UMCI UKRAINIAN MEDIA AND COMMUNICATION INSTITUTE

ABA AMERICAN BAR ASSOCIATION
Rule of Law Initiative

Analytical Report

RISK MAP FOR PERSONAL DIGITAL IDENTITY

2022

Dutsyk, D., Orlova, D., Kifliuk, R., Koltsov, M. (2022) *Risk Map for Personal Digital Identity.* Kyiv: Ukrainian Media and Communication Institute, 98 p.

Authors: **Diana Dutsyk,**
Daria Orlova,
Roman Kifliuk,
Mykhailo Koltsov

General Editor: **Diana Dutsyk**

Layout Design: **Yana Dobrianska**

This Analytical Report has been prepared by Ukrainian Media and Communication Institute NGO within the Personal Digital Identity Protection project supported by the American Bar Association's Rule of Law Initiative (ABA ROLI). The content of the report is the sole responsibility of the Ukrainian Media and Communication Institute (UMCI) and may not reflect the opinions of donors or partners.

CONTENTS

THE IDEA BEHIND THE PROJECT

Ukraine declared its commitment towards a digital state and commenced a dynamic process for the digitalization of various spheres in the country in the autumn of 2019, when the Ministry of Digital Transformation was established, and in 2020 the Unified State Web Portal of Electronic Services Diia was launched.

Unforeseen circumstances, such as the COVID-19 pandemic, caused acceleration of the digital transformation not only in Ukraine but also around the world. According to the McKinsey consulting firm, the first eight weeks of the pandemic marked a five-year leap in the world's adoption of digital consumer and business solutions (The Economist, 2021).

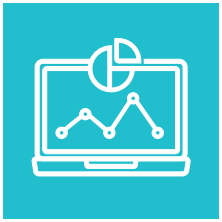
However, the development of technologies is not about benefits only. The digital era has brought lots of challenges that humanity has to deal with right away. Both governments and certain political forces as well as businesses or other actors (such as hackers or terrorists) are trying to influence citizens through the digital environment. In some cases, threats to personal digital identity can develop into threats to State security. Therefore, it is important to develop mechanisms aimed at protecting the rights of citizens, including their digital identity, in the context of constant technological development and the diffusion of information chaos.

For Ukraine, the protection of the digital identity of citizens became a high-profile issue because of the hybrid war that Russia launched against Ukraine in 2014. After all, in some cases, the ad-

vantages of digitization turned into serious vulnerabilities that could have become available to the aggressor. This became especially evident upon the full-scale Russian invasion on February 24, 2022 and after an increased number of cyber-attacks not only on critical infrastructure, but also on the banking system and electronic government services in order to steal citizens' data.

The Ukrainian Media and Communication Institute started to create a map of personal digital identity risks in the autumn of 2021. It was important for us to find out what key vulnerabilities of the digital identity of each of us are in order to understand how to build a policy in the rights and freedoms protection field in the modern digital world. However, the full-scale war meddled in. Though the main array of data had been collected even before these events, we deem it necessary to make the findings public. We have also updated our analytical report, by supplementing it with a number of up-to-date data and a section devoted to the security of personal digital identity in wartime.

The team of



RESEARCH METHODOLOGY

The study under consideration has two components:

1 analysis of experience of representatives of the communication-related professions, in terms of their online presence and interactions;

2 expert assessments of the key dimensions of digital identity risks.

This double focus of the study defined the choice of research methods: **focus-group discussions** and **expert discussions**. The choice of quality methods is related to the tasks of the study concentrated on identifying the most important aspects of the online experience of people and potential challenges, threats and risks through the expertise of relevant professional groups. It is the quality methods that, on the one hand, allow scanning of the field of experience and expertise and, on the other hand, forming a comprehensive vision of the problem under study.

As the scope of the study in question concerns the online sphere, the target group for the **focus-group discussions** was the **journalists** and **communication specialists** (including press-service staff) be-

ing the representatives of professions directly related to the online communication and information processes.The script for the focus-group discussions had a series of questions grouped into key blocks: **understanding of the notion of 'digital identity'; experience in the Internet usage; online risk assessment, digital security and patterns of behavior; digital identity and professional domain.** The objective of the focus-group discussions was to identify the details of the journalists' and communication professionals' experience related to various aspects of their online presence and interaction as well as to establish their thoughts and reflections on these aspects.

There were **4 focus-groups** within the study: **2 – with journalists, 2 – with communication professionals.** The regional representation aspect has also been considered. Two focus-groups were held with representatives of the national media as well as the organizations/ structures/ companies operating at the national level. These two focus-groups were held in Kyiv in the standard focus-group format.The other two focus-group discussions involved participants from different regions and were held online. In total, 27 journalists and communication specialists took part in the discussions.

The second component of the study is holding **expert discussions and developing a risk map** based on these discussions. Based on the preliminary analysis of the issues under investigation, the research team identified 4 key groups (dimensions) of risks associated with personal digital identity: **legal, psychological, reputational and security risks.** Thus, there were four expert groups formed and a script for expert discussions developed. The script is made around the following theme blocks: **the notion of digital identity and the use of the term in the professional discourse; identification and description of risks in the short-, medium- and long-term perspectives (brainstorming); analysis of the situation in Ukraine in terms of key risks; solutions to challenges and risks; analysis of the capacity and necessary resources for implementation of the solutions.** The content of these main blocks varied slightly, depending on the professional focus of the discussion. In addition to the participation in the discussion, the participating experts filled out tables to record main risks, in their opin-

ion, and assess the weight of each risk in the short-, medium- and long-term perspectives. In total, 35 experts took part in the expert discussions. Discussions took place live/ off-line in Kyiv. Moreover, a separate additional expert interview with another digital security expert was held.

The results of the focus-group and expert discussions made a basis of the report prepared by the research team. Also, the research methodology provides for discussion of the report in a mixed expert group made of representatives of four expert groups who participated in the study.

CONTEXT

In 2021, the Digital Transformation Index of Ukraine was evaluated by the European Business Association for the first time. The study assessed the current status of digital transformation in the private and public sectors. For this purpose, 130 general, operational and technical directors of the European Business Association member companies were interviewed. The integral indicator of the Index was 2.81 points out of 5 possible. The overall level of companies' digital transformation received the highest rating among the 5 components of the Index (3.4 points). The lowest were the overall level of digital inclusion development (2.46 points) and the overall level of digital infrastructure in Ukraine (2.6 points). The volume and quality of the provision of state electronic services was estimated at 2.63 points, and the overall level of digital transformation of industries - 2.97 points. Key barriers to the development of digital transformation are called by business representatives:

a excessive regulation and ineffective legislation;

b insufficient funding;

c low digital literacy (Diia. Business, 2021).

Despite the fact that the Index indicators are not ideal, starting from 2019 when the Ministry of Digital Transformation was established with the arrival of President Volodymyr Zelenskyi's team to power, Ukraine has taken a lot of concrete steps in the country's digitalization sector.

Before 2019, no one at the government level had set such ambitious goals as the team of the newly formed Ministry, determining that by 2024:

- 100% of public services will be available to citizens and businesses online;
- 95% of transport infrastructure, settlements and related social facilities will have access to high-speed Internet;
- 6 million Ukrainians will be involved in the digital skills development program;
- the share of the IT product in the country's GDP is to be at least 10% (Ministry of Digital Transformation of Ukraine, 2019a).

In the previous years of independence, few regulatory acts were adopted to stimulate the development of information and digital spheres. Specifically, the Law of Ukraine "On the National Informatization Program" was adopted in 1998. The Law of Ukraine "On Basic Principles of Information Society Development in Ukraine for 2007-2015" was adopted in 2007. In 2013, the government

adopted the Strategy for the Development of the Information Society in Ukraine. However, conservative government structures lacked a strategic vision as well as motivation to drive changes in this sector, relying at least on these documents.

In 2019, President Zelenskyy invited business visionary Mykhailo Fedorov to head the Ministry of Digital Transformation. Thus, the presence of political will combined with a strategic vision of required reforms changed the situation in the sector. A number of laws were adopted and a series of projects were launched, having completely changed the public service sector. So, in 2020, the Ministry of Digitization introduced the Unified State Web Portal of Electronic Services Diia, with an electronic cabinet of a citizen allowing access to the following personal information: voter profile, debts, vehicles, real estate, land, business. This cabinet also allows registration, closure and change of data related to individual entrepreneurs and limited liability companies. During the COVID-19 period, citizens were able to receive a vaccination certificate through the Diia platform. The number of various services of this portal is constantly increasing.

On August 23, 2021, Ukraine was the first country in the world to introduce a citizen's digital passport having full legal effect. The mobile application Diia provides access to a number of digital documents: in addition to a citizen's passport, there is access to a biometric international passport, a tax payer's card, a driver license, a vehicle registration certificate, a vehicle insurance policy, a student card, an internally displaced person (IDP) certificate, and a child's birth certificate. The report of the Ministry of Digitization for 2021 states that the number of the Diia portal users exceeds 13.5 million (in the first half of 2022, this figure already reached 17.5 million Ukrainians), and the number of Diia mobile application users reached 12 million Ukrainians. More than 8.5 million users received an international COVID vaccination certificate. About 70% of families used the integrated package of services eMaliatko (allowing to register a child birth online and to receive up to 10 state services from various authorities, which are needed when a child is born). The number of other services users is also growing (Ministry of Digital Transformation, 2021b).

At the same time, the Ministry of Digitization has commenced the digital transformation of various sectors and industries. To this end, Deputy Ministers for Digital Development (CDTO) have been appointed in each ministry. This also concerns reforms in the digital sphere at the regional level. So, the Regional Development Strategy devotes considerable attention to digital transformation (VoxUkraine, 2021).

The Government states that the economic effect resulting from the introduction of electronic services is UAH 42 billion, and the savings received from online services amounted to UAH 14.7 billion for 2020-2022 (Ukrinform, 2022a).

A comprehensive analysis and evaluation of the results of digitization in Ukraine's various sectors is reflected in the report of the Polissya Foundation for International and Regional Studies (Polissya Foundation for International and Regional Studies, 2020).

However, there was a lot of criticism regarding the projects implemented by the Ministry at the first activity stage of the Ministry of Digital Transformation. First of all, the issue was raised about the safety of the Diia portal users and the security of their private data. There was some skepticism in society regarding the use of the Diia portal. At the first stage of this large-scale project implementation, the Ministry of Digitization did not invest enough efforts to make citizens aware of how secure this service was and what its advantages were. Some IT specialists also expressed concerns about the Diia security (Zaborona, 2020). Leakage of personal data from certain registers intensified criticism (Detector Media, 2022).

Experts also highlighted the risks of possible misuse by the state and law enforcement bodies of the data accumulated on each citizen who uses the Diia services. This could potentially have a negative impact on ensuring, and consequently diminishing, the basic rights and freedoms of citizens.

Another problem that has significantly hindered digital transformation in the country is digital inequality (not all settlements in rural areas have Internet coverage) causing inability for anyone, without exception, to obtain access to the services offered by the Diia portal. For example, elderly people (most of whom do not know how to use smartphones), people with disabilities or internally displaced persons found themselves in a vulnerable position (Institute of Innovative Governance, 2021).

The number of risks in the digital sphere (including the personal digital identity of each citizen) has increased many times after the full-scale invasion of Ukraine by Russia on February 24, 2022. In the first half of 2022, the Government's Computer Emergency Response Team of Ukraine CERT-UA operating under the State Special Communications Service recorded 1,350 cyber attacks the civilian facilities were exposed to (State Service for Special Communications and Information Protection of Ukraine, 2022a). Microsoft company in their report "Defending Ukraine: Early Lessons from the Cyber War" separately noted attempts of some hacker groups associated with Russian special services to steal personal data of journalists, bloggers and media persons. Microsoft also made a conclusion about the correlation of attacks in physical and digital spaces: cyber-attacks often precede missile strikes (Microsoft, 2022).

Of particular note is the situation observed in the settlements occupied after February 24 or those located in war affected regions. There is either no communication and Internet, or the occupiers block access to Ukrainian Internet resources. Citizens of Ukraine, who stayed in these territories, find themselves under an information blockade. Also, they are constantly exposed to the risk of their smartphones being seized and, thus, to the occupiers' access to their personal data.

In this connection, the Ministry of Digitization, according to its head Mykhailo Fedorov, focused on data security in the first days of the full-scale war (Suspilne, 2022a).

The Ministry is also working on the restoration/provision of communication and Internet to critical

infrastructure and military facilities: Ukraine received more than 10,000 Starlink terminals through Elon Musk's SpaceX and other partners. They also plan to focus on the development of military tech, that is, digitalization of the military sphere. In addition, the range of services is expanding on the Diia portal, for example, one can submit an application for compensation for properties destroyed as a result of hostilities.

At the Ukraine Recovery Conference (URC2022), which took place in Lugano on June 4, 2022, the Minister of Digital Transformation stated that "during the war, the digital infrastructure proved to be the most stable. We are not just continuing uninterrupted work, but also launching new services almost every week and building a convenient state for Ukrainians" (Dzerkalo Tyzhnia, 2022a). The "Digital for freedom" program was also presented in Lugano - the technological part of the United24 Ukraine Recovery Plan, which involves Ukraine's transformation into the largest IT hub in Eastern Europe with a focus on security solutions. The "Digital for Freedom" program is divided into 10 large-scale projects, with each one, according to the presentation, requiring 1.5-3 years and from $2 to $5 billion (Forbes, 2022).

Russia's full-scale invasion of Ukraine pushed the issue of protecting digital rights, and therefore personal digital identity, to the background. This topic is not voiced from the mouth of the Government and in the context of the future post-war digital transformation of the country, although it should be one of the key topics in the context of all proposed transformations. The Ukrainian Media and Communication Institute deem it necessary to remain focused on this topic. We view this study of risks to personal digital identity as a pilot and the one that needs to be continued. The topic of personal digital identity protection in the full-scale war requires special attention.

UKRAINIAN DISCOURSE ABOUT THE 'DIGITAL IDENTITY' NOTION

One of the study objectives was to find out how familiar and spread the term 'digital identity' is and how it is understood and interpreted by representatives of different professions that to a certain extent have relation to the digital identity issues.

The analysis of both focus-groups and expert discussions has confirmed that the term 'digital identity' **is not used actively** in the Ukrainian discourse. As the term does not have a uniform definition in the English-language discourse, and the concept of 'digital identity' is still at the stage of formation and filling, it is quite expected that, **in general, Ukrainian professionals** do not use this term widely in their practice and have different **interpretations** regarding its content. Diversity in understanding and interpretation is largely determined by a professional group a person represents as each of these groups focuses on different aspects of digital identity. Personal awareness and varying degrees of interest in the issue, of course, also have an impact on the interpretation of the notion.

Journalists and **communication specialists** who participated in the focus-group discussions mostly perceive the term 'digital identity' in terms of a digital footprint and online self-presentation (for more details please read the section on the focus-group discussion analysis). The analysis of expert discussions has identified a wider range of interpretations and emphases among different professional groups.

Legal experts who discussed the legal risks noted that, although they have heard the term 'digital identity', they do not use it in their professional activities. Several respondents mentioned that they sometimes use or come across the use of the term in more routine contexts to refer to a digital footprint or digital identification, but they do not use this notion in the professional discourse. The legal experts also pointed out that in a legal context the definition should be suitable for law-making, whereas **'digital identity'** is a too vague notion and **'relies on non-existent legal categories',** according to one of the experts.Given this context, most of the legal experts participating in the discussion see focusing on the notion of **'personal data'** instead to be **more relevant**, as this notion is already a part of the legal framework and can be supplemented following new conditions of the development of digital technologies.

Representatives of an **expert group** specializing in **security** matters come across the notion of the digital identity in their professional environment and discourse the most often as compared to other expert groups. The term 'digital identity' is to a certain extent a part of their professional language. However, the security experts operate this notion largely in a narrower sense, i.e., in the context of **electronic identification/ authentication, unique properties of network users.** As a matter of fact, they prefer the notion of the digital identification that signifies technical aspects of being, authorization, activities of users online.

Communication and reputation-building experts who participated in the third expert group discussion interpreted the notion of digital identity quite broadly focusing mainly on such aspects as the digital footprint, the data available online about a person/group/organization and the self-presentation of users on the web. The experts

said that they rarely use this term in their practice, although their professional activity is related, among other things, to the construction of images, forms and contents of online presence of companies/organizations/brands.

Psychology experts, on the other hand, consider digital identity in terms of the **formation of complex personal identity, self-perception and self-presentation on the web.** The participants of this expert group raised a question of the complexity of the concept of identity as such, different theoretical approaches that conceptualize the identity, challenges related to the digital space affecting the processes of identity formation and construction. Moreover, the psychologists also mentioned other related concepts: 'digital self', online identity.

The expert discussions showed that the very notion of digital identity **had not become a part of the professional discourse** in their professional communities yet, although the **issue** of the concept of digital identity is close to each of the expert groups, in different aspects. The discussions also proved the digital identity to be an **extensive, multi-level and multi-faceted subject;** this gives a large scope for identifying various aspects of this phenomenon. Most of the clarity on the subject of discussion and of the consensus in understanding of the term was observed in the expert groups of lawyers and security professionals as their professional fields are more clearly defined with regulatory and technical aspects, respectively. Based on this, their vision of the term is more defined by the practice whereas the fields of communications and psychology give a bit more space for problematization of the very concept, and this was reflected in the expert discussions.

RESULTS OF FOCUS-GROUP DISCUSSIONS WITH JOURNALISTS AND COMMUNICATION SPECIALISTS

Analysis of focus-group discussions with journalists and communication specialists shows that the **notion of 'digital identity' is not spread in Ukrainian discourse.** Most of the focus-group participants had not heard of this term or had a rather vague idea of its meaning. Intuitively, the participants demonstrated understanding of the term and issues, but only a few participants said they were aware of the notion of 'digital identity'.

> *"The first time I heard* (the term - editor) *was when I was invited here. I imagine that there is something like it, but that it is called in such words... It will be interesting to hear, to talk about it."* (a male participant of a focus-group with journalists)

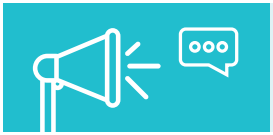
On the other hand, they were more active to mention and respond to the notions of 'digital footprint, 'digital security', 'information hygiene'. Thus, one may conclude that the term 'digital identity' is, as of today, **new, underdefined and, respectively, little used** both in the everyday discourse and in the professional discourse of people working with information and communication in Ukraine.

Meanwhile, the discussions showed that the **issues underlying the concept of digital identity are**

THE RISKS TO THE PERSONAL DIGITAL IDENTITY MENTIONED THE MOST OFTEN BY THE JOURNALISTS AND COMMUNICATION SPECIALISTS;

risk of personal data and correspondence leak,

page hacking risk,



psychological attacks, bullying, verbal attacks, hate speech, deliberate trolling,

compromised reputation risk,

online fraud,

blocking of social media pages,

Emotional exhaustion.

close and relevant to the participants and also strike a chord in people. The participants' reflections on the content of digital identity mainly concerned the digital footprint that one leaves online, the identification aspect of being online as well as the representation of one's personality online.

> *"Getting back to the digital personality, I want it to look like this on social media, so I represent it this way. So, some of my comments, my positioning and so on coincide with this. This is my image, how I want to see myself in the digital world."* (a female participant of a focus-group with communication experts)

Focus group participants demonstrated awareness of various aspects of data to record their online activities: from social media profiles to passwords, geodata, search history, etc.

In the structure of online activities identified by the respondents as the most important for them, the **social networks and communication on messengers** dominate, especially among the journalists. Facebook is a leading platform for journalists, although participants also mentioned Instagram and Telegram separately. The participants indicated the use of e-mail, search engines and online services (including online banking, watching series on streaming platforms, online learning, etc.) a bit less often. The domination of activities associated with social media and messengers in the responses of the participants indicates, first of all, the subjective importance and magnitude of these dimensions of being and interacting online.

Communication specialists also actively use social media and messengers, but the discussions re-

vealed some differences between these two groups under study. It seems that it is common for the **journalists** to **blur the boundaries between the personal and the professional** when speaking of social media use. The communication experts, in general, consider Facebook and other platforms primarily as work tools. This was especially noticeable during the discussions with the press-service representatives from regions.

It is interesting that a significant part of the discussion participants mentioned the segmentation of social platforms and messengers in their lives, especially the journalists. For example, Facebook is mainly a work tool, Instagram is more personal for many, different messengers are for different groups of contacts, etc.

> *"It was surprising that I am, in fact, present on almost all the most popular social networks, and evenly present. Because each bubble, each group uses different messengers. If it's a family, it's Viber.If it's some creative circles, it is Telegram. By the way, in Telegram, this is also about file sharing."* (a female participant of a focus-group with journalists)

> *"For me, Instagram is something purely mine. I try to post photos there... Facebook is for work. By the way, I don't use WhatsApp, although I have many foreign friends there. YouTube is also for work and creativity.* (a female participant of a focus-group with journalists)

Journalists also associate the **active use** of social media and messengers with their **professional activities:** they need to follow the agenda, discussions as well as look for interesting stories, communicate with the heroes of the materials, etc.

> *"Mostly, as my colleague has said, it's a messenger on Facebook, Telegram since recently. Why is this necessary? Because there is lots of information for work."* (a female participant of a focus-group with journalists)

> *"I get all the news via Facebook. Well, of course, I still read other media, I just open them in the browser. But for my work, we focus on creating the content for social media. This includes Instagram, Tik-Tok, this is what happens every day."* (a male participant of a focus-group with journalists)

For communication **specialists**, especially the press-service staff of government agencies, the social media are a part of their **work routine** and formalized professional duties. Their approaches to interaction on social media reflect mainly the established policies in their agencies, in particular regarding reactions to comments.

Constant immersion in the social media (both with peaks of activity and in the background), largely due to the professional operations, leads to an **excessive information and communication load,** that has been mentioned by an absolute majority of the focus-group participants. This aspect was

evident in three of the four focus-groups held (communication specialists from the regions raised less the topic of such a burden).

In addition to fatigue, the information and communication load often results in emotional **exhaustion.**

> *"I find the coolest stories on TikTok. It takes 3-4 hours to find a cool story. Sometimes I just swipe these videos for several days looking for something (…) I understand that I watch TikTok 3-4-5 hours every day. At the same time, I watch a video on YouTube, and I understand that tons of content are pouring out at me. And I understand this, actually, has a huge impact on my perception of the world and my emotional condition."* (a male participant of a focus-group with journalists)

> *"For me, overload is one of the biggest crises of my life. I remember times when people used social networks less. When everything was less online. I was definitely more creative. I used to always have ideas that I wanted to realize. Now, after 10 different purely work topics fall on me, and I have to make a strategic decision on these topics. I'm not even a big boss yet, I'm a mid-level link. I will read all this, come up with some kind of decision for that, and when my girlfriend asks me in the evening what kind of yogurt I want – I am unable*

to make a decision.I don't want to be asked, I don't want to talk, I don't want to read." (a participant of a focus-group communication specialists)

Several participating journalists mentioned the **professional burnout,** which is also associated with a constant presence in the information flow and sometimes causes journalists to quit the profession.

When considering the challenge of information and communication burnout, most participants spoke about the need to **control their private online presence**, to improve time management skills, self-control, to filter information for consumption more carefully, to structure working hours, etc.

"Information overload happens, for sure, because the work, the nature of work is that you have to work almost constantly on a computer and various gadgets. But speaking of some minor chats, especially those that distract attention, then the usual simple way is to set the bell, turn off notifications. And when I have more free time to check something, to laugh at, then I will check." (a male participant of a focus-group with journalists)

"We are all addicted. I've got a tracker also, to monitor myself." (a female participant of a focus-group with journalists)

> *"I have a principle, I mute all the messengers at night. My phone is permanently in silent mode.It does not buzz or ring.Only on rare occasions I turn on the sound."* (a female participant of a focus-group with communication experts)

Another challenge associated with professional activities is **more careful self-representation** on social media. Both journalists and communication specialists talked about it. During the discussions, many journalists commented that they started filtering their activities much more and controlling the level of frankness on social media. Such caution is explained by some to be a responsibility to the audience, by others to be a dictate of the times and new cultural practice in media organizations.

> *"For me, social media are some kind of a platform where, on the one hand, I have to talk about myself and spread my content, and make sure that my content is more actively visited, but on the other hand, I have to behave there rather carefully and be moderately frank. Because the frankness attracts the audience. And one must be frank enough not to offend other people who may have different political views."* (a female participant of a focus-group with journalists)

Additionally, the journalists mentioned the risk of being bullied for an expressed position, it prompts them to be even more modest in their statements on social media. The journalists from regional

media have to take more care about the local context, given the smaller distance with the local environment.

> *"I have already spoken about self-censorship on personal pages. It should be present to some extent. If we were not journalists, it would be taken one way. If we are journalists, it is taken on a different perspective, as a position. Since in the regional media it is even taken not as a position but as playing into someone's hands. Unfortunately, it is..."* (a female participant of a focus-group with journalists)

> *"If there are any political opponents here, squabbling and fighting with each other, then you have to be pro one or another. People, readers, see no other option. That's why very often you simply have to, when you see some injustice, a lie, and it's itching to write in the comments on Facebook, on social media... But you have to tell yourself: you don't need that, it's not your war, you'd better back off. Therefore, an element of self-censorship, as a colleague said, is totally present."* (a male participant of a focus-group with journalists)

Filtering self-presentation on social media is an even more sensitive issue for the staff of press-services, communications departments etc., as their professional context mainly limits building an outstanding personal profile online. Most of the participating communication experts noted that they

are used to this particularity of their work and accept them calmly. However, several participants feel pressure from these limitations on opportunities for their off-work activities.

> *"I have been in the civil service for two years, and it is difficult for me. I still need to get used to it. I can't even write a movie review because this is a personal opinion that may affect how Ukrainian cinema is perceived. I love Ukrainian cinema. And I want to describe it in a post of mine but I can't. Because if I didn't like something, here we go... It's hard for me because you can't even write about cinema."* (a female participant of a focus-group with communication experts)

In addition to the mentioned challenges of information and communication load and the need to filter personal declarations online, the participants also identified a number of risks for themselves associated with their online presence, for example: **the risk of personal data and correspondence leak, hacking of pages, psychological attacks, bullying, compromised reputation etc.**

> *"It seems to me that now, in principle, it is very easy to damage someone's reputation. Because very often there are some slanders, and one may just write a post from their point of view, and everyone will see it, like it, and there will be no response from the other side."* (a female participant of a focus-group with journalists)

The opinions about **potential risks** are defined by both **personal** experience and experience of the social environment. Most participants could recall at least a few instances of **negative experiences** of being and interacting online. The most frequently mentioned stories were when they were a **target of object of verbal attacks, hate speech, deliberate trolling; cases of personal data leaks; online fraud attempts; cases of blocking of their social media pages;** a bit less often – **creation of fake clone pages, mail hacking.**

> *"Most often, this is hate speech with professional activity. These attacks do not happen every day, but every month for sure. For various reasons. Maybe someone out there doesn't like what you're investigating. Some people you write about didn't like it. There may be attacks by various bots, there may be ugly caricatures, collages, photoshopped images of absolutely tasteless kind, just photo collages aiming to, let's say, offend a person. This is, perhaps, a most often piece of negative experience"* (a participant of a focus-group with journalists)

The participants also identified **weaknesses** in their own **online habits** that could cause negative consequences such as data leak or loss, infecting devices with viruses, etc. In particular, cases of using unlicensed software, not enough caution about passwords, etc. were mentioned.

> *"I am ashamed to confess. As we have lots of cases when I accepted to use the unlicensed soft."* (a female participant of a focus-group with journalists)

The participants explained the use of pirated products due to short financial resources, especially when it comes to the operation of regional media.

> *"It's not that we are mean. It's because we don't have any extra financial resources. For the software as well, if we install licensed software on every computer, we just need to work for a month without wages to cover this cost. Unfortunately, we can't, even though we do want."* (a female participant of a focus-group with journalists)

However, there is a trend in the increased use of paid online services, as mentioned by both journalists and communication specialists, citing examples of subscriptions to various content, purchasing access to licensed software.

Basically, the participants demonstrated a sufficient level of awareness of ways to ensure their own **security online**. For example, they cited their own approaches to **making up complex passwords, two-factor authentication, caution when receiving links, avoiding suspicious websites, having several SIM cards** for different purposes, etc.

> *"Firstly, I use two-factor authentication on all my social media. In order to make them secure. Secondly, I use complex passwords that are different for*

> *each of the social media so that they are not the same. And I try to share less information on social media, I don't join discussions, even when I really want to, from my private page. Well, I consciously like, I spread information less. When I am informed of cookies so I have to accept them, I never accept. I read a website through that little sheer."* (a female participant of a focus-group with communication experts)

However, some participants noted that they found exhausting the excessive attention to the digital security. This feeling is also associated with the widespread **perception** of the **illusory nature of digital security** in the modern world. Most participants agreed with the theses that privacy has become practically unattainable, and the personal data of any person is unprotected.

Analysis of the focus-group discussions shows that there are **diverse** practices related to **digital security** at the level of organizations represented by the participants. **International organizations/ projects and some government agencies** are the ones to pay attention to digital security issues the most. This is about regular trainings on digital security issues, established policies. However, **most media** seem to **have no developed policies and approaches**. In such cases, a lot depends directly on journalists and editors. Some of them had trainings beyond their newsrooms; sometimes journalists share gained knowledge with colleagues, this generally improves the understanding of the importance of digital security and ways to strengthen it. It is a frequent situation when digital security issue is a subject of informal discussions within the teams, there may be occasional briefings, but there is **not enough of institutionalized digital security practices** at the level of organizations. The situation is similar in many **government bodies as well as in local self-government authorities.**

"We do not have it to address everybody but, of course, everyone understands something for themselves. That if any important things are said then they are said in personal communication. But as about training, general, or at least a briefing, I don't remember that there was such a thing." (a female participant of a focus-group with communication experts)

"I was not briefed. And before, when I was at my previous jobs, I don't remember any training either. This is more of my knowledge that I received from trainings not related to work, something within the university curriculum." (a female participant of a focus-group with journalists)

RESULTS OF EXPERT DISCUSSIONS

In total, 4 expert discussions were held to identify risks to personal digital identity in various spheres.

Legal risks

were discussed by 10 legal experts. Seven participants represented niche non-governmental organizations dealing with media, protection of human rights, digital rights; two participants were from scientific institutions; one from a government institution. Gender composition of the group: 6 women and 4 men.

Reputational risks

were discussed by 10 experts from the communication sphere. Seven of them work for private entities as freelance consultants or founders of their own communication agencies, and three others represent government bodies. Gender composition of the group: 8 women and 2 men.

Psychological risks

were discussed by 8 professional psychologists. Three participants work individually (private practice), two participants represented scientific institutions, two participants were from non-governmental organizations, one from a state institution. Gender composition of the group: 7 women and 1 man.

Security risks

were discussed by 6 experts from various spheres related to the security subject. One more expert was unable to attend the group discussion and agreed to be interviewed at a different time. When combining all security experts (7), 5 of them represented the non-governmental sector (Ukrainian and international organizations), 1 IT business, 1 a media organization. Gender composition of the group: 6 men, 1 woman.

PSYCHOLOGICAL RISKS

Strategic-level risks:

- decreased physical activity of the population of different age categories;
- a general decline in the intelligence level and analytical skills of the younger generation;
- decreased functionality of the younger generation (the generation growing up on the Internet finds it difficult to make adequate decisions in real life);
- limited opportunities for children to build their own identity in real life;
- harm caused to children's mental development, impact on changes in their sexual attitudes or even behavior as a result of a decreasing age of watching porn to 8 years old;
- increased number of mental illnesses; accelerated transition from mental to psychiatric states;

- modified behavior as a result of cognitive war (including increased cognitive biases and errors in decision-making);
- an increased gap between generations causing frequent conflicts in families.

Personal-level risks:

- online harassment (cyberbullying, cyberstalking and other types);
- Internet addiction;
- compulsive spending of money online;
- formation of multiple identities;
- derealization (loss of touch with reality) and depersonalization (loss of a sense of one's self);
- desocialization (exclusion of individuals from the social group they live in; loss of priorities and value orientations);
- information overload leading to troubled decision-making;
- unawareness of personal boundaries in the Internet space.

Effects of War

About 15 million Ukrainians will need psychological support because of the war, of which 3-4 million will require medical treatment. Such data were published by the Ministry of Health of Ukraine (Ministry of Health, 2022).

Excess pressure on the mental health of Ukrainians is put not only directly through combat actions but also through an aggressive information environment and a continuous flow of negative news. Mohammad Abo-Hilal, a clinical psychiatrist who founded Syria Bright Future, in an article for the Middle East Institute website (Washington, USA) noted that photos and videos of tragic events lead to a "new type" of psychological trauma when a person becomes a virtual witness of these events (Abo-Hilal, 2021).

Based on the analysis of expert discussions held with practicing psychologists and research psychologists, the psychological component is an important element of a person's digital identity, and although they focused (as other expert groups) on the fact that the term ‘digital identity’ itself is not actively used in their professional discourse, this issue remains highly topical in their practice.

"The issue is important, weighty and very timely. I work a lot with psychiatrists and see how online life can affect not only psychological comfort but also mental state. Sometimes this state is aggravated, sometimes mitigat-

ed... But this is an integral part of my practice," said one of the psychologists.

Despite all the advantages and opportunities created by the Internet, the expert discussion was focused on the psychological risks arising for a specific person from using the Internet and being in a complex and changing digital environment.

It is worth noting that psychologists associated most of the risks in the discussion with children and adolescents. These particular age groups: 1) are extremely vulnerable, since their identity is only being formed; 2) are extremely important in terms of building future strategies and future development of society.

The cross-sectoral nature of some risks was also pointed out. For example, the fact that security and psychological areas are very closely related, as well as psychological and reputational ones.

"How a person chooses a password for a particular service is not only a matter of security, but also a matter of psychology", said one of the psychologists.

Particular attention should be given to the problem of a special concern for all the experts present: growing incompetence in the provision of psychological services, an increased number of pseudo-psychologists or pseudo-psychotherapists, or coaches/trainers without adequate education in this domain but conducting lots of trainings online and providing services

> *"Calling yourself a psychologist, psychotherapist, coach, trainer in the online space is not a big deal"; "a variety of services are offered, from stone therapy to NLP programming...",* said one of the psychologists.

We structured the discussed risks into two clusters (at personal and strategic levels). As a number of personal risks become of strategic importance and may lead to considerable social changes in the near future.

STRATEGIC-LEVEL RISKS

First of all, the experts highlighted **decreased physical activity of the population of various age categories**, especially children and adolescents who spend a lot of time using gadgets. Worrisome is the spread of such a social disease as hypodynamia ("reduced activity"), which in turn leads to negative physical, psychological and socio-emotional health effects.

According to the first ever research of the level of physical activity among adolescents by the scientists of the World Health Organization (WHO), the physical activity indicators of more than 80% of adolescents are below the recommended level (WHO, 2019).

Physical activity became even more decreased with the onset of the COVID-19 pandemic (FitBit, 2020).

Physical activity has a positive effect on cognitive development and socialization, primarily of the

child. On the contrary, when decreased it causes **a decline in intelligence level and analytical skills of the younger generation**, the experts emphasize.

> *"Hypodynamia is related to screen practices... Early childhood development is very strongly linked to physicality, which is then followed by delayed or distorted development of the cognitive sphere. ... Children, compared to those whose development was not tied to screen practices, lag behind in the intelligence development because the sensorimotor phase of the intelligence development is locked. It prevents the child from developing the available potential and forming the brain's readiness for the next phases of development. Therefore, in a long-term perspective, we face a serious risk of a very significant decline in intelligence",* said one of the psychologists.

One may add here the loss of communication skills of children and the younger generation: they communicate mostly in writing through various messengers, whilst they are reluctant to talk to each other them, as they find it difficult to express themselves

> *"Children are good at exchanging written messages. But to communicate, to talk to another person in this way...",* said one of the psychologists.

As an example, the American Academy of Pediatrics advises the following:

1. forbid the use of any gadgets (including TV) for children under three years old;
2. allow only one hour of "screen time" per day for children aged 3 to 5 years;
3. allow playing video games up to 30 minutes a day only to children aged 12 years and older (American Academy of Pediatrics, 2011).

Living life on the Internet results **in the decreased functionality** of the younger generation in real life and the reduced ability to make relevant decisions in various life situations. Modern children are **limited in the capacity to form their personal identity in real life, as noted by psychologists during the discussion.**

> *"A child who constantly builds relationships with the help of emoticons, TikTok and so on, does not develop a special ability to build relationships in the real world. ...The capacity of creating one's identity in real world is becoming more and more limited",* said one of the psychologists.

One of the psychologists gave an example of an adult patient who was addicted to games at school and university. He doesn't remember the process of his self-determination, as the real life passed by when all his time was spent online. Now he needs psychological assistance for adaptation in real life and for self-identification.

The experts noted another dangerous trend: **a porn watching age decreased to 8 years old.**

> *"Based on the latest studies, the average age when children watch porn is 8 years old. Two years ago, this threshold was 10-11 years old",* said one of the psychologists.

Watching this kind of videos is detrimental to a child's mental development, affects changes in their sexual attitudes, beliefs or even behavior (Association of Sexologists and Sexual Therapists of Ukraine). In addition to having access to harmful content, children also become targets of online abuse by adults. According to the annual report 2020 of the UK independent, non-profit charitable organisation Internet Watch Foundation (IWF) dealing with search and removal of publications containing children who have suffered sexual violence in the virtual space, the risk to children (especially girls) of becoming sex abuse victims on the Internet has increased significantly in various countries around the world (Internet Watch Foundation, 2021). Ukraine is among the leading producers of publications of a violent nature against children on the Internet (Radio Svoboda, 2021). In early 2022, law enforcement agencies of Ukraine exposed a network that produced and sold porn content involving children including the 6- to 8-year-olds (Ukrainska Pravda, 2022).

Another risk is a change in the cognitive sphere (but not only in the context of the problems observed in a child and adolescent development). Systemic changes *("the cognitive sphere is now being distorted and modified...")* happen as social networks and "smart" technologies spread. Opportunities *"for manipulating other people"* are growing. The experts are focusing on the fact that *"algorithms are aimed at our psychological qualities"* and often work with our emotions.

The conclusions of Ukrainian experts are also confirmed by international studies. Specifically, researchers at Johns Hopkins University point out that new media and new media technologies encourage "fast thinking", which is reflexive and emotional, as opposed to "slow thinking" (rational and reasonable). *"Our cognitive ability can also be weakened by social networks and smart devices. The use of social networks can increase cognitive bias and inherent errors in decision-making,"* they note (Johns Hopkins University & Imperial College London, 2021). Cognitive bias or cognitive illusion is a deviation in judgments accompanied by a possible illogicality in making conclusions about other people and situations (for more details see the works of Kahneman and Tversky).

One more risk is related to **the increased number of mental illnesses; accelerated transition from mental to psychiatric states** *("more time spent in the digital environment is associated with the complications of many psychiatric diseases")*. Practicing psychologists gave examples of mental and psychiatric illnesses of the patients, especially lonely ones, who did not have enough social contacts, and instead (due to work) were forced to spend a lot of time online. The experts are concerned by the fact that *"a significant part of Ukraine's population is at the borderline and psychotic levels."*

The situation is complicated since *"psychological protection mechanisms that work in reality do not work in the virtual world."*

> *"There is no repression in this virtual or digital world. In the real world, we are able to repress and forget [traumatic experiences], though in the digital world a person can constantly be under stress, constantly be triggered and touch these personal traces...",* said one of the psychologists.

The experts also spoke about **an increased gap between generations** as one of the risks.

"The younger generation lives in a virtual world and is often more familiar with how to behave safely [in this world]. However, for the older generation, this space is unknown, this fuels the feeling of fear," says one of the experts. She, therefore, is of the opinion that because of this fear parents increase control over their children without discussing the rules with them which leads to family conflicts.

The experts also point out the difference in the culture of behavior between generations in social networks. For example, parents often post photos of their children on social media without the child's permission and thus do not understand how this fact may affect the child today and in the future *("adolescents say that they were actually against their parents posting such photos. They did not want this trace to remain")*.

Although not all experts agreed that the generation gap issue is becoming increasingly important in the context of digital transformations and the development of new media

> *"I am not convinced that this issue should be distinguished in the context of digital identity. The generation gap always exists, at any time...",* said one of the psychologists.

PERSONAL-LEVEL RISKS

Online harassment of various types and forms (cyberbullying, cyberstalking, flaming, harassment, doxing, etc.) today has grown into a social problem requiring separate studies and solutions. Anyone, whether an adult, a child or an adolescent, can be exposed to online harassment. This problem comprises a range of components, from legal (notably, there is no legislation in Ukraine on the liability for harassment, including online harassment) (Denysenko, 2020) to psychological ones.

Psychology experts focus on the fact that cases of online harassment often involve serious psychological consequences.

> *"It is impossible to ignore talking about contributing to a suicide and depressive conditions, especially with adults. When at some point you have a feeling like "I am being stalked", "I am being followed", this can also provoke psychotic conditions, which will have to be treated with medication..,"* said one of the psychologists.

It must be noted that society mostly focuses on the problem of online harassment of children and adolescents (there are studies (NGO Docudays, 2020), information campaigns, etc. on the subject) but little is said about harassment suffered by adults. The same can be said about other problems that people can face on the Internet.

Another serious risk discussed by the experts is **Internet addiction (addiction to the Internet** in general and various online activities, for example, online games or social networks). According to the research by the United Nations Children's Fund (UNICEF) in 2019, almost one in four adolescents aged 10-17 reported that in the past year they regularly realized they could not think about anything except the moment when they would be able to use social networks again. Most of them are represented by 10-year-old boys (35.2%). Almost one in five felt dissatisfied because they wanted to spend more time on social networks (UNICEF, 2019). Again, there is no data on adults specifically for Ukraine.

Compulsive spending of money online can also be a form of Internet addiction. The experts involved in the discussion highlighted the marketing campaign strategies and the fact that the average age of the people being targeted by advertisement is constantly decreasing

> *"The younger a buyer is to trust a particular brand, the higher chances are that at an older age they will recognize it,"* said one of the psychologists.

Other risks relate to **the formation of multiple identities of one person,** when people present themselves differently in real and virtual lives.

> *"In reality, we are ourselves, but in the digital network we can create a different image for ourselves, a false self, which is extremely dangerous,"* said one of the psychologists.

> *"New virtues are emerging, where, for example, girls act as boys, or vice versa. And this is not a problem of sexuality, but confusion with self-identity,"* said one of the psychologists.

> *"In such a way people express themselves, even if they create a fake identity, it is still part of their consciousness. This is how they want to position themselves. It is them who choose a male nickname or something else... but in digital environments they show other, probably repressed, parts of themselves,"* said one of the psychologists.

In this context, the experts emphasize that the algorithms in social networks and search systems are *"focused on our psychological qualities"*.

> *"So we can talk not only about the influence of our self on the virtual self, but also about how this digital identity affects who we are. And this mutual influence just does not sound anywhere except for the psychological component,"* said one of the psychologists.

Virtual reality and artificial intelligence, according to the experts, create new conditions for the formation of personality and its identity.

> *"Personality cannot exist without a framework. It is determined by the external framework of society and the framework of the very self. However, we have a third component - the artificial intelligence, which is no longer a pure algorithm created by people. It is an artificial essence that learns and evolves by itself, using our aggregated data and returning it to us in some form. In view of this, digital identity is a part of identity, but on the other hand, it already acquires a new quality that needs to be analyzed..,"* said one of the psychologists.

Derealization (loss of touch with reality) and depersonalization (loss of a sense of one's self) also occur when people spend more of their time in the Internet space. This happens because in the virtual space, existential issues, in particular, *"awareness of death, the meaning of life, etc. – are distorted."* A person may not distinguish between their achievements in real and virtual lives *("in network subjectivity you may be ideal, but in reality you will be disappointed with who you are")* – as a result, *"substitution is observed with a subsequent likelihood that this process will even become pathological".*

The Internet and social networks can also accelerate the process of **desocialization of a personality (exclusion of individuals from the social group they live in; loss of priorities and value orientations).** The risks are particularly high again for children and adolescents with unformed identity.

The Internet creates the illusion of ease and security, the illusion of relationships and friendship, which leads to loss of reality and connection with the real social environment. As already mentioned above, this consequently affects the functionality of an entire generation, creates indecisive and irresponsible attitudes in social life.

One more risk that has increased with the development of the Internet, social networks and "smart" technologies is **information overload** having also significant and negative effects on a person's ability to use knowledge, in particular to systematize and critically analyze information, build logical connections, etc.

Furthermore, such a problem as **unawareness of personal boundaries in the Internet space** can create offline risks and negatively affect a person's real life. One of the experts talked about experiments on this issue: *"Adolescents posted certain information about themselves in social networks. Then they gathered a large number of people who shared the information posted by adolescents on the networks. The adolescents were surprised and scared about how they knew about this, but people do not fully realize who is noticing and watching them [on the Internet]."* There is also no awareness that any information published on the Internet may affect a person's life and future.

The experts stressed that these are all new challenges for psychologists, and they need to learn to work with them.

REPUTATIONAL RISKS

Strategic-level risks:

- no alternatives to the reputational crisis in the digital world (as the online reputation is not totally controllable);
- leakage of personal data;
- accelerated (due to the very nature of the social media) uncontrolled spread of negative information about an individual/campaign/state;
- no adequate culture of safe Internet use and personal data protection among most of the citizens;
- interdependence of personal and corporate reputation/reputation of the state;
- weak personal data protection legislation in Ukraine, causing further risks.

Personal-level risks:

- negative digital trace (e.g., back from the childhood or younger years);
- gap between the real and virtual reputation;

- anybody can hack one's identity and to construct a new one;
- porn revenge;
- relative confidentiality (any information sent privately from one individual to another can be only relatively confidential);
- blocked/erased content that a person posts on their social media or other online resources.

Effects of War

Russia does its best to smear Ukraine in the eyes of the Western partners making use of different information warfare, including by discrediting the reputation of Ukraine's high officials (e.g., in the contest of disinformation narrative about trafficking of the weapon supplied by the Western partners (Ukrinform, 2022b).

However, Russian attacks are aimed not only at high-ranking Ukrainian officials but also at active Ukrainian citizens and Ukrainian media and their reputation. Blocking of Ukrainian content shared by individuals (citizens, journalists, bloggers, writers or actors, etc.) on social media has intensified since the russia's full-scale invasion to Ukraine. Restrictions are caused by:

1. respectively programmed algorithms of social media;

2 complaints and attacks by russian or pro-russian users. Some experts are also convinced that russia has an influence on people who moderate Ukrainian content on social media of Meta Company (Texty, 2022).

For example, Facebook blocked access to the online lecture of a member of the board of the Ukrainian Association in Finland, a journalist Nataliya Dmytrenko about the Ukrainian roots of the artist Ilya Repin (Dmytrenko, 2021). And Instagram banned the posts of the Ukrainian writer Kateryna Babkina about the atrocities of the Russian military in Bucha (Babkina, 2022). After the review requests, the posts of both Ukrainian women were restored. However, these are not one-off events but a systemic problem. By making efforts to block personal stories of Ukrainians, russia is trying to share with the world an adverse publicity of the whole of Ukraine, interpreting the aspirations of Ukrainians for self-determination and their own identity as "fascism" and "radical nationalism". In May 2022, Mykhailo Fedorov, the Vice Prime Minister and the Minister of Digital Transformation of Ukraine, met with Nick Clegg, the President of Global Affairs at Meta. One of the outcomes of this meeting was that social media Facebook and Instagram will be blocking Ukrainian content less often (Dzerkalo Tyzhnia, 2022b).

In 2020, the reputational risk topped the list of risks to the majority of companies in different regions of the world, as says the Global Risk Landscape report prepared annually by BDO LLP, a UK accounting and consulting firm. They surveyed 500 executives of companies across Europe, the Middle East, Africa and Americas. 70% of businesses have experienced an event that has threatened its reputation. Over a third of companies (35%) consider themselves to be reactive when it comes to reputational issues, not proactive (BDO LLP, 2020).

The developments of the last two years, in particular, the COVID-19 pandemic and the full-scale war of russia against Ukraine have re-shaped the world and shaken all global processes. Even though the Report: Global risk landscape 2022 by BDO LLP does not put the reputational risks number one, they are still in business focus. This year the reputational risks for business are in the ethical realm (BDO LLP, 2022). Consumers do not want to be engaged with unethical brands, like the ones that have something to do with financing the war and russian terrorism. Thus, the reputational risks may have the direct financial effect.

Since the expert discussion of reputational risks was held before the full-scale Russian invasion, it does not touch the wartime aspects. However, some risks in wartime have been scaled up and bring even greater threats than in peacetime. Especially when it comes to the Government, high and top-level officials.

STRATEGIC-LEVEL RISKS

A reputational crisis in the digital world, either for an individual or for a company and a state, is inevitable and has no alternative. The development of social media and various communication platforms contributes strongly. Communication experts, who participated in the discussion, believe so. Therefore, the best solution is to be prepared and have response strategies.

One also needs to understand a relation between the reputation of individuals and the reputation of organizations they work in, or even the states (when it comes to, for example, the leaders or top officials of the state). This is particularly true for Ukraine in wartime (see the box "Effects of War").

Most experts have come to a conclusion that some of the reputational risks are directly related

to personal data. Therefore, it is extremely important how they are operated by the state, being a manager of numerous registers, as well as how they are operated by certain citizens. Article 35 GDPR says that processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, including the risk of damage to reputation (Association of Ukrainian Human Rights Monitors on Law Enforcement, 2021).

During the discussion, the experts underlined that Ukraine has a low culture of personal data handling, both at the level of the state and at the level of citizens, as well as a low level of digital literacy.

This is also recognized by the Ministry of Digital Transformation. Aiming to foster the adequate personal data handling culture in Ukraine, in 2021, the Ministry of Statistics developed a tool to help the business community master the basic elements of Ukrainian legislation and international standards in the field of personal data protection. This is about the test helping to check any company for compliance with the requirements of the personal data legislation when working with customers. The test is available on the platform Diia. Business (Diia. Business, 2021b). The platform also contains a series of trainings about personal data for businesses and organizations (Diia. Business, 2021c).

They also noted the weak personal data protection legislation in Ukraine causing further risks. Experts in other groups, in particular in the group that discussed legal risks, also pointed out this problem.

> *"Anybody may use another person's personal data, and will not be punished for it. Ukraine hasn't got any legal mechanisms for the protection of citizens on the Internet and any punishment for using information without a person's knowledge, or for stealing their digital identity,"* one of the experts said.

> *"The users may have an impression that nobody regulates the digital environment but, in reality, a person does not fully control their digital identity. Moderators of social media, governmental authorities, owners of registers – all of them have access to personal data left by the users. All this data may "leak" online, or it may be stolen by hackers. The Internet, despite the freedom it gives, is a human-driven environment,"* one of the experts said.

PERSONAL-LEVEL RISKS

Communication experts say that any information published on the Internet in one way or another shapes a person's digital identity and affects their reputation. On the one hand, this is about the information that a person shares about themselves and their activity online; on the other hand, this is about the information that other people share about a person (and this is something that is difficult to influence and change).

Experts also spoke about the negative digital footprint. *"Never forget that they remember everything on the Internet. For example, at a young age, a person may have expressed a controversial point of view online, and then, having grown up, may change it. However, this post can be retrieved (if the person is famous, then this will happen for sure), so this will have a significant damage to the reputation, even if the person no longer thinks so,"* one of the experts said. However, this negative digital footprint can destroy a career or personal life.

Reputational risks are also created by attempts to present oneself as something other than they are.

> *"Quite often, users create themselves significant risks to their reputation trying to form their personality on the Internet different from what they really are,"* one of the experts said.

Stealing, unethical use and fraud of personal or private data can also affect the reputation. For example, personal correspondence may be made public online and used as a tool to destroy someone's reputation. A situation may also arise when third parties (abusers) get unauthorized access to person's accounts, meanwhile a person may still have their access and not suspect anything. Such abusers may send letters, messages, etc. on behalf of a person without their knowledge, one of the experts emphasizes.

Another common tool for reputation destruction is revenge porn (when ex-partners post someone's private sexually explicit photos or videos online).

The experts find it dangerous not only that information about the user (personal data, photos, accounts, etc.) may be stolen but also that other people, for whatever reason, may use the information that we ourselves give them or post in the open access.

The experts agree that one does not fully control their digital identity, and therefore their online reputation. However, one of the experts underlined that it is worth trying to form your digital footprint and digital identity on your own. *"If we, ourselves, do not say about what is important and necessary to us, others will speak for us,"* he believes. It is important to understand that a reputational crisis in the digital world may come one way or another (an account may be stolen, bill collectors may call, etc.), and we have to accept it. However, it is important to know and understand how to deal with the consequences, the expert believes.

SECURITY RISKS

Strategic-level risks

- negligence of register managers in using personal data;
- nlow culture of data use by personnel and representatives of various public authorities that are register holders;
- nno alternatives to Diia, the Unified State Web Portal of Electronic Services (this creates a number of risks in the event of an attack on this application);
- nexcessive influence of the human factor on the data protection and critical infrastructure spheres;
- nan imperfect system of electronic identification;
- nshortage of high-level information security experts in government agencies;
- nno regulations for private companies collecting personal data;
- ninsecurity of digital identities of persons who are government-level decision-makers or have access to critical infrastructure;
- nno internal audit systems in the digital security sphere at the governmental level.

Personal-level risks

- low awareness of citizens (including civil servants) of digital security matters; a commonly low level of digital and media literacy;
- fake identities created in order to lure out data;
- unauthorized access to digital identity;
- digital identity theft;
- linking a person's digital identity to one smartphone.

Effects of War

Massive cyber-attacks on critical infrastructure facilities, public authorities, media, activists, human rights defenders; threat to the integrity of data collected by certain companies, organizations or government agencies; hacking of private accounts of Ukrainian citizens, etc. is a non-exhaustive list of threats brought by the Russian full-scale invasion.

Before the full-scale war, Ukraine was actively developing the sphere of open data. In 2020, Ukraine for the first time made it to the Open Data Maturity ranking (open data maturity as-

sessment in the EU and EFTA countries), being in the 17th place among the EU countries (Open Data Maturity, 2020). Therefore, the issue of data protection arose in the first place. Public authorities were enabled to place information resources, public registers and relevant backups on cloud resources or in data processing centers located outside of Ukraine. Furthermore, in connection with the increasing threat to data integrity, a decision was made to limit or close access to most public registers (Brusko, 2022).

A number of companies engaged in the cloud service market moved from Kyiv. As an example, one of the largest Ukrainian cloud services, GigaCloud, storing the data of thousands of companies and organizations, moved the data storage system from Kyiv to Lviv under the shelling of Kyiv in the first days of the full-scale war. Moreover, it also helped to evacuate the equipment of the Prozorro public procurement system to Lviv (the amount of data stored by this administrator since 2015 reached almost 270 TB, and its entire infrastructure was located in Kyiv in two data centers; in the event of bombings, all data could have been lost). Currently, copies of all data and documents as well as the virtual infrastructure are additionally stored in the Amazon cloud (Ekonomichna pravda, 2022).

The governmental Computer Emergency Response Team of Ukraine CERT-UA ensures monitoring of cyber incidents and maintains the respective register, including assistance provided to prevent, detect and eliminate the consequences of cyber incidents (https://cert.gov.ua/). Their operation intensified to keep the public informed about various cyber threats. For example, Ukrainians were warned about a massive spread of suspicious links imitating the Facebook authorization page aimed at stealing user data (CERT-UA, 2022).

However, threats to certain people and their digital identities have also been intensified be-

cause of the war. The citizens who found themselves in the territories occupied by Russia after February 24, 2022 are the most vulnerable. The biggest risks they face are:

1. informational blockade aimed at cognitive influence and change in behaviour of the residents living in these territories;

2. loss of digital identity due to the physical loss of the phone/computer or access to them by the occupiers (for more information on these threats, see the section "Risks to Digital Identity in Wartime").

Another part of the risks is on the boundary line of the legal and security spheres, as they arise due to the unsettled nature of a number of issues, for example, the use of artificial intelligence for identification of persons, etc., as well as the growth of the government's ability to apply excessive control in the sphere of personal data (due to the new laws adopted under the martial law), and consequently increased risks of abuse when accessing such data, especially by investigators and prosecutors (Brusko, 2022).

More information on how the war influences the sphere of open data can be found in the analysis by Tetiana Oleksiiuk, Ukraine's representative in the Expert Group under the Council of Europe Convention on Access to Official Documents (Oleksiiuk, 2022).

STRATEGIC-LEVEL RISKS

The expert discussion mostly focused on the issues of "the state in a smartphone" promoted by the team of President Volodymyr Zelenskyy, and on Diia, the newly created Unified State Web Portal of Electronic Services. The non-transparency of its launch process, the closeness of the Ministry of Digital Transformation at the first stage of work resulted in criticism by the expert environment, including the IT security experts. The experts indicated that the code of this application is closed. This gives rise to mistrust, as there is no possibility to check the level of protection of the personal data they operate (Zaborona, 2021). This issue was also subject of the expert discussion arranged by the Ukrainian Media and Communication Institute. The Ministry of Digitization, in their turn, stated that Diia does not collect or store personal data of Ukrainians, but only displays the information available in the registers (Dom, 2021).

Moreover, in the course of the discussion, the experts highlighted no alternatives to the Diia service — some services are available only on this portal, but due to digital inequality and different levels of digital literacy not all citizens can use them.

The experts also criticized the idea of unified registers, which was discussed by the government when the expert discussion was in progress.

> *"The register of registers is a destructive practice. On the one hand, it is a good tool for monitoring and controlling the country, and on the other hand, it is a very risky pattern in its own ways. The very Diia accumulates one's*

> *address, passport, driver's license so on. All in all, a lot of data. Before Diia was launched, 5 or 10 applications were to be submitted to various authorities to obtain these documents. And now one can get all this simply in one database".* (a participant of the expert discussion on security risks)

According to one of the experts, the approach to digitalization needs to be modified, in particular, the number of permits in various spheres must be reduced replacing automatic conversion of hundreds of documents into a digital format.

The experts also mention that it is highly important to understand the motivation why various entities and organizations collect personal or sensitive data about citizens, and whether they need these or other data at all.

> *"If every institution is to have a complete set of huge data about me, then the question arises: Why do they need them? Digitization allows them to get the data, but why does this institution need this pile of information?"* (a participant of the expert discussion on security risks)

A further risk is negligence of register managers in using personal data. The experts stressed the low culture of data use by personnel and representatives of various public authorities that are reg-

ister holders. And at the governmental level this is about *"the inability to realize the importance of these risks."* As a result, the experts periodically record unauthorized transfer of data to third parties, data theft, or data fraud (Media Sapiens, 2020a).

One of the experts suggested combating data theft and leaks through disclosure.

> *"However, this disclosure must be communicative. Figuratively speaking, we will disclose data about private entrepreneurs (FOPs) to prevent their falling for fraud, but we will also teach FOPs [digital and simple data protection skills - ed.]...".* (a participant of the expert discussion on security risks)

Although in general *"managing such risks at a global or institutional level requires a clear understanding of the needed level of technical expertise. Actually, the combination — technical experts who support the infrastructure and analysts who shape the vision — should work. This is not the case for the public sector,"* says one of the experts. Most of the participating experts agreed with the shortage of cyber security experts in the public sector. The main reasons for this, in their opinion, are underestimating of its importance by public authorities, low salaries in the public sector (not competitive with market ones) as well as no regulations and budgets allowing public authorities to involve market experts in security consultations [during the full-scale invasion, the Ministry of Digital Transformation created the IT Army of Ukraine, digital experts joined it on a volunteer basis (Suspilne, 2022b). The organizers of the CYBERSEC Award 2022 awarded Ukraine and the Minister of Digital Transformation Mykhailo Fedorov with two special awards "for heroic resistance to Russian aggression and protection of digital borders of the democratic world" (Government portal, 2022).

However, continuing with the HR theme, most of the experts agree that in terms of protection related matters (whether it is about personal data systems or about cyber protection of critical infrastructure facilities) the influence of the human factor should be reduced.

> *"In fact, total management of critical infrastructure by machine algorithms is a certain protective mechanism. However, machine algorithms should not be considered as something existing separately from humans. When introducing them, we introduce our own shortcomings. Thus, no matter how much we intend to remove the influence of the digital personality on decision-making for critical infrastructure, it will still remain to some extent. This is the case when not even the digital personality itself, but the mechanisms aimed at neutralizing its shortcomings, also pose some risks."* (a participant of the expert discussion on security risks)

Particular attention should be given to the protection of digital identity of the individuals who have influence on the national decision-making and access to critical infrastructure, since this is a real risk for the state, especially in wartime.

> *"An attack on a certain digital identity can be commensurate with an attack on critical infrastructure. ... In other words, information about a digital identity,*

> *for example, about the activity of this person in networks, is enough to understand how exactly one can take advantage of their position.*" (a participant of the expert discussion on security risks)

The experts believe that the electronic identification system also needs attention. Despite the fact that the Cabinet of Ministers of Ukraine approved in 2019 the Regulations on the Integrated System of Electronic Identification, the experts spoke about the need for standardization of electronic identifications, primarily in the government and banking spheres. The electronic signature system must be secured. The discussion brought up a case demonstrating gaps in this security system. This is about the case when the petition on the President's website was signed by the name of Joe Biden through a fictitious vote using a stolen key of an improved electronic signature generated by JSC CB "PrivatBank", a qualified provider of electronic trust services (KNEDP). Later on, the State Service for Special Communications and Information Protection of Ukraine alleged that it was a planned hacker attack. A full verification of the electronic trust services system was announced afterwards (State Service for Special Communications and Information Protection of Ukraine, 2021b).

There was no unanimity among the experts regarding the need to regulate digital security issues. Some of them believe that Ukraine should improve its legislation in the sphere of digital security, personal data protection, etc. The others argue that the legislation would not keep up with the development of technology. Therefore, "grassroot regulations" are needed for the entities handling data including private ones, rather than legislative changes

PERSONAL-LEVEL RISKS

All the experts agreed that one of the biggest problems of protecting digital identity at the personal level is the low digital literacy of the population. The majority of Ukrainians are unaware of how to protect themselves online (as well as to protect their personal data), this is also the case of the representatives of public authorities, in particular.

> *"Today there is a problem related to public awareness of digital security at the most elementary level. Every day I communicate with representatives of different communities and they set passwords 1-1-1-1. These are people working in public authorities. So, what can we say about ordinary Ukrainians?"* (a participant of the expert discussion on security risks)

Careless communication and trust in strangers on the Internet, voluntary disclosure of certain information about oneself is also a consequence of low digital and media literacy

> *"Network users need to be aware that with the development of social networks, more and more "fake" persons appear and therefore any disclosure of data and communication with people on the Internet require careful approach. First of*

all, you need to understand your own responsibility for the digital identity formation." (a participant of the expert discussion on security risks)

The experts highlighted the fact that even indirect personal information can create certain risks for a person (for example, *"the water consumption readings show whether we are at home or not, and it can be clear at what moment one [a thief] may come to the apartment"*).

Any person can be exposed to fraud attacks in various ways (both telephone attacks and fishing) to get passwords to mail, social media, banking services, etc. However, money is not always the ultimate goal of fraudsters.

"Everyone thinks that fraudsters are attacking you for money. This mostly happens with elderly people but, in fact, much more valuable is an attack on credentials, the characteristics that tie you to your digital identity, because they enable you to get access to the resources that cannot be otherwise available," says one of the experts. He gave the following example: *"Recently, a very interesting attack on a person, who is about 70 years old, was repelled. Fraudsters tried to lure out her data. There was little money on her card, and I was surprised: why attack a woman who has practically no money? When I followed the attack itself, I saw that the main addresses were coming from Horlivka. So, the main goal was to steal the digital identity of this person. After all, it could be resold to enable someone from the occupied territories of Ukraine to use later this digital identity on the territory of Ukraine. So, in this case, the digital identity of this woman was a much more valuable resource than 500 hryvnias on her pension card."*

The experts also talked about the issue related to the security of devices used by a person. First

of all, the phone/smartphone was discussed ("this is the key to your digital identity and it can be easily lost"). If somebody from the outside gets control of the smartphone, they get access to all the information on it, including documents in Diia, bank cards, etc.

The experts are skeptical about the transition to a contract with mobile operators where a specific SIM card is tied to a specific person ("this solves practically nothing but only creates a black market for active SIM cards").

Also, the discussion emphasized the fact that expensive, more protected smartphones are not affordable to all citizens. "The security of a smartphone depends largely on its price. In addition, the most expensive and safest smartphone models, for example, Pixel, are not sold officially in Ukraine. Therefore, according to one of the experts, the devices of the most vulnerable citizens are the least protected in terms of security". In their opinion, no simple solutions to this problem have been found so far. Shortly before the full-scale Russian invasion, President Zelenskyy announced a state program that would allow vaccinated Ukrainians over 60 to receive a free smartphone with Internet access. However, in wartime, the implementation of this program is pending (Biznes. NV, 2022).

Account security is also an important issue in protecting one's digital identity. *"Respective literacy on the user's part is critical in protecting accounts. However, the platforms themselves encourage the user to have more secure accounts. This applies to both international companies and Ukrainian banks (at least some of them do it well),* - says one of the experts. *However, there is another aspect – protection of personal information. As far as I can see, the main source of the leak of this personal information is public authorities and people who have access to it."* According to the expert, for this reason it is necessary to explain to people why it is very important to protect, for example, the banking information. However, in their opinion, only literacy without establishing a system of protection and control of access to personal information collected by the state may have a much smaller effect than desired.

LEGAL RISKS

Strategic-level risks

- lack or inadequacy of legal regulations for a number of aspects related to citizens' digital identity and citizens' performance in the digital environment. This concerns, in particular, the regulation of:

  a) existing digital identification tools;

  в) digital documents;

  c) processing of meta data and cookies;

- insufficient legal protection of electronic signatures;

- an insufficiently developed criminal law framework for crimes committed online (hate speech, revenge porn, cyber violence, identity theft, etc.).

- insufficient legal regulation of personal data protection, and personal data vulnerable to abuse in the digital space (for example, data theft, publication without consent, etc.);

- Poor handling in the judicial practice of the peculiarities related to the exercising of human rights in the online environment;

- mistrust of Ukraine's justice system as a factor demotivating citizens to use existing legal mechanisms for the protection of digital rights;
- excessive disclosure of registers;
- no regulation covering access to sensitive information (for example, of medical nature);
- no national regulation covering the activities of global technological giants in the use and handling of the personal data of users of platforms/services/applications.

Personal-level risks

- no alternatives to digital existence due to rapid digitalization, including public services;
- impeded exercising of citizens' digital rights due to the digital inequality in Ukrainian society;
- impeded exercising of citizens' digital rights due to poor digital literacy;
- citizens' poor legal literacy, awareness of digital rights and respective protection mechanisms.

Effects of War

The Russian aggression increased risks to the digital identity of every citizen, including those in the information space. Citizens who ended up in temporarily occupied territories after February 24 are especially vulnerable. In addition to physical and psychological violence and information blockade, the occupiers seized mobile phones and other gadgets (Esreso.TV, 2022). This posed a direct threat to the digital identity of citizens, primarily those who stored their personal data electronically, for example, in the Diia services; allowed the occupiers to access the social media accounts of these citizens, etc. Also, with the blockage of Ukrainian mobile operators and access to Ukrainian Internet resources, residents of the temporarily occupied territories lost access to a number of administrative services provided by the State of Ukraine online as well as to the mobile banking system. It is practically impossible to protect the rights of these citizens while they are under occupation, although Ukraine is trying to provide all possible support to those who were caught up in the occupation. For example, the State Service for Special Communications and Information Protection of Ukraine published clarifications of how to correctly delete information from phones so that it would be inaccessible to the occupiers (State Service for Special Communications and Information Protection of Ukraine, 2022).

However, it is not only Russia's actions that make it impossible to exercise the rights and freedoms of the citizens in the occupied territories. After Russia's full-scale invasion of Ukraine on February 24, 2022, the citizens of Ukraine also found themselves forced to partially restrict their rights and freedoms, including the right to freedom of expression and freedom of speech due to the introduction of martial law. Ukraine adopted a number of regulatory and legal documents to introduce these restrictions. The government has also officially notified of a waiv-

er to its obligations under the European Convention on Human Rights and the International Covenant on Civil and Political Rights (UKRAINE: NOTIFICATION UNDER ARTICLE 4, 2022). Nonetheless, media experts and representatives of human rights and non-governmental organizations emphasize the need to find a reasonable limit in the restrictions of rights and freedoms in wartime.

NGO Human Rights Platform monitoring digital rights violations in Ukraine, as early as under the martial law, records violations of right to freedom of expression, the right to privacy and data protection, as well as general nature violations such as blocking of Internet resources, site hacks, creation of fake online resources, dissemination of false information, etc. (Human Rights Platform, 2022a). The Human Rights Platform also prepared a report analyzing the current situation in the sphere of digital rights in wartime (Human Rights Platform, 2022b), where emphasis is made, among other things, on restricted rights and freedoms, justified no in every instance, and on the need to improve the legislation.

The non-governmental organizations Center for Democracy and Rule of Law and Digital Security Laboratory prepared recommendations on restrictions of human rights in wartime, addressed to various stakeholders, including the government and the parliament, with the aim to review a number of restrictions in terms of rationale to avoid lawsuits at the European Court of Human Rights in the future (CEDEM, 2022).

Experts of the 'For the Free Internet' Coalition call to remember that regulation and legal limitation of digital rights must be developed in a transparent and open way, whilst blockage of access may be justified only by a court decision provided that there are valid reasons (ZMINA, 2022).

STRATEGIC-LEVEL RISKS

When discussing the legal risks associated with digital identity, the legal experts focused primarily on digital rights and personal data. Such attention to these aspects is caused by the fact that digital identity is not a legal category, unlike digital rights and personal data, which at the same time denote or affect the cornerstone aspects of digital identity.

The discussion participants noted that digital rights are not a separate group of rights, instead, we are talking about the enjoyment of human rights in the digital environment. *"These are not a certain kind of human rights. These are human rights actually guaranteed by the Convention and the Constitution, but they are exercised specifically in the digital environment, on the Internet,"* the media lawyer mentioned during the discussion. A similar definition is set out, for instance, in the Methodology of Digital Rights Violations Monitoring as carried out by the non-governmental organization Human Rights Platform: "For the purposes of this study, digital rights are human rights in the online environment, which include, inter alia, the right to access the Internet, the right to freedom of expression, the right to privacy and other human rights that are exercised through digital technologies" (Human Rights Platform, 2019).

Ukraine's national legislation practically does not regulate separately the issue concerning the protection of citizens' digital rights. *"Most of the Internet-related rights and freedoms are covered by the general norms of constitutional, civil, criminal and administrative legislation,"* as stated in the expert report by NGO Digital Security Laboratory about the state of Internet freedom in Ukraine in 2020 (Digital Security Laboratory, 2020). At the same time, *"the specifics of the enjoyment of human rights in the online environment are not always properly taken into account in administrative and judicial practice,"* experts emphasize in the report. The lawyers participating in the expert discussion

also mentioned some cases of inadequate consideration and understanding of the issues related to protection of rights in the digital space in the judicial practice.

In general, the experts considered risks to a person's digital identity in three areas: the user, the state, and technological giants. For personal-level risks (for users), see below — Personal-level risks.

As for the state, in addition to the problems encountered in judicial practice, the experts mostly focused on the lack of regulations related to the operation of Diia, the Unified State Web Portal of Electronic Services, as well as on excessive disclosure of registers and the issues concerning access to personal data.

> *"There is Diia, there is no regulation. This is a paradox: no legal regulation of the already existing product".* (a participant of expert discussion on legal risks)

The experts told about the case when scammers created a profile of a woman in Diia using the stolen documents of hers, and issued a bank loan for her name (MinFin, 2021). The lawyers highlight the problem as the lack of personal data protection mechanisms.

Ukraine has put a lot of efforts to disclose the registers managed by government agencies. But today, the experts talk about excessive disclosure and the need to protect the data contained in these registers.

> *"Actually, in Ukraine, registers are excessively disclosed, which makes it very easy to piece together everything about a person: where they live, what means of transport they use and other things. Yes, we have been fighting for greater transparency. However, very easily, due to this great transparency, one day they may find you in the register of private entrepreneurs and come to your house to set it on fire, figuratively. Such risks exist, and the risk of disclosed registers is excessive, which also strongly affects the identity"* (a participant of expert discussion on legal risks)

However, not everyone agreed with this thesis. Some experts believe that Ukraine cannot so easily abandon the disclosure of registers, that the country has been pursuing for years in order to reduce corruption risks (after the full-scale Russian invasion of Ukraine, the government closed access to most registers – author). Nonetheless, most of the discussion participants agreed on the need to update regulations in this sphere.

> *"We need updated regulations. It is clear that we have to come to an agreement in society about changing the privacy-disclosure balance. Why? Because, to be honest, when this legislation on the disclosure of registers and information was being developed, no one took into account personal data protection. This aspect was not valuable. ...Therefore, this balance needs to be rediscovered in the legislation."* (a participant of expert discussion on legal risks)

Also, the discussion emphasized the need to create a competent authority to exercise control in the sphere of personal data protection. One of the experts noted that establishing of the Commission on Personal Data Protection and Access to Public Information was discussed in the parliament.

> *"The main requirement for this central executive authority is to be independent and able to effectively protect personal data. They must have the tools to issue precepts."* (a participant of expert discussion on legal risks)

Special protection is also required for sensitive information that includes, for example, medical or banking information about a person or criminal record data. The disclosure of such information can cause significant harm to a person. To date, there is no clear definition of «sensitive personal data» or respective regulations (Human Rights Expert Center, 2020). Therefore, the debate about whether sensitive data must be given a higher level of protection compared to other data continues.

> *"It should be remembered that there is some sensitive information that needs special protection. This must be taken into account if these issues fall under legal regulation."* (a participant of expert discussion on legal risks)

> *"As to sensitive data, we have no special protection. There is no regulation either for companies or for the public sector."* (a participant of expert discussion on legal risks)

> *"Actually, this is the question we will face when implementing the GDPR: for what purpose the person provides the data to the state. Whether a person provides their data to the state in order to receive some services and to what extent these data can be transferred then to the category of open data so that they would be available to everyone. There will be an extensive discussion, I think, and a rethinking of how all this will be streamlined."* (a participant of expert discussion on legal risks)

There is no mechanism to remove data from the network when these data got there without one's consent and such disclosure caused some harm to a person.

> *"If even the Supreme Court and all courts recognize that it was a violation of rights, how can they be restored? How to remove eventually those personal data from the network, that's the problem."* (a participant of expert discussion on legal risks)

A number of issues related to the operation of technological giants also require a legal solution. After all, they own a large array of user data collected through social media, messengers, various applications, etc. There is no mechanism aimed at regulating this sphere in Ukraine. The American jurisdiction of these companies makes the problem even more complicated.

> *"The main volume of data and the digital identity that a person forms about themselves is contained in social media. And the Internet giants actually own this digital identity. So how the user or the state can influence them – these rules have not been developed."* (a participant of expert discussion on legal risks)

The experts see the risk of citizens' digital identity abuse in data sharing: when, at the request of this or another state (or its law enforcement agencies), a company must hand over the data of certain users. Frequently, the user is unaware of it; there is no appeal mechanism on the part of the user. The experts highlight the fact that non-democratic states, such as Belarus, may abuse the obtained data and violate human rights.

> *"There must be adequate mechanisms to protect users in case of communication between companies and the state."* (a participant of expert discussion on legal risks)

> *"There were two ECHR cases of particular interest. These cases considered the ways of personal data hand-over, including a cross-border hand-over. In particular, the question was raised to what extent another state, a receiver of the handed-over data, can ensure: firstly, personal data protection; secondly, correct use of data. Let's remind ourselves the already mentioned Telegram and what is currently happening in Belarus. ...There should be a procedure regulating whether a private company will have to hand over data at the request of a state, if we clearly know that the level of democracy, the level of human rights protection is insufficient there."* (a participant of expert discussion on legal risks)

As a separate matter, the experts mentioned the lack of regulation of cookies and meta data processing and the rules on targeted advertising (the Ukrainian legislation on advertisement has no such rules). At the same time, the General Data Protection Regulation (GDPR), in force in the EU, prohibits the use of sensitive user data (for example, political views) to customize ads. A fine of 20,000 Euros is imposed for non-compliance with the Regulation. During 2019, the amount of fines collected for such violations in EU countries reached 711.5 million Euros. Also, GDPR obliges social media to store and use personal data of users from European Union countries only upon their notified consent, for a clearly defined purpose and with a mandatory requirement of confidentiality (Media Sapiens, 2020b).

Most of the discussion participants do not believe that technological giants or other companies will be able to apply self-regulation, and therefore they do not see any alternative to reasonable regulation.

"In Spain, companies developed self-regulatory documents aimed at personal data protection. The problem, however, was that they set quite low standards for themselves. This is one of the risks of self-regulation as a phenomenon. No one wants to be limited by stringent conditions. So it seems to me that in such a case everything must start with the national regulation. As long as we do not have a framework to work, we can hardly talk about any further steps."
(a participant of expert discussion on legal risks)

PERSONAL-LEVEL RISKS

On a personal level, the risk to arise first and that the lawyers emphasized in the discussion is the risk of impossibility of creating a digital identity for some Ukrainian citizens due to digital inequality. This becomes a significant issue in the world of non-alternative digital existence due to rapid digitalization, including public services. Digital transformation of all spheres leaves people with no choice.

"This is about access to digital identity. This concerns inclusiveness and possibility of citizens to get this digital identity. This is related both to the wide access to the Internet in Ukraine as a whole, and to the digital skills of the

> *population. This is also about being able to get digital equipment allowing the use of the latest advances in the digital identity sphere.*" (a participant of expert discussion on legal risks)

Now, the crucial question emerges about access to the Internet and availability of necessary equipment. One needs to have everything necessary to receive a service or a certificate online, in particular, with the use of the Internet and a gadget. Having none of these makes it impossible to receive a service or a certificate, this violates the rights of this person to receive them (provided that such a service is rendered online only).

Therefore, upholding the digital rights is closely related to digital inequality that is observed in Ukraine. For example, the COVID-19 pandemic revealed numerous problems with the digital inequality of citizens. In particular, the digital rights of 37% of population with no access to the Internet were limited. 15.1% of population do not have sufficient digital skills, and a large part of the population does not have digital gadgets allowing the full use of public services online (Institute of Innovative Governance, 2021).

The nature of personal-level risks to digital identity lies in the dimension of ignorance of and inability to stand up for one's digital rights, and lack of understanding of the nature of modern digital world. Therefore, in the course of the discussion, great deal of attention was paid to the digital literacy. Although this issue does not belong directly to the legal sphere, the level of citizens' digital literacy affects directly the possibility of exercising their digital rights.

During the discussion, the experts highlighted that when using the Internet, people create a digital

copy of themselves, which exercises their rights and freedoms in the online environment. At the same time, people do not always understand what influence this digital copy has on their real life.

> *"People do not know what information is being collected about them and how it is being collected."* (a participant of expert discussion on legal risks)

> *"People do not understand the value of their data, they do not understand, roughly speaking, what exactly they are paying for the possibility to use free services."* (a participant of expert discussion on legal risks)

> *"Long ago, I worked in the sphere of consumer rights protection. A person came to me with a complaint that while sitting in a cafe, their bank card was stolen and money was withdrawn from it. I asked: "How did the abusers learn the password?" The person says: "I wrote the password on the card."* (a participant of expert discussion on legal risks)

The lawyers also emphasized the passive position of citizens in case of violation of their digital rights, for example, theft of personal data.

> *"As long as someone sold my personal data is accepted as a normal practice in our country, unless I personally go and write a statement or report to the police – nothing will change. We believe that a crime is when someone is killed, raped... But if my personal data is stolen, there is a quick reply: "But they will not protect me, I am not going anywhere, I will not waste time on this."* (a participant of expert discussion on legal risks)

So, it is important to have institutions where citizens can seek protection in the event of their digital rights violation (the right to protect personal data, the right to have data forgotten, etc.), as has been already partially discussed above.

> *"When there was a leakage of personal data right after Diia was created, accusations were heard that it happened because of Diia. Then there was a case with a woman whose name was used to issue a loan through Diia... There must be a controlling authority, some mechanism (perhaps, it will not be limited to one authority). But such challenges need to be responded quickly in order to find out whether Diia or someone else is involved. And people need to know where to apply to do it quickly."* (a participant of expert discussion on legal risks)

RISKS TO DIGITAL IDENTITY IN WARTIME

The war brings risks to all aspects of life and even puts the life itself at threat. These risks multiply in the digital world as the vulnerabilities of the physical identity have an impact on the digital identity.

One may include in the risks arising in wartime:

1. Disinformation and spreading information for emotional destabilization
2. Isolation from the sources of reliable information.
3. Fraud and theft of digital resources.
4. Use of digital traces for hounding and life threatening.

All these risks are confronted with two protective barriers: **psychological and technological.** If the former is based on the trained behavior that tackles the social engineering techniques, the latter is based on specific privacy and confidentiality settings of user accounts and devices.

1. Disinformation

Spreading distorted news reports in the media space has long been a global problem. But one should remember that disinformation received its main impetus back in 2014, with the launch of aggression by the Russian Federation. So, fakes and war are always side-by-side.

This is also confirmed by the observations of the European Digital Media Observatory that noticed a significant surge in disinformation early February, just before the start of combat action days (European Digital Media Observatory, 2022). One may assume that this was done to undermine the trust in social institutions, as it turned out that their stability depended on whether the digital personality was immune and properly trained to face these threats.

If one does not want to fall a victim to or become a broadcaster of disinformation, they should observe the digital hygiene rules. This is not only about making a list of verified sources of information but also about attention to such characteristics as the emotional headline of publications, the history of the source of distribution, etc. Strange though it might sound, in wartime, the principle of "zero tolerance" should be applied: one shall not trust information from any source until it is confirmed by other independent sources.

2. Isolation from the sources of reliable information

If disinformation is aimed at depleting a person's resourcefulness through continuous emotional and cognitive load, the isolation from sources of reliable information aims at creating an informa-

tion vacuum. Such conditions also carry a threat as they can be realized both in the form of censorship and in the form of targeted attacks against media resources.

In such conditions, it is important to focus on those media that observe journalistic standards, as they will have already developed mechanisms for checking information and balancing views. If access to such sources is blocked with technical tools, like digital censorship and access blocking, then one should think of using VPN and alternative platforms to receive content.

The situation is much more complicated when the damaged infrastructure prevents access to reliable information. In such case, it is important to establish horizontal connections with other like-minded people and to explore other possibilities of getting access to information. Although the digital identity exists in the digital world only, it still relies on a community in the physical world, so in the extreme cases like a war, it is important to remember and actively use this connection.

3. Fraud and theft of digital resources

On June 26, 2022, a document showing the chronology of Russian cyber-attacks on Ukrainian infrastructure was published on the website of the European Parliament (European Parliament, 2022). These attacks were aimed at stealing digital data, and they used not only traditional methods of exploiting vulnerabilities but also "deep fake" technologies ment for digital identity spoofing.

Such hybrid threats signify that, on top of the compulsory cyber security techniques like crypto-resistant passwords and two-factor authentication, one should add the verification of the digital identity of a person on the other end. After all, as stated earlier, the psychological and technological

protective barriers do not exist separately from each other, therefore, the hybrid threats should be countered with the hybrid protection.

Most digital identity attacks are made through social engineering and fishing. As a matter of fact, digital identity is thieved through already stolen accounts and access. Therefore, it is important not to ignore the digital hygiene and cyber security requirements since the loss of access to communication tools and accounts automatically means the loss of digital identity.

4. Use of digital traces for hounding and life threatening

Найбільшою загрозою під час війни є втрата цифрової ідентичності. Бо доступ до неї залежить The biggest threat in wartime is the loss of digital identity. Because the access to it depends on physical access to devices: a phone or a tablet or a laptop. And this physical access is easy to lose if a person is threatened physically.

The issue of privacy in the digital world becomes especially critical in time of war. A digital identity in peacetime must strike a balance: to be recognizable enough to pass the verification process but without revealing private information that could cause digital or physical harm.

Managing these risks in wartime is perhaps the most difficult because the interpersonal communication almost totally turns digital, and there is much less means for verification. Moreover, one has to care even about such tiny details like the clarity of the user profile photo as there is a risk that it may be used for identification. This is also the case for the postings on social media: a careless

photo or video may cause a threat in real life. Therefore, not only file metadata but also identification details in the material itself shall be treated with special care.

When recapitulating the risks to digital identity in wartime, let's note that they are still manageable. Although they may be a threat, there are technical tools and practices that allow managing these risks and protecting an individual in both digital and physical worlds. After all, the war blurs the difference between them.

RECOMMENDATIONS

The digital transformation of Ukraine faces rough conditions caused at first by the COVID-19 pandemic and later by the full-scale Russian invasion of Ukraine on February 24, 2022. Risks to the personal digital identity of every citizen, arising in the process of digitalization of various spheres of life, grow in such conditions and may have devastating consequences. Therefore, the task of the government and other stakeholders operating in the sector is to reduce the level of risks and to strengthen the protection of citizens.

Based on the risk analysis presented in this report, we would recommend that all stakeholders involved in digital transformation, both in the government and non-government sectors, should focus their efforts on the following four areas.

1. Overcoming digital inequality.

Digital accessibility for different population groups in Ukraine, including vulnerable people, should become a philosophy of governmental policy in conditions of digital transformation unfolding in various economic spheres and the public sector. Digital inequality must be overcome by the time of digitization of 100% of public services, as the Ministry of Digital Transformation of Ukraine wants to achieve by 2024. However, reaching such high objectives may be slowed down by the war and

the consequent economic recession. Anyway, digital accessibility and overcoming digital inequality should be an integral part of the country's post-war reconstruction plan.

2. Protecting citizens' digital rights.

A wide range of issues related to the digital sphere need legal regulation. But the protection of rights and freedoms of citizens has to be the basis of this regulation. Public discussion of these issues should contribute to finding a new consensus on the citizens' personal data openness and privacy balance; the citizens' freedoms and national security balance. Such a consensus will ensure the legitimacy of the decisions made by the government and the parliament and strengthen trust in them, especially in the rough wartime or the post-war period. This consensus will also prove Ukraine's commitment to the democratic path of development to the Western partners. The updated regulation should be aligned with the new European Union rules in the digital sphere.

3. Strengthening security in the sphere of digital services both in public and commercial sectors.

Taking care of the digital services provision security, it is worth focusing not only on the technical aspects of protecting digital applications or various entities including the critical infrastructure. Raising the level of culture of the data and services use among the digital services sector personnel (for example, the authorities managing registers). After all, it is human errors that often cause data leakage, hacking and other security problems. The security policy philosophy should be to reduce the impact of human factor on the data protection and critical infrastructure spheres. The state

should review approaches to financing this sector, ensuring an adequate level of support to both infrastructure and personnel (in particular, the ability to hire highly professional security specialists on market terms)

4. Improving digital literacy.

The nature of personal-level risks for digital identity lies in the dimension of citizens' lack of understanding of the nature of modern digital world, ignorance of and inability to stand up for their digital rights, poor awareness of digital security issues. Therefore, great deal of attention should be paid to the digital literacy of various population groups including the vulnerable ones. Digital literacy should be integrated into formal education in both secondary and higher education. Still, there have to be developed programs for non-formal education of adults. Digital literacy cannot be considered separately from media information literacy and narrowed down to just learning of technical skills. Critical thinking efforts should remain an important component of such education. Making arrangements for the offline training for certain categories of the population, for example, for seniors or for junior school children, is as much important.

REFERENCES

American Academy of Pediatrics (2011). Media Use by Children Younger Than 2 Years. Retrieved from https://publications.aap.org/pediatrics/article/128/5/1040/30928/Media-Use-by-Children-Younger-Than-2-Years

Association of Sexologists and Sexual Therapists of Ukraine Vplyv pornohrafiyi na formuvannya osobystosti (The influence of pornography on personality formation). Retrieved from https://sexology.org.ua/vpliv-pornografii-na-formuvannya-osobistosti/?fbclid=IwAR178ztELx8LKpFpsYwlWm5eoEHJnTkVZFJ24I0UaCRcUic-4ayllYRfMFFs

Association of Ukrainian Human Rights Monitors on Law Enforcement (2021). Analiz ryzykiv pid chas obrobky personalnykh danykh: shcho vazhlyvo znaty? (Analysis of risks in personal data processing: what one should know?). Retrieved from https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

Babkina K. (2022). Retrieved from https://www.instagram.com/p/Cb7plk8tPTJ/

BDO LLP (2020). Global Risk Landscape report. Retrieved from https://www.bdo.co.uk/en-gb/news/2020/70-per-cent-of-businesses-experience-threats-to-corporate-reputation

BDO LLP (2022). Global Risk Landscape report. Retrieved from https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/global-risk-landscape

Biznes. NV (2022). Vaktsynovani ukraintsi vikom vid 60 rokiv otrymaiut bezkoshtovnyi smartfon z dostupom do internetu — Zelenskyy. (Vaccinated Ukrainians over 60 will receive a free smartphone with Internet

access – Zelenskyy). Retrieved from https://biz.nv.ua/ukr/economics/ukrajinci-vid-60-rokiv-otrimayut-bez-koshtovni-smartfoni-novini-ukrajini-50214813.html

Brusko, Y. (2022). Zakhyst personalnykh danykh v umovakh viyny. Vplyv voyennoho stanu na pravo na pryvatne zhyttya. (Protection of personal data in wartime. The impact of martial law on the right to privacy). Retrieved from https://lexinform.com.ua/dumka-eksperta/zahyst-personalnyh-danyh-v-umovah-vijny-vplyv-voyennogo-stanu-na-pravo-na-pryvatne-zhyttya/

CEDEM (2022). Rekomendatsii hromadskykh orhanizatsii shchodo obmezhen prav liudyny u voiennyi chas. (Recommendations of non-governmental organizations on restrictions of human rights in wartime.) Retrieved from https://cedem.org.ua/news/prava-lyudyny-u-voyennyi-chas/?fbclid=IwAR0HLg54i86f87jGQO-FEEvar4okJ8UsZar5L_eN25MVqyti-52i86LUvqTM

CERT-UA (2022). Retrieved from https://www.facebook.com/UACERT/posts/307433441415921

Denysenko, L. (2020). Zakhyst vid nasyl'stva i peresliduvannya v interneti (kiberstalkinhu). (Protection from violence and harassment on the Internet (cyberstalking)) Retrieved from https://genderindetail.org.ua/spetsialni-rubriki/legal-advice/zahist-vid-nasilstva-i-peresliduvannya-v-interneti-kiberstalkingu-1341437.html

Detector Media (2022). Ofis Ombudsmana povidomyv pro vytik personalnykh danykh ukraintsiv (The Ombudsman's office reported the leakage of personal data of Ukrainians). Retrieved from https://ms.detector.media/kiberbezpeka/post/24086/2020-01-17-ofis-ombudsmana-povidomyv-pro-vytik-personalnykh-danykh-ukraintsiv/

Diia. Business (2021a). Indeks tsyfrovoyi transformatsiyi vid EBA — doslidzhennya stanu tsyfrovoyi transformatsiyi na pidpryyemstvakh (The Digital Transformation Index from the EBA - a study of the state of digital transformation at enterprises). Retrieved from https://business.diia.gov.ua/cases/tehnologii/indeks-cifrovoi-transformacii-vid-eba-doslidzenna-stanu-cifrovoi-transformacii-na-pidpriemstvah

Diia. Business (2021b). Instrument otsinky rivnia zakhystu personalnykh danykh v orhanizatsii. (A tool to assess the data protection level within an organization). Retrieved from https://business.diia.gov.ua/selftesting/data-protection-tool?utm_medium=refer&utm_source=www.kadrovik01.com.ua&utm_term=5441&utm_content=news&utm_campaign=red_block_content_link_marker

Diia. Business (2021c). Treninhy iz zakhystu personalnykh danykh. (Personal data protection trainings). Retrieved from https://business.diia.gov.ua/personal-data-protection-training

Digital Security Laboratory (2020). Internet-svoboda v Ukraini. (Internet freedom in Ukraine.) Retrieved from https://dslua.org/wp-content/uploads/2021/09/Internet-svoboda-2020.pdf

Dmytrenko, N. (2021). Retrieved from https://m.facebook.com/story.php?story_fbid=4017384871632716&id=100000837273635

Dom (2021). Budushchee — za tekhnolohyiamy, nastoiashchee — za "Diieiu": interviu s hlavoi Mintsyfry Mikhailom Fedorovym. (The future belongs to technologies, the present belongs to Diia: interview with the Head of the Ministry of Digitization, Mikhail Fedorov.) Retrieved from https://kanaldom.tv/budyashhee-za-tehnologiyami-nastoyashhee-za-di%d1%94yu-intervyu-s-glavoj-minczifry-mihailom-fedorovym/

Dzerkalo Tyzhnia (2022a). Mintsyfry zaklykalo tekhnolohichni kompanii svitu doluchytys do «didzhytal-lendlizu» dlia Ukrainy (The Ministry of Digitization called on the world's technology companies to join the "digital lend-lease" for Ukraine). Retrieved from https://zn.ua/ukr/TECHNOLOGIES/mintsifri-zaklikalo-tekhnolohichni-kompaniji-svitu-doluchitis-didzhital-lendlizu-dlja-ukrajini.html

Dzerkalo Tyzhnia (2022b). Facebook ta Instagram ridshe blokuvatymut ukrainskyi kontent – Fedorov. (Facebook and Instagram Will Be Blocking Ukrainian Content Less Often – Fedorov.) Retrieved from https://zn.ua/ukr/TECHNOLOGIES/facebook-ta-instagram-ridshe-blokuvatimut-ukrajinskij-kontent-fedorov.html

Ekonomichna pravda (2022). Evakuatsiia danykh: yak GigaCloud pid obstrilamy vyvozyv skhovyshche danykh Prozorro do Lvova. (Evacuation of data: How GigaCloud moved under fire the Prozorro data storage to Lviv). Retrieved from https://www.epravda.com.ua/publications/2022/06/23/688435/

The Economist (2021). The World in 2021

Esreso.TV (2022). Vyluchennia telefoniv i zatrymannia na 30 dniv: terorysty “LNR” zaboronyly liudiam v okupatsii spilkuvatysia z zhyteliamy vilnykh terytorii. (Seizure of phones and detention for 30 days: "LPR" terrorists forbade people under occupation to communicate with residents of free territories). Retrieved from https://espreso.tv/viluchennya-telefoniv-i-zatrimannya-na-30-dniv-teroristi-lnr-zaboronili-lyudyam-v-okupatsii-spilkuvatisya-z-zhitelyami-vilnikh-teritoriy

European Digital Media Observatory, (2022). Fact-checked disinformation on the war in Ukraine detected in the EU – 2022. Retrieved from https://edmo.eu/2022/02/24/fact-checked-disinformation-on-the-war-in-ukraine-detected-in-the-eu-2022/

European Parliament (2022). Russia's war on Ukraine: Timeline of cyber-attacks. Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

FitBit (2020). The Impact Of Coronavirus On Global Activity. Retrieved from https://blog.fitbit.com/covid-19-global-activity/

Forbes (2022). Tsyfrovyi lend-liz. Kliuchovi punkty planu tsyfrovoi transformatsii Ukrainy vid Mintsyfry (Digital lend-lease. Key points of the digital transformation plan of Ukraine from the Ministry of Digitization). Retrieved from https://forbes.ua/news/tsifroviy-lend-liz-klyuchovi-punkti-planu-tsifrovoi-transformatsii-ukraini-vid-mintsifri-04072022-6974

Government portal (2022). Ukrayina otrymala dvi nahorody u sferi kiberzakhystu na SYBERSEC European Cybersecurity Forum (Ukraine got two awards in the field of cyber security at the CYBERSEC European Cybersecurity Forum). Retrieved from https://www.kmu.gov.ua/news/ukrayina-otrimala-dvi-nagorodi-u-sferi-kiberzahistu-na-sybersec-european-cybersecurity-forum

Human Rights Expert Center (2020). "Chutlyvi" personalni dani: yak vony vyznachaiutsia ta yakym normatyvnym zmistom napovniuiutsia? ("Sensitive" personal data: How they are determined and what normative content they are filled with?). Retrieved from https://ecpl.com.ua/news/chutlyvi-personalni-dani-iak-vony-vyznachaiutsia-ta-iakym-normatyvnym-zmistom-napovniuiutsia/

Human Rights Platform (2019). Metodolohiia monitorynhu porushennia tsyfrovykh prav. (Methodology of Monitoring Violations of Digital Rights.) Retrieved from https://www.ppl.org.ua/wp-content/uploads/2019/06/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F-.pdf

Human Rights Platform (2022a). Monitoryng porushennia tsyfrovykh prav v Ukraini (Monitoring of digital rights violations in ukraine). Retrieved from https://www.ppl.org.ua/wp-content/uploads/2022/05/%D0%86%D0%BD%D0%B4%D0%B5%D0%BA%D1%81-%D0%B7%D0%B0-%D0%BB%D1%8E%D1%82%D0%B8%D0%B9-2022-%D1%80%D0%BE%D0%BA%D1%83.pdf

Human Rights Platformb (2022b). Viina u tsyfrovomu vymiri ta prava liudyny. (Digital warfare and human rights.). Retrieved from https://www.ppl.org.ua/wp-content/uploads/2022/07/%D0%92%D0%86%D0%99%D0%9D%D0%90-%D0%A3-%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%9E%D0%9C%D0%A3-%D0%92%D0%98%D0%9C%D0%86%D0%A0%D0%86-%D0%86-%D0%9F%D0%A0%D0%90%D0%92%D0%90-%D0%9B%D0%AE%D0%94%D0%98%D0%9D%D0%98.pdf?fbclid=IwAR35dmIBMwL-MT7AJ-_iF1c6iaFjbrGP-eIXGR-Jmr-x9KOmPmKfK4WhaX_E

Institute of Innovative Governance (2021). Tsyfrovi prava chy hromadske zdorovia: tsyfrovi prava pid chas

pandemii COVID-19 v Ukraini - z urakhuvanniam krashchykh praktyk Yevrosoiuzu (Digital rights or public health: digital rights during the COVID-19 pandemic in Ukraine; based on the best practices of the European Union). Retrieved from https://instingov.org/wp-content/uploads/2021/10/Report_IIG_Ukraine.pdf

IWF (2021). Internet Watch Foundation. Retrieved from: https://annualreport2020.iwf.org.uk/

Johns Hopkins University & Imperial College London (2021). Countering cognitive warfare: awareness and resilience. Retrieved from https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html

Media Sapiens (2020a). Ofis ombudsmana povidomyv pro vytik personalnykh danykh ukraintsiv. (The Ombudsman's office reported the leakage of personal data of Ukrainians.) Retrieved from https://ms.detector.media/kiberbezpeka/post/24086/2020-01-17-ofis-ombudsmana-povidomyv-pro-vytik-personalnykh-danykh-ukraintsiv/

Media Sapiens (2020b). Digital Services Act: yak Yevropeiskyi Soiuz stvoriuie yedynyi tsyfrovyi prostir. (How the European Union creates a single digital space.) Retrieved from https://ms.detector.media/it-kompanii/post/28006/2021-08-18-digital-services-act-yak-ievropeyskyy-soyuz-stvoryuie-iedynyy-tsyfrovyy-prostir/

Microsoft (2022). Defending Ukraine: Early Lessons from the Cyber War. Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

MinFin (2021). Shakhrai v “Diia”. Cherez dodatok na ukrainku oformyly kredyt. (Scammers in Diia. A loan was issued to a Ukrainian woman through the application.) Retrieved from https://minfin.com.ua/ua/2021/07/02/67282762/

Ministry of Digital Transformation of Ukraine (2019a). Tsili do 2024 roku (Goals until 2024). Retrieved from https://thedigital.gov.ua/ministry

Ministry of Digital Transformation (2021b). Zvit pro vykonannya planu roboty Ministerstva tsyfrovoyi transformatsiyiUkrayiny na 2021 rik (Report on the implementation of the work plan of the Ministry of Digital Transformation of Ukraine for 2021). Retrieved from https://cms.thedigital.gov.ua/storage/uploads/files/page/ministry/%D0%97%D0%B2%D1%96%D1%82_%D0%9F%D0%BB%D0%B0%D0%BD_%D0%9C%D1%96%D0%BD%D1%86%D0%B8%D1%84%D1%80%D0%B8_2021.pdf

Ministry of Health (2022). Vplyv viyny na psykhichne zdorov"ya — kolosal'nyy — Viktor Lyashko (The impact of war on mental health is colossal - Viktor Lyashko). Retrieved from https://moz.gov.ua/article/news/vpliv-vijni-na-psihichne-zdorov%e2%80%99ja---kolosalnij---viktor-ljashko

Abo-Hilal, M (2021). The Impact of War on the People of the Middle East. Retrieved from https://www.mei.edu/publications/impact-war-people-middle-east

NGO Docudays (2020). Poperedzhennia ta protydiia kiberbulinhu v dytiachomu seredovyshchi Ukrainy 2020 (Preventing and Combating Cyberbullying in the Children's Environment of Ukraine 2020). Retrieved from http://cyber.bullyingstop.org.ua/storage/media-archives/cyberbuling_%D0%B2%D0%B8%D0%B-F%D1%80%D0%B0%D0%B2%D0%BB15-10_compressed.pdf

Oleksiiuk, T. (2022). Dostup do publichnoi informatsii: ne dopustyty vtrat u zviazku z viinoiu. (Access to public information: Prevention of war-related losses.) Retrieved from https://dostup.pravda.com.ua/blogs/publications/dostup-do-publichnoi-informatsii-ne-dopustyty-vtrat-u-zviazku-z-viinoiu

European Data Portal (2020). Open Data Maturity Report. Retrieved from https://data.europa.eu/sites/default/files/edp_landscaping_insight_report_n6_2020.pdf

Polissya Foundation for International and Regional Studies (2020). Tsyfrovi transformatsiyi v Ukrayini: chy vidpovidayut' vitchyznyani instytutsiyni umovy zovnishnim vyklykam ta yevropeys'komu poryadku dennomu? (Dig-

ital transformations in Ukraine: whether the domestic institutional ones correspond to conditions for external challenges and the European agenda?). Retrieved from http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf

Radio Svoboda (2021). Dity i seksual'ne nasyl'stvo v interneti. Shcho take «sekstynh» i «hruminh»? (Children and sexual violence on the Internet. What is;"sexting" and "grooming"?)Retrieved from https://www.radiosvoboda.org/a/sexing-grooming-sexualne-nasylstvo-v-interneti/31116184.html

State Service for Special Communications and Information Protection of Ukraine (2021b). Sytuatsiya navkolo saytu elektronnykh petytsiy ye splanovanoyu khakers'koyu atakoyu - Derzhspetszv"yazku
(The situation around the website of electronic petitions is a planned hacker attack - State Special Communications). Retrieved from https://cip.gov.ua/ua/news/situaciya-navkolo-saitu-elektronnikh-peticii-ye-splanovanoyu-khakerskoyu-atakoyu-derzhspeczv-yazku

State Service for Special Communications and Information Protection of Ukraine (2022a). Rosiiski khakery prodovzhuiut atakuvaty ukrainsku infrastrukturu, ne hrebuiuchy tsyvilnymy tsiliamy (Russian hackers continue to attack Ukrainian infrastructure even descending to civilian targets). Retrieved from https://cip.gov.ua/ua/news/rosiiski-khakeri-prodovzhuyut-atakuvati-ukrayinsku-infrastrukturu-ne-grebuyuchi-civilnimi-cilyami

State Service for Special Communications and Information Protection of Ukraine (2022). Yak pravyl'no vydalyaty fayly? (How to delete files correctly?) Retrieved from: https://cip.gov.ua/ua/news/yak-pravilno-vidalyati-faili

Suspilne (2022a). Tsyfrova blokada Rosii ta Starlink v Ukraini — interviu z ministrom Fedorovym (The digital blockade by Russia and Starlink in Ukraine — an interview with Minister Fedorov). Retrieved from https://suspilne.media/231124-cifrova-blokada-rosii-ta-starlink-v-ukraini-intervu-z-ministrom-fedorovim/

Suspilne (2022b). Internet-viiska — tse ekskliuzyv Ukrainy. Zastupnyk hlavy Mintsyfry pro kiberpatyzaniv i ataky

na rosiiski servisy. (Internet Army is Ukraine's exclusive. The Deputy Head of the Ministry of Digitization on cyber partisans and attacks on Russian services). Retrieved from https://suspilne.media/253003-ukrainska-it-armia-vid-pocatku-stvorenna-znisila-blizko-dvoh-tisac-rosijskih-cilej-egor-dubinskij/

Texty (2022). Alhorytm banu. Chomu Facebook blokuie patriotychni dopysy i do choho tut uperedzhennia ta pohano napysani alhorytmy. (Ban algorithm. Why Facebook is blocking patriotic posts and why prejudices and poorly written algorithms have to do with this). Retrieved from https://texty.org.ua/articles/104034/facebook-vyznav-pomylkove-blokuvannya-patriotychnoho-zmistu-ale-nichoho-ne-poyasnyv-mozhe-problema-v-alhorytmah/

Ukrainska Pravda (2022). Operatsiya "Pavutyna": sylovyky vykryly 23 torgovtsiv dytiachym porno (Operation "Web": security forces exposed 23 dealers in child pornography) Retrieved from https://www.pravda.com.ua/news/2022/01/14/7320424/

UKRAINE: NOTIFICATION UNDER ARTICLE 4 (2022). Retrieved from https://treaties.un.org/doc/Publication/CN/2022/CN.65.2022-Eng.pdf

Ukrinform (2022a). Shmyhal: Za dva roky ekonomiia vid onlain-posluh stanovyt 14,7 miliarda (Shmyhal: Over two years, savings from online services amount to 14.7 billion). Retrieved from https://www.ukrinform.ua/rubric-economy/3399904-smigal-za-dva-roki-ekonomia-vid-onlajnposlug-stanovit-147-milarda.html

Ukrinform (2022b). Peter Stano, EU Lead Spokesperson for Foreign Affairs and Security Policy. Basically anything that comes out of the Kremlin is a massive propaganda and very often simply lies. Retrieved from https://www.ukrinform.net/rubric-polytics/3528705-peter-stano-eu-lead-spokesperson-for-foreign-affairs-and-security-policy.html

Ukrainska Pravda. Zhyttia (2019). Yaki vony, ukrayins'ki pidlitky: pro sotsmerezhi, seks, alkohol', sport, do-

viru do bat'kiv ta druziv. Doslidzhennya (What are they like, Ukrainian teenagers: about social networks, sex, alcohol, sports, trust in parents and friends. Research) Retrieved from https://life.pravda.com.ua/society/2019/05/22/236974/

VoxUkraine (2021). Potentsial tsyfrovoi transformatsii u hromadakh Ukrainy (The potential of digital transformation in Ukrainian communities). Retrieved from: https://voxukraine.org/potentsial-tsyfrovoyi-transformatsiyi-u-gromadah-ukrayiny/

WHO (2019). New WHO-led study says majority of adolescents worldwide are not sufficiently physically active, putting their current and future health at risk. Retrieved from https://www.who.int/ru/news/item/22-11-2019-new-who-led-study-says-majority-of-adolescents-worldwide-are-not-sufficiently-physically-active-putting-their-current-and-future-health-at-risk

Zaborona (2020). Nebezpeka derzhavy v smartfoni. Rozpovidaiemo pro vrazlyvosti derzhavnoho tsyfrovoho proektu Diia (The danger of the state in a smartphone. We talk about the vulnerabilities of the "Diia" state digital project). Retrieved from https://zaborona.com/nebezbeka-derzhavy-u-smartfoni/

Zaborona (2021). Nebezpeka derzhavy v smartfoni. Rozpovidaiemo pro vrazlyvosti derzhavnoho tsyfrovoho proektu «Diia». (The danger of the state in a smartphone. We talk about the vulnerabilities of the "Diia" state digital project.). Retrieved from https://zaborona.com/nebezbeka-derzhavy-u-smartfoni/

ZMINA (2022). Obmezhennia prav v interneti: ryzyky dlia Ukrainy. (Restrictions of rights on the Internet: risks for Ukraine.) Retrieved from https://zmina.info/articles/obmezhennjia_prav_v_interneti_riziki_dljia_ukrajini/