Public health or digital liberties?

Citizens' tracking during and after COVID-19: implications for democracy in EaP countries

Report on the situation in Ukraine

Institute of Innovative Governance

INTERNATIONAL RENAISSANCE FOUNDATION

B | S | T The Black Sea Trust for Regional Cooperation

A PROJECT OF THE GERMAN MARSHALL FUND

Maksym Dvorovyi., Dmytro Khutkyy., Anna Melenchuk., Anna Mysyshyn., Khrystyna Kvartsiana. Public health or digital liberties? Citizens' tracking during and after COVID-19. Kyiv: Institute of Innovative Governance. 2021. 56 p.

Authors:

Maksym Dvorovyi,
Lawyer, Digital Security Lab
max.dvorovy@gmail.com

Khrystyna Kvartsiana,
Research and Public Policy Specialist, Institute of Innovative Governance
kvartsyana88@gmail.com

Anna Mysyshyn,
Director, Head of the Project, Institute of Innovative Governance
ann.mysyshyn@gmail.com

Anna Melenchuk,
Co-founder, Institute of Innovative Governance
annychkamelenchuk@gmail.com

Dmytro Khutkyy,
Expert, Institute of Innovative Governance
www.khutkyy.com, khutkyy@gmail.com

Designer: Mark Mironchuk

This publication was prepared by the Institute of Innovative Governance with the support from the Black Sea Trust Fund of the German Marshall Fund of the United States (GMF) and International Renaissance Foundation.

The material reflects the position of the authors and doesn't necessarily coincide with the position of the Black Sea Trust Fund of the German Marshall Fund of the United States (GMF) and International Renaissance Foundation.

www.irf.ua
www.fb.com/irf.ukraine

Public health or digital liberties?

Citizens' tracking during and after COVID-19: implications for democracy in EaP countries

Contents

Report summary

1

Report summary

Over the past year, during the pandemic caused by the SARS-CoV2 coronavirus, countries around the world have implemented innovative digital solutions to protect the health of their populations, including through the provision of online public services. And just as the disease could change our world forever, so could innovative methods for monitoring and tracking citizens. Most of these changes are not temporary, and many – such as restrictions on citizens' freedoms and invasions of privacy – could have negative consequences for democracy and human rights after the pandemic. For Ukraine, a country with relatively weak institutions, attention to digital rights and access to digital services is particularly important.

Systematic digitalization of public services in Ukraine, which began with the launch of the "Action" (Diia, in Ukrainian) Unified Public Services Portal, occurred during the quarantine period, which significantly complicated this process. The pandemic has raised numerous issues of digital inequality. In particular, due to the absence of offline alternatives to some public services, there are restrictions on the rights of the 37 percent of the population who do not have access to the Internet, the 15.1 percent who do not have sufficient digital skills, and the significant number of people who do not have the digital devices needed to fully use public services online.

In addition to anti-virus outreach channels, three major digital public services have been introduced in Ukraine to address the effects of the COVID-19 pandemic and quarantine restrictions: online applications for FOPs (sole proprietors) and employees for one-time financial assistance, online registration for unemployment benefits, and the "At Home" (Vdoma, in Ukrainian) mobile application for tracking compliance with self-isolation requirements.

The digital service for applying for financial assistance for sole proprietors and employees was available via the Diia public services portal from 14-31 December 2020. It attracted almost half a million users: a total of 480,207 relevant applications were submitted by Diia users. At the same time, more potential beneficiaries could have received this e-service – it is estimated that about 800,000 people were eligible for such financial assistance. It was possible to submit an application and receive payments only until 31 December 2020, i.e. only for two weeks. This short period of e-service provision limited the digital rights of potential service recipients to a certain extent. Another limiting factor was the condition that only FOPs and employees of legal entities, or FOPs whose main NACE was among those affected by quarantine measures, could apply. Moreover, not all those who needed help were aware of this opportunity, and among those who were, not all had the digital competencies to submit an application.

From 25 April 2020, an e-service for registration of unemployment and application for benefits became available on the Diia online portal of public services. During the entire existence of this e-service, for which detailed data are available (from April 2020 to January 2021), a total of 39,395[1] applications were submitted through the portal. The government estimates[2] that the quarantine measures to reduce the spread of COVID-19 could have resulted in the loss of 113,000 jobs. Accordingly, hypothetically, such a number of people could have sought unemployment benefits because of the coronavirus pandemic. However, it was not possible to obtain this service offline, which imposed certain restrictions on people who did not have computers, smartphones and / or digital skills.

Overall, the ambition to digitize 100 percent of public services by 2024 presents potential risks for accessibility and cybersecurity. Establishing a narrow time frame to achieve this goal, on the one hand, meets public demand for rapid change. On the other hand, setting such a goal puts the quality of the product at risk, in particular in terms of personal data protection and the prevention of excessive profiling, especially in combination with sensitive data, such as health data. Force majeure caused by the COVID-19 pandemic has only complicated the process.

The Vdoma application, which became mandatory for use in April 2020 for those self-isolating under "red zone" quarantine restrictions, has been used by 720,000 people[3].

1. Olesya Danylenko (employee of the "E-Services" program, "TAPAS" project), interview on February 3, 2021, online.
2. Government portal. The only web portal of the executive authorities of Ukraine. You can now apply for unemployment benefits online on the "Diia" portal. 2020. April 25. URL: https://www.kmu.gov.ua/news/oformiti-dopomogu-po-bezrobittyu-teper-mozhna-onlajn-na-portali-diya
3. Serhiy Shcherbyna (RBC Ukraine), "Mykhailo Fedoriv: If it is necessary to make a" COVID-passport", we will do it quickly" 2020. April 25. URL: https://daily.rbc.ua/eng/show/mihail-fedorov-nuzhno-budet-sdelat-covid-1612282857.html

Report summary

According to users, the first version of the app contained a number of technical problems, including a lack of support for foreign SIM cards and English, which led to it being given a low rating on the Google Play Market and Apple's App Store (1.4 out of 5 possible points[4]). Eventually, the developers added authorization for foreign SIM cards and an English version in app updates, but its rating has not improved.

The obligation to install the application without mandatory alternatives violated the digital rights of citizens in several respects. First, it restricted access to this application to people who do not have a mobile cellular internet connection, as there are no stable WiFi connections to the internet either at border checkpoints or at entry-exit checkpoints on the border with the Autonomous Republic of Crimea. Secondly, it imposed a property requirement on the possibility of using the service, as for the application to work satisfactorily the user must have a relatively modern smartphone, whereas 12 million Ukrainians use old-fashioned mobile phones[5]. Third, the digital rights of citizens who do not have sufficient digital skills to download, install and use Vdoma were infringed. In general, according to a 2019 study by the Ministry of Culture, 53 percent of Ukrainians have digital skills below the basic level[6].

An analysis of the regulations governing the use of the Vdoma application did not reveal significant personal data privacy violations after 22 April 2020, when the application came under regulation by a government decree. At the same time, there are problems with the excessive retention period of the data of persons who were in self-isolation, as well as with the transparency of data processing within the Vdoma information service. Thus, the storage of personal data beyond the end of the legal quarantine regime is deemed not appropriate. Moreover, ministries do not properly disclose details about how quarantine data is exchanged between them.

The difficulty of guaranteeing the protection of personal data in COVID-19 patient tracking applications was one of the reasons why, in a resolution of 17 April 2020, the European Parliament decided that the use of such applications should not be mandatory. According to the resolution, any digital measures against the pandemic must fully comply with data protection and confidentiality legislation, and data retention must be decentralized to avoid potential risks of abuse, or loss of trust.

Another important issue is consent for the processing of personal data. When installing a mobile application, a citizen (or user) first enters into a voluntary civil relationship, i.e. at the level of the relationship between the developer of the mobile application and the user, and voluntarily consents to the processing of their personal data. This is commensurate with Article 11 of the Law of Ukraine "On Personal Data Protection", which stipulates that it is only possible to collect and process personal data of a person if they give their consent. However, how voluntary can the installation of the Vdoma app be, if each person who has recently returned from abroad and who has agreed to mandatory self-isolation on crossing the border must be identifiable to those who have been in contact with patients and who may be potential carriers of the virus, or those who have tested positive for the coronavirus disease but do not require mandatory hospitalization? Also, a person usually does not have the opportunity to qualify their "consent to the processing of personal data", for example by limiting the possibility of transferring data to third parties, or by specifying the time after which the personal data must be deleted.

Referring to international experience, namely the General Data Protection Regulation or GDPR, it should be noted that its provisions are perhaps the strictest rules of confidentiality in the world, and these rules play a role in protecting personal data during a pandemic: After all, the regulation requires the minimizing of data collection, as well as "limiting the purposes" of data collection and use. For example, medical data can be collected only to limit the spread of disease and protect the health of citizens. In addition, the GDPR stipulates that data must be adequately protected against both unauthorized exchange and cyber risks[7].

4. Data as of March 4, 2021
5. Ministry of Digital Transformation of Ukraine, response to a request, February 19, 2021.
6. Ministry of Digital Transformation Survey "Digital Literacy of the Population of Ukraine 2019. URL: https://osvita.diia.gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf
7. Eugenia Poremchuk (Public Activist), interview March 16, 2021, online.

Report summary

In contrast, Ukrainian legislation on personal data protection is rather weak and imperfect – the Ukrainian Data Protection Authority is not independent, and EU citizens arriving in Ukraine are also forced to install the Vdoma application, and thus the Vdoma application is subject to the mandatory requirements of the GDPR.

At the same time, the GDPR is among the most advanced pieces of legislation in the world on personal data protection, and the state of Ukraine, in its Association Agreement with the EU, has declared its desire to bring Ukrainian legislation into line with EU law[8].

Among the basic rights that have been strengthened by the GDPR are the right for information to be deleted at the request of the subject (the right to be forgotten), as well as the right to prohibit processing – the personal data controller is obliged to not to process personal data if its subject requests this. The methods by which the administrator can do this are to prevent third parties from accessing the data, or to remove it from a website or application. Such provisions would be quite appropriate for use by Ukraine as well, and would allow the users of the Vdoma application to send a request that their personal information be deleted, or to refuse to allow its processing.

8. Konstantin Korsun, cybersecurity expert, cyber blogger, co-founder of Berezha Security (BSG), interview May 14, 2021, online.

Key recommendations

2

Key recommendations

According to the results of the study, all stakeholders are advised that:

- To ensure the inclusiveness of digital public services, it is necessary to include in the development of this area of electronic services and public policy not only government institutions, but NGOs, international organizations, and other stakeholders involved in advocacy for accessibility.
- To bridge the digital divide, not only online but also offline learning is needed, especially for older people – for example, with the help of assistants. Digital accessibility for people with visual and hearing disabilities should also be a priority for the legislature and the executive.

With regard to digital services aimed at overcoming the consequences of the COVID-19 pandemic (in particular, applying for unemployment benefits and one-off financial assistance for self-employed persons and employees), the Ministry of Digital Transformation is recommended to:

- Introduce more alternative methods for online identification, and install self-service terminals for offline applications;
- To reimburse not only the main CTEA, but also those CTEAs from which the citizen earned a basic income before the lockdown;
- Provide an opportunity to apply to those who did not have time to do so during the last two weeks of 2020, taking into account the relevant funds in the state budget;
- Create a state call centre for e-services.

From the point of view of implementation and technical solutions, according to the results of research there are grounds to recommend that the relevant public authorities:

- equip all border checkpoints with free and high-quality Internet access so that citizens can install and use the Vdoma application.
- provide affordable alternatives to the Vdoma application to citizens who do not have Internet access in their homes, who do not use smartphones, or who have a low level of digital skills.
- take into account the European Commission Recommendation of 17 April 2020 on data protection in COVID-19 pandemic support programmes when developing alternatives to the Vdoma application, with contact tracing[9] applications being based on short-range technologies such as Bluetooth, and not GPS. Making contact tracing a priority over real-time tracking ensures lower risks to privacy.

9. It's about contact "tracing", not "tracking".

Key recommendations

To improve the regulation of the use of the Vdoma application, the government is recommended to prepare the following amendments to the regulations:

- The Diia state enterprise and the Ministry of Finance should update the privacy policy of the Vdoma application, replacing references to invalid resolutions of the Cabinet of Ministers of Ukraine with more current ones, and produce a proper translation of this policy for foreigners entering the territory of Ukraine.
- The government should initiate the development and amendment of legislation that would ensure the legality of the practice of deleting data immediately after self-isolation ends, and harmonize this practice with the requirements of the legislation.
- Public authorities should also make public the procedures for exchanging data between public authorities regarding the Vdoma information system, and ensure the transparency of such exchanges.
- The Cabinet of Ministers of Ukraine, in compliance with the Law on Electronic Communications, should prepare draft regulations on the further incorporation of the EU Directive on Digital Accessibility into Ukrainian legislation.

Khrystyna Kvartsiana

Introduction

3

Introduction

The COVID-19 pandemic has accelerated the process of digital transformation worldwide, and in Ukraine in particular. Education, work, banking and other areas of life have gone online to minimize the spread of the virus. Moreover, digital technologies have become more widely used by governments to provide public services, develop new tools to control the spread of the virus, and to enforce quarantine restrictions.

Despite the many benefits of digital transformation, there are a number of risks in this process that can affect its end results. Unequal access to the Internet and modern digital devices, as well as a lack of digital skills, remain some of the most common obstacles to inclusive digitization, and this has been dubbed the "digital divide." As a new form of socio-economic inequality, the digital divide is a critical problem for society, because if it is not reduced, a large part of the population is at risk of not being included in the digitalization process.

The most vulnerable social groups should also remain in the focus of digital public service developers. These are most often people with disabilities, people with various visual impairments, the elderly, women, children, and people living below the poverty line. Depending on national and local contexts, this list may vary. Currently in the EU some of the most vulnerable social groups are refugees and asylum seekers, while in Ukraine the vulnerable include internally displaced persons (IDPs). And in a global pandemic, as the UN secretary-general has said, the digital divide becomes a matter of life and death for people who cannot access important health information[10].

In Ukraine, the process of digital transformation began several years ago, but only in 2019 did it become a priority for the government. The automation of public services was part of the election programme of Ukrainian President Volodymyr Zelensky, who supported the creation on 2 September 2019 of a specialized body to achieve this goal – the Ministry of Digital Transformation of Ukraine. In April 2020, in the midst of the COVID-19 pandemic, the ministry's team presented the Diia Unified Public Services Portal, which, according to the developers, should become a "universal access point for citizens and businesses to all electronic public services, under common standards."[11]

Since its launch, numerous services have appeared on the portal, including those related to overcoming the effects of the pandemic. In particular, shortly after the launch of the Diia portal, the government of Ukraine presented a mobile application called Diia.Vdoma to track patients and ensure they follow the rules of self-isolation. Such applications have provoked debate among human rights organizations, as such tracking of citizens is an invasion of privacy. Moreover, due to the lack of transparency and clearly defined rules for the use of personal data by digital services and mobile applications for tracking citizens during quarantine, there is an increased risk that the use of such surveillance technologies may violate human rights. Ukraine, as a country with relatively weak institutions, is particularly at risk of violating the principles of personal data protection.

The purpose of this report is to analyse the extent to which the digital services developed and implemented by the government of Ukraine in response to the effects of the COVID-19 pandemic take into account the digital rights of its citizens.

10. United Nations. Digital Divide 'a Matter of Life and Death' amid COVID-19 Crisis, Secretary-General Warns Virtual Meeting, Stressing Universal Connectivity Key for Health, Development 11 June 2020. URL: https://www.un.org/press/en/2020/sgsm20118.doc.htm
11. Ministry of Digital Transformation. The Ministry of Finance has launched the public services portal "Diia". April 2, 2020. URL: https://thedigital.gov.ua/news/mintsifri-zapustilo-portal-derzhavnikh-poslug-diya

Maksym Dvorovyi

Digital rights and how to understand them

4

Digital rights and how to understand them

In the legal terminology of the 21st century it is quite common to find the use of the terms "information rights" and "digital rights" as a separate category of rights, or a subcategory of information rights. The term "digital rights" is used to denote the rights that people have in connection with the use of the latest information technologies, including the Internet.

Some researchers in the post-Soviet space, prone to excessive theoretical discussions about the nature of human rights, even distinguish digital rights as a separate, fourth generation of human rights[12].

In order to avoid confusion in this study, it is important to outline what we mean by digital rights. The UN Human Rights Council in 2018 stressed that all of the rights that a person has offline should also be protected online[13]. Prior to that, a resolution with a similar thesis was adopted by the Council in 2016[14] and 2015[15]. The same thesis was emphasized by the UN High Commissioner for Human Rights Michel Bachelet[16] in her speech of 17 October 2019.

Regional international organizations, whose mandate includes the protection of human rights, have also expressed similar positions. For instance, the Parliamentary Assembly of the Council of Europe, in Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, emphasized that the obligation of member states of the Council of Europe to ensure that everyone within their jurisdiction enjoys the fundamental freedoms enshrined in the European Convention on Human Rights also extends to the use of the Internet[17].

Such a position of international organizations means that the allocation of digital rights as a separate category of rights in the modern world is in fact inappropriate.

What then are digital rights? The concept of digital rights should be considered not as a separate group of human rights that can be regarded as a separate generation, but as a conditional category denoting human rights that can be implemented in the digital environment, and through the digital environment. Given the huge role that the Internet plays in modern life, distinguishing this category is useful for better systemising and studying human rights in the online environment.[18]

Some guarantees of these rights are currently scattered among recommendations, resolutions and other acts of international institutions. This is reflected, for example, in the case law of the European Court of Human Rights, which in Ahmet Yildirim vs. Turkey emphasized that "Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest".[19]

12. Golovko O. Digital culture and information culture: human rights in the era of digital transformations. Information and law. 2019. No. 4 (31). Pp. 37-44. URL: http://ippi.org.ua/sites/default/files/6_13.pdf.
13. UN Doc. A/HRC/38/L.10/Rev.1, The Promotion, Protection and Enjoyment of Human Rights on the Internet, URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement
14. Human Rights Council, A/HRC/32/L.20, 32/... The promotion, protection and enjoyment of human rights on the Internet, URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement
15. Human Rights Council, A/HRC/28/L.27, 28/... The right to privacy in the digital age, URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/L.27
16. Human rights in the digital age - Can they make a difference?, Keynote speech by Michelle Bachelet, UN High Commissioner for Human Rights, Japan Society, New York, 17 October 2019, URL: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E
17. Recommendation CM / Rec (2014) 6 of the Committee of Ministers of the Council of Europe to Member States on the use of the Handbook on Human Rights for Internet Users? URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f3d
18. Human rights online: Agenda for Ukraine / Vita Volodovska, Maksym Dvorovyi - Kyiv: NGO "Digital Security Laboratory", 2019. - 56 p. URL: https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_UKR.pdf
19. Ahmet Yildirim v Turkey App no 3111/10 (ECtHR, 18 December 2012). URL: http://hudoc.echr.coe.int/eng?i=001-115705

Digital rights and how to understand them

However, the right to freedom of expression is not the only right that it is important to observe in the digital context. As mentioned above, the category of rights to be protected in the digital environment includes the rights guaranteed by the European Convention on Human Rights. These include[20]:

- the right to respect for a person's private life and correspondence (Article 8);
- freedom of thought, conscience and religion (Article 9);
- freedom of assembly and association (Article 11);
- the right to an effective remedy (Article 13);
- prohibition of discrimination (Article 14 and Article 1 of Protocol XII);
- protection of property (Article 1 of Protocol I);
- the right to education (Article 2 of Protocol I).

Several other important rights derived from these Convention rights must also be observed and protected, as the PACE emphasized in the above-mentioned recommendation. These include the right to data protection, the right to access information, and the right of protection against cybercrime[21]. Another element of the right of respect for a person's private life is the so-called "right to be forgotten", which was enshrined in the General Regulation on Personal Data Protection[22] following a decision of the European Court of Justice in a case involving Google Spain[23].

The human rights enshrined in the European Convention on Human Rights are also guaranteed at the level of the Constitution of Ukraine[24]. Other rights that have emerged in the digital environment with the development of information technology include the right to participate in the management of public affairs (including through the submission of electronic petitions)[25] and referendums[26], the right to access electronic justice[27], and active suffrage (the possibility to vote)[28]. The possibility of receiving administrative services in a digital format, the introduction of which became a priority for Ukrainian President Volodymyr Zelensky[29] and the government[30] appointed by the Verkhovna Rada after the 2019 early elections, should be mentioned separately (and importantly in the Ukrainian context).

This prompts the question: How should one deal with the "right to the Internet" or the right to access the Internet? In fact, there is a temptation to see this as a separate right, and to describe other rights that are exercised on the Internet as being derived from the basic right to access the Internet. Indeed, the right to access the Internet is enshrined in law in a number of countries, from Estonia to France and Costa Rica, and the need for it is noted in a number of UN, OSCE and Council of Europe documents[31].

At the same time, let us turn to Article 1 of the European Convention on Human Rights: According to it, states are

20. Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950, URL: https://zakon.rada.gov.ua/laws/show/995_004
21. Recommendation CM / Rec (2014) 6 of the Committee of Ministers of the Council of Europe to member states on the use of the Human Rights Handbook for Internet users? URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f3d.
22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, URL: https://gdpr-info.eu/art-17-gdpr/
23. Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
24. Constitution of Ukraine (Information of the Verkhovna Rada of Ukraine (VVR), 1996, No. 30, p. 141), URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
25. Law of Ukraine "On Amendments to the Law of Ukraine" On Citizens' Appeals"on Electronic Appeals and Electronic Petitions" (Vidomosti Verkhovnoi Rady (VVR), 2015, No. 35, p. 341), URL: https://zakon.rada.gov .ua / laws / show / 577-19
26. Draft Law on Democracy through an All-Ukrainian Referendum, URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69060
27. Electronic court. What is it?, URL: https: //wiki.court.gov.ua/pages/viewpage.action? PageId = 6848551
28. Kateryna Kunitska. Voting online: why there are more risks than benefits in Zelensky's initiative. Internet Freedom, June 11, 2020, URL: https://netfreedom.org.ua/article/golosuvannya-onlajn-chomu-v-iniciativi-zelenskogo-rizikiv-bilshe-nizh-perevag
29. I dream of the state in the smartphone – Vladimir Zelensky. Office of the President of Ukraine, May 23, 2019. URL: https://www.president.gov.ua/news/ya-mriyu-pro-derzhavu-u-smartfoni-volodimir-zelenskij-55585
30. Lilia Rzheutska. "State in a smartphone" in Ukrainian: an ambitious plan with many unknowns. DW, September 27, 2019. URL: https://www.dw.com/uk/darzhava-v-smartfoni-po-ukrainsky-ambitny-plan-z-bagat-nevidomimi/a-50616573
31. Maxym Dvorovy. Will we talk about the right to the Internet in Ukraine? Media Detector, November 15, 2019. URL: https://detector.media/infospace/article/172446/2019-11-15-chy-budemo-my-govoryty-pro-pravo-na-internet-v-ukraini/

Digital rights and how to understand them

to guarantee to everyone under their jurisdiction the rights and freedoms provided for in the Convention[32]. A similar obligation is enshrined in Article 2 of the International Covenant on Civil and Political Rights[33]. These norms impose on states a positive obligation to take action to ensure that the rights described in the relevant documents are indeed observed.

In particular, this positive commitment to the right of access to the Internet is addressed by the Special Rapporteurs on Freedom of Expression in their Joint Declaration on Challenges to Freedom of Expression in the Next Decade[34]. According to them, in the coming years, states and other actors should recognize the right to access and use the Internet as a human right, and an integral condition for exercising the right to freedom of expression. That is, the availability of the Internet and providing access to it is, above all, a precondition for exercising other rights.

In conclusion, in this study we do not exclude the possibility of digital rights being considered as a separate category of human rights that needs special recognition or legal consolidation. However, we will use the term "digital rights" only to describe human rights that can be realized in the digital environment, and through the digital environment. It is in this context that issues related to digital inequality, compliance with digital rights in the context of digital services, and the impact of state-implemented applications such as Vdoma on users' digital rights – in particular their right to respect for private life – will be addressed.

32. Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950, URL: https://zakon.rada.gov.ua/laws/show/995_004
33. International Covenant on Civil and Political Rights, ratified on October 19, 1973, URL: https://zakon.rada.gov.ua/laws/show/995_043
34. OSCE, Joint Declaration on Challenges to Freedom of Expression in the Next Decade, 10 July 2019, URL: https://www.osce.org/files/f/documents/9/c/425282.pdf

Dmytro Khutkyy

Research methodology

5

Research methodology

At the beginning of the project, from 19-31 January 2021, a case study was conducted on all thematic blocks in order to identify and analyse the current scientific and applied publications on digital rights theory, EU best practices in this area, and the implementation of digital rights during the COVID-19 pandemic in Ukraine.

The project was performed using a mix of research methods.

A large, separate part of the study was made up of a legal analysis of the regulations of the European Union and Ukraine that ensure digital rights. Study materials were also used to develop interview guides.

Then, from 25 January to 14 February 2021, lists of respondents were compiled and interview requests were sent. To ensure the qualitative data were balanced, the planned sample of respondents consisted of several groups of specialists: a) civil servants; b) former civil servants; c) public activists, d) specialists in international projects, and e) scientists.

In order to better understand the realities of the implementation of digital rights, interviews were conducted on four topics:

1. the impact of their implementation on digital inequality and the rights of vulnerable groups;
2. the implementation of digital rights in the context of digital services;
3. the tracking of citizens through the Vdoma application; and
4. issues of personal data and the implementation of the GDPR.

In total, 20 semi-structured expert interviews were conducted during the field phase from 28 January to 9 March 2021 (a detailed list of the experts interviewed is provided in the appendix). The texts of the interviews were then subjected to a content analysis.

Quantitative data collected for the study were also analysed using statistical methods. These data were gathered from publicly available online sources, from experts as interview materials, and in the form of responses to requests for access to public information. In particular, the study took into account data such as the structure (gender, age, geographical distribution) and dynamics (changes from March through December 2020) of the number of users of services aimed at overcoming the consequences of COVID-19 in Ukraine. In total, the study sent three requests for access to public information, two of which were answered within five working days, and one within 20 working days.

The conclusions from the data obtained and analysed by all methods – desk research, content analysis of semi-structured expert interviews, statistical analysis of user data, and comparative legal analysis – were synthesized in each thematic section, and in the conclusions.

Anna Melenchuk

The impact of the COVID-19 pandemic on digital inequality and the rights of the most vulnerable groups

6

The impact of the COVID-19 pandemic on digital inequality and the rights of the most vulnerable groups

Digital rights are closely linked to the situation with digital inequalities in Ukraine. Despite the rapid development of IT and technology, there is a significant gap in Ukraine in the use of digital technologies between young people and the older generations, between urban and rural residents, and between men and women.

The COVID-19 pandemic has accelerated the digital transformation in Ukraine and around the world, but it has also widened the digital divide. Digital education, online work from home or the use of digital services require basic digital skills, access to the Internet, as well as the availability for use of a computer or at least a smartphone. Moreover, online services need to be tailored to the needs of people with visual or hearing disabilities. These digital preconditions are fundamental human rights and therefore must be provided and protected by the state, especially in times of crisis like the COVID-19 pandemic.

Do all Ukrainians have access to the Internet and technology?

Digital infrastructure, the ability to connect to the Internet, and the availability of a computer or smartphone are prerequisites for an inclusive digital society in which the digital rights of citizens are properly secured and protected. The right to access the Internet is a fundamental human right through which people can exercise their right to freely express and disseminate their opinions. Moreover, the use of the Internet and cyberspace stimulates the development of society as a whole. Each state should be responsible for making the Internet available to all of their citizens. In Ukraine, the right to access the Internet is not enshrined in law – the Law of Ukraine "On Telecommunications" refers only to universal access to a connection to public fixed communication networks, local telephone communications, calls to emergency services and helpline services, and communication by payphones – many of which no longer work at all[35].

On 16 December 2020, taking into account proposals from the President of Ukraine, the Verkhovna Rada of Ukraine adopted the Draft Law of Ukraine "On Electronic Communications", which foresees the provision of affordable fixed broadband Internet access as a universal communication service[36]. The requirements for the quality of this service should guarantee consumers have access to a wide range of services: from social networks and messengers, to Internet banking and video communications. The service will be regulated by the central executive body in the field of electronic communications and radio frequency resources. The right to such a service will be enshrined in Ukrainian legislation from 1 January 2022. The law stipulates a subsidy mechanism to provide access to the Internet, and establishes the obligation of the state to provide universal services in any areas where they are absent or cannot be provided on a commercial basis. The government also presented a draft National Strategy for the Development of Broadband Internet Access in 2020, which was publicly discussed in 2020 and is awaiting approval[37]. However, there are no government programmes in Ukraine to ensure low-income families have access to computers, which is the basis for ensuring the digital rights of citizens[38].

There are 26 million Internet users in Ukraine, both mobile and wired[39]. Some 64 percent of Ukrainians use the Internet once a month or more often, with the highest level of Internet use among people under the age of 45. In large cities, 74 percent of citizens regularly use the Internet, while in rural areas this falls to only 54 percent – and this refers only to those areas in which there is access to the Internet. Some 37

35. The Law of Ukraine on Telecommunications.URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text
36. The Law of Ukraine on Electronic Communications: https://zakon.rada.gov.ua/laws/show/1089-IX
37. Ministry of Digital Transformation of Ukraine. Draft National Strategy for the Development of Broadband Internet Access: https://drive.google.com/file/d/1X9xlLCIpTaXwcOjRdK9l5Mw2cAIZryuQ/view
38. Oleksandr Fedienko (People's Deputy, Verkhovna Rada of Ukraine), interview on 9 March 2021, online. http://www.ukrstat.gov.ua/operativ/operativ2019/zv/az/az_u/az0119_u.htm.
39. Ukrainian Statistics. Number of internet users. URL: http://www.ukrstat.gov.ua/operativ/operativ2019/zv/az/az_u/az0119_u.htm

The impact of the COVID-19 pandemic on digital inequality and the rights of the most vulnerable groups

percent of Ukrainians have never used the Internet – these are mostly older people[40]. Many remote communities and villages have no fixed connections to the Internet, as ISPs do not consider such connections economically justified. In addition, Internet communications in areas close to conflict zones and in temporarily occupied territories in eastern Ukraine are often interrupted and restricted.

The COVID-19 pandemic has sparked discussion about possible ways to cross digital barriers. The implementation of the Decree of the President of Ukraine "On some measures to improve access to mobile Internet", which was adopted in the spring of 2020, has removed some obstacles to the development of new communication technologies and reduced the digital divide between cities and rural areas. Since July 2020, mobile operators have been able to connect about 4.7 million people in remote areas and villages to 4G mobile broadband services. It is expected that by 2023, some 95 percent of Ukrainian territory will be covered by 4G mobile Internet, which is the most efficient and fastest way to provide high-speed Internet across the country. Moreover, in 2021, the Ministry of Digital Transformation of Ukraine plans to provide another 5,000 villages with a combined population of 2.5 million people with high-speed Internet connections. Wired internet will be provided to social infrastructure facilities: schools, local administrative service centres (CNAPs), libraries, village councils, hospitals and FAPs. It is planned to connect 95 percent of social facilities in two to three years.

In declaring these ambitious goals, the government must make sure that there is competition among internet providers, which will ensure prices for Internet services in remote areas and villages are affordable[41]. Unfortunately, due to the pandemic, not all ISPs have been able to maintain their previous levels of profitability. During the quarantine, although the level of demand for the Internet has increased, the level of paid services has also increased, as a result of which a large number of subscribers or even whole districts have been disconnected from the Internet[42].

Are government efforts to boost digital skills effective?

COVID-19 and the abrupt transition to online life have forced Ukraine to prioritize the development of digital skills. According to a poll supported by the Ministry of Digital Transformation, 15.1 percent of Ukrainians do not have digital skills, and 37.9 percent have a low level of digital skills[43]. It is chiefly the elderly population that has a low level of digital skills, or that lacks them altogether.

To help address this issue, in 2020 the Ministry of Digital Transformation of Ukraine launched a national online platform on basic digital skills[44]. The online platform offers digital skills training in an edutainment format, which includes talk shows, movies, and webinars with famous stars and influencers. However, according to experts[45], launching an online platform is not enough. In order for the public to find out about it, and most importantly, in order for there to be public demand for such a platform, an information campaign should be conducted outside the digital space – namely, information about the platform and instructions about how to use it should be disseminated at offline events, via advertising on television, and through other means. The online courses also need to be complemented with offline training sessions and workshops, as people who lack basic digital skills may naturally find it difficult to access online educational series and courses by themselves[46]. To achieve this, the Ministry of Digital Transformation recently announced the creation of offline digital education hubs based at CNAPs, libraries, schools and IT companies. According to official data, as of March 2021, this network of hubs includes more than 6,000 organizations[47]. However, there is no information about

40. Ukrainska Pravda, Internet Usage in Ukraine. URL: https://www.epravda.com.ua/news/2019/10/11/652498/
41. Anastasia Popova (Independent Expert on Digital Inequality), interview March 5, 2021, online.
42. Media Business Reports. Fixed Internet in Ukraine. URL: https://mbr.com.ua/uk/news/analytics/2367-shpd-internet-cerez-volz-misce-ukrayini-u-evropi
43. Ukrainskyi Kurier. Digital Literacy is indispensable.URL: https://ukurier.gov.ua/uk/articles/cifrova-gramotnist-neodminna-vimoga-sogodennya/
44. Ministry of Digital Transformation of Ukraine. Digital Education. URL: https://thedigital.gov.ua/projects/osvita
45. Anastasia Popova (Independent Expert on Digital Inequality), interview March 5, 2021, online.
46. Ibid
47. Ministry of Digital Transformation of Ukraine. Digital Education. URL: https://thedigital.gov.ua/projects/osvita

The impact of the COVID-19 pandemic on digital inequality and the rights of the most vulnerable groups

how many Ukrainians have used the services of these hubs, and there has been no feedback on their activities.

In addition to the government initiatives in Ukraine, digital skills projects are being implemented by NGOs and volunteers. One such case is the Odesa IT-Grandma project, which runs digital literacy courses in libraries[48]. The experience of IT-Grandma shows that local initiatives that are supported by concerned citizens and volunteers are the most effective. Communities and so-called interest centres are built around such initiatives. People with low levels of digital skills share their experiences and help each other gain new digital knowledge.

However, according to experts[49], in the absence of specific incentives to increase the public's motivation to acquire digital skills, no courses, whether online or offline, will be effective. An example of an incentive could be access to e-services, such as free access to various government documents or certificates online. Another important factor that helps people acquire digital skills is mentoring and sharing experiences within the family[50]. Thus, knowledge sharing and support for the younger generation, which usually has better digital skills, could significantly speed up the process of older people acquiring digital skills[51].

Digital accessibility is still not a governmental priority

Most digital platforms and digital services in Ukraine are not adapted to the needs of people with visual or auditory disabilities. In Ukraine, In Ukraine, 300,000 people have visual impairments, of whom 40,000 are blind.[52] As the number of people with visual impairments is very large, the adaptation of digital platforms and services should be an urgent priority. An analysis of the largest digital platforms and services in Ukraine has shown that 95 percent of such services are inaccessible to people with visual and hearing impairments. On average, on each digital platform and digital service that was surveyed for this report using an online accessibility web checker developed by the Institute for Innovative Governance, there were 24 errors found, 80 warnings given, and 70 recommendations made for colour contrast, font size, alt- description of pictures, etc[53].

Thus, problems with digital accessibility remain some of the main obstacles to overcoming digital inequality. The reason for this is the low awareness of this issue and a lack of effective laws and regulations[54]. To be accessible, web platforms must meet the accessibility criteria of the international WCAG consortium. The latest WCAG criteria (WCAG 2.1) contain recommendations on the structure of web pages, and the use of colours, images, audio and video. Moreover web platforms that meet WCAG criteria improve the general user experience, and not just that of users with disabilities[55].

Ukraine has now taken the first steps towards digital accessibility by adopting a regulation on a unified design for the government's web services in 2019 and establishing a Public Council on Web Accessibility in the Ministry of Digital Transformation. However, the regulations lack a clear implementation strategy, and the council has no executive powers.

The implementation of the EU Web Accessibility Directive and the European Accessibility Law could be the key to ensuring that digital accessibility legislation is effective. The Directive and the Law provide a set of rules on digital accessibility to be followed by Member States. Although not all EU Member States have transposed the Directive into national law, it is generally observed. The Directive could be implemented in the national legislation of Ukraine as part of efforts to align national legislation with EU standards. However, the Web Accessibility Directive has not been identified as a priority among all the regulations and directives that still need to be transposed into national law in accordance with Ukraine's Association Agreement with the EU.

48. IT Grandma Project. URL: http://itbabushka.com.ua/
49. Oleksandr Fedienko (People's Deputy, Verkhovna Rada of Ukraine), interview on March 9, 2021, online.
50. Ibid
51. Dzvinka Chepelis (expert, Lviv City Council), interview on March 6, 2021, online
52. Ibid
53. Institute of Innovative Governance. Inclusive Checker. URL: https://inclusivechecker.org/
54. Dmytro Popov (independent digital accessibility expert), interview February 28, 2021, online.
55. Dmytro Popov (independent digital accessibility expert), interview February 28, 2021, online.

The impact of the COVID-19 pandemic on digital inequality and the rights of the most vulnerable groups

Still, a number of the Directive's provisions were transposed into the legislation of Ukraine with the adoption of the Law of Ukraine "On Electronic Communications", which will come into force in 2022. The law sets out the selection of electronic communication services for persons with disabilities and the provision of equal access to them as priorities of state policy in this area. Similarly, the draft Broadband Internet Access Development Strategy in Ukraine proposes to implement measures to make the Internet accessible to people with disabilities. Regarding affordability, the Ministry of Finance considers that a cost for Internet services at the level of 5-6 percent of the monthly pension to be excessive, and it is formulating plans to introduce state aid to provide access to the Internet to vulnerable groups of the population, which will total approximately UAH 240 million (about U.S. $6.4 million) per year. According to the draft Action Plan for the implementation of the strategy, by the end of 2023 it is planned to provide people with disabilities with devices to access the Internet, by the end of 2021 to provide access to the public authorities' websites, and by the end of 2022 to develop software to simplify the provision of access to the Internet for this category of the population[56].

In addition to legislation, the government and society need to be aware of this issue. In Ukraine, a number of civil society organizations promote digital accessibility and support the national and local authorities in adapting public platforms to the needs of people with disabilities. While the role of civil society is important and should be supported through various tools, the government must also be committed to making public web platforms accessible to vulnerable groups.

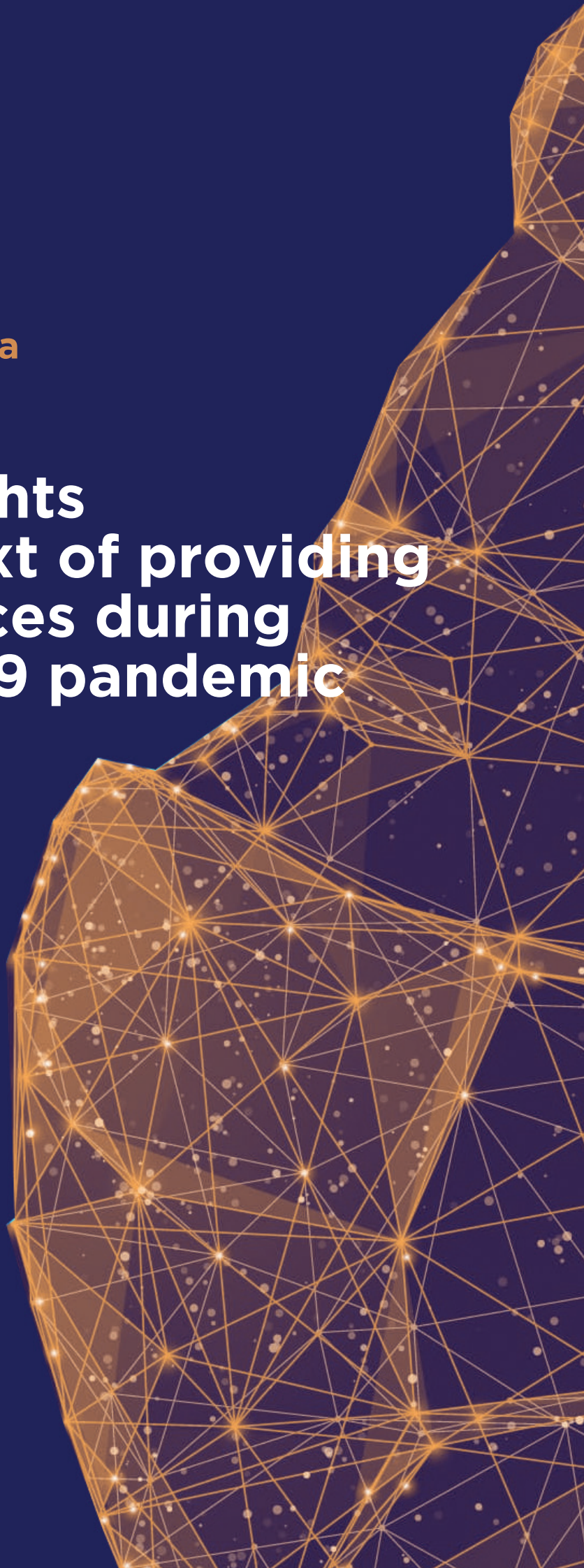
To overcome digital inequalities and ensure the basic digital rights of citizens, especially during the period of the COVID-19 pandemic, access to the Internet, basic digital services, personal computers, and mobile phones must be accessible to everyone – including the most vulnerable. Recognition of this should be reflected in the legislation, and in its implementation. Moreover, these services must be accessible to people with disabilities.

56. Ministry of Digital Transformation of Ukraine. Draft Action Plan for the implementation of the National Strategy for the Development of Broadband Internet Access. URL: https://drive.google.com/file/d/1S9JEEHBnTtY7aSwcS0y1b9OOdDrQPSQy/view.

Dmytro Khutkyy,
Khrystyna Kvartsiana

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

7



Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

In April 2020, with the COVID-19 pandemic already taking hold, the Diia unified public services portal and its mobile application were launched in Ukraine. As of 5 March 2020, nine digital documents could be obtained via the mobile application, including Ukrainian domestic and foreign passports, taxpayer certificates, and birth certificates. Meanwhile, on the Diia portal it was already possible to obtain about 50 public services in a range of areas[57].

According to the UNDP[58] DIA Support Project Manager, there are a total of approximately 1,200 public services in Ukraine, all of which the Ministry of Digital Transformation plans to make available online by 2024[59].

The digitalization of public[60] services expands the digital rights of citizens, as it de facto provides them with an alternative way to receive certain public services – online. In parallel with the development of digital public services in Ukraine, the Ministry of Finance is developing Internet infrastructure to ensure that 95 percent of Ukraine's territory has high-speed mobile and broadband Internet coverage by 2024. According to the ministry[61], achieving this goal will significantly expand the digital rights of citizens, as on the one hand it will provide universal access to the Internet, and on the other it will provide access to public services to citizens living outside large cities, where access to CNAPs is often problematic.

At the same time, the digitalization of public services is a complex process, which, among other things, involves establishing cooperation between ministries and state registers, developing new algorithms for providing services, making changes to legislation, and ensuring there is effective communication with citizens. It should be noted that currently in Ukraine the Ministry of Digital Transformation and the Diia[62] State Enterprise are developing digital tools for the implementation of digital public services. However, having developed and launched a certain service online, the Ministry of Digital Transformation is not seen as the provider of this service, ministry officials note[63]. Rather, the ministry is a "gateway" between the citizen and the relevant body providing the service[64]. However, to establish data exchange between registers, as well as for the collection and processing of user applications, the Ministry of Digital Transformation of Ukraine and the Diia digital platform collect and transmit to various registers the personal data of users, which, depending on the service, can include their name, gender, date of birth, taxpayer identification number, telephone number, e-mail address, address of residence, passport data, etc. At the same time, as the team of the ministry notes, "Diia does not store the personal data of users, but only displays information from the registers, and only at the request of an identified citizen.[65]"

The protection of users' personal data is a priority in the development of any digital platform or e-service, the ministry says[66]. UNDP's[67] DIA Support Project Manager explains that Ukraine has undergone a significant paradigm shift in understanding the value of personal data over the past few years: "The development of personal data protection and cyber protection is very positive, in my opinion,

57. Ministry of Digital Transformation of Ukraine. According to the rating of the Slovo i Dilo portal, Mykhailo Fedorov fulfilled the most promises for the year of the Government's work on March 5, 2021. URL: https://thedigital.gov.ua/news/za-reytingom-portalu-slovo-i-dilo-mikhaylo-fedorov-vikonav-naybilshe- obitsyanok-za-rik-roboti-uryadu
58. Volodymyr Brusilovsky (Action Support Project Manager, UNDP), interview January 28, 2021, online.
59. Ministry of Digital Transformation. Goals by 2024. URL: https://thedigital.gov.ua/ministry
60. Public and public services are used interchangeably in this report.
61. Mstislav Banik (Project Manager, Ministry of Finance), interview on February 12, 2021, online.
62. Government portal. Development of electronic services. URL: https://www.kmu.gov.ua/diyalnist/reformi/efektivne-vryaduvannya/rozvitok- elektronnih-poslug
63. Mstislav Banik (Project Manager, Ministry of Finance), interview on February 12, 2021, online.
64. Mstislav Banik (Project Manager, Ministry of Finance), interview February 12, 2021, online
65. Ministry of Digital Transformation of Ukraine. Mobile Application Security Action. May 20, 2020. URL: https://thedigital.gov.ua/ news / bezpeka-mobilnogo-zastosunku-diya
66. Oleksandra Kovalenko (head of the expert group, Ministry of Finance), interview on February 4, 2021, online.
67. Volodymyr Brusilovsky (Action Support Project Manager, UNDP), interview January 28, 2021, online.

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

and a departure from the formal approach of 'We have computerized information protection systems, and so everything is fine' to a practical approach, with external experts being involved, and there is a partnership with commercial companies." In practice, according to the ministry[68], to ensure compliance with legislation in this area the ministry has an expert group on personal data protection, which appoints a responsible person to assess each digital service for personal data processing and its compliance with the law. According to the head of the DIA project, "the logic of working with user data in the ministry has been worked out in detail with the (parliament's human rights) ombudsman[69]." Moreover, according to the results of an inspection of the Ministry of Digital Transformation and the Diia state enterprise regarding their compliance with legislation in the field of personal data protection, which was carried out by the Verkhovna Rada Commissioner for Human Rights (ombudsman) in June 2020, no violations of the law were identified.

Public activists[70] believe that with low public confidence in government institutions and no oversight of cybersecurity by independent auditors, citizens cannot trust that their data is fully protected: "The default approach in digital security is that there is no reason to trust until proven otherwise, and our experience as Ukrainians reinforces this statement, due to repeated data leaks." With the onset of the pandemic, digital rights have deteriorated significantly, as quarantine restrictions have forced most people with low digital skills, who previously preferred offline services, to start using their digital counterparts. Fraudsters have also become more active during the crisis, and the risks of cybercrime have increased, the expert said[71].

The security of personal data depends not only on rules set out in laws and regulations. It must be ensured thoroughly and constantly, and not only at the moment of a "leakage" of information[72] that leads to negative consequences. Ignoring potential risks until the worst happens is a poor strategy.

In the broad context, the ability to obtain any new online administrative and public services strengthens the digital rights of citizens. However, this report examines only those e-services that aim to reduce and overcome the effects of the COVID-19 pandemic.

E-service: registering as unemployed, and registration for unemployment benefits (from 25 April 2020)

On 25 April 2020, the Ministry of Economic Development, Trade and Agriculture, the Ministry of Digital Transformation, together with the State Employment Service and with the support of the TAPAS[73] project, launched an electronic service for the registration of unemployment and applying for benefits on the Diia[74] online public services portal. This service effectively combines two services: obtaining the status of an unemployed person, and applying for unemployment benefits.

TAPAS, in an effort to make as many services as possible accessible, developed draft regulations that provide for several methods of identification (qualified electronic signature (QES), or the more common Bank ID), which could allow another 30,000-100,000 people to use this e-service, but the State Social Insurance Fund decided to use only QES[75]. Indeed, an advertisement on a government website indicates the possibility of identification using Bank ID or Mobile ID[76]. In general, according to the government, as of 24 April 2020 the number of unemployed registered with the state employment service was 426,400 people, which was 113,000 more than on the same date in 2019[77].

68. Oleksandra Kovalenko (head of the expert group, Ministry of Finance), interview on February 4, 2021, online.
69. Mstislav Banik (Project Manager, Diya State Enterprise), interview on February 12, 2021, online.
70. Pavlo Belousov (Digital Security Expert, Internews-Ukraine), interview February 5, 2021, online.
71. Pavlo Belousov (Digital Security Expert, Internews-Ukraine NGO), interview February 5, 2021, online.
72. Taras Budynkevych (data security expert), interview on February 15, 2021, online.
73. USAID / UK AID Project "Transparency and Accountability in Public Administration and Services / TAPAS".
74. Government portal. The only web portal of the executive authorities of Ukraine. You can now apply for unemployment benefits online on the "Action" portal. 2020. April 25. URL: https://www.kmu.gov.ua/news/oformiti-dopomogu-po-bezrobittyu-teper-mozhna-onlajn-na-portali-diya.
75. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
76. Government portal. The only web portal of the executive authorities of Ukraine. You can now apply for unemployment benefits online on the "Action" portal. 2020. April 25. URL: https://www.kmu.gov.ua/news/oformiti-dopomogu-po-bezrobittyu-teper-mozhna-onlajn-na-portali-diya.
77. Government portal. The only web portal of the executive authorities of Ukraine. You can now apply for unemployment benefits online on the "Action" portal. 2020. April 25. URL: https://www.kmu.gov.ua/news/oformiti-dopomogu-po-bezrobittyu-teper-mozhna-onlajn-na-portali-diya.

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

It is estimated that the quarantine measures imposed to reduce the spread of COVID-19 could result in the loss of 113,000 jobs. Accordingly, a similar number of people could, hypothetically, have sought unemployment benefits due to the coronavirus pandemic.

At the same time, according to the TAPAS[78] project, over the entire duration of the provision of the e-service for which detailed data are available (from April 2020 to January 2021) through the Diia portal a total of 39,395 applications were submitted: 22,419 (56.9 percent) from women, and 16,976 (43.1 percent) from men. Given the age structure of the working population, it is natural that most applications (15,716) were submitted in the age group 26-35 years, and the least (1,788) – in the group 56 years and older (see more details in Figure 1). At the same time, the minimum number of applications (873) was in August, and the maximum (9,214) in November 2020 (see more details in Figure 2).

Diagram 1.

Age distribution of the number of applications for unemployment benefits

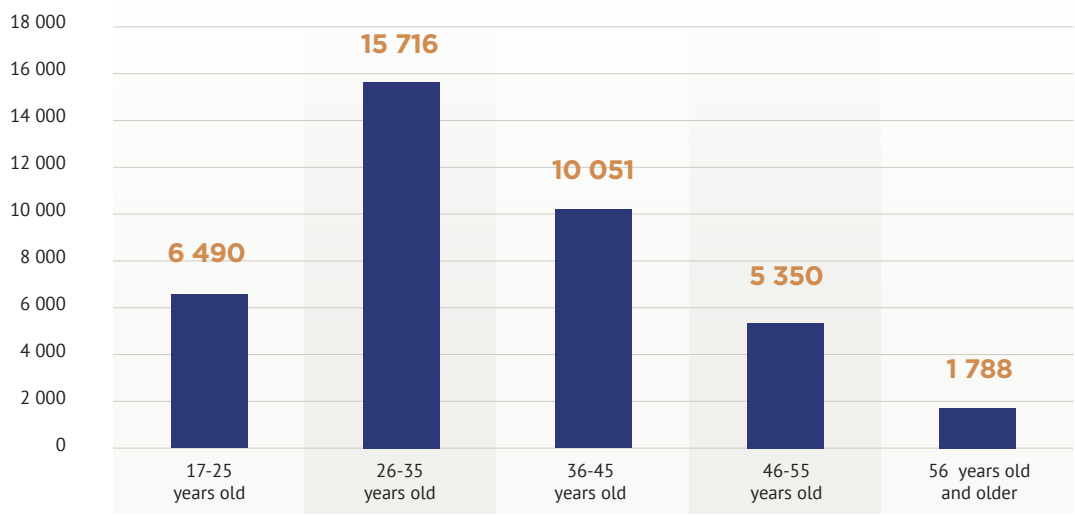
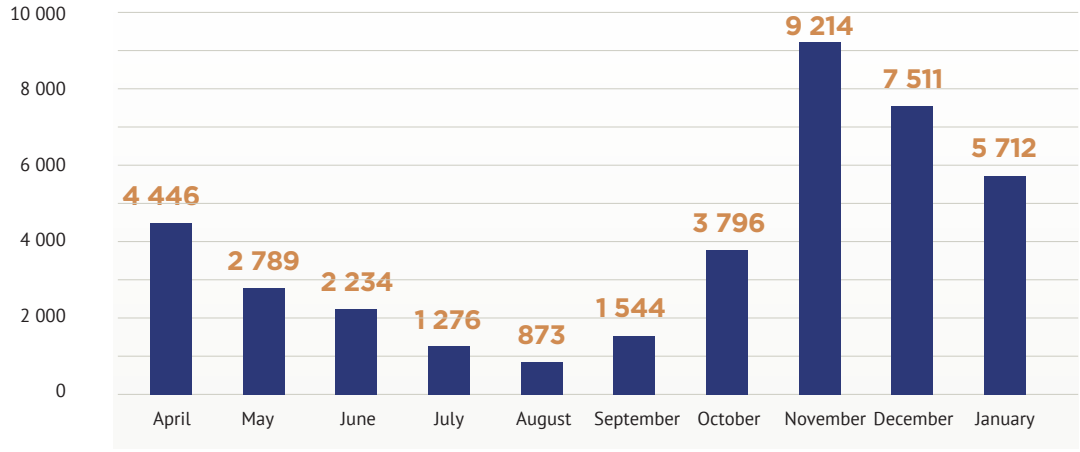


Diagram 2.

Time dynamics of the number of applications submitted for unemployment benefits.



78. Olesya Danylenko (E-Services employee, TAPAS project), interview on February 3, 2021, online.

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

During the peak of the pandemic, the offices of the State Social Insurance Fund were closed and the representatives of the fund worked from home, due to which it was not possible to receive the service offline, which imposed certain restrictions on people without computers, smartphones and / or digital skills[79]. Under normal circumstances, such services should be provided in Centres for Administrative Services (CASs). Moreover, although for users of such services in CASs it appears to be a paper process, in fact, the internal business processes of registration of the service are fully digitized. Even during lockdown there may be self-service terminals available in CASs where a person could use the e-service[80].

E-service: submission of an application for financial assistance to sole proprietors and employees (14-31 December 2020)

14 December 2020. The Ministry of Finance announces the launch of the "most anticipated service of the year" – the submission of applications for financial assistance for sole proprietors and employees[81].

It was possible to make an application and receive payments only until 31 December 2020, i.e., only for two weeks. This was a very short period of e-service provision, which to some extent limited the digital rights of potential service recipients. Another limiting factor was the condition that only those FOPs and employees of legal entities or FOPs whose main Classification of Types of Economic Activity (CTEA) were affected by quarantine measures could apply. However, in the days of the pandemic, the main income could come from non-core CTEA and, accordingly, during the quarantine, sole proprietors and employees with such income also received less income. At first glance, the selection according to the main CTEA looked like a simple and clear criterion. However, it violated the digital rights of sole proprietors and employees whose activities under non-core CTEAs were banned during quarantine, and who were not allowed to apply for financial assistance. That is, it would have been possible to uphold the digital rights of more sole proprietors and employees by developing more flexible criteria. For example, it would have been possible to take into account the amount of pre-quarantine income received from those activities that were now curtailed by quarantine measures). A quantitative criterion of the right to use the service was applied –the amount of the average salary of an employee should be equal to or less than 30 thousand hryvnias per month. This criterion, which narrowed the circle of persons who were granted the right to use the e-service, was also not properly substantiated.

A number of special technological solutions were implemented for this e-service. First, the developers understood that the portal could not withstand a heavy load, and therefore deliberately required identification either by a qualified electronic signature (QES) or by Bank ID[82]. Because of this, in theory, not all persons who had the right to apply for financial assistance could do so, because not all had such means of electronic identification. Their rights to receive this service were effectively limited. And although in practice it is possible to issue, for example, a Bank ID relatively easily and quickly through online banking, in principle this was a narrowing of rights. Still, it should be noted that the availability of two alternative methods of identification (QES or Bank ID) is better than just one, and this expands the range of potential users, and thus their digital rights. Second, the process of obtaining the service itself was explained and organized quite simply. It was noted that the service could be used as a benchmark – it is very convenient for users and can be obtained in two minutes[83]. Third, Diia automatically checked the applicants' data in the Register of Insured Persons of the Pension Fund of Ukraine for compliance with the conditions for receiving benefits. Fourth, the statutory identification procedure did not require a person to sign – from a technical point of view, Diia itself placed a digital stamp on the application[84]. Fifth, the information about users was coded[85]: the Pension Fund

79. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
80. Oleksiy Zelivyansky (coordinator of the E-Services component, EGAP program), interview on January 28, 2021, online.
81. Diia. One-time financial assistance to self-employed persons and employees. 2020. February 14, 2021. URL: https://diia.gov.ua/news/ odnorazova-materialna-dopomoga-fop-ta-manjim-pracivnikam
82. Danilo Molchanov (Deputy Director, TAPAS Project), interview February 3, 2021, online.
83. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
84. Diia.One-time financial assistance to self-employed persons and employees. 2020. February 14, 2021. URL: https://diia.gov.ua/news/ odnorazova-materialna-dopomoga-fop-ta-manjim-pracivnikam.
85. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

of Ukraine transmitted "0" and "1", which meant nothing to an outsider, but the values of these codes were agreed between e-service administrators in advance, which also allowed data processing to be speeded up[86].

Even with these time and legal constraints, almost half a million people used this e-service. According to the TAPAS[87] project, in the last two weeks of 2020, Diia users submitted a total of 480,207 applications: 394,458 applications (82.14 percent of the total) through the mobile application and 85,749 applications (17.86 percent of the total) through the Diia web portal.

In this case, this e-service could potentially get more beneficiaries. According to a TAPAS project representative, about 800,000 people[88] were eligible for this type of material assistance. And although the Ministry of Education issued public explanations and sent push messages via the Diia platform, some people refused to apply for aid, "because they were afraid that the state would come to them and conduct an audit[89]." Moreover, not all those who needed help were aware of this possibility, and among those who did, not all had the digital competencies to apply for the aid[90]. As the representative of the TAPAS[91] project explained, if all those eligible for this service had gone to the local social security offices, they would create queues, get infected and get sick with COVID-19 – so it was decided to provide this service exclusively online[92]. This created a dilemma: either to provide the service both online and offline, and thus provide the right to receive financial assistance to as many people as possible, but increasing the risk of wider coronavirus infection, or provide this service only online and thus limit the rights of some people, while reducing risks of infection. The choice was not easy, and the choice was made in favour of protecting public health. In addition, the public authorities, which know the CTEA and bank account numbers of entrepreneurs, could carry out this service completely automatically. However, from another point of view, everyone should have the right to refuse help – even for their own subjective reasons. In this regard, the requirements for applying for financial assistance observed digital rights.

Citizens who for some reason failed to use the service applied to the Ministry of Finance during and after the period for the submission of applications for one-time assistance. The head of the DIA project explained that most of these appeals came from citizens whose data in the registers was incorrect, and those who wanted to appeal against the list of CTEA codes approved by the Cabinet of Ministers under which one-time financial assistance would be allocated[93]. Among other obstacles that prevented the use of the service were that a person ceased to be employed and there were delays in the filing of tax returns by companies whose employees wanted to use the service. For example, according to one civil servant[94], one of the companies submitted reports on the payment of its Unified Social Payments for employees only on 24 December, a few days before the end of the acceptance of applications on the portal and by the Diia application. As tax reporting was a fundamental criterion for initial selection, the employees of this organization could not use the service when it first became available. Moreover, according to the civil servant[95], a significant proportion of citizens did not fill in the application form's IBAN field. To solve this problem, the developers worked on this issue with fifty banks so that each could provide instructions on how users could find out their IBAN number at their bank. Finally, a separate explanation link was added to the service itself.

In addition, the provision of material assistance to self-employed persons and employees raises a number of issues. Some 400,000 material assistance payments were transferred to applicants in 2020, while the remaining

86. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
87. Olesya Danylenko (E-Services Program Officer, TAPAS Project), interview February 3, 2021, online
88. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
89. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
90. Oleksiy Zelivyansky (E-Services Coordinator, EGAP Program), interview on January 28, 2021, online.
91. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
92. Oleksiy Zelivyansky (E-Services Coordinator, EGAP Program), interview on January 28, 2021, online.
93. Mstislav Banik (Project Manager, Ministry of Finance), interview on February 12, 2021, online.
94. Mstislav Banik (Project Manager, Ministry of Finance), interview on February 12, 2021, online.
95. Mstislav Banik (Project Manager, Ministry of Finance), interview February 12, 2021, online.

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

80,207 received them in 2021[96]. Why, if it was planned for everyone to receive transfers by 31 December 2020, were some applicants paid the following year? By what criteria were transfers made to one person earlier, and to others later? Given that the provision of the same online service occurred at different times for different people, the question of whether there was a violation of digital rights arises. There is also the question of the discrepancy between the number of applications submitted and the number of persons to whom the funds were transferred – there were 3,000 fewer applications made than remittances sent[97]. If the register of persons for payments is simply a regular file with the list of beneficiaries and their details, then it could quite easily be changed by a person with access, who could add a recipient who did not apply at all or remove from the file eligible recipients[98]. So, on what grounds were these public funds transferred? Who formed the final register of persons who were to receive payments? Who will provide explanations to the representatives of the State Audit Office of Ukraine (SASU)? Who is responsible? All of these questions remain open.

Public policy challenges with digital rights and e-services during the COVID-19 pandemic

During the COVID-19 epidemic, how can it be assessed whether digital rights to receive e-services have been observed, or whether they have been restricted? In the best case the full provision of rights, both ordinary and digital, is when services can be received both electronically / online, and on paper / offline. Logically then, the non-provision or withdrawal by the state of the opportunity to receive either online or offline services can be considered a restriction of rights. If, in exceptional circumstances, a lockdown or quarantine is introduced and public services are only available online, then it must be possible for all categories of citizens to use them. That is, it should be possible for everyone to use the appropriate devices (personal computers, mobile phones, terminals, etc.) with software (web platforms, mobile applications, etc.), with training or instruction provided so users can develop the relevant digital competencies. Obviously, such opportunities were not provided for all citizens of Ukraine affected by the lockdown and who needed the appropriate public services. Thus, the rights of some citizens were not protected.

According to one public sector expert, if you were an entrepreneur and wanted to receive financial assistance, you had to buy a new smartphone, install a mobile application and submit an application to Diia, thus the principle of equality in receiving services was violated on the basis of property criteria, which is a violation of the Ukrainian constitution[99]. This thesis was also expressed by the former head of the Diia State Enterprise: people who have neither a computer nor a phone were not able to apply in paper form – and this is a narrowing of rights due to property; that is, all those living outside the digital field were denied their right to assistance[100]. According to the public activist, digital rights to e-services related to overcoming the COVID-19 epidemic are being violated unintentionally, as few people are aware of them. However, ignorance of violations does not mean no one is responsible for them.[101]

At the same time, the state, international partners and public organizations did seek and find compromise solutions – mainly in the form of developing, launching and promoting exclusively electronic services. Of course, in the case of the force majeure caused by the coronavirus pandemic, decisions were made quickly, and e-services developed in a short time, so it is natural that there are some shortcomings. However, as the previous analysis shows, in retrospect some of these shortcomings could have been avoided, and in the long run improved e-services could be introduced.

In general, the rapid digitization of public services produces potential risks to the accessibility and security of citizens' information. Establishing a narrow time frame to achieve an ambitious goal, on the one hand, meets the public demand for rapid change and, if successful, will significantly increase the political capital of the team of the ministry

96. Oleksiy Zelivyansky (E-Services Component Coordinator, EGAP Program), interview January 28, 2021, online.
97. Oleksiy Zelivyansky (E-Services Coordinator, EGAP Program), interview on January 28, 2021, online.
98. Olena Chepurenko (ex-manager, Diya State Enterprise), interview on January 28, 2021, online.
99. Yevhen Poremchuk (Chairman of the Board, NGO "Electronic Republic"), interview on February 4, 2021, Kyiv.
100. Olena Chepurenko (ex-manager, Diya State Enterprise), interview on January 28, 2021, online.
101. Volodymyr Nts (Director, e-Democracy NGO), interview January 28, 2021, online.

and President of Ukraine Volodymyr Zelensky. On the other hand, setting a very short timeframe to achieve goals puts the quality of the product at risk. The force majeure caused by the COVID-19 pandemic only complicates this process.

A freelance consultant to the Verkhovna Rada's Digital Transformation Committee[102] drew attention to the potential risks to personal data security associated with the use of real data in the testing phase of many digital public services. According to the expert, institutional procedures and safeguards for the secure processing of personal data are created only within a year of a certain service being transferred to commercial operation. It is difficult to determine whether this has already happened with digital services from the Diia Unified State Portal, as, firstly, there are bureaucratic barriers to the transfer to the state balance of services developed using funds from donors, and secondly, no relevant decisions have been taken. According to the expert[103], new information about the security of data will probably be available once the State Audit Office completes its audit of the Diia state enterprise for compliance with state policy and the use of budget funds. The audit is being carried out at the request of the parliament's Committee on Digital Transformation.

Prospects for the development of public policy on digital rights related to e-services

IThere are a number of ways to improve the provision of e-services with regard to overcoming the effects of the coronavirus pandemic. In particular, it makes sense to give the opportunity to those self-employed persons and employees who did not have time to apply for financial assistance in the last two weeks of 2020 to apply now. It is also worth reimbursing them not only for their main CTEA, but also for those CTEAs that brought them income before the lockdown. In addition, it is possible to introduce further alternative online identification methods and install more self-service terminals. In addition, when people need help, they currently only have access to chatbots, which is not effective enough; in fact, people are happier when real people communicate with them – so it would be worthwhile to create a call centre for e-services[104]. It would also make sense, as was done with ProZorro[105], to place all the regulations and the open source code for the e-services (along with its entire history of edits) in a repository, such as GitHub[106].

It is also potentially possible to introduce e-services based on best world practices. For example, Apple and Google give states free access to their APIs to develop software that uses Bluetooth technology to help trace the contacts of citizens, so as to identify people infected with COVID-19 and others they have come into contact with[107]. In this way, if a person tests positive for COVID-19, then this data is only stored locally on their device (and therefore their privacy is preserved), and a person can still notify those with whom they came in contact that they are going into self-isolation[108]. Due to the fact that this development is cross-platform, devices with different operating systems can exchange data with each other – and it would be quite possible and logical to add this functionality for tracing contacts and sending push messages to the Diia mobile application[109].

In addition, the Ukrainian authorities are discussing the possibility of introducing vaccination passports, but this will largely depend on the decisions of the WHO and the European Commission[110]. Moreover, following the example of other countries, when people are planning visits to various institutions, they should have access to information through Google Maps, indicating places where people who have tested positive for COVID-19 have been; you can even show the level of congestion in stores (in the same way traffic jams are now displayed) so that people can choose where it is safest to shop[111]. It is also possible to provided

102. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.
103. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.
104. Olena Chepurenko (ex-manager, Diya State Enterprise), interview on January 28, 2021, online.
105. GitHub. Where the world builds software. 2021. URL: https://github.com/.
106. Volodymyr Flonz (Director, e-Democracy NGO), interview January 28, 2021, online.
107. Apple, Google. Privacy-Preserving Contact Tracing. 2021. URL: https://covid19.apple.com/contacttracing.
108. Oleksiy Zelivyansky (E-Services Coordinator, EGAP Program), interview on January 28, 2021, online.
109. Oleksiy Zelivyansky (E-Services Coordinator, EGAP Program), interview on January 28, 2021, online.
110. Danilo Molchanov (Deputy Head, TAPAS Project), interview February 3, 2021, online.
111. Olena Chepurenko (ex-manager, Diya State Enterprise), interview on January 28, 2021, online.

Realization of digital rights in the context of providing digital services during the COVID-19 pandemic

information for other daily activities: for instance, there is a lack of information about the rules of admission to clinics and hospitals that people might need to visit, and what services are available there, and at what time; the same applies to educational institutions and other socially important public institutions[112]. Such e-services would help reduce the risk of COVID-19 infection.

A fundamentally different approach is the competitive model of service delivery. In this model, the state does not create an artificial monopoly on public services but is only one of several market players competing for users with the quality of its e-services. For example, as the civic activist[113] argues, Diia could have an open API that allows individuals and organizations in the public and business sectors to develop and deliver similar e-services, but with a user-friendly interface (e.g., it could be similar to model of operation of the "Taxer" service[114]). Moreover, some experts believe that the Ministry of Finance, the only state body that is a policy maker in the field of e-services, should not code e-services (but instead license database administrators and service providers, as is the case with banking services) and develop public policies (for example, introduce a standard that all public services should be open source (for instance, under a Creative Commons license[115]), and set standards for data protection and storage)[116]. According to the expert, this would not be a "state in a smartphone", but a "smartphone without a state" – there will still be controls, but not controls over citizens, rather controls over standards[117]. Indeed, this approach diversifies risks, creates competition, provides better quality and prices, and reinforces the digital rights of e-service users.

According to UNDP's[118] DIA Support Project Manager, five years is theoretically the shortest possible time in which 1,200 services could be digitalised (achievable by 2026, rather than the government's target of 2024), while the rapid digitalisation of services could potentially pose risks to cybersecurity. Moreover, with there being a focus on rapid results in the development of digital public services, some vulnerable groups may be overlooked – especially the elderly, people with disabilities, the visually impaired, and in some situations internally displaced persons. For example, the lack of offline alternatives to the digital service for applying for one-time financial assistance limited the rights of those who do not use a computer or smartphone for various reasons. "These people need to be included in this process, but perhaps in the pursuit of the result they may be forgotten, or be perceived as a secondary factor," said the expert[119].

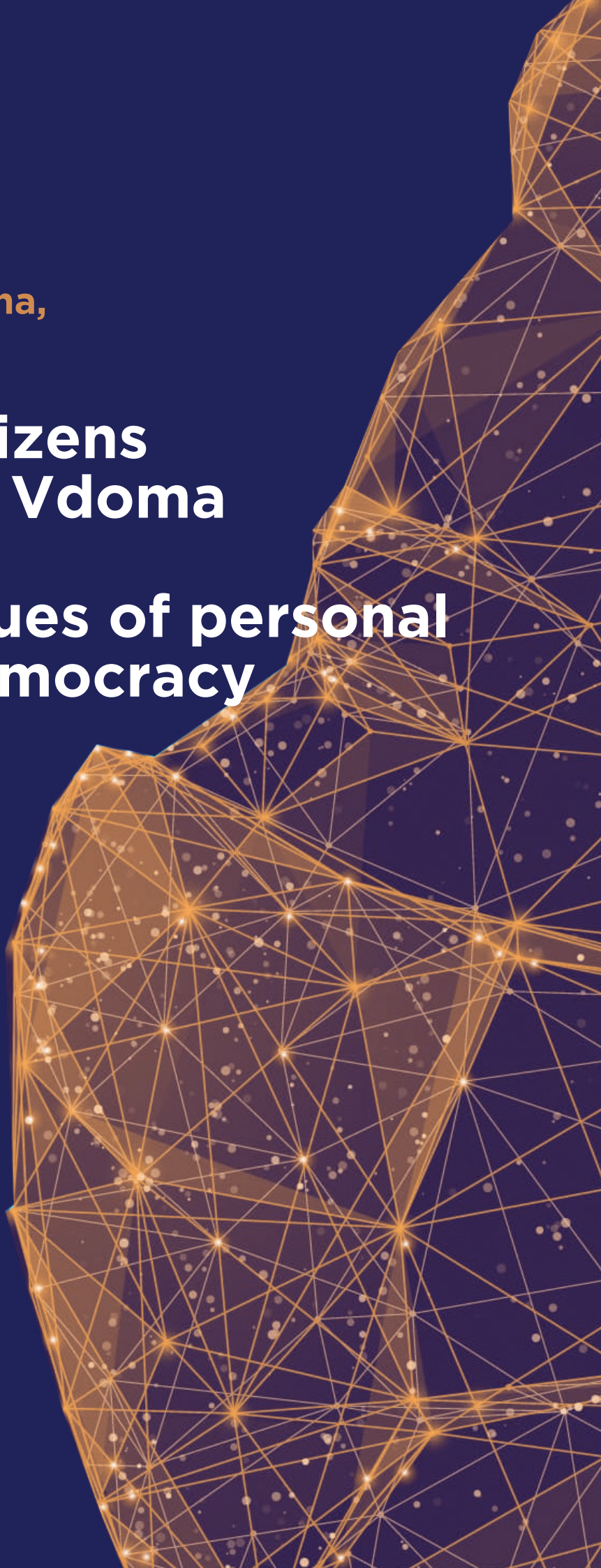
The main way to monitor the observance of digital rights of citizens in the implementation of digital services is for the public sector and society as a whole to pay attention to these issues. To ensure the inclusiveness of digital public services, it is necessary to include in the development of electronic services and public policy in this area not only government agencies, but also NGOs, international organizations, and other stakeholders who advocate for these accessibility issues.

112. Olena Chepurenko (ex-manager, Diya State Enterprise), interview on January 28, 2021, online.
113. Yevhen Poremchuk (Chairman of the Board, NGO "Electronic Republic"), interview on February 4, 2021, Kyiv.
114. Private e-service for informing about the tax legislation of Ukraine, for submitting electronic reports, paying taxes, and checking the debt of private individuals online: https://taxer.ua/uk/.
115. Creative Common. About the licenses. 2021. URL: https://creativecommons.org/licenses/.
116. Volodymyr Flonz (Director, e-Democracy NGO), interview January 28, 2021, online.
117. Volodymyr Flonz (Director, e-Democracy NGO), interview January 28, 2021, online.
118. Volodymyr Brusilovsky (Action Support Project Manager, UNDP), interview January 28, 2021, online
119. Volodymyr Brusilovsky (Action Support Project Manager, UNDP), interview January 28, 2021, online.

Khrystyna Kvartsiana,
Maksym Dvorovyi

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

8



Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

At the beginning of 2020, the world was gripped by a pandemic of a previously unknown disease, which has impacted everyone's normal way of life for more than a year now. The disease, caused by a coronavirus and known as COVID-19, has become a challenge for health systems and forced government to introduce several preventive measures including social distancing and lockdowns. The nature of the transmission of the virus became clear only at the end of March 2020[120], when the disease was already widely spread around the world.

At that time, states and technology giants began to think about how advances in information technology could be used to prevent infection, or at least to inform people that they had been in contact with infected people. The most common digital tools that formed the basis for the development of such solutions involve contact tracing and exposure notification[121]. Contact tracing apps allow people to register their location and share it with the health authorities, who in turn can more accurately identify outbreaks, while exposure notification programs only notify the user if he / she was near a person who later tested positive for COVID-19. This is achieved through the exchange of information with other smartphones via Bluetooth.

One of the best-known examples of contact tracing technology is the Singapore-based TraceTogether[122] application, which helps identify an infected person nearby using Bluetooth on a user's smartphone and permission to locate. Although the vast majority of Singaporeans use the application digitally, for those who do not own a mobile phone or do not want to install the application on it, there is an offline alternative device available to all residents for free - Token. Like the application, the Token device captures only proximity data using Bluetooth technology, does not collect geolocation data, and has no cellular connection.

As of January 2021, 78 percent of Singapore's population used Tracetogether[123], while in the EU similar applications have not had as much success. Despite 67.5 percent to 85.5[124] percent of French people being identified as potential users of France's TousAntiCovid application, it has been downloaded by only about 5 million citizens on the Google Play Market[125]. There are similar figures for the Italian application Immuni[126]. It is worth noting that the use of applications for tracking patients in the EU is not mandatory for citizens and residents. Thus, in a resolution of 17 April 2020, the European Parliament decided that any digital measures against the pandemic must fully comply with data protection and confidentiality legislation, and the use of applications should not be mandatory. In particular, data retention should be decentralized to avoid potential risks of abuse, or loss of trust. The resolution also states that decisions to implement any digital measures against a pandemic should include cessation provisions to prevent their use after the end of the pandemic.

In the European Commission Recommendations of 17 April 2020 on data protection in programmes supporting the COVID-19 pandemic, the European Commission declared contact tracing[127] applications based on short-range technologies such as Bluetooth rather than GPS to be the most promising in terms of health. The priority of contact tracing

120. WHO. WHO Transmission of SARS-CoV-2: implications for infection prevention precautions: Scientific Brief. 9 липня 2020 року. URL: https://www.who.int/news-room/commentaries/detail/transmission-of-sars-cov-2-implications-for-infection-prevention- precautions#:~:text=Current%20evidence%20suggests%20that%20transmission,%2C%20talks%20or%20sings.

121. Volodymyr Brusilovsky (Action Support Project Manager, UNDP), interview January 28, 2021, online.

122. Singapore Government Agency Website. TraceTogether, safer together. URL: https://www.tracetogether.gov.sg.

123. Tham Yuen-C. More than 4.2 m people using TraceTogether, token distribution to resume soon: Lawrence Wong. The Straits Times. URL: https://www.straitstimes.com/singapore/politics/parliament-more-than-42m-people-using-tracetogether-token-distribution-to- resume.

124. University of Oxford. Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. 16 квітня 2020 року. URL: https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

125. TousAntiCovid. Google Play Store. URL: https://play.google.com/store/apps/details?id=fr.gouv.android.stopcovid&hl=en&gl=US.

126. Immuni. Immuni Official Website. URL: https://www.immuni.italia.it.

127. This is contact tracing, not tracking.

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

over real-time tracking is due to there being lower risks to privacy[128].

In general, according to the European Commission, every EU country except Bulgaria, Luxembourg, and Sweden has already developed, or is in the process of developing, an application to trace the contacts of patients with COVID-19[129]. However, only some of these applications are compatible with their counterparts in other European countries – meaning that they can exchange information when the user travels within the EU.

Another area in which states have tried to use technology has been to monitor compliance with quarantine conditions. Attempts by the Ukrainian authorities to use digital tools resulted in the creation of the Diia Vdoma application, the name of which was later shortened to Vdoma. It was launched on 7 April 7 2020 – and it immediately became a subject of controversy in civil society and the human rights community in Ukraine[130].

What is Vdoma?

Vdoma is an application designed to monitor compliance with the rules for self-isolation. Monitoring is performed by checking the compliance of a photo of a person's face with a reference photo taken during the installation of the mobile application, and the geolocation of the mobile phone at the time the photograph is taken[131]. This is how its operation was described by the Ministry of Digital Transformation in April 2020, and how it is described in the current regulations.[132]

After installing the mobile application, the person can receive a message (push-message) at any time of the day. If you receive a message, the person must take a photo of their face within 15 minutes using the mobile application. In the case of a mismatch between the geolocation or photo, the inability to communicate with a person through the mobile application, the application's deletion, or the placing of restrictions on the transmission of information via a mobile application, the National Police will be notified of a violation of the obligation to self-isolate. The sending of such a notification is the basis for further monitoring by the National Police and the National Guard of a person's obligation to self-isolate.

According to information provided by the Ministry of Digital Transformation of Ukraine, the Vdoma application was developed by a team from the ministry, in cooperation with the Ministry of Health, the Ministry of Internal Affairs and the Public Health Centre of the Ministry of Health[134]. According to a resolution of the Cabinet of Ministers of 2 April 2020, the Ministry of Digital Information was to develop an electronic service by 5 April 2020 to monitor compliance with self-isolation and / or medical observation. According to Mikhail Fedoriv, the application was created in four days, and then constantly updated . The lack of time to develop and properly test the application and the rapid commissioning due to critical infection rates have affected the effectiveness of the Vdoma application. Since April 2020 the application has been updated at least once on the App Store and Google Play Market platforms. As of today, according to the Minister of Digital Transformation Mikhail Fedoriv, the application has been downloaded by 720,000 people[135] (of which more than 500,000 downloads were made from Google Play Market[136]).

128. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN
129. Official Journal of the European Union. COMMUNICATION FROM THE COMMISSION. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection. April 17, 2020. URL: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel- during-coronavirus-pandemic / mobile-contact-tracing-apps-eu-member-states_en.
130. BBC News Ukraine. Action at home: an application that will monitor Ukrainians in self-isolation. April 8, 2020. URL: https://www.bbc.com/ ukrainian / features-52217877.
131. Cabinet of Ministers of Ukraine. Observe at home. April 27, 2020. URL: https://www.kmu.gov.ua/news/projdi-observaciyu-vdoma.
132. VRU. Legislation of Ukraine. Resolution of the Cabinet of Ministers of Ukraine No. 1236 of December 9, 2020 "On Quarantine and Restrictive Anti-Epidemic Measures to Prevent the Spread of Acute Respiratory Disease COVID-19 Caused by SARS-CoV-2 Coronavirus in Ukraine". April 10, 2021. URL: https://zakon.rada.gov.ua/laws/show/1236-2020-%D0%BF/
133. Pulse. Results 2020: "Short deadlines and a lot of work, it was an extraordinary test for our team," - Mstislav Banik. January 2021. URL: pidsumki-2020-stisli-termini-ta-velike-navantazhennya-tse-buv-nadzvichajnij-test-dlya-nashoyi-komandi-mstislav-banik
134. Sergey Shcherbina. "Mikhail Fedorov: If you need to make a" COVID-passport "- we will do it quickly." RBC-Ukraine. February 3, 2021. URL: https://daily.rbc.ua/eng/show/mihail-fedorov-nuzhno-budet-sdelat-covid-1612282857.html
135. Sergey Shcherbina. "Mikhail Fedorov: If you need to make a" COVID-passport "- we will do it quickly." RBC-Ukraine. February 3, 2021. URL: https://daily.rbc.ua/eng/show/mihail-fedorov-nuzhno-budet-sdelat-covid-1612282857.html
136. Vdoma. Google Play. Data as of March 4, 2021. URL: https://play.google.com/store/apps/details?id=en.gov.diia.quarantine&hl=en

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

The functionality of the application, according to its description on Google Play Market, has not changed significantly, and includes registration at the place of medical observation or self-isolation, photo confirmation that a person remains at the place of medical observation or self-isolation, as well as the ability to make an emergency call to the Ministry of Health hotline. The application requires a number of permissions to use, including permission to obtain an approximate and accurate location of the user using GPS and cellular base stations, and to access the phone camera to take photos and videos[137]. In general, this means that when using the application, information belonging to the category of sensitive personal data as defined under Article 7 of the Law of Ukraine "On Personal Data Protection" – namely biometric data – will be obtained from the user.[138]

The installation of the application was initially voluntary, despite its initial description on Google Play Market as being mandatory[139]. At the same time, in fact for some categories of people (such as those returning from abroad or coming to Ukraine from a red list country) the installation of such an application has effectively been mandatory, as the only other option was a 14-day period of quarantine in hospital. Since 22 July 2020, the obligation to install the app has been enshrined in law.[140]

At the same time, it must be remembered that the mobile application is only one element of the Vdoma service, the infrastructure of which is integrated within the Diia unified state web portal of electronic services. This element of infrastructure allows self-isolation to be monitored with limited data transfer paths – and in this study we will focus on the functionality of the application and its impact on human rights, almost without touching on the processing of personal data by the Vdoma service in general.

Vdoma availability

With citizens being obliged to use the Vdoma application upon arrival in Ukraine from a number of countries, the question of the availability of the application became acute. According to Mikhail Fedoriv, "today it is one of the best applications in the world in terms of convenience[141]." Since its launch, the application has been available for free download in the App Store and Google Play Market, provided you have an Internet connection. For many travellers, this was the first obstacle, because WiFi connections, for example, at Boryspil airport, are not stable[142], and without successfully installing and registering to use the application they could not cross the border. Problems with installing the application due to the lack of a high-quality Internet connection also hindered citizens crossing entry-exit checkpoints (CPVR) on the border with the Autonomous Republic of Crimea, according to the co-coordinator of the public organization CrimeaSOS Olga Kuryshko[143]. In addition, the activist stressed there were problems with access to rapid testing for coronavirus infection on the administrative border with Crimea[144].

Pavlo Belousov, a digital security expert, noted that in practice the application did not work on devices with versions of the Android operating system that are more than 6-7 years old[145]. Therefore, to be able to use the application, the user had to own a relatively modern smartphone,

137. Vdoma. Google Play. Data as of March 4, 2021. URL: https://play.google.com/store/apps/details?id=en.gov.diia.quarantine&hl=en

138. Law of Ukraine "On Personal Data Protection" (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2010, No. 34, p. 481). URL: https://zakon.rada.gov. ua / laws / show / 2297-17.

139. Does the use of "Action at Home" threaten digital rights? Digital Security Laboratory. April 8, 2020. URL: https://dslua.org/ publications / chy-zahrozhuie-vykorystannia-diy-vdoma-tsyfrovym-pravam /.

140. Resolution of the Cabinet of Ministers of Ukraine No. 641 of July 22, 2020 "On the establishment of quarantine and implementation of enhanced anti-epidemic measures in the area with a significant spread of acute respiratory disease COVID-19 caused by coronavirus SARS-CoV-2". URL: https://zakon.rada.gov.ua/laws/show/641-2020-%D0%BF/ed20200722.

141. Sergey Shcherbina. "Mikhail Fedorov: If you need to make a" COVID-passport "- we will do it quickly." RBC-Ukraine. February 3, 2021. URL: https://daily.rbc.ua/eng/show/mihail-fedorov-nuzhno-budet-sdelat-covid-1612282857.html

142. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

143. UKRINFORM. CrimeaSOS declares failures in the application "Act at home" on the occupied peninsula. April 15, 2021. URL: https: // www. ukrinform.ua/rubric-crimea/3198631-u-krimsos-zaavlaut-pro-problemi-z-dodatkom-dij-vdoma-na-okupovanomu-pivostrovi.html.

144. UKRINFORM. CrimeaSOS declares failures in the application "Act at home" on the occupied peninsula. April 15, 2021. URL: https: // www. ukrinform.ua/rubric-crimea/3198631-u-krimsos-zaavlaut-pro-problemi-z-dodatkom-dij-vdoma-na-okupovanomu-pivostrovi.html.

145. Pavlo Belousov (Digital Security Expert, Internews-Ukraine NGO), interview February 5, 2021, online.

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

which directly violates the rights of 10-15 percent of people who travel abroad and do not own smartphones, according to the Ministry of Infrastructure[146]. Moreover, such technical requirements for installing the application potentially limit the rights of 12 million Ukrainians who use old-fashioned mobile phones (not smartphones)[147].

Lilia Oleksyuk, a freelance adviser to the Verkhovna Rada's Committee on Digital Transformations, also noted the property barrier: "COVID-19 has raised another question: do people have (advanced) enough (devices) to get digital services? And what about those who can't put Vdoma on their phone, because it's not a smartphone, but a simple phone? The developers did not even think that such a situation could also occur. Although GPS tracking works on both types of devices, this option hasn't been considered at all[148]." In this context, the civic activist[149] noted that a customer-centric approach to developing such an application should take into account the needs of all categories of users, and include other, more affordable digital tools that also support geo-location and photo-confirmation, such as chatbots.

Comments from users who have used Vdoma indicate that earlier versions of the application are incompatible with foreign SIM-cards[150]. However, to successfully activate Vdoma, the user had to enter an SMS-confirmation code sent to their mobile phone. Since initially the code could be sent only to a Ukrainian mobile number, a significant number of Ukrainians and foreigners coming from abroad had their access to the service limited due to the inability to register using a foreign number[151]. Moreover, the first version of the application was available only in Ukrainian, restricting foreigners' rights of access to it. Authorization from a foreign number and an English version of the Vdoma application are now available.
In addition to the above-mentioned problems with the availability of the application, both experts drew attention to the problems with accessing the service posed by travellers having a lack, or low level, of digital skills. According to a 2019 study by the Ministry of Digital Literacy of the Population of Ukraine, 53 percent of Ukrainians have digital skills below the basic level[152], which prevents this category of the population from fully using digital services, including the Vdoma app. Moreover, 15.1 percent of Ukrainians do not have the ability to connect to the Internet at all, and have never used it. Given that a significant percentage of citizens have low levels of digital skills, the lack of convenient offline alternatives to the Vdoma application is a problem, as it complicates the access of vulnerable groups to this public service. The development of alternative tools is much more costly and may require additional funding, but as the civic activist[153] noted, it is a necessary component of an inclusive digitalisation process.

Another problem in the context of accessibility and, in a broad sense, equality with regard to the application was the relatively simple possibility of avoiding installing it altogether – even when entering the territory of Ukraine from a "red list" country. Thus, since border guards are only obliged to check if citizens whose aircraft have arrived from the "red list" countries have installed the application, some people arriving from "red list" countries but who transited through a "green list" state are not checked. This was confirmed by one respondent to this study who returned by plane from a "red list" country by way of a country on the "green list."

In the absence of sociological research on the experiences of users in using Vdoma, the rating of the application on the platforms Google Play Market and App Store can be considered an approximate indicator of quality. On both platforms, the rating of the application is 1.4 out of 5 possible points (on Google Play Market the rating was calculated

146. Administration of the State Border Guard Service of Ukraine. At the border, you can decide on self-isolation with the addition of "Action at home" or observation. April 27, 2020. URL: https://www.kmu.gov.ua/news/na-kordoni-mozhna-viznachitisya-shchodo-samoizolyaciyi-z-dodatkom- dij-vdoma-chi-observaciyi

147. Ministry of Digital Transformation of Ukraine, response to a request, February 19, 2021.

148. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

149. Pavlo Belousov (Digital Security Expert, Internews-Ukraine), interview February 5, 2021, online.

150. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

151. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

152. Ministry of Digital Transformation of Ukraine. Research "Digital literacy of the population of Ukraine". 2019. URL: https: //osvita.diia. gov.ua/uploads/0/585-cifrova_gramotnist_naselenna_ukraini_2019_compressed.pdf.

153. Pavlo Belousov (Digital Security Expert, Internews-Ukraine NGO), interview February 5, 2021, online.

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

based on the results of 10,142 users, and on the App Store 1,546 users[154]). Among the main technical inconveniences of the application, according to experts, are incorrect location data for photographs and problems with face recognition technology, which caused erroneous data transmissions to the police[155], with the user's device falsely reporting a violation of self-isolation when the user was actually at home. This problem is evidence by the significant gap between the number of reports of quarantine violations received, and the actual number protocols on administrative offenses being issued: According to data from the National Police, for the period of 17 March 2020 to 19 February 2021, the National Police received 108,055 reports of violations of quarantine rules from the Vdoma application, as a result of which 71,254 home visits were made, after which only 96 administrative protocols were drawn up under Article 44 of the Code of Ukraine on Administrative Offenses[156].

According to the public activist[157], one of the decisive factors prompting users to give a low rating to the application was the lack of proper technical support: "In the case of any other application, if something does not work, the user can simply complain or delete it and choose another. In the case of Vdoma, there are no options. That's why users try to influence (the developers) through (giving poor) ratings and comments."

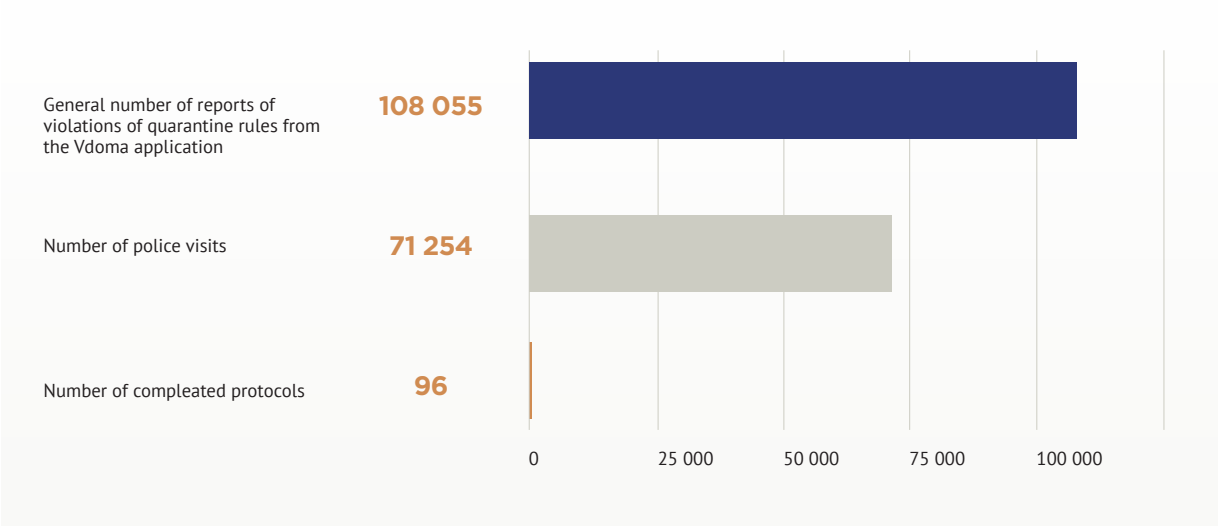
In an interview in the summer of 2020, one of the developers of the application actually admitted that the application only works at certain times – between 0900 and 2100[158]. This indicates the questionable effectiveness of the application in general, as it in fact allowed unmonitored movement within Ukraine for a significant period of time.

Vdoma and privacy

The launch of this application has raised a number of questions: How legitimate is the creation and implementation of such an application? How does it match with the right to respect for the private lives of citizens? Is interference with this right justified in order to protect public health? Is the extent of such intervention proportional to the threat to public health?

Diagram 3.

Statistics on notifications generated by the Vdoma application



154. Data as of March 4, 2021.

155. Pavlo Belousov (Digital Security Expert, Internews-Ukraine), interview February 5, 2021, online; Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

156. National Police of Ukraine, response to a request, February 22, 2021.

157. Pavlo Belousov (Digital Security Expert, Internews-Ukraine), interview February 5, 2021, online.

158. Maria Romanenko. "I went out of the shower and waited for the police": what's wrong with the application "Act at home" ?. Hromadske. July 29, 2020. URL: https://hromadske.ua/posts/vijshov-z-dushu-j-ochikuvav-na-policiyu-sho-ne-tak-z-dodatkom-dij-vdoma

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

In order to answer these questions, it is necessary to analyse international standards in the field of human rights protection – primarily the right to respect for private life – as well as to consider the issue of legislative consolidation to support the functioning of the application. The study will also analyse the extent to which the application was used to bring quarantine violators to administrative responsibility.

A number of researchers are of the opinion that the introduction of quarantine restrictions is inconsistent with the Ukrainian constitution, given the government's use of excessive discretion in accordance with the Law of Ukraine "On Protection of the Population from Infectious Diseases"[159]. As no ruling on the constitutionality of quarantine measures has been made by the Constitutional Court of Ukraine at the time of the research, we will proceed from the presumption of the constitutionality of these measures and use the principle of the "friendly attitude to international law" developed by the Constitutional Court of Ukraine in its own jurisprudence, which takes into account the rulings of the European Court of Human Rights (ECHR).[160]

The right to respect for private life: international standards

The right to privacy is protected by both international and national legal instruments. In particular, it is enshrined in Article 17 of the International Covenant on Civil and Political Rights[161], Article 8 of the European Convention on Human Rights[162], and Article 32 of the Constitution of Ukraine[163]. This right is not absolute and may be subject to restrictions, although the natures of the restrictions in the relevant documents may be different.

Thus, the International Covenant prohibits arbitrary or unlawful interference in the right to privacy. The Constitution of Ukraine allows the storage of confidential personal information only in cases specified by law, and only in the interests of national security, economic prosperity and human rights. The European Convention allows interference that is carried out in accordance with the law, and that is necessary in a democratic society in the interests of national and public security, or for the economic well-being of the country, to prevent riots or crimes, to protect public health or morals, or to protect the rights and freedoms of others.

The provisions of the European Convention outline the so-called "three-part test" of human rights restrictions: restrictions must be provided for by the law, pursue a legitimate aim, and be necessary in a democratic society. The case law of the European Court of Human Rights is also used to determine whether a state's monitoring of a person's movements is an interference with their right to respect for their private life, as guaranteed by Article 8 of the Convention. In particular, in its judgment in Uzun vs. Germany, the ECHR emphasized that the use of GPS beacons mounted on the car of a suspect of extremism by a prosecutor was an interference with the applicant's right to privacy as it revealed more information about the person's behaviour, thoughts and feelings than the use of other tracking methods[164]. The state's retention of personal data is also an interference, as the Court emphasized in S and Marper vs. the United Kingdom[165].

159. Berko ST, Kolotylo MM, Bocharov KV Protection by human rights courts from excessive state intervention during the COVID-19 pandemic in Ukraine. Kyiv, 2020. 33 p. URL: https://drive.google.com/file/d/15Hn4dbD1wZ7oHM_j2IDGinfHrYJPzQns/view

160. Constitutional Court of Ukraine. Decision of the Constitutional Court of Ukraine No. 6-rp / 2016 in the case on the constitutional petition of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine on the constitutionality of the provisions of part five of Article 21 of the Law of Ukraine "On Freedom of Conscience and Religious Organizations" notifications of public worship, religious rites, ceremonies and processions). September 8, 2016. URL: http://ccu.gov.ua/sites/default/files/docs/6-pn-2016.pdf

161. International Covenant on Civil and Political Rights, ratified on October 19, 1973, URL: https://zakon.rada.gov.ua/laws/show/995_043.

162. Convention for the Protection of Human Rights and Fundamental Freedoms of November 4, 1950, URL: https://zakon.rada.gov.ua/laws/show/995_004

163. Constitution of Ukraine (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1996, No. 30, p. 141), URL: https://zakon.rada.gov.ua/laws/ show / 254% D0% BA / 96-% D0% B2% D1% 80

164. Uzun v Germany App no 35623/05 (ECtHR, 2 September 2010). URL: http://hudoc.echr.coe.int/eng?i=001-100293

165. S and Marper v the United Kingdom [GC] App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008). URL: http://hudoc.echr.coe.int/ eng?i=001-90051

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

Although the GDPR is not yet binding on Ukraine, we should not forget about another international document in the field of personal data protection – namely the Council of Europe Convention № 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data[166]. Article 5 of Convention № 108 establishes a number of principles for processing personal data, namely: the lawfulness of their processing; storing data for defined and legitimate purposes, and using them in a manner compatible with these purposes; the completeness, relevance and non-redundancy of data; the accuracy and up-to-dateness of data; and that data retention is no longer than necessary to achieve the goal.

Legitimate purposes for restrictions

Moving away from the classical structure of analysis via the three-component test, let us examine legitimate purposes of restrictions. There is no general controversy that restricting the right to privacy, in particular by introducing the need to monitor the contacts of infected people, or by monitoring compliance with the rules of self-isolation, may be done in pursuit of the goal of protecting public health. The Syracuse Principles on Restrictions and Derogations under the International Covenant on Civil and Political Rights state that measures taken to protect public health must be specifically aimed at preventing disease and take into account international WHO health regulations.[167]

On 30 January 2020 the Director-General of WHO declared COVID-19 a public health emergency of international concern.[168] This allowed states to impose more human rights restrictions. Among the recommendations made by the WHO to prevent the spread of the virus was the isolation of all infected people, and the quarantining of all loved ones who came into contact with infected person[169]. In view of this, restricting the right to privacy by monitoring compliance with quarantine and isolation in order to prevent the spread of a disease can indeed be done in pursuit of the goal of protecting public health.[170]

Foreseeability of legal restrictions

Any restriction on the right to respect for private life must be provided for by law. The requirement for the predictability of rights restrictions means that a rule of law that restricts a person's right is "predictable" if it is formulated with sufficient clarity to enable each person to regulate his or her behaviour, if necessary, through appropriate consultation. The law should define with sufficient clarity the limits of discretion granted to the competent authorities and the procedure for its implementation, taking into account the legitimate purpose of the measure, in order to provide a person with adequate protection against arbitrary interference.

An important factor for the Vdoma application are the dynamics of its implementation. As mentioned, the application was launched on 7 April 2020. At the time of its launch, the application was mentioned in only one government document – the resolution requiring the Ministry of Digital Transformation to create it[171]. Despite the fact that the application was to be installed by a person independently and voluntarily, its Privacy Policy at the time of creation and at least until 13 April 2020 allowed the transfer of data from the application to the Ministry of Interior, the National Police, Public Health Centre, and other state bodies, and only after that was it stipulated that

166. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ratified on 06.07.2010, URL: https://zakon.rada. gov.ua/laws/show/994_326

167. Syracuse Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights. September 28, 1984. URL: https://undocs.org/pdf?symbol=en/E/CN.4/1985/4

168. WHO. Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV). January 30, 2020. URL: https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations- (2005) -emergency-committee- regarding-the-outbreak-of-novel-coronavirus- (2019-ncov)

169. WHO Transmission of SARS-CoV-2: implications for infection prevention precautions: Scientific Brief. July 9, 2020. URL: https://www.who.int/news-room/commentaries/detail/transmission-of-sars-cov-2-implications-for-infection-prevention-precautions

170. Malone v the United Kingdom App no 8691/71 (ECtHR, 2 August 1984). URL: http://hudoc.echr.coe.int/eng?i=001-57533

171. Resolution of the Cabinet of Ministers of Ukraine No. 255 of April 2, 2020 "On Amendments to the Resolution of the Cabinet of Ministers of Ukraine of March 11, 2020 No. 211". URL: https://zakon.rada.gov.ua/laws/show/255-2020-%D0%BF

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

such data would be transmitted exclusively to the Ministry of Internal Affairs and territorial bodies of the National Police[172]. Despite a person giving their consent to the processing of data via the app, which was a sound basis for processing even sensitive biometric data and health data, the legitimacy of their further processing by the authorities was questionable, because at that time Ukrainian legislation did not contain the grounds for the further processing of the relevant data by third parties. There should be safeguards at the legislative level that would make it impossible for the unrestricted transfer of data between public authorities.

The relevant legislation was adopted on 13 April 2020, but entered into force only on 18 April 2020. The Law of Ukraine "On Amendments to the Law of Ukraine On Protection of the Population from Infectious Diseases to Prevent the Spread of Coronavirus (COVID-19)" stipulated in its transitional provisions that for the period of quarantine and within 30 days of the implementation of anti-epidemic measures the processing of data related to a person's health status, place of hospitalization or self-isolation, their surname, name, patronymic, date of birth, place of residence, work (study), is permitted in order to counteract the spread of coronavirus disease (COVID-19) without consent of that person[173]. Despite this having several positive aspects, in particular the establishment of the purpose of data processing and the limited period of permitted processing (for the quarantine period and 30 days thereafter, after which the data are subject to depersonalization and / or destruction), this act lacked a key element – determining which public authorities receive the authority to process personal data without the consent of a person, and what the scope of that personal data might be[174].

Such parameters for personal data processing were detailed only on 22 April 2020 on the adoption by the Cabinet of Ministers of Ukraine of Resolution № 291[175]. These parameters have remained almost unchanged since the adoption of the resolution, and were included in successive quarantine resolutions. In particular, they are to be found in the current government decree "On the establishment of quarantine and the introduction of restrictive anti-epidemic measures to prevent the spread of acute respiratory disease COVID-19 caused by coronavirus SARS-CoV-2" of 9 December 2020.[176] The only significant change, made in August 2020, was the addition of permission to process personal data to provide information on the dates of crossing the state border of Ukraine by persons with a confirmed case of COVID-19, their registered place of residence, their place of actual residence, information about communication means (phone number), and data on those from the State Border Guard Service Administration, the State Customs Service and the State Migration Service who came into contact with such a person[177].

Returning to the Vdoma application: It was only on 22 April 2020 that it entered the regulatory field, and the purpose of its use (the processing of personal data using the application) was determined. Only from this moment it can be considered that this data processing was carried out for specific and lawful purposes, in accordance with Article 6 of the Law of Ukraine "On Personal Data Protection"[178]. Also, only from that moment was it clear to which data various state bodies could obtain access, and for what purpose. Thus, it was made clear that the data would be provided to the National Police solely for the purpose of monitoring those who were self-isolating, and those who had violated quarantine rules.

172. Maxim Dvorovy. Coronavirus, treating the infected and privacy: how far can the state and technology companies go and where are the human rights? Digital Security Laboratory. April 15, 2020. URL: https://dslua.org/publications/koronavirus-trekinh-infikovanykh-ta-pryvatnist-iak- daleko-mozhut-pity-derzhava-i-tekhkompanii-ta-de-tut-prava-liudyny/

173. Law of Ukraine "On Amendments to the Law of Ukraine" On Protection of the Population from Infectious Diseases"on Prevention of the Spread of Coronavirus Disease (COVID-19)" (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2020, No. 19, p. 127). URL: https://zakon.rada.gov.ua/laws/ show / 555-IX

174. Vita Volodovska. "No time to agree": what's wrong with the new "anti-virus" law. Digital Security Laboratory. April 17, 2020. URL: https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antyvirusnym-zakonom/

175. Resolution of the Cabinet of Ministers of Ukraine No. 291 of April 22, 2020 "On Amendments to Certain Acts of the Cabinet of Ministers of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/291-2020-%D0%BF

176. Resolution of the Cabinet of Ministers of Ukraine No. 1236 of December 9, 2020 "On the establishment of quarantine and the introduction of restrictive anti-epidemic measures to prevent the spread of acute respiratory disease COVID-19 caused by the coronavirus SARS-CoV-2 in Ukraine". URL: https://zakon.rada.gov.ua/laws/show/1236-2020-%D0%BF

177. Resolution of the Cabinet of Ministers of Ukraine No. 712 of August 12, 2020 "On Amendments to the Resolution of the Cabinet of Ministers of Ukraine of April 24, 2020 No. 331 and of July 22, 2020 No. 641". URL: https://zakon.rada.gov.ua/laws/show/712-2020-%D0%BF

178. Law of Ukraine "On Personal Data Protection" (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2010, No. 34, p. 481). URL: https://zakon.rada.gov.ua/laws/show/2297-17

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

Therefore, it can be considered that the monitoring of self-isolation from that moment was an intervention provided for by law that met the standards of legality.

One small point: The privacy policy of the Vdoma app still links to Resolutions of the Cabinet of Ministers of Ukraine № 211[179] and 255[180], most of the provisions of which have expired. These links in the Policy should be updated.

Referring to the provisions of the Law of Ukraine "On Personal Data Protection", it is stated that consent must be expressed in writing or in a form that allows it to be concluded that consent has been given. Analysing the Vdoma application, during actual registration, users do not have the opportunity to consent to, or refuse to give consent to, the processing of their personal data. It should be noted that users actually have no choice at all – they are forced to transfer their data, because otherwise they would not be able to use the application. Such consent is conditionally voluntary. So it turns out that the very fact of a person going on to use the service is regarded as their giving consent to the processing of their personal data.[181]

Necessity of interference in a democratic society

In the aforementioned case of S and Marper vs. the United Kingdom, the European Court of Human Rights, analysing the need to intervene in a democratic society, noted that national law should contain adequate safeguards against the misuse of personal data by the state.[182] In particular, the court stressed the need to comply with the principles of personal data processing guaranteed by the Convention № 108.

In the context of the Vdoma application, it is worth mentioning such principles as the data minimization to be processed, as well as the storage of processed data for periods no longer than is necessary for the purpose of processing. It follows from the legislation, as well as the Privacy Policy of the Vdoma app, that data for the purpose of monitoring compliance with the self-isolation regime may be transmitted only to the National Police and the Ministry of the Interior, which are the competent authorities. At the same time, they receive data on the person's last name, first name, patronymic, date of birth, place of self-isolation, registered place of residence, place of actual residence of the person, and information about means of communication (phone number), which is generally justified and proportionate.

Each data subject has the right to easy ascertain how, when, by what means, etc. their personal data is being processed. Returning to the text of the Privacy Notice, which is the main information document in the application on how it processes personal data (realising the user's right to information), it should be noted that although there is a list of rights, it is unclear how the user can ensure they are observed. Users can contact a chatbot with any questions about the app, but this is not the best option, as in order to properly exercise the rights of a personal data subject a separate address for such requests should be created, or a separate service responsible for processing these requests, and it is in the Privacy Notice that the mechanism for exercising one's rights should be clearly defined[183].

Data storage is more problematic. Thus, the above-mentioned "coronavirus" law of 13 April 2020 established that data collected within 30 days of the end of the quarantine period are subject to depersonalization, and if this is impossible, deletion[184]. At the time of the adoption of this law, it seemed that the quarantine would be over fairly quickly, and therefore such a rule was reasonable.

179. Resolution of the Cabinet of Ministers of Ukraine No. 211 of March 11, 2020 "On Prevention of the Spread of Acute Respiratory Disease COVID-19 Caused by SARS-CoV-2 Coronavirus on the Territory of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/211-2020-%D0%BF

180. Resolution of the Cabinet of Ministers of Ukraine No. 255 of April 2, 2020 "On Amendments to the Resolution of the Cabinet of Ministers of Ukraine of March 11, 2020 No. 211". URL: https://zakon.rada.gov.ua/laws/show/255-2020-%D0%BF.

181. Ruslana Tsitsinskaya (lawyer, personal data protection expert), interview on March 2, 2021, online.

182. S and Marper v the United Kingdom [GC] App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008). URL: http://hudoc.echr.coe.int/eng?i=001-90051

183. Anastasia Svitlychna (lawyer-expert on human rights and personal data protection), interview on March 10, 2021, online.

184. Law of Ukraine "On Amendments to the Law of Ukraine" On Protection of the Population from Infectious Diseases"on Prevention of the Spread of Coronavirus Disease (COVID-19)" (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2020, No. 19, p. 127). URL: https://zakon.rada.gov.ua/laws/ show / 555-IX

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

However, in practice, it means that that data on each person who registered with the Vdoma app at the beginning of quarantine in the spring of 2020 still have to be stored. The government attempted to rectify this situation in February 2021 by stipulating that personal data processed in the system should be depersonalized and, if depersonalization was impossible, deleted within 30 days of the end of a person's period of self-isolation[185]. Notification of data deletion from the system is now sent to each person who has completed self-isolation[186]. This is a good approach, but it contradicts the norm of the "coronavirus" law on the retention of data for 30 days after the end of quarantine – which could lead to the this rule being struck down court. That is why the regulation of this issue will require changes in legislation.

In summary, the operation of the Vdoma application is broadly in line with international standards for the protection of the right to respect for private life, although some changes to the law and privacy policy would be desirable to address conflicts.
At the same time, the issue of the transparency of data processing within Vdoma application remain problematic. The procedure for information interaction within the service is determined at the level of agreements between the Ministry of Digital Transformation and other bodies. However, the manner of interaction between these systems has not been made public, and is provided by the responsible authorities only under a freedom of information request[187]. Information on the legal basis and procedure for the transfer of information between public authorities should be properly disclosed and updated by those responsible for the application and the system – i.e. the Ministry of Digital Transformation and the Diia State Enterprise.

Vdoma and risks to democracy

Following the mass rollout and implementation of measures to counter the COVID-19 pandemic around the world, a number of international human rights organizations and activists highlighted the point that overcoming the pandemic should not be achieved at the cost of democracy. Thus, on 25 June 2020, the Institute for Democracy and Election Support (IDEA) published an open letter entitled "A Call to Defend Democracy", which has already been signed by more than 500 individuals and organizations. " It is only through democracy that societies can build the social trust that enables them to persevere in a crisis, maintain national resilience in the face of hardship, heal deep societal divisions through inclusive participation and dialogue, and retain confidence that sacrifice will be shared and the rights of all citizens respected,[188] "the letter reads in part. To a large extent, the letter was a response to the tendency of authoritarian and even some democratic governments to seize significant powers during the pandemic.

The main risks to democracy in a global pandemic arise through the obligations of governments to ensure the safety of their citizens and to minimize the spread of the virus. The most common measures to achieve this goal have been tighter controls on the free movement of citizens through quarantine restrictions, a ban on mass gatherings, and mandatory isolation upon arrival from places with high risks of infection with COVID-19. Strengthening law enforcement controls over compliance with quarantine restrictions has de facto given governments more powers to monitor society. At the same time, it should be understood that any restrictions on citizens' rights imposed to counter the spread of the COVID-19 pandemic must be based on scientific evidence,

185. Resolution of the Cabinet of Ministers of Ukraine No. 104 of February 17, 2021 "On Amendments to Certain Acts of the Cabinet of Ministers of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/104-2021-%D0%BF

186. Resolution of the Cabinet of Ministers of Ukraine No. 104 of February 17, 2021 "On Amendments to Certain Acts of the Cabinet of Ministers of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/104-2021-%D0%BF.

187. Vita Volodovska. "No time to agree": what's wrong with the new "anti-virus" law. Digital Security Laboratory. April 17, 2020. URL: https://dslua.org/publications/ne-chas-dlia-zghody-shcho-ne-tak-iz-novym-antyvirusnym-zakonom/.

188. Institute for Democracy and International Assistance. A CALL TO DEFEND DEMOCRACY. 25 червня 2020 року. URL: https://www.idea.int/news-media/multimedia-reports/call-defend-democracy

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

and be non-discriminatory, proportionate to the goal, and limited in duration[189]. Therefore, when implementing applications to monitor self-isolation, in particular at home, it is important to understand that any information collected for COVID-19 surveillance purposes can only be used for medical purposes, and that it cannot be used for any other purposes. Although the privacy policy defines the purpose of collecting and processing personal data by the Vdoma application as counteracting the spread of coronavirus disease (COVID-19), in practice, as the public activist[190] noted, it is virtually impossible to determine whether users' personal data is indeed used for its intended purpose. The world has already seen the first cases of police using data collected through applications to combat the spread of COVID-19 for their own, unrelated purposes.[191]

According to a report by the international non-governmental organization Freedom House, entitled "Democracy under Lockdown", since the outbreak of the coronavirus, the state of democracy and human rights has deteriorated in 80 countries, including Ukraine[192]. Freedom House experts say that among the main problems exacerbated by the pandemic are abuse of power, corruption, lack of protection for vulnerable groups, and a lack of transparency regarding information about COVID-19.

Lilia Oleksyuk, the adviser to Ukraine's parliament on issues of digitalization, drew attention to problems with communications about anti-coronavirus measures, including in the Vdoma application, noting that the lack of a proper information campaign on measures aimed at overcoming the COVID-19 pandemic only reduces public confidence in government institutions[193]. Indeed, according to a survey conducted by the Razumkov Centre's sociological service from 24-29 April 2020, only 32 percent of Ukrainians trust the government of Ukraine (4.3 percent fully trust it), 36 percent the National Police (6.2 percent fully trust), and 29 percent the Ministry of Health (5 percent fully trust)[194]. As administrators and third parties which receive personal data processed by the Vdoma application, these authorities must ensure maximum transparency in their policies for using users' personal data, as well as properly communicate to make citizens aware of their rights and responsibilities in a health crisis.

Due to the involvement of several agencies in the Vdoma project, exactly who is accountable for the application is unclear. The developer of the application was the Diia state enterprise, according to information received from the Ministry of Digital Transformation[195]. However, the press service of the ministry has reported that the application has now been fully transferred to the Ministry of Health. Problems with coordination between the agencies involved with the app resulted in poor support for users, who repeatedly failed to obtain the support for they needed to use the application[196].

In order for the Vdoma application to be considered better protected in terms of cybersecurity, it will be necessary to conduct an independent professional analysis of the application's source code, conduct at least two independent professional tests of the penetrability of all elements of the application (the server, client, and the communication channels between them). There will also have to be an independent professional audit of the general security system of the application (including documentation and the requirements of regulatory documents on information security), as well as for the source code of the application and the documentation for it to be published. Accordingly, after all these audits and tests, it will be necessary to

189. Human Rights Watch. Human Rights Dimensions of COVID-19 Response. 19 березня 2020 року. URL: https://www.hrw.org/news/2020/03/19/ human-rights-dimensions-covid-19-response#_Toc35446577

190. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

191. Singapore's interior minister said police could use data from the government's COVID-19 contact tracking application for criminal investigations. See: Andreas Illmer. BBC News Singapore. Singapore reveals Covid privacy data available to police. January 5, 2020. URL: https://www.bbc.com/news/world-asia-55541001

192. Sarah Repucci, Amy Slipowitz, DEMOCRACY UNDER LOCKDOWN. Freedom House. October 2020 року. URL: https://freedomhouse.org/sites/ default/files/2020-10/COVID-19_Special_Report_Final_.pdf

193. Lilia Oleksyuk (chairman of the association, Waibit NGO), interview on February 24, 2021, online.

194. Razumkov Center. Citizens' assessment of the situation in the country, the level of trust in social institutions and politicians, electoral orientations of citizens (sociological survey, April 2020). May 4, 2020. URL: https://razumkov.org.ua/napriamky/sotsiologichni- doslidzhennia / otsinka-gromadianamy-sytuatsii-v-kraini-riven-doviry-do-sotsialnykh-instytutiv-ta-politykiv-elektoralni-oriientatsii-gromadian- krom 2020

195. Press service of the Ministry of Digital Transformation of Ukraine. Letter dated January 27, 2021.

196. Pavlo Belousov (Digital Security Expert, Internews-Ukraine NGO), interview February 5, 2021, online.

Tracking citizens through the Vdoma application: Problem issues of personal data and democracy in Ukraine

correct all vulnerabilities in the Critical, High and Medium classes, and conduct repeated retests / audits to confirm that the identified deficiencies have been corrected. If the application was developed from the beginning without complying with security requirements (which is most likely for the Vdoma application due its very short development time), then usually the much more rational solution is to create a new application rather than fix all of the existing vulnerabilities. Given the numerous cases of failure of the application, as well as the questionable level of its security and lack of any objective data regarding its security, it would be reasonable to ban its use in Ukraine until all of its technical deficiencies are corrected and its source code and documentation are published – along with the conclusions of independent professional experts on cybersecurity and personal data protection on whether the app has an acceptable level of security, and whether users' personal data is safe when using it.[197]

197. Konstantin Korsun, cybersecurity expert, cyber blogger, co-founder of Berezha Security (BSG), interview May 14, 2021, online.

Anna Mysyshyn

Conclusions

9

Conclusions

The COVID-19 pandemic has been a challenge for all of us, forcing us to adapt to a more online lifestyle, which in turn has created the possibility of there being number of human rights violations – especially of those rights that can be implemented in and through the digital environment. Digital inequality, the violation of digital rights of users in the context of receiving digital services, and violations of data processing rules and the security of personal data – all of this has resulted from the state's introduction of innovations to ensure the health of Ukrainian citizens.

The pandemic and the shift to studying remotely have created digital inequalities in education. Many pupils, students and teachers do not have access to the Internet, or the technical means and skills to work with online tools at home. To overcome digital inequalities and ensure that basic digital rights are protected, especially during the pandemic, access to the Internet, basic digital services, personal computers and mobile phones must be accessible to everyone, including the most vulnerable. An important step in this regard should be not only the enshrinement of relevant provisions at the legislative level, including the implementation of best international practices for Ukraine, but also the training of the population in digital literacy and awareness, and for this training to be inclusive and accessible to all.

To ensure compliance with quarantine restrictions and the self-isolation of individuals who may be potential carriers of SARS-CoV2, the Ministry of Digital Transformation developed the Vdoma application to collect, process and store data from returnees from countries where COVID-19 outbreaks have been reported, and from those who have been in contact with a COVID-19 patient or someone who showed signs of being infected with the virus.

Analyzing the feedback from users of this application, we can conclude that its sometimes faulty functionality has created a number of inconveniences – application crashes, difficulty in uploading photos or even the sending of false messages about violations of the observation regime. These have caused stress and negative emotions among the population.

As for e-services aimed at overcoming the effects of COVID-19 – several have been created. However, these are not without some drawbacks and they were introduced exclusively electronically, which to some extent violated the digital rights of those who do not have access to digital devices and the Internet. However, it should be borne in mind that these e-services were developed under force majeure.

In general, the rapid digitization of public services poses potential risks to citizens' information accessibility and security. Digitizing 100 percent of public services at the theoretically maximum possible rate would create a potential risk to cybersecurity. Moreover, when there is a focus on rapid results in the development of digital public services, those populations that are vulnerable may be overlooked. This applies in particular to the elderly, people with disabilities and internally displaced persons. For example, the lack of offline alternatives to the digital service for applying for one-time financial assistance limited the rights of those who do not use a computer or smartphone for various reasons.

With regard to the Vdoma application and its compliance with international standards for upholding the right to respect for private life, there are a number of flaws – namely as to who is the subject of personal data processing and who is held to account in cases where this data becomes public knowledge (through imposing sanctions, bringing to administrative responsibility, or through other measures).

However, the Vdoma application generally meets standards for observing the right to respect for private life. After the delay in settling its regulatory status in April 2020, it was clearly determined which types and which amounts of data from the Vdoma system certain authorities are authorized to use. At the same time, despite the application being in practical use, there are problems with the excessive statutory retention of data of persons who were in self-

Conclusions

isolation, as well as with the transparency of data processing within government agencies involved in the Vdoma information service. Thus, the storage of personal data until the end of the legal quarantine regime is not appropriate. Also, the ministries have yet to publish documents on how quarantine data is exchanged between them: it can be obtained only though submitting requests to the Ministry of Education, the Ministry of Health, and the Ministry of Internal Affairs.

Referring to international experience, namely the provisions of the General Data Protection Regulation or GDPR, it should be noted that among the fundamental rights that have been improved by this regulation is the right for information to be deleted at the request of the subject (the right to be forgotten), as well as the right to prohibit processing – the controller of personal data may not process personal data if the subject requests that it not do so. The administrator can achieve this by preventing third parties from accessing the data, or by removing data from a website or application. Such provisions would be quite appropriate for use in Ukraine as well, and would allow users of the Vdoma application to send a request to delete their personal information, or to forbid its processing.

The basic goal of personal data protection should therefore be to protect the key rights and freedoms of citizens. The protection of personal data must take into account all of the stages related to personal data, from collection to destruction, or loss of relevance. The means that for the implementation of personal data protection there should be an appropriate mechanism, based on the current Law of Ukraine “On Personal Data Protection”, which will harmoniously implement key European standards, with clear definitions of freedom of information and personal data protection, as well as details of how liability for violations of personal data protection standards should be determined.

Recommendations

10

Recommendations

The pandemic has pushed Ukraine into rethinking its digital transformation strategies and how to ensure digital rights, which might not have happened for years otherwise. It is difficult to say what the long-term impact of COVID-19 will be on digital rights, but if the digital transformation continues to change our lives, now is the time for decision makers to consider how to make digital life inclusive and convenient for everyone.

With regard to ensuring digital rights and overcoming digital inequalities, the government needs to ensure that there is competition among ISPs to ensure that the Internet is affordable in remote areas and villages. Moreover, there should be government programmes in Ukraine to provide low-income families with computers. In addition, in order to bridge the digital skills gap, it is necessary to provide not only online but also offline learning – especially for older people. Digital accessibility for people with visual and hearing disabilities should also be a priority for the legislature and the executive. It is recommended that the EU Digital Accessibility Directive be transposed into Ukrainian legislation in the near future.

To ensure the inclusiveness of digital public services, not only government agencies, but NGOs, international organizations, and other stakeholders advocating for accessibility issues should be included in the development of electronic services and public policy in this area.

In the context of the Vdoma application, a number of legislative changes need to be made to improve the regulation of its use. Thus, the Diia State Enterprise and the Ministry of Finance should update the privacy policy of the Vdoma application, replacing the references to invalid resolutions of the Cabinet of Ministers of Ukraine with more current ones. The government should initiate the development and amendment of legislation that would ensure the legality of the practice of deleting data immediately after self-isolation ends, and harmonize this practice with the requirements of the legislation. Public authorities should also make public the means by which information is exchanged between public authorities with regard to the Vdoma information system, and ensure the transparency of such data exchanges. To improve the accessibility of the application, we advise that the state not monopolize its development, but to allow private companies and non-governmental organizations to take part, provided that the state monitors compliance with standards.

In order for the Vdoma application to be considered more secure from the point of view of cybersecurity, there should be an independent professional analysis of the application's source code, at least two independent professional tests of the secureness against penetration of all elements of the application (server, client, and communication channels between them), and an independent professional audit of the general security system of the application (including its documentation and the requirements of regulatory documents on information security). The source code of the application and documentation for it should also be published. Once all these audits and tests are completed, it is necessary to correct all vulnerabilities in the Critical, High and Medium classes, and conduct repeated retests / audits to confirm that the identified deficiencies have been corrected.

If the application was originally developed without compliance with security requirements (which is most likely for the Vdoma application due to its very short development time ahead of its launch), then the much more rational solution is usually to create a totally new application, rather than to fix all of the current one's vulnerabilities.

Given the numerous cases of failure of the Vdoma application, as well as its questionable level of security, and lack of any objective data on its security, it would be reasonable to ban its use in Ukraine until all technical deficiencies are corrected, its source code and documentation published, and independent professional experts on cybersecurity and personal data protection have determined whether the app has an acceptable level of security and can keep the personal data of its users secure.

Recommendations

In order to protect the digital rights of those who could not use the e-services in question, it is recommended that the deadline for applying for financial assistance be extended for sole proprietors and employees. Such e-services should also be available offline, for example, in CNAPs. In future, it makes sense to introduce new e-services: using Google Maps to show places where there are concentrations of people, and tracking the contacts of people infected with COVID-19 and other people with whom they have come into contact. It is proposed to apply a competitive model of service delivery – according to which the state formulates public policy and develops standards, while the development of specific e-services is done by the public and private sectors on a competitive basis.

In a broader context, it is recommended that digital transformation be approached more strategically, with its long-term implications in mind. To do this, it is necessary to constantly monitor and evaluate the implementation of digital services and their compliance with digital rights, both internally (by the developers) and externally (with the participation of external auditors) and publish the results of such evaluations in the public domain. In addition, quality must be preferred over quantity, and the goal of the digitization of 100 percent of public services by 2024 poses a risk to the quality of e-services. How inclusive could such services be, and would the digital rights of the citizens that use them be properly protected?

Appendices

11

Appendices

Name	Last Name	Position	Affiliation	Status
Mstyslav	Banik	Project Manager of "Diia"	Ministry of Digital Transformation of Ukraine	Government official
Pavlo	Byelousov	Digital security expert	NGO "Internews Ukraine"	Public activist
Taras	Budynkevych	Data security expert	Privat Bank	Private sector specialist
Volodymyr	Brusylovskyi	Project support manager of "Diia"	UNDP	International project specialist
Olesia	Danylenko	Employee of the program "E-Services"	"TAPAS" Project	International project specialist
Oleksii	Zeliv'ianskyi	Component coordinator "E-Services"	"EGAP" Project	International project specialist
Oleksandra	Kovalenko	A head of the expert group	Ministry of Digital Transformation of Ukraine	Government official
Volodymyr	Kossak	Head of Department	I.F. National University of Lviv	Researcher
Kostiantyn	Korsun	Cybersecutiry expert	"Berezha Security" company	Private consultant
Danylo	Molchanov	Associate director	"TAPAS" Project	International project specialist
Liliia	Oleksiuk	A Head of the association	NGO "Vaibit"	Public activist
Dmytro	Popov	Independent digital accessibility expert	Individual consulting	Public activist
Anastasiia	Popova	Independent expert on digital inequality	Individual consulting	Researcher
Yevhen	Poremchuk	Chairman of the Board	NGO "E-republic"	Public activist
Yevheniia	Poremchuk	Expert	NGO " E-republic"	Public activist
Anastasiia	Svitlychna	Expert	Lawyer Data Protection - Consultant GDPR - DPO	Researcher
Oleksandr	Fediienko	Chairman of the committee	Verkhovna Rada of Ukraine	Deputy
Volodymyr	Flonts	Director	NGO"E-democracy"	Public activist
Dzvinka	Chepelis	Expert	Lviv city council	Government official