PROTECTION OF PERSONAL DATA DURING WARTIME

2023

PROTECTION OF PERSONAL DATA DURING WARTIME

Author: *Uliana Shadska,* a lawyer in the field of digital legislation, an expert in personal data protection and ethics of technology

Literary editor: *Maryana Doboni*

Design and layout: *Olha Zolotar*

Translation: *Taras Omelchenko*

We express special thanks for contributing to the preparation of the research to ***Vadym Pyvovarov, Tetiana Avdieieva, Tetiana Doroshenko, Volodymyr Batchaiev, Anastasiia Malynka,*** and all others who raise issues regarding the right to personal data protection.

Research «PROTECTION OF PERSONAL DATA DURING WARTIME. LIST OF UKRAINIANS» was made as part of the project «Documentation of war crimes committed by the Russian Federation» with the financial support of the National Endowment for Democracy, USA. The views of the study authors do not necessarily reflect the official position of NED or the US Government.

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

Асоціація УМДПЛ UMDPL Association

Freerights ASSOCIATION

TABLE OF CONTENTS

SHORT SUMMARY

On February 24, 2022, Russia initiated a full-scale invasion of Ukraine. This war against the Ukrainian people shocked the entire world with its level of brutality toward the civilian population and demonstrated that modern military strategies are no longer limited to traditional means of warfare. Unprecedented technologies are being employed to gather information about the population and infrastructure, including the use of artificial intelligence systems and more. The battle is taking place not only on the ground but also in cyberspace, where conventional weaponry is combined with state-of-the-art technologies.

Personal data has become a tool for achieving hostile objectives, including the commission of war crimes against humanity and other dangerous phenomena such as persecution, surveillance, deception, the spread of disinformation, and hatred, among others. This is a war where every individual can become a victim, regardless of their location. The digital front line knows no geographical boundaries or borders. It infiltrates everywhere – into homes, offices, personal smartphones, anywhere and anytime. Through metadata analysis, specific individuals can be identified, military operations can be predicted, connections between individuals can be studied, and targeted psychological attacks against the population can be carried out. Today, there is still limited research on the threats to individuals or entire communities from the deliberate use of data, especially in international armed conflicts. Consequently, there are insufficient legal instruments to counteract this.

During the years 2022-2023, our team collected facts regarding instances where Ukrainians became victims of crimes involving the use of personal data. We also documented cases that directly indicate violations of the law in this area because all consequences have their causes. To achieve this, we analyzed over 200 materials obtained from open sources, including official reports from Ukrainian law enforcement agencies, media publications, and comments from eyewitnesses of violations and from civil activists. We have summarized all of this data and presented it in this analytical report.

The **main goal** is to demonstrate the reasons and consequences of unauthorized use of personal data. To draw the attention of the Ukrainian government, the international community, and the scientific community to the risks of privacy violations and the necessity of reforms in this field.

The analytical report consists of six sections, in which stories are published about:

- how detailed profiles of Ukrainians in temporarily occupied territories were created using personal data. The content addresses questions such as which categories of individuals primarily experienced persecution and how personal data of the population is collected and for what purposes;
- unauthorized leaks of personal data contained in closed state databases;
- violations of data protection legislation in local self-government bodies;
- unauthorized leaks of confidential information in the healthcare system;
- the use of personal data of Ukrainian children. The content reveals hypotheses regarding the purposes of data collection and risks to physical safety;
- the use of social networks and other technologies for data collection, surveillance, tracking, deception of the population, dissemination of disinformation, hatred, etc.

In the conclusions section, recommendations are provided that can be implemented today to influence the situation that has led to negative consequences.

The **overall map** of issues and their causes presented in this document:

- can stimulate a substantive discussion on the information security of the population. Before the onset of Russia's full-scale armed aggression against Ukraine, data protection issues were not widely discussed in society. Not because they did not exist, but because most incidents were latent. Now we have enough arguments that the protection of personal data is important not only for preserving financial assets on bank cards but also for human life and health;
- can assist experts in developing data protection mechanisms, including analyzing which category of individuals and type of information is most vulnerable. This includes mapping threats and forming hypotheses about control methods to prevent future breaches;
- can become essential material for research into the relationship between

a person's physical and «digital body»[1] (or profile). Digital technologies have become a part of virtually every aspect of life. In scientific circles, the term «digital body» has already been used, referring to information about a person that reflects their genetic, social, cultural, and economic identity. Images, beliefs, biometric data, and other information stored in the digital space essentially represent a person. Understanding the relationship between the physical and «digital body» is necessary for assessing potential threats to both individuals and entire communities;

- can help define the concept of «digital harm» in the legal field and its cause-and-effect relationship, particularly in the context of international humanitarian law; the possibility of reconciling the right to privacy with the norms regulating armed conflicts; as well as policies regarding the obligations of individuals who establish facts for war crime investigations;
- can provide a better understanding of the threats that digital technologies can pose to the population and how to respond to these risks and mitigate them. A theory of digital harm is needed. In order to connect theory with practice, a conceptual foundation is required.

Today, there are many discussions about the use of personal data. A deep understanding of the full range of threats to individuals will require a reevaluation of the overall concept of their protection. Specifically, we need to ask questions such as:

- What guarantees are there that data collected for the protection of the state will not be used against its citizens?
- What dangers exist in the abuse of such information?
- What methods can ensure the security and preservation of human dignity in the digital space?
- How can transparency and oversight be ensured in this process?

1 Chris Shilling, "The Body in Sociology," cited from: Claudia Malacrida and Jacqueline Low (eds), Sociology of the Body, Oxford: Oxford University Press, 2008; Carey Jewitt, Sara Price and Anna Xambo Sedo, "Conceptualizing and Researching the Body in Digital Contexts: Towards New Methodological Conversations across the Arts and Social Sciences", Qualitative research, Vol. 17, No. 1, 2017.

PREFACE

The civilian population of Ukraine has been suffering during the Russian armed aggression. In addition to rocket attacks, Ukrainians have endured humiliation, torture, and even killings based on factors such as their nationality, native language, beliefs, profession, interests, family ties, service, or even friendships[2]. According to eyewitness accounts, people disappeared in the occupied territories of Ukraine following a certain algorithm. Initially, military service members, law enforcement officers, local officials, and their relatives were targeted. Subsequently, civil activists, journalists, and other individuals with pro-Ukrainian views were also at risk. Russian military forces searched for these individuals based on lists with detailed information about them, including family composition, employment history, military service, education, and property ownership, among other details. It is essential to note that the existence of these «at-risk groups» did not mean that all other residents of the occupied territories could feel safe. The occupiers' cruelty had not only a practical purpose (acquiring information, coercing cooperation, etc.) but was also aimed at achieving the war's global goal – the destruction of Ukrainian identity. Torture, alongside extrajudicial executions, deportations, and forced passportization became a means of forcing individuals to renounce their Ukrainian identity[3].

Russian occupiers, along with individuals cooperating with them, engaged in information warfare, including propaganda efforts targeting the population in various regions of Ukraine. They collected data and compiled lists of Ukrainians. It is crucial to highlight that they also collected and manipulated personal data of Ukrainian children from various sources and under various pretexts to remove them from their legal, ethnic, and cultural environment.

A significant portion of information about individuals could be obtained from publicly available sources on the internet. However, in addition to this, during 2022-2023, law enforcement agencies increasingly exposed traitors among government officials who willingly collaborated with Russians and provided them with necessary information. Leaks were particularly identified within local self-government bodies and medical institutions. Additionally, occupiers obtained data through intimidation, torture, and deception of the population.

2 Article 75 of the Protocol Additional to the Geneva Conventions of August 12, 1949, relating to the protection of victims of international armed conflicts, prohibits physical punishments and torture of all kinds «at any time and in any place whatsoever, whether committed by civilian or by military agents.»

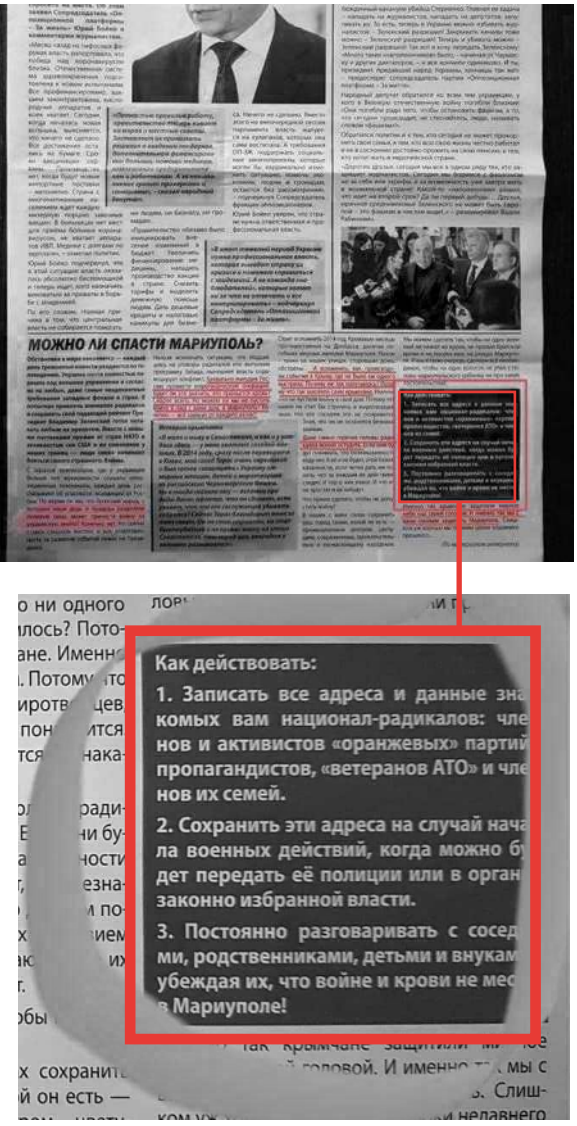
3 Russian army: doomed to cruelty and torture. Access mode: *https://umdpl.info/news/rosijska-armiya-pryrecheni-na-zhorstokist-katuvannya/*

As mentioned earlier, all consequences have their causes. The facts presented below directly point to a weak personal data protection system. Adequate information security mechanisms for closed databases, especially during the occupation of Ukrainian territories, were not provided. In many cases, government officials were not properly instructed on how to handle information. This is confirmed by the results of inspections conducted by Ukrainian law enforcement agencies and the Office of the Ukrainian Parliament Commissioner for Human Rights. While not all events listed in this document are the results of investigations with credible evidence, they provide enough arguments for civil society, government authorities, and the scientific community to take notice.

We are grateful to all those who raise these issues, provide evidence and arguments, investigate criminal activities in this field, and hold offenders accountable. Such facts should not go unnoticed or disappear from the internet. After reading this report, we hope that you will have no doubts about the importance of protecting the right to privacy.

LISTS OF UKRAINIANS IN TEMPORARILY OCCUPIED TERRITORIES

(Image source: Anzhela Bets / unsplash.com)



Collecting personal data of Ukrainians was taking place even before the full-scale invasion of Ukraine. People were sharing various data and opinions in social media, indicating that propaganda activities among the population in the eastern regions had been ongoing for some time. One fact posted online caught our attention, namely the photograph of a newspaper excerpt[4]. In an article titled «How to Save Mariupol,» residents were urged to record the data of ATO veterans, local pro-Ukrainian activists, political figures, and their family members so that (as stated in the newspaper) when military actions started, this information could be handed over to the «new authorities,» i.e., the occupiers. Newspapers with logos of the opposition OPFL party were distributed to Mariupol residents' mailboxes by unknown individuals[5]. At the time, a representative of this faction in the Mariupol City Council commented on the content of this publication, stating it was a provocation. It was claimed that someone had printed a fake newspaper. Regardless of who actually distributed this publication, the fact of collecting information about individuals remains unchanged.

According to eyewitness accounts, Russian military personnel or individuals supporting the armed aggression against Ukraine would approach people in the occupied territories with complete dossiers on them. They would go door-to-

4 In Mariupol, anti-Ukrainian subversive newspapers were distributed through mailboxes on behalf of the Opposition Platform - For Life (OPFL) party. Access mode: *https://www.0629.com.ua/news/3091656/v-mariupole-ot-imeni-opzz-po-poctovym-asikam-razbrosali-antiukrainskie-gazety-podryvnogo-haraktera-foto?fbclid=IwAR3FDWEjWH0aQVsgd1MJjGmdd8fRouFlOle6XDrQnDZCrGHIk9DTxJAzwm0*

5 «Opposition Platform - For Life» (OPFL) is a banned pro-Russian political party of a social orientation in Ukraine.

door with lists, walk the streets, and set up checkpoints where they conducted so-called «filtration.» During the war's active phase, particularly in the occupied territories, they gathered information about various segments of the population as a whole. This was done through torture, blackmail, or deceiving people. For example, pensioners were offered a certain amount of money for their personal data, while children were given gifts. All the cases mentioned in the text require further detailed clarification and investigation..

1. KYIV REGION

The Ivankiv territorial community in the Kyiv region was one of the first to suffer from the full-scale invasion. Heavy fighting took place near the Chornobyl Exclusion Zone as Russian forces attempted to break through to Kyiv. The former district center and surrounding villages were liberated in April after being under siege. Residents of the village of Kolentsi reported that the occupiers practically knew the people living there by name. They had lists that included the addresses of Ukrainian service members, including ATO participants. They searched for and abducted people, holding some in captivity while releasing others, and tragically, some were killed. Witnesses also noted that they had lists of registered firearm owners and were searching for them at their registered addresses[6]. Similar incidents were documented in Bucha and Irpin.

(Image source: palinchak / freepik.com)

6 Media reports; testimonies from victims and witnesses. Mothers were threatened to be shot in front of their children. How the largest community in Ukraine survived the occupation. Access mode: *https://lb.ua/society/2022/04/25/514634_materiv_hotili_rozstrilyati_ochah.html*

During interviews with the media, residents of the village attempted to answer questions about where the Russians obtained information about the local population. They expressed suspicions that perhaps there were traitors among their fellow villagers who directly identified the sought-after categories of individuals. Even if this were the case, there still remains the question of whether this is indeed the sole source of information, given the volume of data. This will have to be further investigated.

2. KHERSON REGION

In April 2022, the then-mayor of the occupied city of Kherson reported that Russian occupiers had obtained the personal data of over a hundred local activists, and nearly all of these people were abducted.

«The 'well-wishers' completely leaked the database of all activists who were in the city. They had personal records on every one of my deputy mayors, information from their wives' lineage to the nickname of their favorite dog. The same goes for the territorial defense and Kherson participants in hostilities in Donetsk and Luhansk, with details about where they lived and what they owned,» the mayor stated in an interview with the media[7].

He was certain that such information could only have been provided by someone who had access to confidential information. According to the mayor, over a hundred people were abducted. The temporary detention facility in Kherson on Teploenerhetyky Street was one of the places where Russian military personnel tortured Ukrainians. Local residents who went through this torture chamber reported that the Russians already had lists with personal data of individuals. People who had served in the Armed Forces of Ukraine, law enforcement agencies, as well as activists, journalists, and others, were brought to this detention center. There, they were interrogated to find out if they were cooperating with Ukrainian security services and if they had plans to implement Resistance Movement activities[8].

7 Media reports; the interview with the mayor of Kherson during the temporary occupation in 2022. Access mode: *https://zmina.info/news/mer-hersona-povidomyv-shho-okupanty-otrymaly-dani-ponad-sotni-misczevyh-aktyvistiv-lyudej-vykraly/?fbclid=IwAR1_iczqCGhHFIX7QwnxnHyhyR_im39xIKo_4zoc2ce2gdvdSy8FPYQBL3M*

8 Media reports citing testimonies from victims and law enforcement data. Kherson residents talk about torture in detention. Access mode: *https://suspilne.media/318636-ne-davali-spati-pidijmali-ta-vimagali-kricati-slava-rosii-hersonci-svidcat-pro-katuvanna-v-itt/*

The Permanent Representative of the President of Ukraine to the Autonomous Republic of Crimea, Tamila Tasheva, mentioned during a press conference that over 500 Ukrainians were held in basements in the Kherson region. According to her, in places like the town of Novooleksiivka and the city of Henichesk, the occupation «administrations» or Russian military had lists of activists who had participated in the civilian blockade of Crimea in 2015[9]. They would take people from their homes and streets.

To pass through a checkpoint, individuals needed a special pass. According to the National Resistance Center, this was how the Russian occupiers controlled the movement of people and collected data about connections between Ukrainians. When filling out the pass, people would specify the purpose of their travel and information about the individuals they were visiting[10]. Viktoriia, a Kherson region resident, recounted that her nephew was detained during document checks (the so-called «filtration») at a checkpoint in Armiansk. His name was on the lists of activists that Russians were hunting for. After the detention, they put a bag over his head and took him to a recreation base located near Skadovsk. [11]

With the aim of suppressing resistance, Russian forces carried out a process known as «population filtration» designed to identify and detain Ukrainians who could potentially resist the establishment of the new pro-Russian authorities or simply be dissatisfied with their actions. Special filtration camps and detention points for the detainment and torture of those arrested were established in the occupied territories. According to Yale University[12] as of September 2022, Russia had created 21 locations for filtration activities on Ukrainian territory. The exact number of «torture chambers» is difficult to determine, but in June 2023, the National Police of Ukraine reported[13] the discovery of 53 places of illegal detention and torture of individuals in the de-occupied territories.

9 Media reports; the statement by the Permanent Representative of the President of Ukraine to the Autonomous Republic of Crimea, Tamila Tasheva. Access mode: *https://www.ukrinform.ua/rubric-regions/3476810-na-zahoplenij-hersonsini-vorogi-trimaut-u-pidvalah-i-katuut-majze-piv-tisaci-ludej.html*

10 Occupiers are collecting data on residents of the occupied territories using special permits. Access mode: *https://espreso.tv/zagarbniki-zbirayut-dani-pro-meshkantsiv-okupovanikh-teritoriy-za-dopomogoyu-spetsperepustok-tsns*

11 Filtration in the Kherson region and Crimea: where Ukrainians are disappearing. Access mode: *https://mipl.org.ua/filtracziya-na-hersonshhyni-i-v-krymu-kudy-znykayut-ukrayinczi/*

12 U.S. report identifies 21 'filtration' locations run by Russia for processing Ukrainians. Режим доступу: *https://www.reuters.com/world/exclusive-us-report-identifies-21-filtration-locations-run-by-russia-processing-2022-08-25/*

13 Crimes committed by Russian military during full-scale invasion of Ukraine (as of June 15, 2023). Access mode: *https://www.npu.gov.ua/news/zlochyny-vchyneni-viiskovymy-rf-pid-chas-povnomasshtabnoho-vtorhnennia-v-ukrainu-stanom-na-15062023*

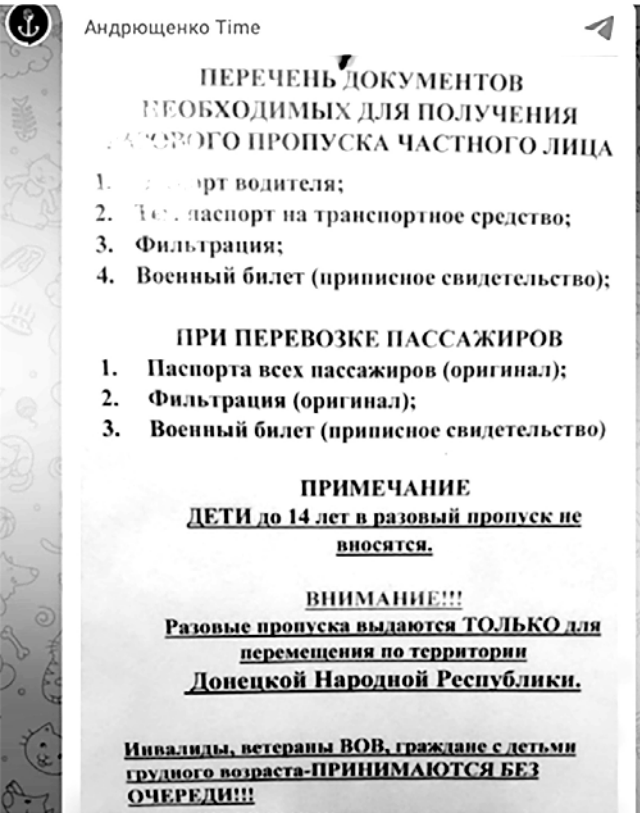
In addition, personal data of the population was collected through other means. The acting head of the Kherson Regional State Administration, Dmytro Butrii, told Suspilne News that the occupying authorities paid pensioners 10,000 rubles per month in exchange for their personal data. Elderly Ukrainians were forced to accept these payments because they had no other means of survival. According to a resident of the Kherson region, her elderly mother did not have a bank card, so she did not receive pension payments for some time after the occupation. One day, a postwoman came to her and asked for her passport, identification code, and spent a long time writing something down without explanation. Then she handed over 20,000 Russian rubles for two months. When the woman asked, «What were you writing there?» she was told that it was necessary to confirm the receipt of the pension. According to the management of the Pension Fund of Ukraine, over 70,000 people used postal services to receive social payments in the Kherson region[14].

(Image source: zinkevych / freepik.com)

3. DONETSK REGION

We previously mentioned that in the Donetsk region (particularly in the city of Mariupol), local residents were urged to record and provide information about ATO veterans, pro-Ukrainian activists, politicians, and their family mem-

14 In the Kherson region, representatives of the occupying authorities deliver pensions in rubles to people's homes and collect personal data. Access mode: *https://suspilne.media/267847-na-hersonsini-predstavniki-okupacijnoi-vladi-nosat-pensii-v-rublah-po-domivkah-ta-zbiraut-osobisti-dani/*



The list of documents necessary to obtain a one-time individual pass

1. The driver›s passport
2. Technical passport for the vehicle
3. Filtration
4. Military ID (registration certificate)

When transporting passengers:
1. Passports of all passengers (original)
2. Filtration (original)
3. Military ID (registration certificate)

NB: Children under 14 are not entered in the one-time pass.

Attention!!!
One-time passes are ONLY issues when traveling around the Donetsk People›s Republic.

Persons with disabilities, Great Patriotic War veterans, and citizens with infants are received without having to wait in line.

(Image source: Telegram channel Андрющенко Time)

bers even before the full-scale invasion. Meanwhile, when Mariupol was already under occupation, according to reports from the Ukrainian government, Russian occupiers continued to collect data on the local population. According to Petro Andriushchenko, an advisor to the mayor of Mariupol, one of the pretexts for obtaining information was the collection of applications for the alleged restoration of damaged housing. He explained that the data was necessary for mobilization and a pseudo-referendum, and this was part of the preparations. For example, to obtain a one-time pass for entry or exit from Mariupol, it was mandatory to submit a military ID. Registration was conducted by the commandant's office, verifying the data provided in the housing restoration applications. In this way, they not only formed lists for the referendum but also restored military records[15].

15 The Telegram channel of Petro Andriushchenko, an adviser to the Mariupol mayor.

4. KHARKIV REGION

Residents of Izium in the Kharkiv Oblast shared their experiences with the media. One woman had to leave her home before the occupation, but her cousin, who was not a soldier but a local rescuer, remained there. Nevertheless, he ended up on the lists of Russians who kidnapped him from his home. He was tortured, but fortunately, he was eventually released[16].

They also came for a 61-year-old man named Mykola, an electrician, veteran footballer, and coach who lived in the village of Vesele. The occupiers had a complete dossier on him, with information about his social circle, the people he helped, and even the fact that in 2015, as a local council deputy, he facilitated the allocation of land to ATO participants. They tortured him to find out who he was cooperating with and what information he was passing on and to whom[17]. Soldering irons were used to burn crosses on some local residents' bodies to extract the names and addresses of ATO participants, territorial defense fighters, and individuals with pro-Ukrainian positions. The detained Ukrainians were threatened with the death penalty in a minefield and with reprisals against their families, who were still in the occupied city[18].

5. ZAPORIZHZHIA REGION

In the city of Enerhodar in the Zaporizhzhia region, an engineer from the Zaporizhzhia NPP reported in the media about the abduction of many plant employees[19]. According to the eyewitness, people were disappearing as if following a certain algorithm. First, public activists in Enerhodar, then ATO participants and their relatives, and finally, anyone who identified themselves as Ukrainians[20].

In March 2022, Russian forces occupied the town of Vasylivka and immediately began searching for local activists. Ukrainian journalists and officials

16 Media reports citing eyewitness accounts. Access mode: *https://life.pravda.com.ua/society/2022/05/11/248583/*

17 Media reports citing the testimony of a victim. Access mode: *https://www.youtube.com/watch?v=H0-zP49kVHI*

18 Media reports; eyewitness accounts. Access mode: *https://glavcom.ua/country/incidents/bili-strumom-i-vipaljuvali-khresti-na-tili-rashisti-zhorstoko-katuvali-meshkantsiv-kupjanska-video-875931.html*

19 Media reports, statements from a ZNPP engineer. Access mode: *https://www.unian.net/war/okkupanty-prevratili-proverku-zhenshchin-na-kpp-zaes-v-pytku-rabotnik-stancii-novosti-vtorzheniya-rossii-na-ukrainu-11940765.html*

20 Media reports, statements from a ZNPP engineer. Access mode: *https://www.unian.net/war/okkupanty-prevratili-proverku-zhenshchin-na-kpp-zaes-v-pytku-rabotnik-stancii-novosti-vtorzheniya-rossii-na-ukrainu-11940765.html*

were subjected to particularly brutal torture[21]. In April 2022, representatives of the self-proclaimed city administration gathered the heads of housing cooperative associations[22] to demand personal information about residents[23].

Mayor of Melitopol, Ivan Fedorov, reported on his Telegram channel that the Russians forced local residents to obtain special permits. This was a way for them to collect personal data to track people's movements between settlements[24]. According to a report from the Zaporizhzhia Regional Military Administration dated May 20, 2022, Russian occupiers started giving pensioners 10,000 rubles in exchange for their data *(passport, pension certificates, etc.)* at the Center for Administrative Services in Melitopol. The same practice was reported in the town of Mykhailivka where the occupiers registered pensioners supposedly to pay their pensions[25]. That is, in addition to specific lists of individuals, they were also creating databases of the population. It can be assumed that this was done to manipulate, distort, or subsequently destroy data.

According to the National Resistance Center[26], the Russian occupiers later expanded the list of social groups within the population that they tried to bribe in exchange for obtaining passport data. They offered financial assistance to low-income families, mothers with children under three years old, and other socially vulnerable groups. People were pressured to take Russian documents against their will. Forced passportization also took place in places of detention.

Each of the incidents mentioned above requires investigation by Ukrainian law enforcement agencies to determine the source of the detailed dossiers on Ukrainians that ended up in the hands of Russian military personnel. In the following sections, we will explore the facts regarding possible sources of such information.

21 Media reports citing law enforcement agencies.. Access mode: *https://www.slidstvo.info/news/okupanty-iaki-katuvaly-ukraintsiv-strumom-i-khimichnymy-reaktyvamy-vyiavylysia-biytsiamy-dahestanskoho-omonu/*

22 ***A housing cooperative association is a condominium association or co-ownership association created to simplify the management and use of property in a multi-apartment building.***

23 As reported by the Enerhodar mayor Dmytro Orlov on his Telegram channel.

24 Media reports, statements from the mayor of Melitopol. Access mode: *https://espreso.tv/melitopol-stae-zakritim-mistom-ni-vikhati-do-nogo-ni-viikhati-zvidti-nemozhlivo-mer-fedorov*

25 As provided in the report of the Zaporizhzhia Regional Military Administration. Access mode: *https://t.me/zoda_gov_ua/8041*

26 Occupiers have increased the scale of bribing the population to obtain passport data. Access mode: *https://sprotyv.mod.gov.ua/okupanty-zbilshyly-masshtaby-pidkupu-naselennya-dlya-otrymannya-pasportnyh-danyh/*

STATE CLOSED PERSONAL DATABASES

(Image source: pressfoto / freepik.com)

Today, practically no organizations or institutions exist that do not collect personal data. The only thing that sets them apart is the purpose and type of information they process. For example, stores typically need email addresses and phone numbers for marketing products. Internet companies collect behavioral data about individuals, such as which websites they visit, what they search for, and what they view, to create a digital product that forms the basis for advertising and more. Banks, medical, insurance, travel, and other services cannot operate without personal data. However, the widest range of information about an individual is collected by the government.

Government authorities establish databases to carry out their functions in various areas, such as law enforcement, healthcare, social services, education, and more. Personal data can be stored on paper, in information systems, or on other media. This means that threats to data leakage can arise not only from cyberattacks but also from the actions of employees themselves.

The main problem is that individuals have very limited tools to control the use of their personal data. If someone decides to find out something about someone else, they can purchase almost any information for a certain sum of money. Unfortunately, there is still a lack of research in this area today, so it is challenging to determine, say, in which sectors data breaches occur most frequently. We can rely only on cases that have become known and had consequences.

Throughout 2022-2023, there were numerous reports from law enforcement agencies, civil activists, and the media about unauthorized access to and the sale of state databases containing personal data of citizens of Ukraine and European Union countries. This includes various types of information that are sold, including to Russian citizens, for a fee. The key question is: how do criminals gain access to closed state databases? There have been reports of specific officials who had access to them being exposed. However, not all the perpetrators were government officials.

In the so-called darknet, there is a vast amount of offers to sell various databases, including secret ones. These databases can contain thousands of files with information about anyone. Today, there is a thriving industry that offers services to compile dossiers on any individual. Therefore, it cannot be said that the problem lies solely in hostile cyberattacks. There is already enough evidence that a significant portion of data breaches occur through

social engineering, where individuals with access to information intentionally or unintentionally disseminate it. Poor protection of state registries, a low level of digital literacy among employees, and a lack of proper control contribute to the active development of the sale of personal data belonging not only to citizens of Ukraine but also to other countries worldwide. This segment of the shadow market operates on both specialized underground platforms and widely-used platforms like Telegram, Viber, etc. Moreover, it is important to note that in many cases, perpetrators do not hack databases but simply purchase stolen data and use it to search for information about specific individuals[27]. Therefore, the focus is not solely on the issue of technical data security but on organizing the data processing process as a whole.

1. UNAUTHORIZED ACCESS TO GOVERNMENT DATABASES

In April 2023, the Kyiv City Prosecutor's Office reported that they had uncovered an organizer who was selling the personal data of Ukrainians. The Obolon District Prosecutor's Office in Kyiv announced the suspicion[28] of a capital city resident engaged in the illegal sale of confidential information from closed databases.

The pre-trial investigation revealed that in 2022, the man gained access to information from databases, including those of the Main Service Center of the Ministry of Internal Affairs of Ukraine, the Pension Fund of Ukraine, the State Tax Service, the Bureau of Technical Inventory, the State Service of Ukraine for Geodesy, Cartography and Cadaster, and banking structures, among others. The perpetrator, along with his accomplices, created an information system on the internet and, with the goal of enrichment, established the sale of personal data of citizens by providing access to the registers for 2,000 euros per month. The suspect[29] personally met with interested individuals and, after receiving payment, provided them with a link to the website along with a login and password for access.

27 Your address, passport, and accounts can be easily purchased on the darknet for $100. How does the market for «personal data breaches» work? Access mode: *https://forbes.ua/inside/vashu-adresu-pasport-ta-rakhunki-mozhna-legko-kupiti-v-darkneti-za-100-yak-pratsyue-rinok-probivu-personalnikh-danikh-28012022-3431*

28 Part 2 of Article 361-2, Part 5 of Article 27, Part 3 of Article 362 of the Criminal Code of Ukraine.

29 Part 2 of Article 361-2, Part 5 of Article 27, Part 3 of Article 362 of the Criminal Code of Ukraine.

During the search at the man's place of residence, system units, hard drives, and other devices containing unlawfully obtained confidential information were confiscated, as well as phone numbers, identification documents, seals, passports of Russian citizens, documentation related to the group's activities, and funds equivalent to 340,000 euros. The question arises: how did these individuals gain access to closed state databases? Therefore, during the preparation of this text, we sent a request for clarification to the Prosecutor's Office. There were still no responses as of the time of this report's publication.

2. SALE OF PERSONAL DATA OF CITIZENS OF UKRAINE AND THE EUROPEAN UNION

Cyber police officers have uncovered a large-scale operation involving the sale of personal data of citizens of Ukraine and the European Union. The criminal activity was organized by a 36-year-old resident of the city of Netishyn in the Khmelnytskyi region. The man was an administrator of closed groups on Telegram. It was mainly there that the sale of personal data upon request was carried out. Among the information offered for sale were passport data, individual taxpayer identification numbers, birth certificates, driver's licenses, and bank accounts. The database contained personal information of over 300 million individuals, including citizens of Ukraine and European Union countries. Depending on the volume of information, the perpetrator demanded from $500 to $2,000 for access to the data. According to the information discovered, citizens of Russia were among the buyers of the data. Law enforcement officers conducted a search at his residence and seized mobile phones, hard drives, SIM cards, computer equipment, and server hardware, where they found restricted access databases[30]. The question also arises: how did these individuals gain access to closed databases?

A similar scheme was also uncovered by the Security Service of Ukraine. The organizer turned out to be an entrepreneur from Cherkasy who purchased specialized server equipment for collecting and processing personal data. He engaged two residents of the capital in his illegal activities, who assisted him in creating and administering online services. In particular, they created a specialized internet platform and a Telegram bot through which they sold passport

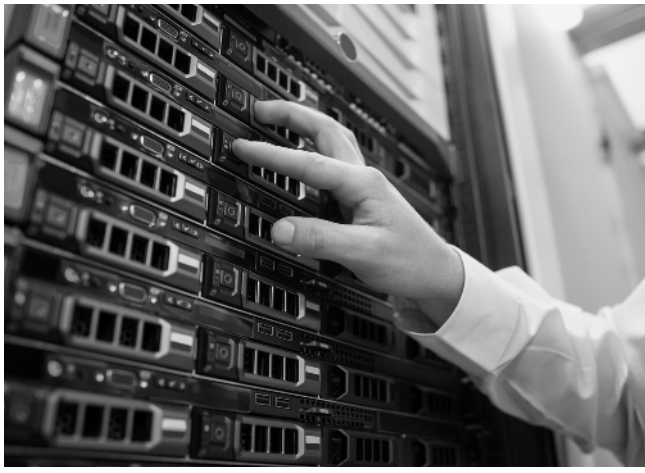
30 The official Facebook page of the Cyberpolice. Access mode: *https://www.facebook.com/cyberpoliceua/posts/pfbid0wATw3mv1Sw25ssF8QdJAHEMB8z4eKHyyLyDuAQREaPpHR2YnrpyoJt9iDZvenpxml*

data, phone numbers, and vehicle information belonging to residents from various regions of Ukraine. According to the investigation, to gain access to electronic databases, clients purchased subscriptions to relevant internet resources and were offered the chance to buy a «subscription» for a month, costing up to $200. To find clients, they used specially created Telegram channels and received payments in cryptocurrency. Among potential clients of such internet services were representatives of Russian special services seeking confidential information about military service members.

During searches at the addresses of the criminals, computer equipment and other material evidence of the crime were found. The organizer of the scheme has been informed of the suspicion under Part 1 of Article 361-2 of the Criminal Code of Ukraine (unauthorized sale of information with restricted access stored in electronic computing machines (computers) protected in accordance with applicable law). At the time of the publication of this material, the investigation was still ongoing to establish all the circumstances of the crime and hold those responsible accountable.

3. AN EMPLOYEE OF THE CABINET OF MINISTERS OF UKRAINE WAS TRANSFERRING CONFIDENTIAL INFORMATION AND PERSONAL DATA OF UKRAINIANS

In June 2022, the Security Service of Ukraine announced on its official website that it had conducted a multi-stage special operation to neutralize an FSB spy network, engaged in intelligence and subversive activities within the state authorities of Ukraine. As a result of this operation, individuals holding positions as the head of a department in the Secretariat of the Cabinet of Ministers of Ukraine and the head of one of the directorates in the Chamber of Commerce and Industry were detained.



(Image source: wavebreakmedia / freepik.com)

These officials had been passing information to the aggressor country, including details about Ukraine's defense capabilities, border arrangements, and personal data of Ukrainian law enforcement officers. They were not doing this for a fee being paid for the information from $2,000 to $15,000 per assignment. The amounts depended on the level of secrecy and the importance of the collected data. The perpetrators would print, photograph, and store secret documents on flash drives. To transfer files, they would arrange meetings through a closed Telegram channel with their «contact,» one of the employees of the Chamber of Commerce and Industry. According to the investigation, the data transmission scheme worked as follows: the government official would pass the information to their «contact» in the Chamber, and the contact would then transmit it to Russia through encrypted communication channels. Both criminals have been informed of the suspicion of committing a crime under Article 111 (state treason) of the Criminal Code of Ukraine. The court decided to detain them in custody as a preventive measure[31].

4. "PRIVATE DETECTIVES" WERE SELLING CONFIDENTIAL INFORMATION FROM GOVERNMENT DATABASES

In May 2023, the Security Service of Ukraine announced[32], that their cybersecurity experts had «neutralized» the criminal activities of a private detective agency in Kyiv that was selling information from closed databases of state institutions. The illegal operation was organized by a former investigator from one of the city's police precincts who had refused to undergo certification within the police force and resigned from the law enforcement agency in 2015. Later, he teamed up with an acquaintance to establish a private detective agency.

Under the guise of a legal business, they collected confidential information about citizens for their clients, including data stored in closed government registries. They utilized their «old» connections among various officials and law enforcement representatives for this purpose. The cost of a «dossier» on one person ranged from $800 to $2,600. The amount depended on the volume of

31 The official website of the Security Service of Ukraine. Access mode: https://ssu.gov.ua/novyny/sbu-vykryla-rosiisku-ahenturu-do-yakoi-vkhodyly-posadovtsi-kabminu-i-torhovopromyslovoi-palaty-ukrainy-video

32 The investigation was conducted by the Security Service of Ukraine in Kyiv and the Kyiv region under the procedural guidance of the Kyiv Regional Prosecutor's Office.

personal data and the urgency of the «order.» For instance, «detailed profiles» included not only passport data but also information about individuals' phone numbers, vehicles, as well as details about border crossings and administrative violations. Both «detectives» were apprehended while receiving payment for a «folder» containing constituent data on a resident of the capital. During searches at their residential addresses, mobile phones and computers with evidence of illegal activity were found. Additionally, an investigation is underway to determine whether there was any potential sale of confidential information to an aggressor country[33].

(Image source: official page of the Security Service of Ukraine)

5. LAW ENFORCEMENT OFFICIALS ILLEGALLY COLLECTED PERSONAL DATA OF THE POPULATION IN THE TERNOPIL REGION

In June 2023, the State Bureau of Investigation reported suspicions against a law enforcement officer in the Ternopil region who unlawfully collected personal data of volunteers from the Territorial Defense Forces of the Armed Forces of Ukraine and their family members. Subsequently, this information was made public on one of the Russian resources.

The suspect systematized and stored information such as the names of service members, their dates of birth, registration and residence addresses, ownership of movable and immovable property, firearms and special equipment, as well as contact phone numbers of their relatives. The State Bureau of Investigation did not specify the purpose of collecting this data or how it was later used, including how it ended up with Russian propagandists. However, the mere fact of unauthorized data processing can have significant conse-

33 The official website of the Security Service of Ukraine. Access mode: *https://ssu.gov.ua/novyny/sbu-zatrymala-u-kyievi-dvokh-pryvatnykh-detektyviv-yaki-torhuvaly-konfidentsiinoiu-informatsiieiu-iz-derzhavnykh-baz-danykh*

quences. The law enforcement officer has been informed of the suspicion[34] of illegally collecting, storing, and using confidential information[35].

This is not an isolated case, as another group of law enforcement officers was found in the Ternopil region to have unlawfully collected data about the region's residents. Specifically, they systematized detailed information about dates of birth, place of registration, residence, ownership of movable and immovable property, firearms, special equipment, and so on. This was reported by the press service of the Ternopil Regional Prosecutor's Office. The law enforcement officer has been charged with the illegal collection, storage, and dissemination of confidential information[36]. Pre-trial investigation was conducted by investigators from the Territorial Office of the State Bureau of Investigation located in Lviv.

6. IN THE SUMY REGION, A LAW ENFORCEMENT OFFICER WAS EXPOSED FOR SELLING CONFIDENTIAL INFORMATION FROM GOVERNMENT DATABASES

The Security Service of Ukraine has exposed a law enforcement officer in the Sumy region who was selling the personal data of Ukrainian citizens[37]. According to the investigation, a member of the operational unit of the National Police in the Sumy region was obtaining confidential information from closed state databases, including those of the Border and Migration Services of Ukraine, and then selling it to interested parties. He was not acting alone but in collaboration with other individuals. The organizers of the scheme were searching for potential buyers on thematic internet forums. Interested parties would order the necessary information from them and then pay the agreed-upon amount in cryptocurrency for this service. The cost of each «order» ranged from several hundred dollars, depending on the

34 The official website of the State Bureau of Investigation. Access mode: *https://dbr.gov.ua/news/dbr-vikrilo-pravoohoroncya-na-nezakonnomu-zbirani-personalnih-danih-ternopilskih-teroboronivciv-yaki-potim-zyavilis-na-rosijskih-resursah*

35 The official website of the State Bureau of Investigation. Access mode: *https://dbr.gov.ua/news/dbr-vikrilo-pravoohoroncya-na-nezakonnomu-zbirani-personalnih-danih-ternopilskih-teroboronivciv-yaki-potim-zyavilis-na-rosijskih-resursah*

36 Part 1, 2 of Article 182 of the Criminal Code of Ukraine.

37 As reported on the Facebook page of the Security Service of Ukraine in the Sumy region.

volume. Afterward, the criminals would illegally obtain and transfer the data to their «clients» through closed electronic communication channels.

According to the investigation, among the «clients» who received such «services» were citizens and residents of Russia and Kazakhstan. During authorized searches conducted at the place of residence and work of one of the scheme participants (a police officer), computer equipment, flash drives, and mobile phones containing evidence of illegal activities were discovered and seized. Pre-trial investigation is ongoing to hold all individuals involved in this unlawful activity accountable.

7. AGGREGATION OF CLOSED GOVERNMENT DATABASES

In the context of data leakages, it is also necessary to mention the initiative to create a single state registry of conscripts, individuals eligible for military service, and reservists, which will be populated through interactions with other systems and citizen databases[38]. Such actions are essential to expedite the process of updating information about conscripts, individuals eligible for military service, and reservists.

Specifically, the Cabinet of Ministers of Ukraine adopted Resolution No. 1493 dated December 30, 2022, to envision the cross-checking of personal data of individuals. To accomplish this, it was instructed to verify information about individuals based on data processed in state information resources, namely:

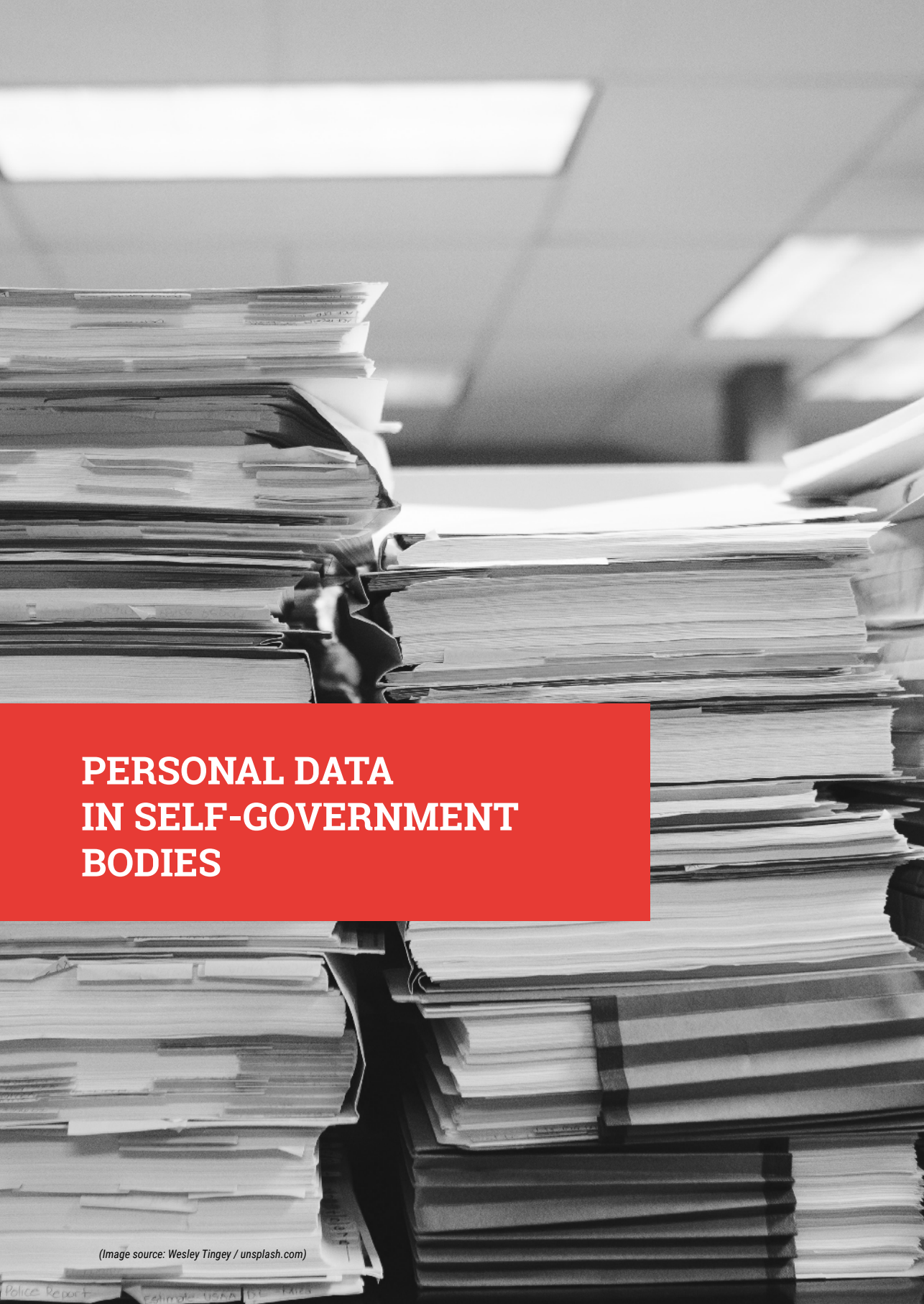
- The Unified State Demographic Register;
- The State Register of Individuals - Taxpayers;

(Image source: freepik / freepik.com)

38 The collection of current data on conscripts, those eligible for military service, and reservists will be automated and sped up in Ukraine. Access mode: https://sud.ua/uk/news/publication/258417-v-ukraine-avtomatiziruyut-i-uskoryat-sbor-aktualnykh-dannykh-o-prizyvnikakh-voennoobyazannykh-i-rezervistakh

- The State Register of Civil Status Acts of Citizens;
- The Register of Insured Persons of the State Register of Compulsory State Social Insurance;
- The Unified Information Database on Internally Displaced Persons;
- The departmental information system of the State Migration Service.

Perhaps, informational interactions between various government agencies are indeed a necessary measure for organizing mobilization efforts and enhancing the country's defense capabilities. However, it is also crucial to emphasize that when making such decisions, the current legislation of Ukraine regarding the protection of personal data must be taken into account (which requires urgent reform), as well as consideration of the existing system of state control in this area, the state of information security of government systems, and the overall organization of work with confidential information, including the wide range of risks that exist today.



PERSONAL DATA IN SELF-GOVERNMENT BODIES

(Image source: Wesley Tingey / unsplash.com)

Local self-government bodies (hereinafter referred to as LSG bodies) manage affairs in the interests of specific territorial communities. The executive authorities of village, town, and city councils have jurisdiction over various sectors, including housing and communal services, education, healthcare, social welfare, defense, budgeting, law enforcement, and more. The execution of these tasks necessitates the collection and processing of significant volumes of personal data of the population.

Each year, LSG bodies adopt new decisions, implementing electronic document management systems, installing comprehensive video surveillance systems, and creating modern websites with online services for residents. The development of technology, alongside its advantages, also entails a certain spectrum of risks, which significantly escalate during wartime.

In January 2022, experts from the Association UMDPL held meetings with representatives of LSG bodies from various regions of Ukraine to understand the specific challenges they face when processing personal data. It turned out that most of these challenges were related to organizational processes in data processing and the absence of internal control mechanisms. During these discussions, officials acknowledged their need for further training and qualifications in this field. Only a small number of employees in these units attended specialized training events.

We also found that a relatively small number of LSG bodies had developed and implemented internal regulatory documents governing this sphere. Even among those LSG bodies that had adopted internal policies in the privacy sphere, these documents were often copied from other sources and not tailored to the specific activities of the institution. The absence of internal regulation for all data processing processes leads to risks ranging from the violation of the overall data processing cycle to potential data leaks. Issues related to data collection and storage remain unregulated as well. It is common for LSG bodies to accumulate an excessive amount of information, with another prevalent problem being data aggregation. Consolidating different databases into a single one poses risks both for internal management (making it more difficult to comply with legal requirements, such as differentiating information or timely data deletion) and for individuals whose information is contained in these databases, as it may lead to unintended identification through their shared profile. Additionally, virtually no LSG bodies conducted risk assessments in the field of data processing.

The majority of the problems encountered by local self-government bodies (LSG bodies) during wartime are not new or unique to the present day. Assessing the damage and negative impact on the country's situation due to inadequate protection of personal data in LSG bodies during times of war is not an easy task. However, numerous media reports indicate attempts to gain access to databases containing personal data (also those managed by LSG bodies), including by kidnapping officials and committing acts of violence or blackmail. Additionally, there are individuals who, through various means, voluntarily provided or disclosed information held by municipal councils.

1. THE MAYOR PUBLISHED THE PERSONAL DATA OF SERVICE MEMBERS

At the beginning of October 2022, information appeared in the media about the mayor of the Borshchiv City Council publishing statements from service members, containing their personal data such as contact phone numbers and surnames. A photo of the document appeared on the city council's website. Following this, an administrative protocol was drawn up against the mayor under the article related to the violation of document usage, which led to the disclosure of official information. His actions were classified under Part 1 of Article 212-5 of the Administrative Offenses Code of Ukraine (violation of the procedure for using documents in the defense sphere, leading to the disclosure of information). While holding the position of mayor of the Borshchiv City Council, he committed a violation of the requirements of the standard instruction on the procedure for keeping records, storage, use, and destruction of documents containing official information […] leading to the disclosure of official information in the country's defense sector — as stated in the ruling. The mayor did not appear at the court hearing but submitted a written request for the case to be considered without his participation. He acknowledged his guilt and did not file an appeal. The court also found the man guilty and imposed the minimum punishment under this article - a fine of 1,020 hryvnias. In addition, he must pay a court fee of 496 hryvnias[39].

At present, we cannot speculate on the real motives behind the mayor's actions. It is possible that the official made such a decision without fully realizing

39 Zaxid.NET. Access mode: *https://zaxid.net/mera_borshheva_oshtrafuvali_za_rozgoloshennya_informatsiyi_pro_viyskovih_n1550640?fbclid=IwAR17aruvpsC7q5PeQEsQtX7Ehl2e98ZvxQrDDVgvUgOYqM9cMeO9Y3tB8Ps*

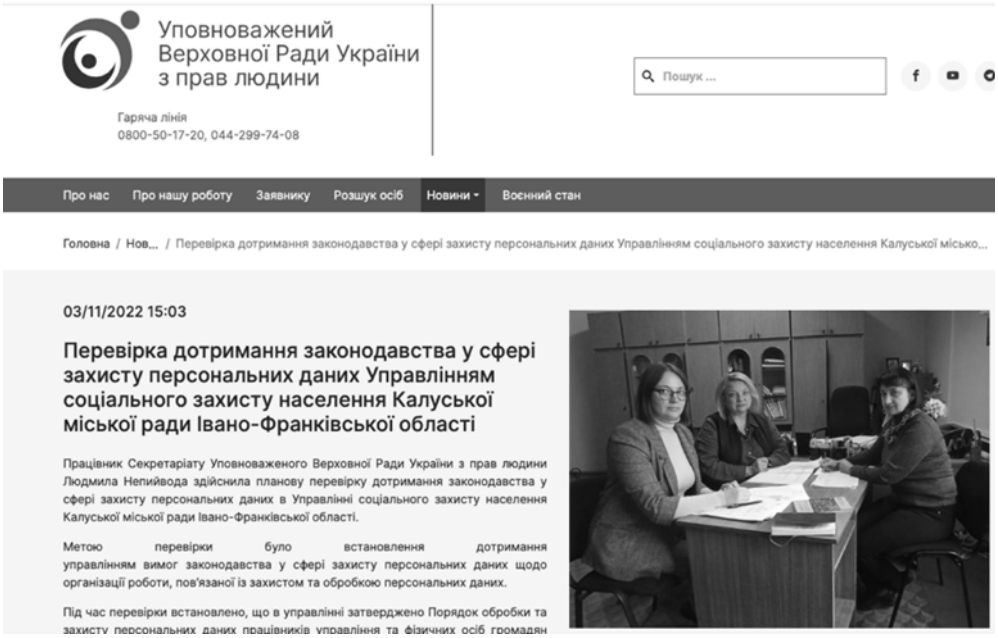
the potential consequences and later expressed remorse and took responsibility. However, in this situation, it is important to focus on the organization of personal data protection processes within the institution as a whole. Therefore, in the preparation of this document, we sent a request to the Borshchiv City Council to inquire about how this municipality ensures data security, including whether relevant internal documents have been developed and whether a responsible person has been appointed in accordance with the law. In response, we were informed that there are no documents regulating this area in the city council, and no responsible person has been appointed. It is important to note that this situation is not unique to this city council. This case became known through the media, but there are many other instances that indicate problems with enforcing the law

2. THE OFFICE OF THE UKRAINIAN PARLIAMENT COMMISSIONER FOR HUMAN RIGHTS REPORTED VIOLATIONS IN LOCAL SELF-GOVERNMENT BODIES

During 2022, announcements regarding planned and unplanned inspections of municipalities concerning compliance with personal data protection legislation were posted on the official website of the Ombudsman. In particular, visits were made to the Social Welfare Department of Kalush City Council in the Ivano-Frankivsk region, the Social Welfare Department of the Dnipro Regional Military Administration, Perechyn City Council, and Uzhhorod City Council. Almost all of these local government bodies were found to be in violation of personal data protection laws. The following shortcomings were highlighted:

- failure to notify the Commissioner for Human Rights about the processing of data that poses a particular risk to the rights and freedoms of individuals and about the responsible person organizing work in this area[40];
- the Dnipro District Military Administration has no procedure in place for the processing of personal data. Employees with access to data do not sign confidentiality agreements, and there is no record of employees

40 Verification of compliance with personal data protection legislation by the Social Welfare Office of the Kalush City Council in Ivano-Frankivsk Oblast. Access mode: *https://ombudsman.gov.ua/news_details/perevirka-dotrimannya-zakonodavstva-u-sferi-zahistu-personalnih-danih-upravlinnyam-socialnogo-zahistu-naselennya-kaluskoyi-miskoyi-radi-ivano-frankivskoyi-oblasti*



Monitoring Compliance with Personal Data Protection Laws by Kalush City Council›s Social Welfare Department in Ivano-Frankivsk Region, as per the Ukrainian Parliament Human Rights Commissioner›s Website

who have access to data. The procedure for deleting data whose storage period has expired has not been determined, and there is also no notification to the Commissioner for Human Rights about the processing of special categories of data and the responsible person for this. There is no record of operations related to the processing of personal data;

— the Department of Social Policy of Uzhhorod City Council has no appropriate regulatory legal acts in place regulating the processing of special categories of data, specifically information about health status and actions related to domestic violence. Some individual files of social service recipients contain excerpts from the medical and social expert commission report of the Ministry of Health of Ukraine, which includes disability group and the applicant's diagnosis. The department receives information in electronic form about detected cases of domestic violence in the form of tables. Additionally, there is no separate provision defining general requirements for data processing and protection, and no responsible person has been appointed[41].

41 Monitoring compliance with the right to appeal and planned inspection of compliance with legislation in the field of personal data protection in Zakarpattia. Access mode: *https://ombudsman.gov.ua/news_details/monitoring-doderzhannya-prava-na-zvernennya-ta-planova-perevirka-doderzhannya-zakonodavstva-u-sferi-zahistu-personalnih-danih-na-zakarpatti*

Perhaps, such notifications may appear somewhat formal at first glance. However, it is important to note that they address the underlying causes (non-compliance with legal norms) of the consequences already described in previous sections and elsewhere in this report.

3. AN OFFICIAL FROM THE CITY OF MYKOLAIV HEADED A RUSSIAN ESPIONAGE AGENCY

The SBU neutralized Russian espionage agency headed by an official from Mykolaiv: the traitor was detained during a meeting at the Mayor›s Office

In Mykolaiv, the counterintelligence unit of the Security Service of Ukraine neutralized a Russian agent, one of whose tasks was to organize a powerful espionage group of Russian special services. The traitor turned out to be the head of the Municipal Enterprise «Mykolaiv Funeral Service,» who was apprehended right in the city council during a meeting. He was collecting data on the location and movements of units of the Armed Forces of Ukraine in the region. Another of his tasks was to «inform» the aggressor about the operation of critical infrastructure objects in Mykolaiv and other matters discussed during working meetings in the city council. The official attempted to involve two subordinates and two other residents of the city in intelligence and subversive activities, including a senior officer from the district police department. It was also established that the perpetrator was providing Russian agents with per-

sonal data of Ukrainian service members, police officers, employees of the Security Service of Ukraine and Prosecutor's Office, as well as lists of deceased Ukrainian defenders[42].

It is hard to imagine that one official could have had access to all the mentioned types and categories of data. This is more likely a result of an improper information processing ecosystem where proper measures were not taken to comply with data protection laws and ensure their security.

42 The SBU neutralized a Russian agency led by an official from Mykolaiv: the traitor was apprehended during a meeting with the mayor. Access mode: *https://ssu.gov.ua/novyny/sbu-zneshkodyla-rosiisku-ahenturu-yaku-ocholiuvav-chynovnyk-iz-mykolaieva-zradnyka-zatrymaly-pid-chas-narady-u-mera-video*

MEDICAL DATA

(Image source: Ante Samarzija / unsplash.com)

The issue of personal data protection should be one of the key components in the healthcare system. First and foremost, privacy plays a vital role in building society's trust in the medical field. The confidentiality of an individual's information is necessary to protect them from potential stigmatization, discrimination, and other risks associated with medical diagnoses, lab results, or visits to healthcare providers. There have already been numerous cases where the unlawful use of medical information (disclosure, distortion, alteration, etc.) has caused significant psychological and physical harm to individuals. For example, in 2021, several stories came to light that demonstrated the risks of disclosing medical information.

At the time, Olena[43] lived in a small town in eastern Ukraine. She was a human rights activist who often advocated for the protection of human rights. However, she found herself in need of legal assistance when she discovered that information about her health condition had been unlawfully disclosed. Elena had a serious illness and was under the care of a local hospital. But due to a breach in the security of her personal data, her medical information ended up in the wrong hands, leading to her becoming a victim of blackmail. She linked this incident to her professional activities.

Another story involves a schoolgirl named Nadiia, who had certain health issues. In the clinic where she was undergoing rehabilitation, the mother of one of her classmates worked and decided to inform her son about Nadiia's medical visits. As a result, information about the girl's health became known at school. Initially, this seemed like a misunderstanding, but the consequences turned out to be serious. Nadiia faced stigma, ridicule, and discrimination. Her classmates began to avoid her, and some even spread false rumors about diagnoses that did not exist. The girl experienced significant psychological stress, which had a negative impact on her physical well-being.

These examples are provided solely to illustrate that the issue of personal data protection violations within the healthcare system encompasses such complex life stories. That's why, according to legislation, medical information belongs to a special category of data since it poses a high risk to an individual's rights and freedoms, thus requiring stringent protective measures.

Furthermore, personal data can also become a target for external adversaries. This concerns not only specific individuals but also national security.

43 The name has been changed for anonymity reasons.

Throughout 2022-2023, there were reports of leaks from medical information systems, which serve as a serious signal of issues in this sphere and the lack of accountability for individuals who have access to this information. Wrongdoers who unlawfully gain access to medical databases can use this data for fraud, blackmail, or pass it on to adversaries for the commission of war crimes.

1. IN THE KHERSON REGION, MEDICAL WORKERS WERE UNLAWFULLY TRANSFERRING PERSONAL DATA

In June 2022, the Office of the Prosecutor General reported[44] the prosecution of the deputy general director of a healthcare institution from the medical department of the Kherson Regional Children's Hospital for committing state treason during martial law [45]. According to the investigation, the suspect voluntarily agreed to cooperate with Russian intelligence officers and representatives of the occupying authorities of the aggressor country.

(Source: the official website of the Security Service of Ukraine)

On his own initiative, the official informed representatives of the aggressor country that the hospital's archives contained medical documentation, including records and personal files of employees of the Main Directorate of the National Police in the Kherson region. After this disclosure, Russian military personnel gained access to the personal data of the police personnel in the region.

On May 17, 2023, the Security Service of Ukraine reported[46] the detention of a nurse from one of the local hospitals in Kherson who had been transmitting confidential information about local residents to the enemy. Even after the liberation of the city from temporary occupation, she stayed and continued to work in the medical institution, engaging in intelligence and subversive activ-

44 The Telegram channel of the Prosecutor General's Office. Access mode: *https://t.me/pgo_gov_ua/4460*

45 Part 2 of Article 111 of the Criminal Code of Ukraine.

46 The official website of the Security Service of Ukraine. Access mode: *https://ssu.gov.ua/novyny/sbu-zatrymala-medsestru-yaka-pratsiuvala-na-fsb-i-zlyvala-vorohu-personalni-dani-ukrainskykh-zakhysnykiv*

ities against Ukraine. The woman collected constituent data about Ukrainian defenders who were receiving treatment at the medical facility.

She also spied on the locations of the Defense Forces units stationed in the regional center's territory. According to investigators, she came under the scrutiny of Russian intelligence services due to her public support for the aggressors in one of the anti-Ukrainian groups on Telegram.

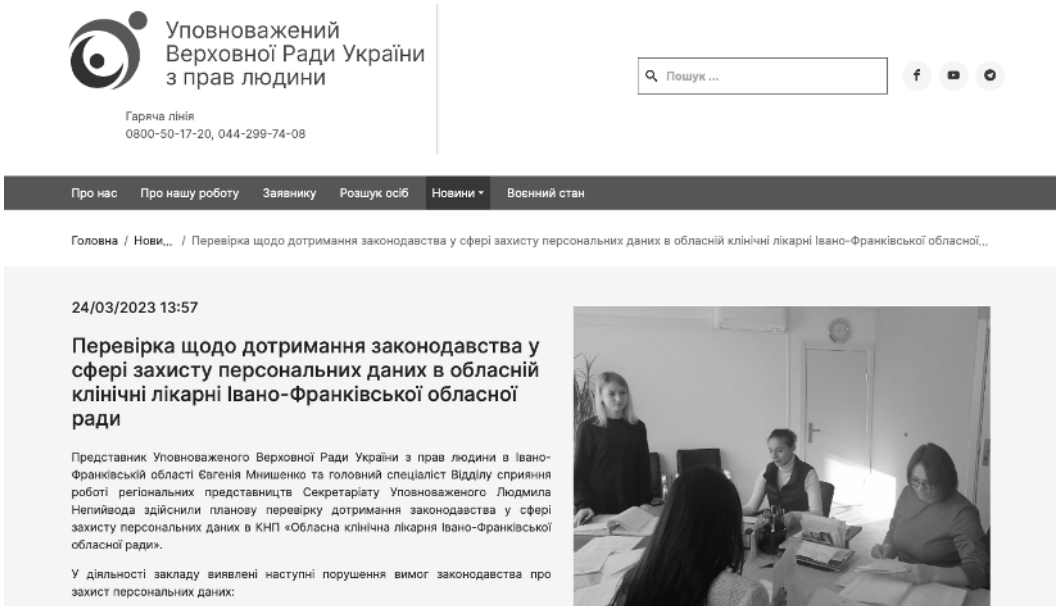
2. VIOLATIONS OF LEGISLATION IN THE REGIONAL CLINICAL HOSPITAL OF THE IVANO-FRANKIVSK REGIONAL COUNCIL

During 2022-2023, representatives of the Ombudsman's Office conducted inspections of medical institutions to assess their compliance with the law in this area. In March 2023, it was reported that in Ivano-Frankivsk region, a planned inspection was conducted at the Municipal Non-Profit Enterprise «Regional Clinical Hospital of the Ivano-Frankivsk Regional Council,» where the following violations of personal data protection legislation were identified:

- no internal regulatory document has been adopted to establish procedures for handling data, considering the specific activities of the healthcare facility, labor relations, etc.;
- no responsible person for the protection and processing of personal data within the hospital has been designated;
- the enterprise did not inform the Ombudsman about the processing of personal data posing a special risk to the rights and freedoms of individuals, including information related to their health;
- no contingency plan in case of unauthorized access to personal data, damage to technical equipment, or the occurrence of emergencies has been developed[47].

Based on the inspection results, an official report was prepared, and corrective measures were prescribed. Considering all the circumstances, including cases relating to the nationwide medical database «HELSI,» there are grounds to believe that this is not the only institution disregarding the law in the field of protecting personal data.

47 The Ombudsman's official website. Access mode: *https://www.ombudsman.gov.ua/news_details/perevirka-shchodo-dotrimannya-zakonodavstva-u-sferi-zahistu-personalnih-danih-v-oblasnij-klinichni-likarni-ivano-frankivskoyi-oblasnoyi-radi*



Monitoring Compliance with Personal Data Protection Laws by Regional Clinical Hospital of the Ivano-Frankivsk Regional Council, as per the Ukrainian Parliament Human Rights Commissioner›s Website

Based on the inspection results, an official report was prepared, and corrective measures were prescribed. Considering all the circumstances, including cases relating to the nationwide medical database «HELSI,» there are grounds to believe that this is not the only institution disregarding the law in the field of protecting personal data:

- the Unified State Demographic Register;
- the State Register of Civil Status Acts of Citizens;
- the State Register of Individuals - Taxpayers.

The primary purpose of such data transfer is to verify personal information[48]. Once again, before making any decisions regarding the creation, aggregation, or exchange of information between databases of personal data, it is essential to thoroughly assess the risks related to data protection

48 Doctors will be able to share your personal data: what you need to know. Access mode: *https://ogo.ua/articles/view/2023-05-15/132451.html?fbclid=IwAR0u4pE4Or-HT9DMUvjbzNJLIJHzplaCB1tYPHTM0lU0_RZdqF0sqG5XDus*

3. VIOLATIONS DURING THE OPERATION OF THE ELECTRONIC HEALTHCARE SYSTEM

The official website of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine[49] reported[50] a series of inspections carried out to ensure compliance with the requirements for the protection of personal data during the operation of the electronic healthcare system. In particular, the National Health Service of Ukraine (NHSU), SOE «Electronic Health», «HELSI UA LLC», Municipal Non-Profit Enterprise «Center for Primary Medical and Sanitary Care of the Pechersk District», and Municipal Non-Profit Enterprise «Center for Primary Medical and Sanitary Care 'Rusanivka' of the Dniprovskyi District of Kyiv» were inspected.

According to the Ombudsman, the inspections revealed that the legislation on personal data protection is not correctly applied during the operation of the electronic healthcare system. Owners of electronic medical information systems collect personal data of patients, including medical data, with the consent of the data subject. Such consent is obtained either when the data subject applies to a healthcare institution and signs a declaration with a doctor or during registration in the electronic medical information system, including making an appointment with a doctor. In the former case, consent is given by placing a mark in electronic form when signing the declaration. As established during the inspections, healthcare institutions do not always inform the data subject about obtaining their consent, sometimes marking consent themselves instead of the patient and without the patient's knowledge.

Furthermore, in such cases, patients are not informed about the owner of their personal data, the purpose of data collection, their content and scope, who they may be transferred to, their rights defined by law. According to the Ombudsman, in this way, individuals are deprived of the opportunity to exercise and protect their rights as personal data subjects. During the inspections, it was also found that some owners of medical information systems incorrectly define the purpose of processing personal data and the relationship with healthcare institutions regarding the processing of patients' personal data.

49 The supervisory authority in the field of personal data protection.

50 Incorrect application of legislation in the field of personal data protection has been identified during the operation of the electronic healthcare system. Access mode: *https://www.ombudsman.gov.ua/uk/kontrol-za-doderzhannyam-vimog-zakonodavstva-zpd/rezultati-perevirok/viyavleno-nepravilne-zastosuvannya-zakonodavstva-v-sferi-zahistu-personalnih-danih-pid-chas-funkcionuvannya-elektronnoyi-sistemi-ohoroni-zdorovya*

The owner of a medical information system should process the personal data of the patient for the purpose of the healthcare institution and act as the data administrator in such cases, without the need for the consent of the data subject. However, owners of medical information systems obtain consent from data subjects for the purpose of processing personal data for the healthcare institution, specifying their own purpose of processing personal data too broadly. As a result, patients, when giving consent to the processing of personal data, do not know what they are actually agreeing to.

Based on the results of the inspections of the NHSU, it was recommended to revise the technical requirements for the electronic medical information system to connect it to the central database of the electronic healthcare system, as approved by the NHSU order dated February 6, 2019, No. 28. As regards HELSI UA LLC, it was recommended to revise the documents and align with the personal data protection legislation the relation of HELSI UA LLC as patients' personal data manager with healthcare institutions, with which a contract for using the information and telecommunications system «HELSI» is concluded, as well as to cease obtaining consent from data subjects for the processing of personal data for which the healthcare institution is the data owner. Additional inspections are planned to clarify all circumstances of personal data processing by owners of medical information systems.

In this context, it is worth mentioning the news in the media that during the full-scale invasion, Kyivstar acquired 69.99% of the shares of HELSI Ukraine. HELSI is a large private medtech startup launched in 2016, a key player in the market of medical information systems working with both public and private hospitals. This startup has ambitious goals, aiming to meet all the healthcare needs of individuals. High-quality, modern interaction between doctors and patients will allow a greater emphasis on prevention rather than treatment of serious diseases. The service has indeed facilitated access to state healthcare to some extent. It is possible to use it to find any doctor and make an appointment, receive electronic referrals, and more. All this data is automatically synchronized with the user's personal account from the central database of the Unified Electronic Healthcare System.

As of May 2023, the platform had over 25 million registered users. Medical institutions across the country and approximately 50,000 healthcare professionals are connected to the system. For many Ukrainians, it came as a surprise that this information system is private, not state-owned, and that pri-

vate entities have access to the health status of Ukrainians. According to the Ukrainian Law «On Personal Data Protection», such information belongs to a special category of data and requires special protection and processing procedures.

In August 2022, HELSI was acquired by Ukraine's largest mobile operator, Kyivstar, which belongs to the Alfa Group. The medical startup HELSI became part of the medical infrastructure in Ukraine. Questions began to arise in the public about who developed this IT service, promoting it at the state level, and why it was acquired by Kyivstar during wartime. Of particular concern was the fact that among the co-owners of Kyivstar are entrepreneurs who ended up on the sanctions lists of the United Kingdom after the start of the full-scale invasion.

Kyivstar and HELSI have had a long-standing partnership. For instance, the operator assisted subscribers in getting vaccinated by sending targeted SMS messages. Previously, this was not a matter of concern, but now questions have been raised about how the personal data of millions of Ukrainians are being handled, who is monitoring it, and who has access to it.

In addition to this, in May 2023, a scandal erupted on social media regarding fake records in Helsi accounts. Ukrainians were sharing stories on social networks about someone making appointments with doctors, receiving referrals, diagnoses, etc., without their knowledge. The exact number of accounts with fake records in HELSI was not specified. This issue could have existed for years. Why did it only become known now? Most Ukrainians do not frequently access their HELSI accounts, but posts on social media triggered an avalanche effect, and many people started checking their accounts, only to discover that someone had illegally used their sensitive personal data.

The medical service's management immediately dismissed the hacking version, assuring that patients' personal data was not compromised. The system only allows information to be entered by doctors, so third parties supposedly cannot interfere. In other words, these «virtual appointments» were not the work of hackers but rather medical professionals. What would be the point for doctors to create records of appointments that never took place? One of the possible reasons is the healthcare reform that started in April 2018. Its main principle is «money follows the patient.» More patients and procedures mean more state funding. The NHSU allocates funds for this purpose under a special program. The Ministry of Health of Ukraine is also aware of fake visits in HELSI

and assures that it will identify such cases and respond accordingly. The cost of these expenses and how long the state paid for treatment that never occurred are unknown[51].

The processing of personal data stored in medical information systems is of great importance not only for protecting an individual's privacy but also for national security as a whole. Therefore, there are still the following questions:

- Who owns (who is the official owner of) the «helsi.me» medical information system?
- Who made the decision to create this database and regarding the obligations of Ukrainian citizens (as well as medical institutions) to provide data to this system? Specifically, what regulatory acts, resolutions, and orders allowed this?
- Who specifically oversees the protection of personal data in this system?
- What measures has the state taken to ensure the protection of information in this system?

The Association UMDPL has sent a request to the Ministry of Health of Ukraine asking for clarification on these and other questions but received no response apart from the general phrase that «everything is carried out in accordance with the legislation on the protection of personal data.»

51 Doctors have been creating fake patient visits In the Helsi medical service for years. This might have resulted in financial losses for the state. How the Ministry of Health and Helsi plan to address this issue. Access mode: *https://forbes.ua/innovations/ukraintsi-masovo-skarzhatsya-na-feykovi-zapisi-do-likariv-u-servisi-helsi-u-nogo-ponad-25-mln-koristuvachiv-u-chomu-problema-i-chomu-vona-vinikla-ne-sogodni-11052023-13607*

PERSONAL DATA OF CHILDREN

(Image source: Annie Spratt / unsplash.com)

The issue of information security for a child as an adult must be considered from various angles. Personal data of a child can be processed by different institutions or organizations, which, in turn, are obligated to ensure their reliable protection and prevent unauthorized leaks and, consequently, the criminal use of information. However, children themselves may also provide personal information on the internet or freely share it in other ways, thereby exposing themselves to danger.

On one hand, the internet provides tools that allow children to explore the world around them. On the other hand, it opens up new possibilities for tracking, storing, and analyzing data about children's actions with an unprecedented level of detail. For example, based solely on information from social media, one can create a profile of a child and learn about their whereabouts, education, personal events, appearance, social connections, parents' financial situation, lifestyle, and behavioral patterns.

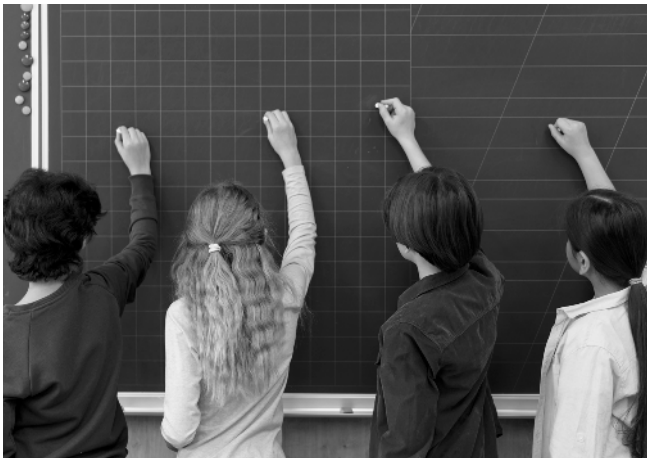
Any activity a child engages in on the internet and social media can serve as a source of information for their digital profile: posts, likes, photos, drawings, online orders, and more. Every user action leaves a digital footprint, and information published online can have consequences that may not manifest immediately but rather in the long term. Revealing a child's personal information can lead to unwanted contacts, various financial schemes, or even abduction.

1. THE HEAD OF A COMMUNITY IN THE KHARKIV REGION HANDED OVER PERSONAL DATA OF UKRAINIAN SCHOOLCHILDREN TO THE OCCUPIERS

On July 23, 2022, the head of the Kharkiv Regional Military Administration, Oleh Syniehubov, announced that the leader of a community in the Kharkiv region, which was then under occupation, had collaborated with the Russians and provided them with personal data of schoolchildren' from educational institutions. According to him, this information was handed over for issuing new version diplomas under the occupation regime. He also emphasized that the state betrayal by the public servant was deliberate but did not mention her name[52].

52 Suspilne News. Access mode: *https://suspilne.media/263657-golova-odniei-z-gromad-harkivsini-zdala-okupantam-personalni-dani-skolariv-sinegubov/?fbclid=IwAR1cPunJ-y4qBnM8b-3N5-139TRiWf4zWmUm_z8RvTDohE1J9aInaKTtU3g*

This incident requires an effective investigation by law enforcement agencies, and we hope that Ukrainian society will find out how such a thing could happen. At the same time, if we look at how the processing of personal data works, especially in state systems, it can be assumed that the information contained in the educational institution's database was processed in violation of the law. There were no established rules of operation, procedures for restricting access in the event of a territorial occupation, etc. The process of illegal activity may have occurred in advance or with the involvement of other individuals who helped gather information from various registers. This is important to consider during the investigation or analysis of similar situations because the main focus may shift only to the criminal activity of specific individuals and not the overall data protection system. It is necessary to thoroughly investigate possible causes to minimize such consequences in the future.



(Image source: freepik / freepik.com)

2. IN THE KHERSON REGION, CHILDREN WERE ENCOURAGED TO REGISTER ON A RUSSIAN WEBSITE, SUPPOSEDLY TO RECEIVE GIFTS

Children were encouraged on social media to register on a website to receive gifts. This information was posted on the Russian Telegram channel @VGA_Kherson, positioning itself as an official source from the administration of the Kherson region. The announcement included clear criteria for children who could participate in the so-called «campaign:» ages 3 to 17 and registration within this particular region. In addition to submitting an application on the website, participants were also required to provide copies of their documents.

At the same time, as part of manipulative tactics, children were asked to make wishes (e.g., for toys and gadgets) and on a non-material level, wish for a meeting with the President of Russia or «top government officials.» «Also, perhaps someone wishes to work as a journalist and try themselves in this

(Image source: Telegram channel Kherson Region Administration

The Kherson Region Administration: Children from the Kherson region can receive gifts thanks to the ‹Tree of Wishes.› / Children aged 3 to 17 can take part in the event registered in the Kherson region. The deadline for applications has been extended till December 20. / To participate in the event, you should go to the treeofwishes.rf website and apply there with your wish. You must also attach copies of your documents…

new role, someone may wish to go on television or to Lake Baikal (translated from Russian – ed.),» the announcement read.

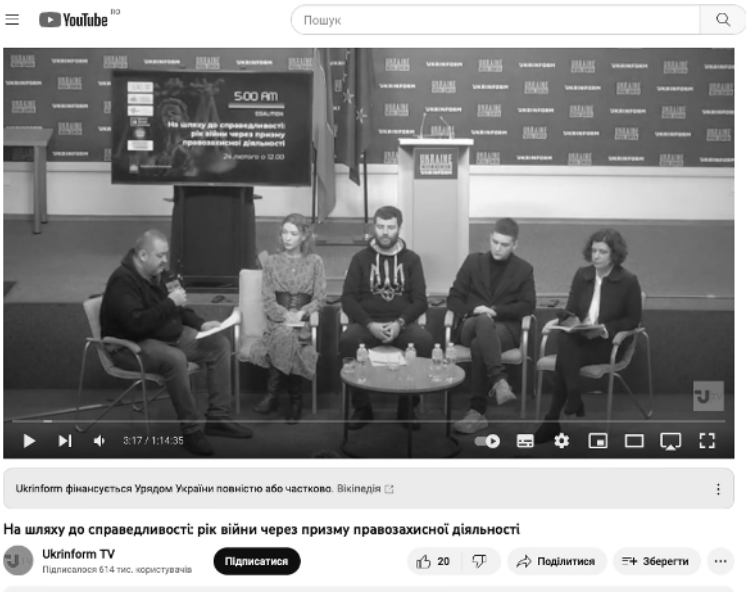
Human rights activists put forward various versions, including the possibility that the Russians may have needed this information for preparing the deportation of Ukrainian children before the potential withdrawal of Russian forces from the captured Ukrainian territories[53].

3. CHANGING THE PERSONAL DATA OF CHILDREN ABDUCTED FROM UKRAINE

Throughout 2022, Ukrainian human rights activists repeatedly reported that Russians were altering the personal data of children before deportation. For instance, during a press conference, it was mentioned that:

«The Russians essentially changed their ages and then moved them to the territory of Crimea. The children were kept there without being able to return because according to their documents, they were no longer considered children, and their freedom of movement was unlawfully restricted by the Russian Federation,» said human rights defender Kateryna Rashevska.

53 ZMINA. Access mode: *https://zmina.info/news/okupanty-proponuyut-dityam-hersonshhyny-podarunky-v-obmin-na-personalni-dani-pravozahysnyky-kazhut-pro-ryzyk-novyh-deportaczij/?fbclid=IwAR2YG6hIKOOFxHyUFWM0vgEBFGUpoafoyvmeRhsvzf4h-Bl53O_D5u_dlZU*



16,000 deported children have been identified. In 2022, 400 children were sent to Russian families. Significant efforts will be needed to locate these children, find the families they were transferred to, and repatriate them to Ukraine, according to the human rights advocate[54]. She also mentioned Russian «re-education camps,» which are a form of «Russification, militarization, and indoctrination» camps..

Another Ukrainian human rights activist[55], who was in the occupied territories of Donetsk region in 2022, commented on the situation. She noted that despite the ongoing war for many years, it is still difficult for her to comprehend the events taking place in the territory where her childhood unfolded.

«3The alteration of the personal data of Ukrainian children is just one of the countless horrifying tactics that occupiers use to cover up the truth and erase the traces of their crimes. This is not only a violation of children's rights but also an attempt to erase their roots, cultural heritage, and history from their memory. The fates of these children have been thrust into the darkness of uncertainty. They were shuffled from one place to another.

54 Video from the press conference in Ukrainian. Access mode: *https://www.youtube.com/watch?v=-c8uqGihYGk*

55 The individual expressed a desire to provide a comment anonymously.

The persistent efforts of human rights organizations, government agencies, and the international community should be directed towards uncovering the truth, investigating war crimes, and holding the guilty accountable. Voices should resound loudly, demanding justice. May this tragedy serve as an impetus for all nations to understand the importance of protecting children's rights and peaceful coexistence without any form of violence. Let it serve as a reminder that no crimes or injustices can destroy the spiritual strength and determination of the Ukrainian people to fight for justice and freedom.»

SOCIAL NETWORKS AND MOBILE CONNECTION

(Image source: freepik / freepik.com)

Among the threats that are crucial to highlight during wartime is digital surveillance, which can be carried out through the analysis of metadata. Such developments are quite progressive in defense, law enforcement, and intelligence activities. Various sources of information can be used for this purpose, including social networks.

The term «social network» was first proposed by sociologist J. Barnes in 1954, describing it as a system of connections between agents. When interfaces for online communication between people emerged, they began to be seen as a global resource with a wide range of socio-psychological functions. Some social networks have more users than the populations of most countries in the world. There are many platforms where people communicate online, ranging from local platforms specific to a particular region to global ones like Facebook and Instagram. Today, there are many discussions about the consequences of their use. There is an opinion that social networks know more about people than they know about themselves because through predictive algorithms and data processing, they can learn virtually any information based on online behavior analysis.

Microtargeting is used to identify specific types of people in order to subsequently direct them with targeted information to shape their beliefs. Mechanisms already exist to determine which images or messages are liked by certain people or, conversely, trigger negative emotions in them. This means that technology can be used to make one person or large groups of people take certain actions. During wartime, knowledge about people, their interests, needs, geolocation data, movement patterns, and financial transactions take on an entirely different significance than in peacetime.

The problem lies not in the platform itself but in the content posted on it. Social media is a technology that enables the «scalability» of information, which can be expressed through text, images, videos, or audio. Initially, it was assumed that individuals could control this themselves, but later it became clear that there is no final understanding of how to use this tool, its advantages, and risks for both individual persons and states as a whole. Many scientists are trying to understand the real impact of such technologies on human memory and behavior[56]. For example, anthropology is already studying online interactions, focusing on cultural analysis.

56 Boyd D. and Ellison, NB 2007 «Social Network Sites: Definition, History, and Scholarship» Journal of Computer Mediated-Communication, 13 (1) 210–2302.

Often, there is no need to use special means to obtain information because people themselves disclose it. They publish data online not only about themselves but also about others: their whereabouts, texts, photos, and more. They record this information on their mobile devices. In the first months of the full-scale war in Ukraine, social media platforms saw the use of «incitement» technologies, such as messages that encouraged users to share more about themselves and talk about their views on the situation, and so on. These manipulations make people feel compelled to publicly justify themselves by providing the required content and recording it on their mobile devices. What makes it most dangerous is that through these actions online, individuals may unknowingly expose themselves to the risk of physical harm in the real world. Among other things, they may become targets of surveillance and face threats of violence and hate crimes. In the era of the information revolution, military operations that affect data can cause as much harm to civilian populations as the destruction of civil infrastructure. Therefore, online platforms that process large volumes of data from nearly all countries in the world can be used as tools for preparing, inciting, initiating, and conducting armed conflicts. Therefore, a state, especially one experiencing aggression, should have the capability to analyze scenarios of such threats and have legal instruments for their regulation and counteraction. This applies not only to social networks but also to mobile phones, applications, etc.

In the report of the International Committee of the Red Cross following a symposium on digital risks in armed conflicts, an example was given of the consequences of cyberattacks on mobile devices of Syrian refugees[57]. People were subjected to persecution, and some were killed. It was also recognized that «the use of digital technology during armed conflicts for purposes other than as means and methods of warfare» is a unique problem, and it was emphasized that information manipulation through technology and social platforms, which largely contain personal data, can cause significant harm to the population during armed conflicts. Perhaps the international community is not yet ready at an official level to acknowledge and regulate digital weapons as a new means and method of conducting armed conflicts, but there is already cautious discussion of the consequences and the need for (re)interpreting the specific content of the rights to privacy and data protection in light of applicable norms of international humanitarian law. In Ukraine, cases of using mobile phones, applications, and other devices for criminal activities have also been recorded.

57 Faine Greenwood, «Data Colonialism, Surveillance Capitalism and Drones», in Doug Specht (ed.), Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping, University of London Press, London, 2020.

1. COLLECTING PERSONAL DATA OF UKRAINIANS THROUGH SOCIAL MEDIA

In August 2022, information started to surface in the media regarding local Telegram chats in the Chernihiv region that were sharing a link to a bot account, which allegedly offered payment for participating in surveys.

This bot had the username — @money_for_polls_bot[58]. After launching the bot, the aggressor country received chat histories in Telegram, access to contacts, and the locations of individuals[59]. Since local residents share various types of data in local online communities, this allows for obtaining detailed information about what is happening in the region. This includes information about the consequences of war crimes, personal data of people, their moods, and more. Similar messages were recorded in other regions as well.

(Image source: freepik / freepik.com)

In the Volyn region, there was the dissemination of advertising claiming to offer financial assistance allegedly from the organization «Red Cross.» The advertisement directed users to a Telegram channel named «Society of the Red Cross,» which had up to 200 subscribers, although the official account of this organization has many more followers. Users were also concerned that there was no information about such payments on the pages of the mentioned Ukrainian banks. Scammers manipulated the timing of payments, stating that they were processed quickly so that potential victims would not suspect fraud due to haste

58 It has been established that unauthorized sessions are taking place through the MoneyForPolls 1.24.0 application, PC 64bit, version 5.10.0, the device's geolocation is Russia, Moscow, IP-address 109.172.113.59, host 109.172.113.59, name of the internet provider: RU-DATAMAX-M-20091118, Russian Federation.

59 Please note: Russians are collecting personal data of residents of the Chernihiv region through Telegram. Access mode: *https://cheline.com.ua/news/society/zvernit-uvagu-rosiyani-zbirayut-personalni-dani-zhiteliv-chernigivshhini-cherez-telegram-307168?fbclid=IwAR1T0ZF36Y-wTGRIpzucYSxy7UGTlVMhO6wdgNcT4MLgfETBzfngarYuaqM*

and would not have time to think it over. Since entering personal data (bank card number) was required to receive the fake assistance, it can be concluded that the criminals not only spread false information but also engaged in phishing (a type of fraud)[60].

2. GATHERING INFORMATION ABOUT UKRAINIAN PRISONERS OF WAR AND THEIR RELATIVES THROUGH MOBILE «SMS QUESTIONNAIRES»

In January 2023, the Ministry of Defense of Ukraine announced on its Telegram channel that Russian websites were sending SMS messages to the families of Ukrainian service members, offering them to fill out a questionnaire that purportedly would help locate those in captivity within Russian territory or in the Russian-occupied territories of Ukraine[61].

At the time, the Coordination Headquarters for the Treatment of Prisoners of War warned that under the guise of «assistance» to families searching for their missing loved ones, Russian special services were collecting personal data, which could ultimately harm the situation of Ukrainian service members in captivity and hinder their release. They recommended ignoring any unofficial messages, not providing any personal information about relatives to suspicious individuals, websites, or messengers, and reporting cases of illegal collection of personal data to Ukrainian law enforcement agencies. For the safety of Ukrainian military, all inquiries and discussions should be conducted exclusively with the Coordination Headquarters for the Treatment of Prisoners of War, the only specialized state institution responsible for assistance and the release of POWs.

These were not isolated incidents; similar messages were sent on a mass scale. Additionally, through social media and mobile phone messages, individuals are being tricked into providing information under the guise of being family members of Ukrainian service members, including those missing in action.

60 In Volyn, there is a spread of a fake regarding assistance from the «Red Cross.» Access mode: *https://rayon.in.ua/news/567749-na-volini-poshiryuyut-feyk-pro-dopomogu-vid-chervonogo-khresta*

61 The official Telegram channel of the Ministry of Defense of Ukraine.

This way, they collect contact information of military unit commanders, details about their whereabouts, etc. People often respond to the requests from these «relatives and close ones,» attempting to help them and inadvertently providing information to hostile agents.

3. OBTAINING LOANS IN THE NAME OF MISSING PERSONS AND CAPTURED SERVICE MEMBERS

In Ukraine, there have been cases where fraudsters conducted financial schemes using the bank cards of individuals who were missing in action or of Ukrainian prisoners of war. Criminals reissued SIM cards and gained access to the online banking of these individuals. They withdrew funds from the accounts of Ukrainian service members and also opened credit cards, misappropriating loan amounts.

As Olesia Danylchenko, Deputy Director and Head of the Ukrainian Interbank Payment Systems Member Association (EMA) pointed out[62], if a person had been out of contact for an extended period, their phone number would be used to reactivate a SIM card using various schemes. It is crucial to note that this criminal activity also involves the collection of personal information about the individual, including their military service status, captivity, or disappearance, as well as information about their family.

(Image source: freepik / freepik.com)

62 Як в Україні шахраї оформлюють кредити на військових. Режим доступу: *https://www.obozrevatel.com/ukr/ekonomika-glavnaya/fea/yak-v-ukraini-shahrai-oformlyuyut-krediti-na-vijskovih-sut-shemi.htm?fbclid=IwAR0uzz0WH0vhgkO79wNeMQE4aHM8nSTnjdRYfkzKgCasJPH2vvg-JqYMnJ0*

4. FAKE CHATBOTS OF UKRAINIAN GOVERNMENT AGENCIES

In July 2022, the National Resistance Center reported[63] on new elements of hybrid warfare from Russia. This included the creation of fake chatbots impersonating Ukrainian government entities. For example, numerous fake duplicates have been identified for the «eVoroh» chatbot, which is used for reporting the enemy's location. While some are blocked, others continue to emerge. Distinguishing a genuine chatbot from a fake one is almost impossible.

They appear identical at first glance. Enemy chatbots not only disrupt the operation of the legitimate ones but also gather personal data from informants. Therefore, the Center for Strategic Communications, the Ministry of Digital Transformation of Ukraine, the State Special Communications Service, and the Cyberpolice jointly developed a bot checker enabling users to verify chatbots. If it is a fake bot, the bot checker will notify users and provide a link to the authentic one. If the bot is not in the database and the user still has suspicions, they should report it to the Cyberpolice. Thus, over 35,000 people reported suspicious channels and chatbots on Telegram within just one month. Thanks to the vigilance of Ukrainians, this collective effort led to the blocking of more than 300 hostile profiles.

63 Information resistance: How to detect fake chatbots on Telegram. Access mode: *https://sprotyv.mod.gov.ua/informaczijnyj-sprotyv-yak-vyyavlyaty-fejkovi-chat-boty-v-telegram/*

CONCLUSIONS

(Image source: freepik / freepik.com)

The right to respect for one's private and family life is enshrined in the Constitution of Ukraine. Article 32 specifies that the collection, storage, use, and dissemination of confidential information about a person without their consent is not allowed, except in cases determined by law and only in the interests of national security, economic well-being, and human rights. In its decision[64] of January 20, 2012, the Constitutional Court of Ukraine provided an official interpretation of Article 32 of the Constitution of Ukraine, saying that information about an individual's personal and family life (personal data about them) includes any information or a set of information about an individual that can be used to identify them.

There are many different banks of personal data, which can be categorized as closed or open. Closed databases include government databases collected by authorized government authorities, while private databases are formed by various organizations, commercial institutions, banks, etc. In the absence of proper legal regulation and a system of control, this creates a risk of unauthorized use of data for various purposes. While it may not be possible to prevent all threats, they can be significantly minimized.

This document highlights cases where violations of a person's privacy have led to consequences for their life and health. At the same time, there may be other situations where people, due to the breach of personal data protection, lose their property, become victims of cybercrime, discrimination, stigma, persecution, and disinformation. These cases may not be widely known because people attempt to deal with their problems independently (personal lives, sensitive information related to loved ones and children), or they simply may not be aware of violations of their rights and freedoms. Therefore, ensuring the security and privacy of citizens is a key mission of the state aiming to implement innovative digital solutions. It is crucial to start discussing specific steps for reform in this area today by asking: **what needs to be done right now?**

64 The decision of the Constitutional Court of Ukraine in the case of the constitutional submission of the Zhashkiv District Council of the Cherkasy Region regarding the official interpretation of the provisions of Article 32, Part 1, Part 2 of Article 32, Part 2, Part 3 of Article 34 of the Constitution of Ukraine. Access mode: *http://zakon2.rada.gov.ua/laws/show/v002p710-12*

1. LEGAL REGULATION

In January 2011, the Law of Ukraine «On Personal Data Protection» came into effect, regulating legal relations related to protecting and processing personal data. This law was based on the EU Directive from 1995, a time when technology was not as widespread as it is today. Therefore, Ukraine currently lacks legislative standards for regulating data protection in the network, particularly in e-commerce and the digital transformation of public and private services. Uncontrolled data leaks pose reputational risks for the state in terms of its services and overall information security. This means that in order to protect society from 21st-century threats, a comprehensive reform in this area is necessary.

Unaddressed commitments

In September 2017, the Association Agreement between Ukraine and the EU came into effect, with the aim of opening up markets between Ukraine and the European Union and establishing cooperation between them. Article 15 of the Agreement requires Ukraine to harmonize the protection of personal data with European and international standards, modernize its national legislation, ratify a number of international instruments (including the Council of Europe's Convention 108+), and implement recommendations from the OECD, which, as of today, have not yet been addressed.

By signing the Association Agreement, Ukraine committed to adopting a new law on personal data protection and creating a new independent institution to ensure state control in the field of digital rights of Ukrainians. In 2021, certain steps were taken, including the registration of two bills, No. 5628 and No. 6177, which introduced new requirements for data protection and the establishment of a separate supervisory authority. These bills faced criticism[65] from civil society and required further refinement. Subsequently, an updated bill, No. 8153, was registered on October 25, 2022, which, at the time of writing this material, was still under consideration in the Verkhovna Rada of Ukraine[66]. That is, it has been more than a year since these initiatives were introduced, yet there have been no significant changes in the legal regulation of this issue, despite nearly daily reports from Ukrainian law enforcement agencies about

65 Analysis of the draft Law of Ukraine «On Personal Data Protection» No. 5628. Access mode: *https://www.helsinki.org.ua/articles/analiz-proiektu-zakonu-ukrainy-pro-zakhyst-personalnykh-danykh-5628/*

66 Draft law «On Personal Data Protection.» Access mode: *https://itd.rada.gov.ua/billInfo/Bills/Card/40707*

massive data leaks, including from state databases. Adopting a new law on personal data protection complying with international standards is a crucial step toward protecting human rights and national interests in general, as well as our country's becoming a full member of the EU.

2. NATIONAL STRATEGY

Unlike many countries around the world, Ukraine has not adopted a national strategy for the protection of personal data. This means that there is no answer at the state level to questions such as: what are the specific goals and tasks of ensuring the protection of personal data of the population? There is no qualitative and quantitative data on the current situation, threats, plans to overcome challenges, necessary resources, etc. We are not talking about a formal document that will gather dust somewhere but a specific framework with a clear action plan for all database owners, including government authorities and especially during martial law.

Such a document should, at the very least, include the following:

1. A qualitative analysis of the current situation

It is challenging to make informed decisions in the field of personal data protection without understanding the specific nature of the problem. Relying solely on subjective opinions is insufficient. A detailed analysis is needed of how data processing occurs in each individual department or institution. An effective methodology for analysis and an independent evaluation system are required. This will help identify key issues, develop individual mechanisms for solving them, and create appropriate internal documentation such as privacy policies, job instructions, rules, etc.

2. Strengthening the capacity of the state control system

Currently, the Office of the Ombudsman is responsible for oversight in this area according to the law. However, it is widely acknowledged that the Ukrainian Parliament Commissioner for Human Rights lacks the institutional capacity to effectively carry out this function. Ukraine needs to establish a separate independent body responsible for implementing the state's policies regarding digital rights. Since it is unclear when these changes will take place, it is essen-

tial to enhance the authority that currently exists. For instance, a significant portion of public awareness and educational activities among the population can be undertaken by civil society, digital startups, the scientific community, and student organizations. In such a scenario, the Office of the Ombudsman could facilitate cooperation, set priorities, and moderate this interaction.

3. Legal regulation of new technological solutions

Over the past year, Ukraine has taken significant steps towards digital transformation, with many government services being digitized. However, when officials introduce new applications or digital ecosystems, legal professionals often question how they are regulated and how the rights and lawful interests of individuals will be protected in case of violations.

Any technological solution should be implemented with an accompanying set of relevant legislation. Germany provides a good example of shaping its legal system in the world of technology by employing regulatory sandboxes. They progressively address issues in specific sectors rather than attempting to cover everything at once. For instance, when they needed to regulate the use of automated machines, including liability for causing damage, they introduced amendments to the Road Traffic Act. To understand where we «lag behind» in terms of legal regulation, it is necessary to conduct a thorough analysis of technological progress and the associated risks that have arisen as a result.

4. Increasing public trust in state institutions

The process of digitization often faces resistance from society because people do not understand how their personal data will be used. Therefore, in addition to proper legal regulation, the right strategic communication should be established. Honesty is key, not only about the benefits of technology but also the risks. Possibilities for collaborative problem-solving in crisis situations should be created. Overall, people are not opposed to disclosing information about themselves but want to receive proper security guarantees. The results of the massive CES 2020 survey in the United States, China, and France showed that data protection is becoming a new criterion of trust, which will concern people as much as the quality of services provided.

It is also essential not to forget that digital transformation is occurring not only in the social sphere but also in law enforcement. Clearly, the war in Ukraine has driven the development of new technological solutions for exerting control

over the population. In the future, urban surveillance systems, facial recognition programs using artificial intelligence and biometric information, and many other directions related to defense, public, and national security will further develop. All these technologies operate based on data. If the right policies are not formulated, protests may arise in the future. Technologies should continue to evolve but within the framework of addressing all threats and ensuring legal compliance.

5. Educational activities for the population and professional training

One of the most common reasons why the Law on Data Protection is not being enforced is that it is challenging to understand. Ignorance does not exempt one from responsibility, but it must be acknowledged that legislation in this field requires detailed explanation, awareness, and adaptation. In EU countries, significant efforts are made to ensure that the population, government agencies, municipalities, and businesses understand the legal norms regulating data processing, cybersecurity, and electronic communication, know the practical aspects of implementation, and are aware of the risks associated with non-compliance.

Professional training and responsibility, especially within the framework of public administration, are of paramount importance. There is a misconception that the vulnerable point is the technical protection of systems against cyberattacks. However, as demonstrated by examples, including those mentioned in this document, the problem lies not so much in the programs as in people. Lack of control, inaction, and perhaps even indifference to some extent give rise to social engineering. There is no point in expending significant resources on developing a virus program when those who have access to the data can themselves transmit, sell, or disseminate the required information.

Creating a culture of respect for private and family life in society should be a strategic goal of state policy.

Strategy serves as a guide and ambitions for Ukraine on how to secure a safe future. It is about showcasing the country's values in the digital world and «revealing the significance of personal data in government activities and the economy as a whole,» as well as building people's trust in innovative initiatives.

3. PERFORMANCE OF DUTIES BY THOSE RESPONSIBLE FOR DATA PROTECTION

Government authorities, private companies, and other entities independently determine the procedures for processing personal data and security measures. Most violations of the law in this field are related to the fact that all these processes are not organized in accordance with the law or lack internal controls.

For example, they may collect an excessive amount of personal data, process them for purposes incompatible with those for which they were initially collected, lack the necessary documents to regulate data processing procedures, or fail to appoint a responsible person where required by law. In order to ensure an adequate level of data protection, it is necessary to adopt a series of measures that will initially lead to an improvement in the overall situation and, in the long term, contribute to the development of a society where the right to respect for private life is guaranteed.

As mentioned earlier, there is no unified approach to organizing data management because each institution or organization has its own specific activities. However, there are basic requirements and procedures stipulated by law and international standards that must be implemented to protect information. Among the key organizational measures are:

- carrying out a general analysis of activities (separately for each data processor): conducting an audit to determine what personal data the organization collects, processes, and stores; identifying possible risks and weaknesses[67];
- awareness of responsibilities: understanding legal requirements, including the principles of legality, fairness, and transparency in data collection and processing;
- minimization of data processing: ensuring that data processing is limited only to the necessary information to fulfill defined purposes;
- developing internal documentation;
- organizing procedures for the transfer of personal data, including cross-border transfers;
- appointment and professional training of a responsible person;

67 Clarification on how to assess risks and what international standards exist. Access mode: *https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf*

- establishing mechanisms to ensure the rights of data subjects, such as access to data, correction of errors, data deletion, and data portability;
- implementing internal control rules for personal data processing, including monitoring and violation detection.

Every person should have a clear understanding of how their data is processed and protected, including being confident in a proper information security system.

4. PROTECTION OF PERSONAL DATA OF CHILDREN

International and national provisions establish children's right to the inviolability of their personal life. According to the UN Convention on the Rights of the Child and other important documents, no one can unjustifiably and unlawfully violate these rights[68]. A child's personal life encompasses their physical inviolability, personal identity, confidentiality of information, as well as physical and spatial privacy.

The concept of «self-determination» refers to an individual's ability to decide which aspects of their personal life to disclose and to what extent. «Autonomy» means the capacity for self-regulation in thoughts, feelings, and actions[69]. The UN Convention on the Rights of the Child recognizes that parents should ensure the realization of children's rights, taking into account their abilities and best interests[70]. Traditionally, it was believed that adults determined how children should manage their personal lives. However, children's needs in personal life may differ from those of adults and may conflict with them[71]. For instance, the practice of «sharenting» (parents sharing information about their child on social media) may contradict a child's right to inviolability, while parents' right to express opinions conflicts with this right. Adults' determination of children's needs in personal life can limit their autonomy and independence, as well as reduce the inviolability of their private life. At the same time, children are increasingly becoming subjects of technological surveillance by various entities,

68 Committee on the Rights of the Child, General Comment No. 16. (2013), p. 12.

69 Abstract of the German Federal Constitutional Court's judgment of 15 December 1983, 1 BvR 209.

70 Tobin and Field, «Article 16».

71 Submissions from Parental Rights Foundation; Action Canada for Sexual Health and Rights, p. 4; Commission Nationale de l'Informatique et des Libertés (CNIL), p. 11.

such as governments, private companies, and peers[72].

Research has shown that, on one hand, parents are concerned about the privacy and safety of their children in the digital space. On the other hand, many do not control their children's electronic devices or allow them to use digital services without restrictions[73]. Growing up, children demand more respect for their personal lives from parents, schools, and other entities. They view personal space as important for creative self-expression and the development of independent thought. It is important for parental control to be balanced and take into account the child's needs and opinions, including their capacity for independent development.

The current generation of children is the first to be born in the era of digital technologies. Even before birth, a child's identity begins to form through images that parents share online. These images often contain personal information. Currently, about 80% of children in developed Western countries leave a digital footprint before the age of two[74]. CModern children are increasingly engaged in online activities at an early age compared to the past. With each passing year, the number of children communicating online increases. Many children under the age of 13 have profiles on social media (38% of children aged 9 to 12, according to European studies), and most of them have two to five profiles[75]. Пандемія коронавірусної хвороби (COVID-19) посилила цю тенденцію.

Much more often, self-assessment and self-esteem, important for the formation of personality and identity, develop in the digital space under the influence of values and trends dictated there. Children use the internet to continuously document their lives. When a child can turn on a smartphone before learning the alphabet, protecting their personal data becomes a critical issue because, due to their age, they may not yet be able to assess potential risks. Often, children share their personal data on social media, gaming chats, forums, etc.

In the virtual world, personal data has transformed into a digital commodity that can be used in various ways:

72 Jane Bailey and Valerie Steeves, Defamation Law in the Age of the Internet: young people's perspectives (Law Commission of Ontario, Canada, 2017); submission from Ariel Foundation International.

73 Monica Anderson «A majority of teens have experienced some form of cyberbullying», Pew Research Center, 27 September 2018.

74 Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 42.

75 Submission from Information and Data Protection Commissioner, Albania, p. 14.

- for marketing purposes, to create advertisements and sell products or services;
- for spam, password cracking, account hacking, and similar activities;
- for fraudulent schemes or blackmail, where a child's data is used to obtain their parents' financial information;
- for tracking, as knowing a child's usual whereabouts can enable criminals to kidnap or harm them;
- for psychological influence, such as harassment and cyberbullying to manipulate a child into certain actions;
- for psychological influence, such as cyberbullying, [76]to manipulate a child into certain actions;
- for recruiting into various organizations or groups that aim to harm a child's life and well-being, including death groups, streamers, etc.

In the conditions of war, the number of threats to children has significantly increased. Children can be particularly vulnerable in armed conflicts. Criminals can use their data for spreading propaganda, recruitment, kidnapping, political manipulation, and even altering their national identity. Most violations indicate that problems occurred for several reasons:

- owners of personal information databases failed to ensure all necessary procedures for data protection in accordance with national legislation and international standards;
- there is a weak system of digital literacy among the population in place.

Ukraine needs a comprehensive approach to the protection of children's personal data at both the state and local levels. This process should start with a quality risk assessment. In other words, it is necessary to investigate the entire range of potential threats to a child due to the unlawful use of their personal data by government authorities, businesses, private individuals, and even parents. Were the activities of all children's data processing entities systematically analyzed, today we would have answers to questions such as: How did the head of one of the communities in the Kharkiv region

76 Cyberbullying involves threats, insults, and other forms of aggression online. It often includes the posting of intimate photos or personal details on the internet. As a result, a child may experience deep depression, which can lead to irreversible consequences.

transfer all the data of Ukrainian schoolchildren to the occupiers? What was the database protection system and control mechanism there?

In addition to government agencies, local self-government bodies, educational institutions, etc., businesses also process large amounts of personal data. In some cases, this is done covertly, and the obtained data is used, for example, for marketing purposes, while in others, they collect data directly to provide services to children. Among the common services that children may use are:

- educational services (courses, creative workshops, etc.);
- sports services (including the processing of personal data for issuing memberships and video surveillance in facilities);
- social networks;
- online stores, postal services;
- online games, clubs, and interest-based associations, entertainment platforms;
- healthcare or social support services, etc.

Therefore, these are large volumes of data that need to be controlled. If we look at international practice, quite strict requirements for processing children's data are established in EU countries, where the General Data Protection Regulation (GDPR) is in effect[77]. This document defines that children require special protection regarding their personal data, especially when it is used for marketing purposes or creating a personal profile. The EU provides guarantees for children's safety online and requires parental consent when a child is provided with an online service. Therefore, anyone processing a child's data from the EU online has to figure out how to obtain this consent from parents. Otherwise, there are sanctions: fines of up to 4% of the annual turnover (or up to 20 million euros).

For instance, the Irish regulatory authority (DPC) has presented a document titled «Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing»[78]. This is the result of over three years of work, during which the situation in this field and the opinions of many stakeholders, includ-

77 This European Union regulation contains provisions for the protection of personal data, including that of children. It establishes requirements for the collection, processing, and storage of children's personal data, including the requirement to obtain consent from the child's parents or guardian.

78 Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing. Режим доступу: *https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf*

ing children themselves, were analyzed. This document sets out principles for privacy protection and ways to implement them.

In the United States, there is the federal law «Children's Online Privacy Protection Act» (COPPA), which requires the establishment of measures to protect children under the age of 13 online. Any information about a child can only be processed with the consent of their legal representatives. Several states also have local laws that establish liability for cyberbullying and harassment on social media.

The French government plans to require social media platforms to verify the age of users and obtain parental consent for those under the age of 15. If the European Commission approves this document, companies will have two years to implement user verification procedures during registration on their web resources. The law will allow parents to request the suspension of their children's accounts under the age of 15, as well as demand tools from websites to limit the time spent on a particular platform. The document emphasizes that these legislative efforts are only part of a series of other government measures aimed at protecting children from cyberbullying and other crimes[79].

This means that measures for the safety and protection of children's personal data cannot be limited to just one general law. This issue needs separate attention, including at the legislative level. For example, schools play a significant role in children's everyday experience in terms of the privacy of their personal lives. The COVID-19 pandemic, followed by the full-scale war in Ukraine, forced some schools to close and switch to online mode. The transition to online education has exacerbated the existing power imbalance between companies providing access to online services and children, as well as between governments and children and parents, with several governments deviating from current data privacy laws for children. This means that private entities regularly monitor children's digital records. Digitizing and storing data about children's education encompasses characteristics of thinking, learning trajectories, engagement levels, reaction speed, pages read, and videos watched. Most children and parents do not have the ability to challenge the privacy rules of educational technology companies or opt out of providing data, as education is mandatory. When schools choose educational apps and web tools, the main focus is on the curriculum and cost, not on confidentiality. In September

79 France approves law requiring parental consent for minors on social media. Режим доступу: *https://www.france24.com/en/france/20230629-france-approves-law-requiring-parental-consent-for-minors-on-social-media*

2020, an analysis of 496 educational technology apps in 22 countries found that many of them collect device identifiers, and many apps collect location data and share user data with third parties. Data security is a concern. For example, Microsoft reported 5.7 million malware incidents affecting its users from August 24 to September 24, 2020[80]. Schools themselves store a significant amount of information about children and are increasingly monitoring them by observing students' online activities and using surveillance cameras. The use of all technologies requires accountability, informed consent, purpose limitation, data minimization, transparency, and security guarantees. Educational processes should not undermine the exercise of the right to privacy and other rights, regardless of where and how education takes place, and should not exacerbate existing digital inequalities[81].

Educating the population is also of great importance. Often, risks related to children's information can arise due to a lack of knowledge about the law, insufficient awareness of potential issues, and actions needed to prevent negative consequences. If adults are well-informed about their rights, responsibilities, and potential threats, it will be a guarantee that digital literacy becomes a part of a child's upbringing. This can help prevent problems related to digital addiction, psychological disorders due to online bullying, or cybercrimes.

Parents should familiarize themselves with new technologies or programs together with their children, discuss their advantages and risks. They should monitor the content to stay informed about their children's interests and «become friends» on social media to understand the primary audience and how relationships are formed with it (e.g., whether there are negative comments, predominant reactions, subscriptions, etc.). They should explain that photos or other published content remain on the internet forever. What may seem very fun to publish today may not look the same, say, in ten years. It is necessary to explain that exchanging personal or parental data for gifts is unacceptable, as some Russians did in the Kherson and other regions. It is extremely important to jointly define the boundaries of personal privacy and discuss which data publication can have consequences not only for the child but for the entire family.

80 Submission from Human Rights Watch, para. 49.

81 Резолюція 75/166 Генеральної Асамблеї; Submissions from ombudsman of Autonomous City of Buenos Aires; ECLAC; Council of Europe.

The essence of digital rights is that a person should perceive personal data as their property and not be afraid to question third parties about why they are collecting them and what will happen with them next. This should already be taught from a young age. For example, when parents see that someone is taking photos or publishing information about their child without permission, they have the right to object to this. If such situations arise at school or in daycare, it is worth informing educators and teachers about your position in advance. It is also possible to propose that the institution's management develop internal rules for handling children's data, and then familiarize other parents with them.

If a child is already capable of independently sharing information about themselves, it is important to caution them against disclosing personal data to third parties or leaving personal information (such as passwords, residence addresses, banking details, etc.) on various websites. Online behavior is analyzed and can potentially be used, including for criminal purposes. The more people take a categorical stance against any violations of privacy, regardless of whether they are committed by government authorities, businesses, or individuals, the greater the chance that the overall landscape will change.

Respecting the privacy of children is the most crucial means of safeguarding their interests. An approach focused on protecting children's interests requires adults to actively seek the opinions of children and take them seriously. All parties - government, companies, communities, individuals, and parents - must recognize children as bearers of their rights. However, digital literacy alone is not enough without decisive and consistent actions by the government to ensure the protection of children's privacy, data security, and child safety.

NED
NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

Асоціація УМДПЛ UMDPL Association

Freerights ASSOCIATION