
The report has been prepared within the timeframe of the project “To monitor internet freedom situation in Ukraine and raise awareness of digital rights violations in Ukraine”, which is implemented by the NGO “Human Rights Platform” with the financial support of the American Bar Association Rule of Law Initiative.

Full version of the report is available on the website of the Human Rights Platform via the link “War in the digital dimension and human rights”.

Opinions, conclusions, or recommendations are those of the authors of this publication and do not necessarily reflect the views of the American Bar Association's Rule of Law Initiative.
CONTENTS

I. INTRODUCTION 4

II. DIGITAL WAR 5
  1. “Digital battlefield,” or cyber attacks on Ukraine 5
     1.1. Cyber attacks on websites of public bodies, institutions, organisations, media 5
     1.2. Phishing attacks 5
     1.3. Creating fake web resources and spreading false information 6
  2. Response to Russia’s information war on the Internet 6
     2.1. Blocking Web Resources 6
     2.2. Launching an IT army 6
     2.3. Blocking Telegram channels and pages on Instagram 7
     2.4. Revising the social media policies 7

III. AMENDMENTS TO LEGISLATION 9

IV. ACCESS TO THE INTERNET DURING THE LEGAL REGIME OF MARTIAL LAW 11

V. FREEDOM OF EXPRESSION AND NATIONAL SECURITY DURING THE LEGAL REGIME OF MARTIAL LAW 12

VI. PERSONAL DATA PROTECTION DURING THE LEGAL REGIME OF MARTIAL LAW 13

VII. ACCESS TO INFORMATION DURING THE MARTIAL LAW 14

VIII. RECOMMENDATIONS 16

IX. ANNEXES 18

Annex 1. Response of the Head of PR Department of the Armed Forces of Ukraine on clarification of the meaning of certain terms, used in the Order of the Commander-in-Chief of the Armed Forces of Ukraine “On the Organization of Interaction Between the Armed Forces of Ukraine, Other Components of the Defense Forces and Media Representatives During the Legal Regime of Martial Law” No 73 of 03.03.2022. 18

Annex 2. Response of the National Center for Operational and Technical Management of Telecommunications Networks (NCU) of May 16, 2022 regarding the disconnection of settlements on the territory of Ukraine from mobile and Internet communication between February 24 and April 30, 2022 and regarding the number and list of websites that were blocked during the above period. 18
On February 24, 2022, a large-scale invasion of the Russian Federation into Ukraine started. On the same day, martial law was introduced by the Decree of the President of Ukraine throughout the territory of our country.

The invasion affected Ukrainian cities, towns, villages and settlements and Ukrainian cyberspace as well. Hostile hackers have directed a lot of efforts to disrupt the ordinary operation of critical infrastructure facilities in Ukraine, particularly in the energy and financial sectors, as well as in the field of public services provision. Every day, cyberpolice, together with Ukrainian cyber volunteers and allies from around the world, is fighting fiercely against the invaders and their assistants in the virtual world.

The situation described could not but affect digital human rights.

The “Platform for Human Rights” CSO (hereinafter - PHR) has monitored changes to the legislation and collected facts that reflect the course of the “digital war” between February 24 and April 30, 2022, and analysed their impact on digital human rights in Ukraine.

In this report, we present the research findings and outline our conclusions about the current situation in this area.
II. DIGITAL WAR

1. “Digital battlefield,” or cyber attacks on Ukraine
   As a result of the work carried out by experts of the CSO “Platform for Human Rights” for the period from February 24 to April 30, 2022, the following violations of digital rights by the Russian Federation were detected:

1.1. Cyber attacks.
   32 (thirty-two) cyber-attacks on websites of public bodies, institutions, organisations, and media occurred during the reporting period. Among them:
   1) 6 cyber-attacks on official websites of public bodies (the Cabinet of Ministers of Ukraine, the Verkhovna Rada of Ukraine, the Ministry of Foreign Affairs, the Security Service of Ukraine, and other public bodies);
   2) 23 cyber-attacks on websites of mass media;
   3) 3 cyber-attacks on websites of institutions and organisations.

1.2. Phishing attacks.
   From February 24 to April 30, 2022, 15 fifteen reports of phishing attacks were recorded, aimed at a wide circle of users and at certain public authorities. Various malicious files were disseminated during this period among the citizens of Ukraine, most of which had names related to the war:
   - “Evacuation Plan”;
   - “Instruction on behaviour during artillery attacks”;
   - “Information about war criminals of the Russian Federation”;
   - “Mobilization registry.xls”; and others.

1.3. Creating fake web resources and spreading false information.
   29 (twenty-nine) facts of the dissemination of false information were recorded from February 24 to April 30, 2022. Fakes have been spread via Telegram channels, chats, e-mails, hacked websites of local self-government bodies, and fake websites created by the occupants. The primary purpose of such dissemination was to stoke panic moods about the course of Russia’s large-scale invasion of Ukraine.

In the reporting period, we recorded 76 (seventy-six) facts of violations of digital human rights of a general nature, which were undertaken by Russian hackers consisting of 32 (thirty-two) cyber-attacks, 15 (fifteen) reports on phishing attacks and 29 (twenty-nine) facts of dissemination of false information.
II. DIGITAL WAR

2. Response to Russia’s information war on the Internet

Blocking web resources in Ukraine was conducted out-of-court from February 24 to April 30, 2022.

Based on the Decree of the President of Ukraine of 24.02.2022 No 64/2022 «On the Introduction of Martial Law in Ukraine», approved by the Law of Ukraine of 24.02.2022 No 2102-IX «On Approval of the Decree of the President of Ukraine «On the Introduction of Martial Law in Ukraine»; within the framework of the legal regime of martial law the National Center for Operational and Technical Management of Electronic Communication Networks of Ukraine (NCU) during this period repeatedly appealed to providers of electronic communication networks and/or services of essential Internet resources with a persistent request to block Internet resources, autonomous systems (AS), web resources, and addresses.

During this period, NTSU recommended providers of electronic communication networks and/or services block 854 web resources that ensured the dissemination of information in the interests of the aggressor country.

It is also worth paying attention to the sanctions applied to ISPs who did not perform NCP orders: they were excluded from the Register of Telecommunications Operators and Providers. Specifically, the National Commission for State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services decided to exclude Netasist LLC and Netassist LLC from the relevant register.

Blocking of web resources was also carried out by other public authorities. In particular, on February 26, 2022, Cyberpolice announced the blocking of 38 websites in cooperation with volunteers. The blocks were applied to the online resources of the Russian government, the largest media, as well as banks.

2.2. Launching an IT army

The Ukrainian government planned to create a cyber army long before the large-scale invasion but did not manage to timely approve the structure of such a state army and all the necessary regulations for its activities. According to the Decree of the President of Ukraine «On the Implementation Plan of the Cybersecurity Strategy of Ukraine» of February 01, 2022, the Cabinet of Ministers of Ukraine had a task to create, by the first half of 2023, the cyber army in the system of the Ministry of Defense of Ukraine, providing them with adequate financial, personnel and technical resources to deter armed aggression in cyberspace and to fight back.

In the early days of the full-scale Russian invasion, Minister of Digital Transformation Mykhailo Fedorov in his Telegram channel proposed to convene a Ukrainian IT army of developers, e-specialists, designers, copywriters, marketers, targetologists, etc., and launch the relevant Telegram channel IT ARMY of UKRAINE. The main idea of creating this channel was to combine the efforts of IT specialists on a volunteer basis to counter the Russian Federation on the cyber and information front. A large number of Ukrainian and international IT professionals immediately joined the initiative.
Today, the Ukrainian IT Army is a self-organised volunteer movement. According to the head of the State Service of Special Communications Viktor Zhora, the estimated number of volunteers in the cyber army is 400 thousand people. The IT army makes a big difference in the cyber defence of Ukraine and plays a unique role in the digital war. Cyber volunteers helped block the operation of more than a thousand Russian web resources, as of April 30, 2022.

2.3 Blocking social media pages, video hosting
On 26.02.2022 the Ministry of Digital Transformation of Ukraine asked YouTube to block Russian propaganda media channels, according to the «Obozrevatel» website.

In parallel, similar appeals were sent to Facebook and Instagram (both by Meta), as well as to Rakuten (Viber) and Paypal, with requests to block the activity of «Instagram pages.»

On 01.03.2022 «Ekonomichna Pravda» referred to M. Fedorov’s Telegram channel in its report that “Meta Platforms” had also started blocking those Russian resources that spread misinformation.

2.4. Revising the social media policies
Meta Platforms Inc. («Facebook» and «Instagram» social media, messengers «Messenger» and WhatsApp).
Since 26.02.2022 Ukrainians were allowed to close their Facebook profile and hide lists of friends from Ukraine and Russia. In parallel:
- Instagram removed the ability to view followers and subscriptions of private profiles;
- names and other data of advertisers from Ukraine were hidden;
- cooperation with Ukrainian fact-checkers, CSOs and the government intensified;
- Russian users were banned from ad broadcasting and content monetising;
- warning algorithms about the publication of a potential fake were added: Meta company claims that their algorithms can recognise photos taken more than a year ago, and when posting such a photo, the network just in case warns the user of sharing an old photo;
- the possibility for users was introduced to “hid” from the list of recommendations those pages and profiles that repeatedly spread false content; their publications will appear at the bottom of the feed;
- cooperation with the Ministry of Digital Affairs was launched on restricting access to Russian state media and journalists;
- access to RT and Sputnik pages were restricted in the EU before the relevant decision was made at the Union level. Also, the rating of these pages on Instagram and Facebook has decreased for the whole world - from now on, RT and Sputnik publications appear less often in people’s feeds. If links to RT and Sputnik are distributed to Stories on Instagram, these Stories are also displayed at the end of the list;
- the possibility to send disappearing messages in Messenger and Whatsapp was added, as well as the function of automatically deleting all chats in Whatsapp once in a certain period of time to protect the correspondence of users in case of loss of the phone;
- the feature to send messages en masse to Whatsapp, Messenger and Instagram was limited;
- end-to-end chat encryption on Messenger and Instagram was added;
- opened a hotline of the State Emergency Service of Ukraine, as well as a hotline for psychological support in Whatsapp.
On 11.03.2022 the rules on dissemination of information on Facebook and Instagram were revised. Specifically, users in Armenia, Azerbaijan, Estonia, Georgia, Hungary, Latvia, Lithuania, Poland, Romania, Russia, Slovakia and Ukraine are allowed to publish threats and calls for violence against Russians and Russian military. In fact, calls for cruelty as «death to the Russian occupiers» were not blocked by moderators of these social media.

On 14.03.2022 Meta Platforms revised its rules and banned calls for violence against Russians. Albeit, wishing death to Russian soldiers in the context of their invasion of Ukraine remained acceptable.

**Twitter:**
Since 28.02.2022 Twitter reported that:
- it created the **selected content in the «Moments» section** of Twitter on the war in Ukraine, which offers news and resources that become available in real time and in many languages;
- added prompts for the functions «Search» and «Home,» with a list of **important resources** on digital security in English, Ukrainian and Russian;
- created the **special event pages** that are available in 12 languages in more than 67 countries;
- created the **Topic** section to help people get information directly in the «Home» section, as well as a **list on Twitter** which suggests the reliable news sources;
- added the **labels** for the government and state-affiliated profiles that meet the specified criteria;
- suspended the recommendation of certain tweets from users to those people who use Twitter in Ukraine and Russia to reduce the risk of spreading harmful content;
- blocking numerous profiles, through which attempts were made to deny violent actions or spread misleading statements about such actions and victims of such actions during the war;
- **suspended** advertising in Ukraine and Russia, so that the search results show critical information about public safety first, and advertising did not distract from communication on Twitter;
- if the content violates Twitter rules, disciplinary measures are taken at a tweet or profile level. Such measures include, in particular, the removal of content.

Therefore, in response to Russia's large-scale invasion of Ukraine, public and video platforms have revised their policies to spread some types of content and have implemented certain mechanisms to protect users from aggressive actions on the part of Russia.
From February 24 to April 30, 2022, the Ukrainian legislation underwent many drastic changes related to the introduction and operation of the legal regime of martial law in Ukraine. Most of these changes have a direct effect for digital human rights. All in all, 12 (twelve) regulatory legal acts relating to digital rights were adopted during the reporting period, namely:

1. Decree of the President of Ukraine No 64/2022 «On the Introduction of Martial Law in Ukraine» of February 24, 2022 due to the Russian Federation's military aggression against Ukraine. Immediately, on the same day, the Verkhovna Rada of Ukraine adopted the Law No 2102-IX «On Approval of the Decree of the President of Ukraine» On the Introduction of Martial Law in Ukraine». As a result of their adoption, martial law was introduced throughout Ukraine from 05 hours 30 minutes on February 24, 2022 for 30 days.

During March - May 2022, the term of the legal regime of martial law has been extended three times and remains valid until August 23, 2022.

2. Order of the Commander-in-Chief of the Armed Forces of Ukraine «On organization of interaction between the Armed Forces of Ukraine, other components of the defense forces and media representatives during the legal regime of martial law» No 73 of March 03, 2022. The order is aimed at preventing the leakage of classified information, preventing the spread of information by media representatives (including foreign) and public persons-influencers [opinion leaders, bloggers, etc.], when such a disclosure entails awareness of the enemy about the actions of the Armed Forces of Ukraine and other components of the defense forces, or such a disclosure may adversely affect the progress of the assignments during the legal regime of martial law. This Order contains a list of information, the dissemination of which is prohibited during the legal regime of martial law.

3. The Resolution of the Cabinet of Ministers of Ukraine No 263 «Some issues of ensuring the operation of information and communication systems, electronic communication systems, public electronic registers in martial law» came into force on March 12, 2022. This Resolution granted the right to ministries, other central and local public bodies, state and municipal enterprises, institutions, organizations belonging to their management - for the period of martial law - to stop, limit the running of the information, communication and electronic communication systems, as well as public electronic registers. The rationale behind this step was to ensure the proper functioning of information, communication and electronic communication systems, and public electronic registers, and to protect the information processed in these systems and the public information resources themselves.

5. Two more Laws of Ukraine related to digital human rights came into force on March 16, 2022. These were the Laws of Ukraine «On Amendments to Certain Laws of Ukraine on Prohibiting the Production and Distribution of Information Products Aimed at Promoting the Actions of the Aggressor State» and «On Amendments to Certain Legislative Acts of Ukraine on Strengthening Criminal Liability for the Production and Distribution of Prohibited Information Products.» The Criminal Code of Ukraine got two new articles, Article 436-2 «Justification, recognition of the legitimacy, and denial of armed aggression of the Russian Federation against Ukraine, glorification of its participants» and Article 435-1 «Insult to honor and dignity of the serviceman, threat to the military.»

6. On March 19, 2022, a decision of the National Security and Defense Council of Ukraine of March 18, 2022 «On the implementation of a unified information policy in martial law» was put into effect by the Presidential Decree. It obliged all national channels to broadcast a single round-the-clock telemarathon «United News #UAtogether.» The decision of the NSDC laid down that the implementation of a unified information policy in martial law - is a priority issue of national security, which is implemented by uniting all national TV channels, the editorial policy of which consists mainly of information and/or information-analytical programs made available on a single information platform of strategic communication - the 24/7 information marathon «United News #UAtogether.»

7. The Law of Ukraine “On Amendments to the Criminal Procedural Code of Ukraine” and the Law of Ukraine “On Electronic Communications” came into force on improving the efficiency of pre-trial investigation «as a hot pursuit» and counteracting cyberattacks. The amendments aim to speed up the procedure for investigating the crimes and simplifying the receipt of electronic evidence, such as: information from personal devices, public video cameras and evidence about the receipt of communication services.

8. Another law entered into force on March 27, 2022, No. 2160-IX «On Amendments to the Criminal and Criminal Procedural Codes of Ukraine on ensuring counteraction to unauthorized dissemination of Information on transportation, movement of weapons, weaponry and combat supplies to Ukraine, movement, relocation or deployment of the Armed Forces of Ukraine or other military formations created in accordance with the laws of Ukraine, committed under martial law or state of emergency» of 24.03.2022. This Law supplemented the Criminal Code of Ukraine with Article 114-2, which provides for criminal liability for unauthorized dissemination of the mentioned information, committed under martial law or emergency.

9. On April 03, 2022, the Law of Ukraine On Amendments to the Criminal Code of Ukraine on Improving the Efficiency of Combating Cybercrime under Martial Law came into force. The law amended articles 361, 3611 of the Criminal Code of Ukraine in order to bring terminology in line with the Law of Ukraine No. 1089-IX «On Electronic Communications» of December 16, 2020 and the requirements of national legislation in the field of cybersecurity. Specifically, the term «electronic computing machines (computers), automated systems, computer networks or telecommunication networks» was replaced by «information (automated), electronic communication, information and communication systems, electronic communication networks.»

Given the amendments into legislation that have a direct impact on digital human rights and were adopted between February 24 and April 30, 2022, one may conclude that most of them have established additional limitations on the freedom of expression. Seven of the twelve regulations that entered into force during this period set additional restrictions on the dissemination of certain types of information and also reinforce responsibility for violating such restrictions.

Even though the main reason for additional restrictions is the protection of the national interests of Ukraine, protection of Ukrainian statehood from crimes against national and public security, one of the major objectives of the Ukrainian state should be to ensure guarantees of freedom of speech, free receipt, collection and dissemination of information with respect to the restrictions related to martial law.
The right to access the Internet has known special obstruction as a result of Russia's large-scale invasion of Ukraine. There have been numerous attempts to disrupt the normal operation of electronic communication networks of Ukraine, to disable the Internet on its territory, to block access to the web resources of public authorities and military administration of Ukraine, banks, media, influential civil society organizations, etc.

Operational and technical management of electronic communication networks under martial law is handled by the special public body - the National Center for Operational and Technical Management of Telecommunication Networks under the State Service for Special Communications and Information Protection of Ukraine (hereinafter - the Center). This Center manages electronic communication networks during martial law and, together with electronic communication operators, develops plans to restore the operation of electronic communication networks, plans for operational replacement of damaged lines, routes and communication channels, plans for use of reserves in case of network overload and may, if a threat is detected, make decisions and instruct suppliers to block or disconnect certain regions or settlements from the Internet.

Analysis of the information, which was posted on the official website of the State Service for Special Communications and Information Protection of Ukraine (hereinafter - the State Service), allows drawing conclusions that for the period from February 24 to April 30:

Public authorities did not make decisions to disconnect from the Internet, and Internet providers, on their own initiative, did not disable or block the provision of the Internet.

The National Center for Operational and Technical Management of Telecommunications Networks limited the speed of the Internet in some settlements for a certain time, since priority in the Internet provision was given to the critical needs of the Armed Forces of Ukraine and critical infrastructure facilities.

Despite the war and the enemy's attempts to leave Ukrainians without Internet, the providers tried to restore access to the network quickly. The analysis of the above information, which was published by the Center on network damage, as a result of which there were Internet outages or speed degradation, indicates that only four regions have not undergone interference with the Internet network in this period: Transcarpathian, Kirovohrad, Ternopil, Khmelnytsky and Cherkasy regions. Most areas suffered from enemy action. The network in Chernihiv, Kherson, Donetsk, Zaporozhye, Kyiv, Mykolaiv, Luhansk, Sumy, Kharkiv suffered the greatest damage. Minor damage was noted in Dnipropetrovsk, Odessa, Poltava, Vinnytsia, Volyn regions, Lviv, Rivne, Zhytomyr, Ivano-Frankivsk, Chernivtsi regions.

The launch of the Starlink satellite communication service in Ukraine and the supply of terminals that communicate with satellites, played a special role in restoring access to the Internet. Three days after Russia's full-scale invasion of Ukraine, SpaceX launched support for the Starlink service in Ukraine and sent the first batch of terminals. All regulatory restrictions on the use of Starlink for the period of wartime have been abolished, so now everyone in Ukraine can theoretically install a terminal and use the Internet from SpaceX.
As already noted, the introduction of martial law in Ukraine given Russia's large-scale invasion of the territory of Ukraine and the need to protect national interests in the realm of security and defense prompted amendments to the legislation of Ukraine and specifically to the Criminal Code.

The extent of these norms' impact for the freedom of expression directly depends on their implementation practice. During the monitoring, experts drew attention to reports about criminal proceedings opened based on the mentioned novels.

The collected information proves that the amendments began to be actively applied by law enforcement officers. 26 (twenty-six) reports on the opening of proceedings or investigations under the new articles of the Criminal Code of Ukraine were recorded in the reporting period:
- 7 (seven) reports on the opening of criminal proceedings under Article 114-2 of the Criminal Code of Ukraine;
- 13 reports on the investigation of criminal proceedings under Article 436-2 of the Criminal Code of Ukraine (9 - reports for justifying, recognizing as legitimate, denying the armed aggression of the Russian Federation against Ukraine; 4 (four) reports on the fact of glorification of persons who carried out the armed aggression of the Russian Federation against Ukraine);
- 1 (one) notice of investigation of a criminal offense under Art. 435-1 of the Criminal Code of Ukraine;
- 5 (five) reports on investigating criminal offenses under Article 111-1 of the Criminal Code of Ukraine.

V. FREEDOM OF EXPRESSION AND NATIONAL SECURITY DURING THE LEGAL REGIME OF MARTIAL LAW
VI. PERSONAL DATA PROTECTION DURING THE LEGAL REGIME OF MARTIAL LAW

The introduction of martial law in Ukraine in face of the large-scale aggression of the Russian Federation had a tangible impact on personal data protection in our country.

On the one hand, as already noted, the validity of Article 32 of the Constitution of Ukraine is temporarily limited, which guarantees non-interference in personal and family life, and on the other hand, it became clear to everyone that proper protection of personal data during the war has become of particular importance, because only in this way a person can be protected from numerous threats and even life saved (for instance, when it comes to personal data of military personnel and their families, law enforcement officers, officials of public and local governments, as well as journalists, civil society activists and volunteers, etc.).

After the introduction of martial law in Ukraine, a number of regulatory acts were adopted aimed at strengthening the protection of personal data.

Many applications and other online services were launched to solve various issues related to the war, the use of which can protect the confidentiality of personal data.

In particular, the Ministry of Digital Transformation of Ukraine (hereinafter - the MinDigital) has rolled out ten new functions in the Diya application, namely «Assistance to the army,» «Bayraktar Game,» «eDocument,» «Assistance under eSupport program,» «Assistance to employees and individual entrepreneurs,» «Notification about damaged and destroyed movable and immovable property,» «Assignment of the status of an internally displaced person and assistance to internally displaced persons,» «Diya - TV,» «Diya - Radio,» chatbot in Telegram «Ye-Vorog».

The developers have also created multiple applications. In particular, the monitoring revealed information on at least 11 applications that appeared after February 24, 2022, aimed at reducing the impact of Russian military aggression and helping IDPs affected by it. Here we are referring to «RussianWarCrimes,» «Bachu,» «SpyBuster,» «WhoAreYou,» «Air Alarm» and others.

At the same time, the information about secure personal data processing during their use of these applications is insufficient or rather contradictory.

In addition, 6 applications have been created to help IDPs and victims of armed aggression of the Russian Federation - this is the application «KyivTvSyrovyy,» the «Helsi,» the applications «TacticalMedAid,» «Bebbo,» «Tribefy,» «Lepta» and others.

During this period, at least 5 chatbots were launched for public awareness in the period of martial law: a chatbot in Telegram «StopRussiaChannelMrya,» a chatbot in Telegram «Caring,» a chatbot in Telegram «People's Avenger,» a chatbot in WhatsApp «SES Hotline,» and another one "EcoShkodaBot".

All in all, the martial law introduction in Ukraine served as an impetus for creating and using multiple applications and services. However, these applications were often created hastily and have been improved already «on the go.» Accordingly, there are reasonable concerns about whether they ensure the confidentiality of the personal data they collect. Importantly, there is currently a lack of testing of these applications, as well as those applications and services that claim that they do not collect or process personal data and verify the veracity of such statements.

Therefore, these applications, in addition to helping solve specific war-related issues, potentially risk violating users' data protection rights. Accordingly, there is a need to strengthen control over their compliance with the Law of Ukraine «On Personal Data Protection» requirements.
Because of the martial law introduction in Ukraine for the period of the legal regime of martial law, temporarily, it is allowed to restrict the right to freely collect, store, use and disseminate information by oral, written or other means of choice. This is prescribed under paragraph 3 of the Decree of the President of Ukraine «On the Introduction of Martial Law in Ukraine» No. 64/2022 [approved by the Law of Ukraine «On the Approval of the Decree of the President of Ukraine» On the Introduction of Martial Law in Ukraine «register. No. 2102-IX dated 24.02.2022). Therefore, the right to access public information was limited during martial law.

This immediately and negatively affected the practice of implementing the Law of Ukraine «On Access to Public Information» in all possible aspects, from providing answers to inquiries, ending with the publication of information on official websites of authorities and restriction or complete termination of access to information in public registers.

After martial law's introduction, consideration of information requests began to be systematically postponed by many public authorities.

Although Part 2, Article 14-1 of the Law of Ukraine «On Chambers of Commerce and Industry in Ukraine» recognizes the threat of war, armed conflict or a severe threat of such conflict, enemy attack, general military mobilization, military actions, declared and undeclared war, the imposition of a curfew, etc. - force majeure, it also contains a reservation that the circumstances of force majeure shall objectively prevent the fulfilment of obligations.

Therefore, a delay in considering a request for public information is acceptable only if the provision of a response within the deadlines determined by law is objectively impossible. This means that the introduction and enaction of martial law itself is not a sufficient reason for delaying the consideration of the request. And, therefore, in the actions of information managers, who refer to this aspect only, there is an abuse of this norm.

**On the restriction of public access to public registers**

The monitoring handled by our Organization from February 24 to April 30, 2022 revealed that access to 20 public electronic registers was limited during the mentioned period.

Closing some open data portal registries and public registries is not deemed a proportionate and feasible means to protect national security. Per the requirements of Part 3 of Article 6 of the Law of Ukraine «On Access to Public Information», restricted information should be provided if it was lawfully made public earlier.
On the top of closing registers, the failure to provide public information on requests, negative dynamics were also noted in terms of obligations of public information managers to publish it. Despite the requirement of the Law of Ukraine «On Access to Public Information» regarding the urgent publication of information on facts threatening the life, health and/or property of persons, and on the measures applied in this regard, such information was not published.

In a nutshell, we can conclude that from February 24 to April 30, 2022, the restriction of the right to access public information was not justified in every case and met the requirements of the Laws of Ukraine «On Access to Public Information,» «On the Legal Regime of Martial Law» and the Presidential Decree «On the Introduction of Martial Law in Ukraine»:
- delays in responses to requests received during the period of hostilities contradicted the current legislation and were not proportional and necessary;
- information managers restricted access to information without taking into account the balance between public necessity and national security;
- closing access to some public registers was not necessary under martial law;
- negative dynamics in public information published did not comply with the Law of Ukraine “On Access to Public Information” in terms of urgent disclosure of information on facts threatening the life, health and/or property of persons, and on measures applied in this regard.
**VIII. RECOMMENDATIONS**

1. **To the Verkhovna Rada of Ukraine:**
   - To amend Article 114-2 of the Criminal Code of Ukraine, more clearly outlining sources of information, reprinting of which exempts a person from liability, and provide for non-prosecution of persons in case of reprinting information from other sources, in particular foreign media;
   - Eliminate duplication of criminal offenses in Articles 111-1 and 463-2 of the Criminal Code of Ukraine;
   - Eliminate contradictions regarding the legal assessment of the illegal dissemination of the symbols of the Russian military invasion into the territory of Ukraine, namely contradictions that exist between Article 362-2 of the Criminal Code of Ukraine and the requirements of the Law of Ukraine No. 2265-IX «On the Prohibition of Propaganda of the Russian Nazi Totalitarian Regime, Armed Aggression of the Russian Federation as a Terrorist State against Ukraine, Symbols of the Military Invasion of the Russian Nazi Totalitarian Regime into Ukraine.»

2. **Cabinet of Ministers of Ukraine:**
   - Develop the procedure for governing the activity of printing enterprises, publishing houses, television and radio organizations, television and radio centers and other enterprises, institutions, organizations and institutions of culture and mass media; use of local radio stations, television centers and printers for military needs and explanatory work among the troops and the population; introduction of bans on the operation of reception and transmission radio stations of personal and collective use and information transmission through computer networks during the legal regime of martial law;
   - Take measures aimed at updating the broadcasting of Espresso, Priamyy and 5 TV channels in the digital network of T2;
   - Develop a mechanism for checking applications and various Internet services for compliance with the requirements of Ukrainian legislation on personal data protection.

3. **To the Ministry of Defense of Ukraine, General Staff of the Armed Forces of Ukraine:**
   - To publish on their official websites the vocabulary of terms used in the order of the Commander-in-Chief of the Armed Forces of Ukraine «On the organization of interaction between the Armed Forces of Ukraine, other components of the defense forces and representatives of the media for the duration of the legal regime of martial law» No. 73 of 03.03.2022.

4. **To all public authorities, other state and local self-government bodies:**
   - Revise the approaches to providing replies to the information requests and - in the case of massive postponement of requests consideration for the duration of martial law - to change it. The delay in providing a response to a request should be allowed only in the case of an objective impossibility of providing the requested information. In other cases, this legal basis should not be applied;
   - Consider restoring public access to registers (access to which has not been restored yet) if the grounds for restricting access to them have disappeared or were unjustified, applying a «three-step test» in deciding on this issue.
5 To civil society organizations:
- Maintain monitoring of the implementation of the Articles 111-1, 435-1, 462-2 of the Criminal Code of Ukraine and analyze it, specifically for proportionality of the interference with the right to freedom of expression;
- Initiate amendments to legislation to address the problems identified above;
- Scrutinise mobile applications and various Internet services for compliance with the legislation of Ukraine, in particular with requirements on personal data protection.
IX. ANNEXES

Annex 1. Response of the Head of PR Department of the Armed Forces of Ukraine on clarification of the meaning of certain terms, used in the Order of the Commander-in-Chief of the Armed Forces of Ukraine “On the Organization of Interaction Between the Armed Forces of Ukraine, Other Components of the Defense Forces and Media Representatives During the Legal Regime of Martial Law” No 73 of 03.03.2022.

Annex 2. Response of the National Center for Operational and Technical Management of Telecommunications Networks (NCU) of May 16, 2022 regarding the disconnection of settlements on the territory of Ukraine from mobile and Internet communication between February 24 and April 30, 2022 and regarding the number and list of websites that were blocked during the above period.