevant decision of an independent and impartial judicial agency that found that the content was illegal, and such decision must include the determination of the illegality of the content in a particular jurisdiction, describe and provide an Internet identifier for such content, analyze evidence to support the grounds for the decision, and, where applicable, indicate the periodicity of the restriction;

   ▪ where intermediaries use an out-of-court content restriction mechanism, they do not have to assess the content in a meaningful way — but should send reasonable complaints to the person who created the relevant content (*notice-and-notice*);

   ▪ any content restriction should be limited to a specific content unit, and the least restrictive technical measures should be used to restrict it, including the possibility to restrict access to the content in a specific geographic area and/or for a certain period of time with the possibility of periodic review