Public health or digital liberties?

Citizens' tracking during and after COVID-19: implications for democracy in the Eastern Partnership countries

Institute of Innovative Governance

B | S | T The Black Sea Trust for Regional Cooperation
A PROJECT OF THE GERMAN MARSHALL FUND

INTERNATIONAL RENAISSANCE FOUNDATION

DIGITAL COMMUNICATION NETWORK

SSTAA

PMO Business Consulting

WE WATCH THE GOVERNMENT FOR YOU
WATCH DOG MD

This publication was prepared by the Institute of Innovative Governance (Ukraine) with cooperation with Digital Communication Network (Armenia), Social-Strategic Researches and Analytical Investigations Public Union (Azerbaijan), WhatchDogs. (Moldova), PMO Business Consulting and Digital Communication Network (Georgia), East Center (Belarus) 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.

Authors

Anna Melenchuk
Institute of Innovative Governance (Ukraine)

Anna Mysyshyn
Institute of Innovative Governance (Ukraine)

Andrea Castanga
Institute of Innovative Governance (Ukraine)

Olena Dudko
Institute of Innovative Governance (Ukraine)

With contributions from

Dmytro Khutkyy - Institute of Innovative Governance (Ukraine)
Khrystyna Kvartsiana - Institute of Innovative Governance (Ukraine)
Maksym Dvorovyi - Institute of Innovative Governance (Ukraine)
Ashkhen Grigoryan – Digital Communication Network (Armenia)
Ani Grigoryan - Digital Communication Network (Armenia)
Andrei Yeliseyeu - EAST Center (Belarus)
Valeriu Pașa - WatchDog.MD (Moldova)
Dragomir Doina - WatchDog.MD (Moldova)
Ilqar Huseynli – Analytical Investigations Public Union (Azerbaijan)
Elxan Heyderli - Analytical Investigations Public Union (Azerbaijan)
Mariam Nozadze – PMO Business Consulting (Georgia)
Ema Todua - PMO Business Consulting (Georgia)
Teona Tomashvili - Digital Communication Network (Georgia)

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

About IRF

The International Renaissance Foundation (IRF) is one of the largest Ukrainian charitable foundations that has been developing an open society in Ukraine since 1990 where everybody has a sense of dignity, citizens are involved in the formation of the state, and the authorities are transparent and responsible. We work on the development of Ukraine in which human rights are securely protected and positive changes work for the benefit of the citizens. The foundation was founded by the philanthropist George Soros and is part of the Open Society Foundations international network.

Public health or digital liberties?

Citizens' tracking during and after COVID-19: implications for democracy in the Eastern Partnership countries

Contents

Introduction

1

Introduction

This report has been developed to analyse the situation of COVID-19 tracing apps and digital tools in EaP countries: Armenia, Azerbaijan, Belarus (withdrew from EaP on 28 June 2021), Georgia, Moldova, Ukraine. For each country (except Belarus), an individual report was developed in order to analyse and evaluate the impact of the above-mentioned technologies in the country.

The scope of this report is to present a comparative analysis of the digital public solutions adopted during COVID-19 and provide a series of recommendations.

The individual countries' reports on which this analysis is based are the following:

Azerbaijan: Citizens' tracking during and after COVID-19: report on the situation in Azerbaijan (By Social-Strategic Researches and Analytical Investigations Public Union).

Moldova: Citizens' tracking during and after COVID-19: report on the situation in Moldova (By WhatchDogs. MD and Digital Communication Network in Moldova).

Georgia: Citizens' tracking during and after COVID-19: report on the situation in Georgia (By PMO Business Consulting and Digital Communication Network in Georgia).

Armenia: Citizens' tracking during and after COVID-19: report on the situation in Armenia (By Digital Communication Network in Armenia).

Ukraine: Citizens' tracking during and after COVID-19: report on the situation in Ukraine (By the Institute of Innovative Governance).

Context

2

Context

At the beginning of 2020, the world was shaken by a viral pandemic, which changed everyone's normal way of life for more than a year. The disease, caused by a coronavirus and known as COVID-19, has become a challenge for health systems and forced governments around the world to introduce several preventive measures including social distancing and lockdowns. At the end of March 2020, when the disease was already raging in the world, several national governments introduced mechanisms for monitoring and self-isolation for people exposed or symptomatic to COVID-19 in order to contain the effects of a global pandemic.

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 an infected person. In particular, governments and stakeholders involved in the fight against COVID-19 started relying on data analytics and digital technologies (including tracing mobile applications) to address this new threat. These digital efforts deployed by national governments, health-care institutions as well as businesses to prevent larger scale propagation of the virus were often approved as part of extraordinary measures to fight the pandemic, including the declaration of a state of emergency in many cases.[1] Eastern Partnership (EaP) countries namely Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine were among those countries.

While even prior to the pandemic, digital services and IT technology had become an increasingly important part of citizens' lives, it was the emergency situation that facilitated the spread of their adoption. In particular, the prolonged emergency situation pushed governments, including in the EaP countries to develop new digital solutions to fight the pandemic. For example, mobile applications which ensure contact tracing and exposure notification were introduced all over the world. Contact tracing apps allowed people to register their location and share it with health authorities, who in turn can more accurately identify outbreaks, while exposure notification programs only notify users if they have been around a person who later found a positive test for COVID-19.

This report presents a comparative analysis of the EaP countries on their adoption of digital instruments during the pandemic and their implications on citizens' lives. Ultimately, the scope of the analysis is to assess how digital solutions, including COVID-19 tracing apps, were implemented during the emergency period and whether their implementation can be related to any risks for democracy and human rights.

This report is focusing on the EaP countries since digital rights including the right to personal data protection and privacy were reportedly being violated on a larger scale before and during the pandemic in these countries in particular. Moreover, implications of COVID-19 related digital solutions aren't temporary and many of them may have a negative impact on democracy and human rights in the post-COVID time. For instance, contrary to the member-states of the European Union where personal data protection is ensured by GDPR, countries in the EaP region lack effective and comprehensive data protection systems.[2] Moreover, enhancing the right to data protection in EaP has been recognized as a clear priority by the governments, most international partners and stakeholders. Indeed, it was noted that digitalisation poses potential threats in EaP countries such as privacy and cyber security issues which can create additional obstacles to EaP states' participation in the EU digital single market and further political integration with the European Union.[3]

In April 2020 the Council of Europe issued a statement on digital solutions and contact tracing[4] in which it is mentioned

1. Council of Europe Joint Statement on the right to data protection in the context of the COVID-19 pandemic , March 30 2020
2. European Parliament Eastern Partnership 3.0 Principles, priorities, and prospects May 2020
3. European Council on Foreign Relations A digital agenda for the Eastern Partnership June 9, 2021
4. Council of Europe Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe April 28, 2020

Context

that while it is crucial to invest "all efforts in preventing further propagation of the virus", it is also important to note that digital contact tracing raises new questions that cannot be neglected before deciding to implement such population-wide digital measures. In particular, the statement recognises that digital solutions to trace and fight the spread of the virus should respect three different but related elements:

A. Effectiveness

The benefits of such digital epidemic solutions (including contact tracing) override the benefits of other alternative solutions which would be less intrusive.

B. COVID-19 purpose identification

The digital solutions implemented to fight the virus should be introduced only in the context of tracing and fighting the virus.

C. Minimisation of risks related to privacy, data protection and transparency

Data processed within digital instruments should be reduced to the strictest minimum and any data that is not related or necessary should not be collected and stored.

While many European countries implemented tracing apps and other digital solutions to fight COVID-19, this report is focusing on the EaP countries. Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine are important cases to study due to their unique situations in terms of national legislations and institutional capacity as well as integration with the European Union, particularly in the field of Digital Single Market.

All EaP countries have established bilateral relations with the EU in order to deepen mutual cooperation, increase stability and carry out the reforms in the field of digital transformation, including in the data protection field. For instance, GDPR is considered the toughest privacy and security legislation globally, and it imposes strict obligations on collecting and processing personal data. The EU Member States and any other entities that handle data of EU citizens are subject to GDPR provisions, including strict procedures that governments have to put in place to ensure purpose limitation of data collection and principles such as integrity and confidentiality.

The EaP countries have experienced different level of integration and adaptation to GDPR standards[5]: for instance, despite internal political issues, Ukraine[6], Georgia and Moldova have implemented several reforms to pursue the harmonization of national legislation to GDPR standards and data protection, while Armenia, Azerbaijan and Belarus[7] experienced a slower integration due to lack of political interest or the creation of local data protection standards. However, all of the EaP countries have committed themselves through EaP dialogue to regularly take recommendations and implement reforms to comply with the European policies. In particular, the EaP countries are particularly interested in adopting digital instruments harmonized to the EU standards if the harmonization can produce effective and visible benefits to citizens. For instance, by creating "paperless" opportunities for local businesses, increasing administration transparency, and promoting effective e-governance among the citizens.

However, given the pandemic and the course of digital transformation in the EaP countries, the COVID-19 tracing measures pose additional challenges to the protection of personal data and privacy. Indeed, EaP region is highly susceptible to cyber-attacks and their various actors which in the past harvested personal data for fraudulent purposes[8]. Also, implementing legislative instruments and shared procedures to fight corruption at all levels remain a challenge for every EaP government. As a result, efficient human rights and data protection policies are still lacking in the region.

5. EU4Digital Roaming deal one step closer as draft agreement presented to Eastern partners July 1, 2020
6. Council of Europe Newsroom EU and Council of Europe working together to strengthen the Ombudsperson's capacity to protect human rights January 30, 2020
7. Rödl&Partner Belarus will get its own "GDPR" – What companies should prepare for August 12,2019
8. Paper Policy. Hybrid Threats in EaP Countries: Building a Common Response 2019

Definitions

3

Definitions

What are COVID-19 tracing apps and e-services?

For the purposes of this report, one may refer to the legal definition of COVID-19 tracing apps. In Europe there is no widely accepted definition of COVID-19 tracing apps. The European Court of Human Rights has not given any ruling or judgement in this matter so far and the official definition of the notion after reviewing pending applications has not been issued.[9] Nevertheless, the United States of America has quite an impressive legal practice using this term since 2020. The Public Health Emergency Privacy Act (S. 3749) refers to COVID-19 tracing app with regards to any public or private entity that collects, uses, or discloses "emergency health data" electronically or by wire or radio communication, or that develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application "for the purpose of tracking, screening, monitoring, contact tracing, or mitigating, or otherwise responding to the COVID-19 public health emergency."[10] In the context of this report, such an app is devised by the government of a respective country, namely by a Ministry of Healthcare or a Ministry of Digital Transformation (as in Ukrainian case) to track the spread of coronavirus and people who had contacted the infected person. Moreover, the app ensures the self-isolation period throughout lockdown.

Referring to "e-services", the European Commission defines them as "services which are delivered over the Internet or an electronic network involving minimal human intervention, and that are impossible to ensure in the absence of information technology."[11] Thus, e-services include a wider variety of digital instruments such as live statistics, forms, rendering services like doctor appointments to potential recipients of COVID-19 virus or citizens concerned about their health. Some EaP countries did not have a fully-functioning COVID-19 tracing app developed. Instead, they used several e-services to inform its population about the danger of COVID-19 and number of patients. This report is therefore referring to the above-mentioned tools according to the definitions provided.

What are the threats of COVID-19 tracing apps and e-services in the EaP region?

The biggest challenges that are posed by COVID-19 tracing apps and e-services in EaP countries are connected to the fragile democratic institutions. Indeed, many experts[12] pointed out that tracing apps de facto "normalize" state surveillance[13] and pose serious threats vis-à-vis privacy and government transparency.[14] In theory, the use of geolocation data-collecting apps can allow data-sharing only with explicit consent. When a user installs the app, a person is asked to give explicit and informed consent to the collection and sharing of their personal data. However, the range of personal data that COVID-19 related apps collect and share can be very broad and it is difficult for users to understand. In some particular cases, tracing apps may continue to run in the background even in case the smartphone is not in use. Some apps can also exchange information with other apps through application programming interfaces (APIs), generating more detailed information.[15]

First, it is the governments' obligation 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 at high risk of COVID-19 infection. Strengthening law enforcement control over compliance with quarantine restrictions has de facto given them more powers to monitor society.[16]

9. European Union Agency for Fundamental Rights Coronavirus Pandemic in the EU – Fundamental Rights Implications: with a Focus on Contract-Tracing Apps March 21- April 30, 2020
10. 116 Congress 2d Session A Bill to protect the privacy of health information during a national health emergency
11. European Commission Electronically supplied services
12. Experts interviewed in six EaP countries for the purpose of this report. More information about the interviews taken could be found in the individual EaP countries' reports on which this report is based.
13. Carnegie Europe Coronavirus Tracking Apps: Normalizing Surveillance During States of Emergency October 5, 2020
14. Euronews Privacy fears stop us using COVID contact tracing apps. It's not the only reason they've failed August 5, 2021
15. OECD Tracking apps can embody varying degrees of privacy and data protection April 23, 2020
16. Ibid.

At the same time, it should be understood that any restrictions on the rights of citizens imposed to counter the spread of the COVID-19 pandemic must be based on scientific evidence, non-discriminatory, proportionate to the goal and limited in duration. Therefore, in the context of implementing applications for 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, excluding use for any other purpose. Indeed, this personal data cannot be freely transmitted to governmental agencies or any private entities advertising vaccination and stored for a long period of time. The Council of Europe statement reported in the previous section[17] is one of the many documents delivered by international organisations that stress on this feature of COVID-19 tracing apps.

However, tracing apps are not the sole tools that governments used to fight COVID -19. For instance, digital services and communication are also tools that countries widely use to inform citizens and keep them updated on lockdown and healthcare procedures. However, overall EaP region has affected by various level of political instability, given the conflict in eastern Ukraine, protests in Belarus, tensions between Azerbaijan and Armenia etc. Therefore, digital tools also pose serious risk in relation to human rights violation and government abuses. In particular, in various cases the national legislation regulating digital instruments has not been aligned with fully democratic standards and norms that protect citizens from abuses (For example GDPR).[18]

Another aspect to pay attention to is related to the judicial power and how abuses are persecuted in the region. The EaP countries have leveraged the derogation mechanism[19] to the European Court of Human Rights. For instance, Armenia, Moldova and Georgia notified the Secretary General of the Council of Europe that they were invoking this provision to face the ongoing pandemics.[20] Clearly derogation is not illegal and it can been requested by countries in exceptional circumstances.[21] Nevertheless, this example clearly shows that in time of pandemic various states are more prone to create exceptions in relation to common norms that regulate judicial power at the international level. In addition to that, in all EaP countries there is a national legislation on the state of emergency that has been used to implement emergency measures to fight the virus.[22]

Therefore, one can argue that under the current exceptional circumstances, not only the rights of citizens are often restricted, but also the level of judicial protections from court and national and international laws are subject to be weakened. This is obviously not something negative per se, however in fragile democracy this can lead to government abuses, particularly in the digital field, where legislation is often weak or not sufficient to fully protect citizens. Therefore, this report analyses in what ways and to what extent COVID-19 tracing applications and other digital measures that have been implemented in the EaP countries impacted on democracy and human rights.

17. Council of Europe Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe April 28, 2020
18. Lexology Ukraine – The impact of the GDPR outside the EU October 16, 2019
19. EJIL:Talk! Supervision of Derogations in the Wake of COVID-19: a litmus test for the Secretary General of the Council of Europe April 6, 2020
20. Oxford Academic COVID-19 pandemic and derogation to human rights May 4, 2020
21. Verfassungsblog COVID-19 and Derogations Before the European Court of Human Rights April 10, 2020
22. K.A.C. Group Emergency Mode vs. State of Emergency. What are the differences? March 23, 2020

Armenia

4

Armenia

Background

The first case of COVID-19 was registered in Armenia[23] on 1 March[24]. In a bit more than a week the government declared a strict lockdown followed by a state of emergency. With the State of Emergency declaration on 16 March, the Interagency office on the Prevention of CoronaVirus was upgraded and granted increased authority and called the 'Commandant Office', with Deputy Prime Minister Avinyan leading efforts as the 'Commandant'.[25] Moreover, the creation of the Commandant's office received special power in order to put in place social and economic measures to fight the virus under the auspices of the government.[26]

It is also important to stress that Armenia developed national pandemic plans in the past. However, the Commandant's office decided not to activate the plan as it was outdated and had not been revised since 2009.[27] The new national response plan was thus created by using the recommendations of the WHO, under which the Ministry of Health was leading the sanitary response to COVID-19 while both the National Centre for Disease and Control and Ministry of Health are coordinating surveillance communications and international reporting.[28]

Despite Armenia's geographical position and relative isolation from the rest of the so-called "red zones" in Europe, the virus managed to spread extensively making Armenia a high-risk country. Currently, Armenia has one of the highest ratio per capita in the Caucasus region and as of August 22, 2021 236,742 total Coronavirus cases have been registered in Armenia. The intensive expansion of the infection in Armenia has several reasons such as delayed measures implemented by the Commandant's office and the tendency of both citizens and government of not taking the virus seriously.[29]

In the first months of the pandemic the Government's response to this situation was poor in terms of information dissemination and it focused mostly on repressive measures such as lockdowns.[30] This generated a huge wave of disappointment and complaints by media representatives and civil society. However, it is important to mention that after a number of consultations with a wide array of stakeholders the government started to focus more on prevention and digital cases-tracing.

Yet, the COVID-19 situation in Armenia has also generated many problems regarding data protection and privacy issues in Armenia. An amendment authorised the government to gather information available from mobile operators and consolidate them into a centralized database, including the location of users' mobile phones, the phone numbers of people whom they contacted including the start and end times of the communication.[31] The laws essentially gave the authorities access to citizen's cell phone data to track the contacts of COVID-19 patients[32]. The government justified that with the necessity of identifying the circle of contacts of those who test positive for COVID-19 so as to place them under quarantine.

The government clarified that these measures were conducted exclusively within the framework of State of the Emergency declared due to the pandemic. This means that the data gathered from mobile operators was expected to be deleted after the end of the State of the Emergency. However, these measures raised many concerns among the opposition, the Human Rights Defender's Office (HRDO)[33], civil society and the public in general[34].

23. Individual Report Citizens' tracking during and after COVID-19: report on the situation in Armenia September 21, 2021
24. EVN Report Covid-19: Updates From Armenia March 13, 2020
25. COVID-19: Health System Response Monitor Policy responses for Armenia September 10, 2020
26. Egov □□□□□□□□□□□□□ □□□□□□□□□□ March 16, 2020
27. COVID-19: Health System Response Monitor Policy responses for Armenia September 10, 2020
28. The Government of the Republic of Armenia Decisions of emergency commandant August 18, 2020
29. IALS Student Law Review | Volume 8, COVID Special Issue The Impact of COVID-19 Related Emergency Measures on the Democracy and Human Rights in Armenia Winter 2021
30. EVN Report Covid-19: Updates From Armenia March 13, 2020
31. Human Rights Watch Armenia: Law Restricts Privacy Amid COVID-19 Fight. Any Limits Require Human Rights Protections April 3, 2020
32. Individual Report Citizens' tracking during and after COVID-19: report on the situation in Armenia September 21, 2021
33. Human Rights Defender of the Republic of Armenia Legal position of the Human Rights Defender on draft laws restricting the privacy of correspondence and other rights March 31, 2020
34. EVN Report Observations About Armenia's COVID-19 Response July 6, 2020

Armenia

Functionality and Development

It is important to stress that Armenia developed two different versions of the COVID-19 tracing app. The first app developed in March 2020 enabled people to provide information through answering questions pertaining to their health as well as their location and phone number. The questions included in the app were developed by the World Health Organization. The tracing app was developed to relieve the pressure from the COVID-19 testing thus providing opportunities for citizens to "test" themselves.[35]

The second application had a tracing function. It was devised to track social contacts and location of the infected people. However, this app was not very well promoted by the government, so less people used it.

On 19 March, during the government session Deputy Prime Minister and Commandant Tigran Avinyan announced that the country started to work on the developing of tracing app called 'COVID-19 Armenia' which was designed to track cases in the country. He mentioned that the government and the Commandant's office was "envisaging to have a phone app which will enable people to provide information through answering questions, mentioning their location and phone number"[36]. He also remarked that the app will be based on survey developed by World Health Organization and the fact that "Armenians will be able to understand whether they have COVID-related problems and what they should do in this case[37]". After that his advisor made clarifications stating that the app was provided by Iranian developers and was adjusted to local conditions.[38] In fact, the tracing app was developed to relieve the pressure on the testing procedure by providing opportunities for citizens to "test" themselves.

The app could thus have served as a platform for testing which was both less time-consuming and more cost-effective for the country[39]. Nevertheless, several concerns were raised by cyber security experts and human rights activists as the app lacked transparency and the data storage policy was not clear enough. Concerns among cyber security experts as well as human rights activists resulted in a movement with a demand to provide transparency regarding the mode and principles of the operation of the tracing app[40]. On 8 April, the government of Armenia announced that the app had proven successful in finding new coronavirus cases as 1500 users were put in "a red zone", 31 people were isolated, and four were diagnosed with coronavirus after they used the self-diagnosis function of the app.[41]

Specific Threats

Within the framework of this study in Armenia several interviews with experts were conducted to evaluate possible risks related to the use of the app. Interviews have been conducted in a semi-structured way with experts from various fields such as cyber security, political science and civil society.[42]

Cybersecurity professionals expressed their concerns regarding the tracing apps. In particular, one of the experts interviewed said the first app "was neither effective nor safe". The second Armenian app was not used sufficiently. Taking into consideration that it has been used only until August 2020, it can be concluded that the percentage of newly revealed cases is statistically insignificant.[43]

Concerns regarding the tracing apps posing a threat to national security were shared by other experts during the interviews as well. Some of them were not sure how the data collected by the app would have been used. To draw parallels with other COVID-19 tracing apps developed in the EU it is worth mentioning that their functions have been strictly regulated by data protection laws. This idea is shared by another cyber security specialist who not only considers the two tracing apps as violations of human rights but also agrees that it is a direct threat to national security.

35. European Emergency Number Association Covid-19 Apps April 23, 2020
36. Ibid.
37. Tigran Avinyan reports on the tracing app during Government session 19 March, 2020
38. Ibid
39. AntiFake The draft on installing app to use data is a rope around our neck, media expert's opinion, May 24 2020; 2
40. MDI Announcement on providing transparency regarding the personal data processing system, June 6, 2020
41. Jam-news Online app helps American gov detect and monitor citizens infected with April 9, 2020
42. Individual Report Citizens' tracking during and after COVID-19: report on the situation in Armenia September 21, 2021
43. Interview, Individual Report Citizens' tracking during and after COVID-19: report on the situation in Armenia September 21, 2021

Armenia

Apart from expert interviews, an online survey was conducted to reveal public opinion on the use of the COVID-19 tracing apps. 66.7% percent of respondents were aware of the tracing apps. However, only 23.8% of them had installed the app on their devices. 57.1% of potential users considered them dangerous in terms of personal data collection and stressed on possible sensitive personal data leaks to third parties. Respondents to the survey conducted within the scope of this study in Armenia mentioned that COVID-19 tracing apps could lead to human rights violations. However, 42.19 % of respondents think that these restrictions were necessary while 28.6% of respondents think that they were somewhat necessary and only 23.8% regarded them as unnecessary[44].

Conclusions

The situation in Armenia presents human rights and democratic risks related to the adoption of the COVID-19 tracing apps. In particular, the lack of adoption of GDPR had a negative impact on the users' experience of the app. The development of this instrument raised some concerns in citizens and civil society activists regarding personal data protection and democratic development of the country. Nevertheless, data provided by the Armenian government suggest that the tracing app and self-diagnosis instruments had positive effects. Yet, the great majority of people interviewed and surveyed during the study mentioned that they had little interest in these potential benefits of the apps and therefore they barely used these mobile applications.

44. Individual Report Citizens' tracking during and after COVID-19: report on the situation in Armenia September 21, 2021

Azerbaijan

5

Azerbaijan

Background

The response of the government of Azerbaijan to COVID-19 pandemic was instantaneous: the Cabinet of Ministers of the Republic of Azerbaijan adopted two decrees aimed at preventing the spread of the virus and tackling the consequences of pandemic. On 30 January 2020, the Cabinet of Ministers announced the Action Plan 'to prevent the spread of a new disease in the Republic of Azerbaijan'. It was followed by a decision No. 73-1 "On the rules for quarantine-organisation, prevention and other necessary measures in case of a threat of emergence or spread of infectious, parasitic and mass non-communicable diseases"[45].

Due to the high number of positive cases on 24 March 2020, the government adopted a 'special quarantine regime' and imposed multiple severe measures restricting people's freedom of movement. This raised questions of possible privacy violations following the application of obligatory SMS approval system for residents willing to leave their homes. On 12 June 2020, further regulation was introduced requiring those tested positive to the virus to self-isolate at home and commit to being tracked through a COVID-19 tracing application, which enables authorities to verify their location at the place of residence[46].

Therefore, the government of Azerbaijan has developed two platforms, a tracing app called "E-Tabib"[47], and an informative e-service called "Protect yourself against Coronavirus". 'Protect yourself against Coronavirus' platform was developed under the assistance of the UNDP Baku Office.

E-Tabib' was designed to be an application which will inform the users in real-time about the number of patients in Azerbaijan and, at the same time, inform people who were in close contact with the virus.[48] 'E-Tabib' application was created with the assistance of «The Association for the Management of Medical Territorial Units» public entity (TƏBİB).[49]

These services were promoted by the Government among the population, but they did not become commonly used, and the rate of downloads remained pretty low. The reason behind low use of the apps was that they were never deemed as obligatory.

Functionality and Development

As mentioned in the previous sections, two different digital tools were developed in the country. The first platform 'Protect yourself against Coronavirus' was essentially an informative tool for citizens while E-Tabib was a tracing app developed to track and stop the circulation of the virus. [50]

"Protect yourself against Coronavirus" collects basic personal information, such as First Name, Last Name, Email, Phone Number. It was developed to provide first-hand medical advice if a person asks specific questions concerning the symptoms[51]. It was developed by the Ministry of Health in cooperation with the Baku Office of UNDP. The primary aim was to inform the nationals and help them decide whether to seek appropriate medical care. This e-service is available on the website of the Centre for Public Health and Reforms of the Ministry of Health of the Republic of Azerbaijan.[52] It is worth mentioning that the service is not intended to diagnose or treat any disease (including COVID-19) or other medical conditions, but only to inform about potential dangers.

Only people with a full resident status in Azerbaijan could access the app, as it requires a national phone number and some other data accessible to residents only. Also, the platform is not translated into English or any other foreign languages.[53] In the main section of the portal, the platform asks users several questions to determine the level of care required, and based on these answers,recommendations are provided. In terms of data policy, it requires a consent of the user to collect and process personal data.

45. Azərbaycan Respublikası Nazirlər Kabineti Koronavirus (COVID-19) infeksiyasının Azərbaycan Respublikasının ərazisində geniş yayılmasının qarşısının alınmasına dair əlavə tədbirlər haqqında March 30, 2020
46. Azərbaycan Respublikası Nazirlər Kabinetinin 2020-ci il 1 may tarixli 161 nömrəli Qərarında dəyişiklik edilməsi haqqında "Azərbaycan Respublikasının ərazisində hava-damcı yolu ilə keçən yoluxucu xəstəliklər zamanı karantin nəzarətinə götürülmə Qaydaları"nın təsdiq edilməsi barədə" May 1, 2020
47. Reliefweb UNICEF Azerbaijan Country Office COVID-19 Situation Report No. 9 as at 24 June 2020 June 29, 2020
48. Individual Report Citizens' tracking during and after Covid-19: Report on the situation in Azerbaijan September 21, 2021
49. CoronavirusInfo "E-TƏBİB" MOBİL TƏTBİQİNİ YÜKLƏYİN
50. Individual Report Citizens' tracking during and after Covid-19: Report on the situation in Azerbaijan September 21, 2021
51. Ibid.
52. Azərbaycan Respublikası Səhiyyə Nazirliyinin KORONAVİRUS HAQQINDA MƏLUMATLAR

Azerbaijan

On the other hand, E-Tabib is a COVID-19 tracing app. It was developed by the Data Processing Centre of the Ministry of Communications, Transport and Higher Technologies of the Republic of Azerbaijan.[54] Through a system of notifications, the app notifies people whether they were around the potential carriers of the virus based on the information provided to the app. If a person accidentally came in contact with a carrier of the infection (for example, in a queue, in a store, etc.), they would be notified and invited to take a laboratory test[55]. Apart from the notification function, the app showcases the COVID-19 statistics around Azerbaijan and is accessible in terms of contacting the national anti-coronavirus hotline.

The only personal information collected by the app is a mobile number. Once the person inserts a mobile phone number and types the code received, they are presented with "Terms of Use" which consist of 10 Articles[56]. These terms are very basic and enshrine typical legal contractual obligations: intellectual property rights, guarantees, applicable law (the Laws of the Republic of Azerbaijan) and the possibility of unilateral termination.

Since its release in July 2020, E-Tabib has been accused by human rights activities in collecting sensitive personal data[57]. For example, when a user opens the app for the first time, E-Tabib does not ask for an explicit permission to access GPS data, but it has some GPS features integrated[58]. Vusala Mammadova, a famours presenter of the Azerbaijani ITV channel, described her experience of the app as "making me feel more of a criminal than a patient" in a post on Facebook.[59] According to Mammadova, the same day she received a positive COVID-19 test result she also received an SMS stating: "You have Covid! If you leave home, you will carry criminal responsibility!" and several intimidating calls.[60]

Specific Threats

The report on Citizens' tracking during and after COVID-19 in Azerbaijan was based on a population survey and interviews with experts and members of civil society. The report concluded that there are no specific concerns regarding the 'Protect yourself against Coronavirus' platform. The information provided by the users was already in the open access on the Internet and the use of this instrument was based on the fact that citizens are personally concerned about their health conditions and want to receive medical assistance online.

On the other hand, E-Tabib tracing app raided much more concerns. Firstly, there are a lot of discrepancies between the information provided on a webpage of the app (which is visible to the public eye) and the actual policy of the app which is stated in Terms of Use[61]. It is expressly stated on the website that the "E-Tabib application does not collect any personal information other than your mobile phone number"[62]. Nevertheless, Article 5.1 explicitly sets forth that the app collects ID number and information about location[63]. That means that citizens are not aware which information is collected and processed, and they are also not aware of any potential misuse of such information by the governmental bodies.

Secondly, the Centre for Public Health and Reforms of the Ministry of Health of the Republic of Azerbaijan possesses the right to disclose personal information. This poses a serious threat for citizens as the data collected may be used by third actors to track the location and the habits of citizens and it is a clear violation of the EU GDPR policy and the right to privacy.[64]

53. Ibid.
54. COVID-19: Health System Response Monitor Police responses for Azerbaijan June 14, 2021
55. CoronavirusInfo "E-TƏBİB" MOBİL TƏTBİQİNİ YÜKLƏYİN
56. Etabib Müqavilə June 26 2020
57. Individual Report Citizens' tracking during and after Covid-19: Report on the situation in Azerbaijan September 21, 2021
58. Ibid
59. https://www.facebook.com/vuss.m/posts/10220096782224485
60. OCmedia Claims of false accusations dog Azerbaijan's anti-Covid app December 16, 2020
61. Faktoxla E-Tabib illigaly collects personal information July 7, 2020
62. CoronavirusInfo "E-TƏBİB" MOBİL TƏTBİQİNİ YÜKLƏYİN
63. Faktoxla E-Tabib illigaly collects personal information July 7, 2020
64. Etabib Privacy Policy May 16, 2020

Azerbaijan

Thirdly, the development of the app raises concern on the policy on keeping personal data. Personal information is saved for the duration of one month even after the termination of the contract and deletion of the application.[65] Thus, personal data may be transferred to third parties inside or outside the Republic of Azerbaijan even after the individual user had cancelled the app.

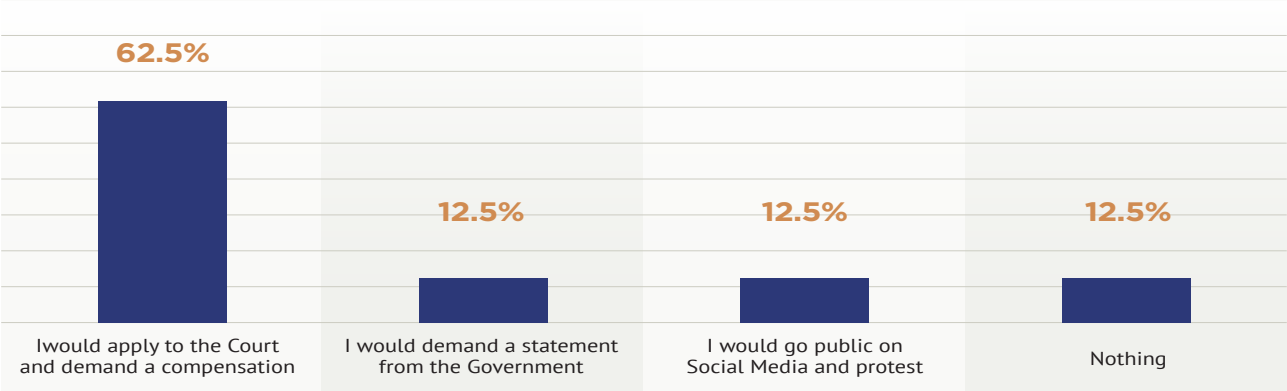
It is also crucial to stress that in a survey submitted to 80 citizens of Azerbaijan about privacy concerns (Table 1), 62,5% of people stressed that in case of a privacy breach they would apply to the court, 10% would demand statement from the government, and another 10 people (12,5%) emphasized that they would go publicly protest[66]. This means that the great majority of Azerbaijani citizens are sensitive to the topic of personal data and privacy. Thus, this topic can potentially raise political tensions in the country.

Conclusions

The app E-Tabib presents several issues related to the misuse of personal data and scope of the app in Azerbaijan. In particular, there are concerns on how the app was developed and in what ways and to what extent public authorities can access the data. Considering that there are several issues related to law enforcement[67] and data on cybercrimes are poorly collected[68], the adoption of such instruments have negative impact on human rights and democratic development of the country. Indeed, the data illegitimately collected through the app could potentially be used to monitor and map citizens' political opinions as well as other sensitive data related to their health and social situation. Moreover, the country lacks a proper legislative procedure that can be used by citizens to report abuses of the government or anyone else involved in misuse of personal data that can be shared by the app or any other digital instruments.

One of the solutions could be the adoption of stricter rules and conditions of the app in line with GDPR users. Also, more transparency about the data processed by the Centre for Public Health and Reforms of the Ministry of Health of the Republic of Azerbaijan could ensure a more positive experience for user and legal accountability in case of future misuse of the processed data.

Table 1.
Results of the survey conducted in Azerbaijan



65. Ibid.
66. Individual Report Citizens' tracking during and after Covid-19: Report on the situation in Azerbaijan September 21, 2021
67. Azerbaijan Human Rights Centre together with the International League for Human Rights and the World Organization against Torture Compliance of the Republic of Azerbaijan with the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment and Punishment April 28-May 16 2003
68. OSAC Azerbaijan 2020 Crime& Safety Report June 5, 2020

Georgia

6

Georgia

Background

Soon after confirmation of the first case of COVID-19 in the country (26th of February 2020), Georgia announced a state of emergency across the country and imposed various restrictions. On 16 March, the spokesperson of the Government of Georgia Irakli Chikovani announced special measures to fight the pandemic such as the suspension of free movement and access to the transport services and a limitation of social interaction through local curfews.[69]

In order to prevent uncontrolled expansion of disease in the country, a state of emergency was declared throughout Georgia on 21 March, which was approved by Parliament of Georgia compliant with the rules and procedures determined under constitution.

During the state of emergency, some of the basic human rights were suspended to avoid social interaction and thus, mitigate widespread infection across the country.[70] The new regulations introduced limits to schooling and education and the municipalities with the highest rate of incidence cases were declared as quarantine zones.[71]

The restrictions imposed by the government became stricter with the growth of confirmed cases in late March/ early April 2020 when a strict «lockdown» was announced and a curfew introduced. The state of emergency lasted for three months and several restrictions were gradually lifted at the end of May 2020, while most of the restrictions were removed until the end of November, when new restrictions were imposed to fight the so-called second and then the third waves of COVID-19.

Functionality and Development

In order to keep the population informed during the emergency period, the government disseminated information via SMS to everyone in Georgia to keep the population updated about measures and recommendations to fight the virus.[72] In addition, to ensure the availability of information on epidemic situations and related decisions, measures and restrictions, the government of Georgia developed a unified platform-STOPCOV.GE, where all the information about Covid19 situation was published.[73]

In addition to the traditional measures for mitigating the spread of the virus, the government of Georgia introduced a COVID-19 tracing app with the aim of simplifying tracking of contacts and getting better control on monitoring the epidemic situation in the country. The tracing application named "STOP COVID" was introduced in April 2020 by the Technology Department of the Ministry of Health. The information about the availability of the application was published on official webpage-STOPCOV.GE, and was available for Android as well as for IOS users.

In terms of development, the application STOP COVID was developed by the Austrian NGO NOVID20, in cooperation with the Austrian software company Dolphin Technologies. The application replicated the system of a similar French App with minor differences[74]. The Georgian App used Bluetooth and GPS technologies for investigating contacts who had exposure with Covid19 infected persons. Another important detail is that the application did not require a formal user registration.[75]

The application design provided several security tools to ensure privacy of users' data, in particular, each user was given a unique ID. A strong encryption mechanism was used to ensure anonymity of data. Moreover, the application was based on a decentralized data storage mechanism which means that all information acquired by STOP COVID was stored in the user's phone. This enables customers to have control over any information and decide what type of information to share via the app.

69. Caucasus Research Resource Center Webhomeh x Settype
70. Government of Georgia Measures implemented by the government of Georgia against Covid-19 Report
71. UNICEF UNICEF Georgia COVID-19 Situation Report June 21, 2021
72. Netgazeti მთავრობა: აუცილებელი საჭიროების გარეშე სახლიდან არ გახვიდეთ March 16, 2020
73. Government of Georgia Measures implemented by the government of Georgia against Covid-19 Report
74. Government of Georgia Georgian StopCovid App becomes hugely popular on the French AppStore May 5, 2020
75. Individual Report Citizens' tracking during and after COVID-19: Report on the situation in Georgia September 21, 2021

Georgia

In particular, users could voluntarily report if they were infected by COVID-19 and share their geolocation to warn other people. Nevertheless, a study found out that STOP COVID could potentially keep data for 3 years, which is the longest period of all the apps analysed.[76] Also, the Georgian app was among the apps that collected the most personal information from the users.[77]

Specific Threats

The country report on Georgia[78] showed that STOP COVID did not have any significant sign of critical non-compliance with the protection of users' privacy and personal information, mostly because the Georgian legislation on privacy and data protection has been developed in line with the EU standards. In particular, the data protection legal framework in Georgia has been largely harmonized with the EU's ePrivacy Directive (Directive on Privacy and Electronic communications (Directive 2002/58/EC)) and the General Data Protection Regulation.

Thus, Georgia has a national Law on personal data protection that provides a legal foundation for securing human rights and freedoms, including the right to privacy, in the course of personal data processing. The law prohibits processing of special category data containing personal information (e.g. political attitudes, private lives, etc), unless the data is necessary to be processed for public health protection, health care or protection of health of a natural person by an institution (employee), and if it is necessary to manage or operate the health care system. (article 6. 2(c)). Therefore, the data collected by the App could be legally used only within the purpose of fighting the pandemic.

However, according the country report on Georgia, the major challenge for democracy and human rights with regards to the COVID-19 tracing app is the long storage period of personal data (3 years). Also, the app collected a lot of sensitive data about users, including information about their family, health conditions and geolocation. If breached, this personal data could be used for many illegal purposes against citizens and the country as a whole.

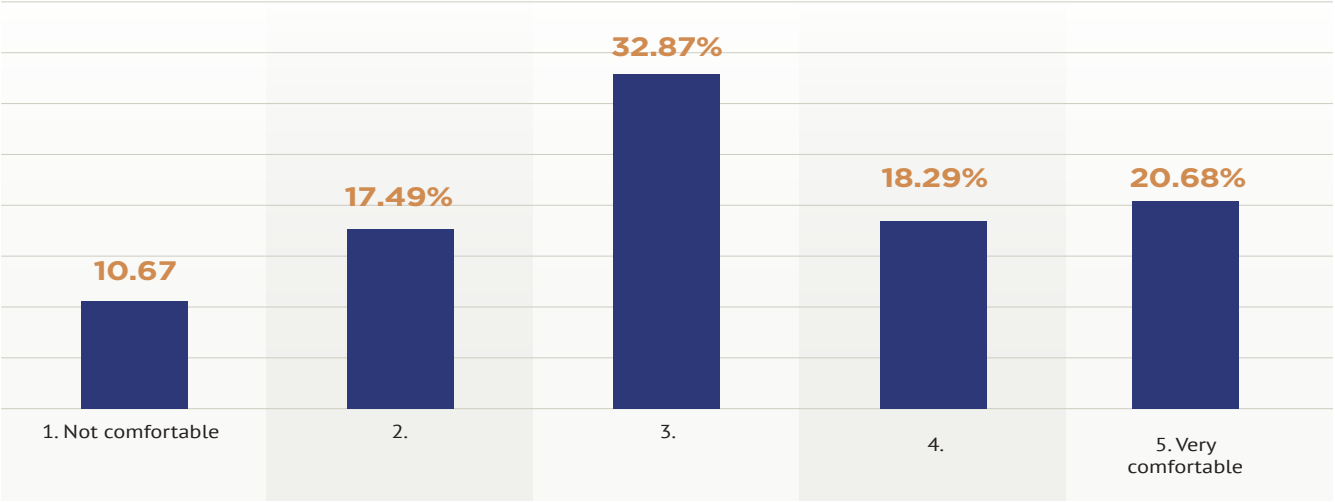
Also, the report claims that the data on the users are not sufficient to estimate a satisfactory level of tracking through the app. According to information provided by the Ministry of Internally Displaced Persons from the Occupied Territories, Labor, Health and Social Affairs of Georgia (MoLSHA), the application was downloaded by 295,991 users, which represent 8% of the total population of the country. However, detailed statistics about the number of users who deactivated the application is not available in official databases. According to the information provided by MoLSHA, the application recorded a total of 11,437 possible cases. However, this does not mean that these cases were detected by STOP COVID and only indicates how many people have detected its infection voluntarily.

Lastly, the level of satisfaction of the users is also quite low. A quantitative survey conducted within the framework of this study (Table 2) showed that around 33% of the STOP COVID users provided a neutral opinion in terms of usability, while only around 39% of respondents assessed the use of the app as comfortable or very comfortable to use. However, 68% of surveyed respondents indicated that they would not recommend the app. The feedback from the users of app shows that the application itself was not inconvenient to use did not see the clear benefits of using STOP COVID app for detecting the infection spread.

76. Elkhodr M, Mubin O, Iftikhar Z, Masood M, Alsinglawi B, Shahid S, Alnajjar F Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search and Content Analysis J Med Internet Res 2021;23(2):e23467
77. Ibid.
78. Individual Report Citizens' tracking during and after COVID-19: Report on the situation in Georgia September 21, 2021

Georgia

Table 2.
Evaluating the Usability and Convenience of STOP COVID App



Conclusions

In conclusion, the Georgian STOP COVID was certainly an app that had a clearly a Covid-19 purpose and thus could potentially help citizens to track their contacts. However, its effectiveness in terms of tracking was limited by the low number of users and the lack of perceived utility by Georgian citizens. Moreover, the app presented some minor issues that could potentially lead to privacy and data protection challenges. However, as the Georgian legislation has been aligned in the past with the EU standards, the report does not show any potential data protection or democracy threat linked to the STOP COVID app.

Moldova

7

Moldova

Background

The SARS-COVID19 virus was confirmed to have reached Moldova on 7 March 2020, when a Moldovan citizen resident in Italy was tested positive.[79] Since the beginning of the pandemic in Moldova, the Parliament has voted twice for the introduction of the state of emergency and has delegated to the Commission for Emergency Situations the authority to regulate COVID-19 situation in the country. The state of emergency was established between 17 March and 15 May, 2020 during the first wave[80] and between 1 April and 30 May, 2021 during the second wave.[81] However, the emergency status was cancelled by a Decision of the Constitutional Court from April 28th, 2021.

Despite the emergency status and ongoing efforts to handle the pandemic, the government was criticised for the way it was handling the crisis.[82] In particular, several accusations were raised in relations on how the Government ensure correct and professional collaboration with media institutions, refraining from unfounded accusations and insinuations against journalists who request public interest information.[83]

Another element of criticism is related to the testing procedures adopted by health organizations. In the early stages of the pandemic the Republic of Moldova tested only symptomatic people while asymptomatic people were not being tested. In later stages, individuals who have come into proven contact with infected people were not tested nor informed about potential risks.[84]

Digital tools to fight COVID-19 in Moldova

The Republic of Moldova did not introduce any COVID-19 contact tracing tool. According to the WatchDog.MD report, a tracing app was not used largely due to lack of competence and interest from the authorities[85]. This situation might also be linked to the above-mentioned testing issues, as a tracing app can be effective only if the testing procedures are reliable. The only digital response measures applied in Moldova were purely informative.

WhatchDog.MD noted that one of the measure taken was the activation of the ArcGIS COVID-19 online platform, which presents the latest numbers of COVID-19 cases in the country. The information on the platform is presented in Romanian and Russian, and it contains the data on the number of confirmed and suspected cases of infection, the number of deaths and the number of people that have recovered. The data is disaggregated by age, sex, geographical location, time of case registration (day/month), and the confirmed cases among pregnant women. The platform also shows the number of accumulated views. However, the platform has a cumbersome name and has not been widely promoted to the extent to be used by the general public as an information tool.

Another digital method used by the authorities was to send short text messages warning the citizens to call a doctor if they have symptoms such as «fever or cough».[86] The message informed about the obligation to respect the quarantine for those who came from abroad and urged everyone to stay at home. Shortly after then Minister of Health, Viorica Dumbrăveanu, said that the text messages were part of an extensive information campaign.[87] The Minister also added that the text messages were sent due to a collaboration with the mobile operators and that «neither the Ministry of Health nor the Government owns the telephone numbers''. However, the WatchDog.MD report shows that there are several issues related to storing personal data and the information campaign performed by the Moldovan government, including severe restriction of media freedom and access to clear and reliable information[88]. Therefore, despite the digital communication performed by the government, the digital instruments adopted were not

79. World Health Organization Republic of Moldova Situation
80. Privesc Declarații de presă după întrevederea Președintelui Republicii Moldova, Igor Dodon, cu conducerea de vârf a țării
81. Media-azi Cum a reușit celula de criză a jurnaliștilor să solidarizeze breasla pe timp de pandemie June 22, 2020
82. BalkanInsight Moldova Authorities Accused of Lacking Transparency About Pandemic March 23, 2020
83. Ibid.
84. European Observatory on Health Systems and Policies COVID-19 Health System Response Monitor (HSRM) December 15, 2020
85. Individual Report Citizens' tracking during and after COVID-19: Report on the situation in Moldova September 21, 2021
86. Council of Europe Digital Solutions to Fight Covid-19. 2020 Data Protection Record October, 2020
87. Radio Europa Libera Moldova Coronavirus: audieri în Parlament, mesaje SMS și scanere la graniță February 27, 2020
88. Individual Report Citizens' tracking during and after COVID-19: Report on the situation in Moldova September 21, 2021

effective to keep the citizens properly informed about the risk of the pandemic and the regulations adopted.

Specific Threats

Paradoxically, the decision of not implementing a tracing app might have had beneficial consequences. Indeed, while the importance of the right to personal data protection is recognized (in particular Article 28 of the Constitution which provides the right to intimate, family, and private life) and the country had adopted several legal acts based on the EU standards (such as the National Law No. 133 of 8 July 2011 on Personal Data Protection[89] which is based on the EU Directive 95/46/EC on data protection and storage of data[90]). However, its application is still not fully enforced.

For example, the violation of data protection regulations in Moldova is not prosecuted. Moreover, personal data protection legislation is still not fully enforced by public authorities.[91] Additional challenges are also represented by the Transnistrian de facto authorities: in 2020 the self-proclaimed government of Transnistria has announced it would use facial recognition to identify people who break quarantine.[92] However, these instruments were never implemented in the territory of Moldova under the full control of the Chisinau's government.

Conclusions

Thus, the adoption of a tracing app could have led to potential threats for Moldovan citizens, particularly in terms of sharing of sensitive personal data with third parties. The country still lacks effective data protection regulations, mostly due to the lack of political willingness to enforce regulations that are already adopted by the national legislation[93]. For instance, the abuse of facial recognition can be a serious threat for the democratic consolidation of the country, especially if the abuses are linked to the political situation in the region of Transnistria where the law enforcement is particularly problematic. One example of such issue was the use of facial recognition procedures that took place in Transnistria during the lockdown. Despite their limited during an emergency situation related to the COVID-19 virus, the abuses of facial recognition devices could potentially have dramatic human rights impacts for all the citizens of Moldova.

Moreover, the lack of information and the poor digital information campaign performed during the COVID-19 pandemic by the public authorities proved the lack of government's capacity to introduce e-services. Indeed, the above-mentioned challenges can prevent the country from fully benefiting from digital transformation.

89. DataGuidance Law No. 133 of 8 July 2011 on Personal Data Protection
90. DataGuidance Data Protection Directive (Directive 95/46/EC)
91. Anticoruptie Despre protecția datelor se vorbește foarte mult, însă și mai mult se duce în eroare, decât să se ofere soluții corecte January 28, 2020
92. Новости Приднестровья Нарушителей самоизоляции выявляют с помощью системы распознавания лиц March 28, 2020
93. Individual Report Citizens' tracking during and after COVID-19: Report on the situation in Moldova September 21, 2021

Ukraine

8

Ukraine

Background

A day after the WHO announced COVID-19 pandemic, the government of Ukraine adopted a nation-wide quarantine on 12 March 2020. At that time, there were only three confirmed cases of the virus in the country[94]. However, the Government of Ukraine had serious concerns for the situation of Ukrainians living abroad. When strict lockdowns were approved in many EU member states, the government of Ukraine issued several statements to prevent the return of thousands of Ukrainian labor migrants.[95] In particular, the President of Ukraine Volodymyr Zelensky made an urgent statement to suspend air traffic from and to Ukraine starting 16 March 2020. Later, the National Council of Security and Defense of Ukraine ordered the close of the air space for commercial flights at 00.00 on 17 March 2020[96]. On 20 March there were 41 confirmed cases, and local governments of Ukrainian regions started introducing emergency measures to contain the virus. In four days, the measures were expanded to the territory of the whole country.

During the quarantine period (which lasted until May 2020), the government of Ukraine decided to continue the implementation of its digital transformation strategy. Such government-lead initiative was proclaimed by the President Zelensky in order to expand digital services available for Ukrainian citizens which became even more important during the pandemic.[97] A key pillar of the strategy was the development of the the Diia Portal, a unified portal for governmental services which is accessible on personal devices. The reinforcement of the Diia Portal was part of the governments' campaign "State on a Smartphone" which president Zelensky announced in early 2020.[98] A significant support to the "State on a Smartphone" campaign was also provided by EU member states (namely Estonia and Sweden) which helped the government of Ukraine to harmonize several e-governments instruments to the EU standards.[99] Thus, at the edge of the coronavirus emergency Ukraine was in a very particular situation: on the one hand the country was in the process of providing more digital services to its citizens and on the other hand, the Ukrainian government was trying to harmonize different digital practices through an effective bilateral cooperation with EU member states.

This unique position turned out to be very effective to provide digital tools to citizens during the pandemic. For instance, in terms of functions, the Diia Portal was created as a platform with multiple services available for citizens (around 50 governmental services and nine digital documents, such as ID card and a birth certificate are available on the portal[100]). The portal was also connected with a specific mobile app that allowed users to access documents and individual data directly on their smartphones. As a result, during the quarantine Ukrainian citizens could apply for unemployment benefitsand or file a request for financial assistance directly through the Diia Portal.[101] Indeed, citizens could download the Diia Portal app from Google Play Market or App Store and get a digital authorization to access their data through a Bank ID or electronic signature.[102] Clearly, the access to Diia Portal was extremely popular during the lockdown and in 2021 it was reported that almost 10 million people used Diia instruments.[103]

Moreover, the government of Ukraine decided to expand the Diia Portal and create an additional tool to track the cases of infections in the country: the app "Vdoma". Vdoma is dedicated to the control and support of citizens during the regime of self-isolation through specific features that monitor and track the behavior of the users[104]. In April 2020, Vdoma was declared obligatory for any individual arriving

94. Zaxid.net Історія хвороби. Як ми прожили перший рік глобальної пандемії March 11, 2021
95. OpenDemocracy The pandemic has returned migrant workers to Ukraine. Will they stay? June 24, 2020
96. Finbalance РНБО:Україна закриває кордон для авіаційного, залізничного та автобусного сполучення March 14, 2020
97. Atlantic Council Covid crisis accelerates Ukraine's digital revolution February 10, 2021
98. The Ukrainian Weekly Zelenskyy administration launches "State in a Smartphone" app February 14, 2020
99. ERR Feature | How Estonia is helping Ukraine develop e-governance September 4, 2020
100. The Ministry of Digital Transformation. Diia Portal , May 17, 2021
101. Урядовий портал Оформити допомогу по безробіттю тепер можна онлайн на порталі «Дія» April 25, 2020
102. Ibid.
103. Ukrinform Ministry of Digital Transformation: Every fourth Ukrainian uses 'Diia' app May 17, 2021
104. Individual Report Citizens' tracking during and after COVID-19: Report on the situation in Ukraine September 21, 2021

Ukraine

from a "red zone" country. Later in 2021, the app was made mandatory for more categories of citizens. As of today (September 2021), Vdoma must be downloaded for most of the residents and travelers within the territory Ukraine.

Functionality

The app Vdoma was developed in four days by the Ministry of Digital Transformation of Ukraine, in cooperation with the Ministry of Health of Ukraine, the Ministry of Internal Affairs, and the Public Health Centre of the Ministry of Health[105]. The fast development of the app raised several issues, particularly in terms of and personal data protection and cyber security[106].

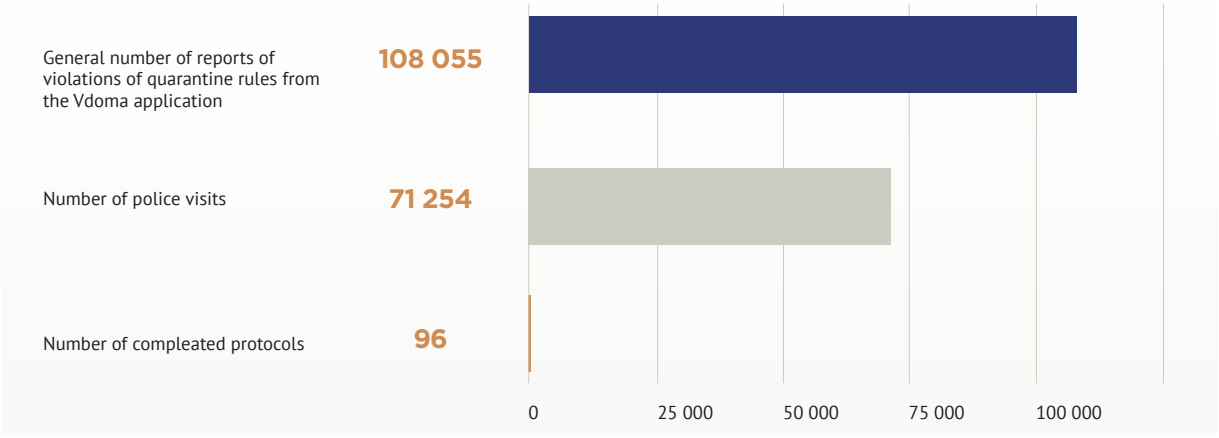
Indeed, the app requires the users to upload a reference photo during the registration. Moreover, every user must give the permission for the geolocation of the phone at the moment of taking a photo.[107] This is aimed at verifying the correct application of the regime of self-isolation. In case the user of Vdoma is requested to self-isolate, they can get a push notification at a random hour on the phone. After receiving the notification, the user is obliged to take a photo of a face to prove its location.[108] If the user fails to upload a picture within 15 minutes or the app detects any discrepancy in the geolocation and/or in the uploaded picture, the person is automatically considered not in compliance with a self-isolation regime and thus can be persecuted.[109] Indeed, there were many cases of violations of the quarantine regime detected by the app and later recorded by the police (Table 3).

Risks for democracy

Vdoma requires several authorizations from the users, such as the access to the location through GPS and mobile data, and the access to the camera. Thus, the collected data are substantial in terms of quality and quantity. Clearly, the misuse of such data can have a strong impact on the democratization process of Ukraine as the law enforcement remain dramatically low in the country.[110] Any incorrect use of the data is therefore hardly persecuted, particularly if the misuse is related to vulnerable groups.[111]

Another issue is related to the transfer of the data between different entities. Under Article 7 of the law "On Protection of the Personal Data", any biometric data should be considered as sensitive[112]. As installing the Vdoma app is

Table 3.
Statistics on notifications generated by the Vdoma application



105. Ibid
106. Ibid
107. The Page Selfies, ineffective technical support and termination of self-isolation: what is wrong with Dii Vdoma mobile app April 26, 2021
108. Ibid.
109. USAID, Freedom House, Truth Hounds, PROgress, ВостокSOS Human rights in Eastern Ukraine during the coronavirus pandemic February 8-12, 2021
110. CMI Police in Ukraine: corruption versus reform 2020
111. Ibid.
112. Law "On Protection of the Personal Data", Закон України про захист персональних даних August 14, 2021

Ukraine

no longer optional for many categories[113], it is crucial that the data are processed by health-related authorities and collected exclusively for scientific and medical reasons[114]. The Government of Ukraine has constantly reported that Vdoma has been collected data only for medical purposes as mentioned in the description of the app on the official website.[115] However, currently it is impossible to find out if these regulations were properly met. On the contrary, several analysis report that it is impossible to guarantee that bad practices are not applied[116] or personal data are not used by the National Police of Ukraine for their own needs.[117]

Another potential risk is related to the lack of security. The app has been declared as secure by the Ukrainian government, but the report shows[118] that there was no cyber security audit of the app conducted by independent experts.[119] This is also linked to the fact that Vdoma app was developed in only four days. In case there are no security protocols fully implemented in the app, the obligatory nature of the app poses a considerable threat to personal data protection[120]. Moreover, despite the government declared that the app is safe and secure, many users experienced troubles using the app and many others feel insecure about the app itself.[121]

Conclusions

The Vdoma app was introduced with the aim of fighting the spread of COVID-19 in Ukraine. The Ukrainian government has also conducted an intensive digital development reforms strategy supported by the EU. Nevertheless, the app has raised several issues, particularly related to the fact that users have little control of inputs (e.g. upload of pictures) and the principle of accountability has not been fully respected in relation to the store and use of data.

This poses crucial risk for the democratic development of Ukraine. First, the app has not been fully audited by independent cyber security experts. As a consequence, it is unclear whether the data of the users are fully protected and not misused by any state authorities. It is therefore recommended for the to conduct independent cyber security audits in order to track any vulnerabilities of the app, as well as conduct an evaluation of the compliance of Vdoma to GDPR.

Second, law enforcement in the country remains dramatically low. COVID-19 tracing app remains problematic as it is unclear how the data of users are processed and used. This situation can easily lead to abuses as pictures, data and geolocation of citizens can be accessed by public bodies (or even third parts) in ways that are not in line with the goals of the app and the emergency context in which it was launched. For instance, in theory it is quite simple to collect sensitive information of citizens through pictures and any inputs that they are obliged to upload on Vdoma. In a worst case scenario, this data can also be used to track political orientation of citizens or map political minorities and vulnerable groups. Clearly, the exploitation of data processed by a tracing app can easily be used to manipulate or negatively influence the democratic development in the country. There were no reported cases of using this data in such purposes so far, but most experts interviewed during this study in Ukraine mentioned that such manipulations are very likely to take place in the long-term perspective, such as the next elections[122].

113. Visit Ukraine Now
114. Human Rights Watch Human Rights Dimensions of COVID-19 Response March 19, 2020
115. Hromadske International Love it or Hate it, Ukraine's Self-Isolation App "Dii Vdoma" Already Has 200K Users. And a Few Bugs July 29, 2020
116. Institute of Innovative Governance Citizens' tracking during and after COVID-19: Report on the situation in Ukraine September 21, 2021
117. Remonews The police see everything. How Ukrainians cheat VDOMA app- Ukraine news September 14
118. Institute of Innovative Governance Citizens' tracking during and after COVID-19: Report on the situation in Ukraine September 21, 2021
119. Ibid.
120. Ibid.
121. Hromadske International Love it or Hate it, Ukraine's Self-Isolation App "Dii Vdoma" Already Has 200K Users. And a Few Bugs July 29, 2020
122. Institute of Innovative Governance Citizens' tracking during and after COVID-19: Report on the situation in Ukraine September 21, 2021

Belarus

9

Belarus

The context of Belarus is very particular, due to the ongoing political demonstrations against the Belarusian government and President Alexander Lukashenko, particularly during and after the 2020 presidential elections. Therefore, the outbreak of COVID-19 pandemic was not the only shuttering experience for Belarusians in 2020-2021.

The turbulent political times have contributed to a major negligence vis-à-vis COVID-19 measures.[123] The authorities of Belarus did not develop an adequate response to the pandemic and President Lukashenko made several bizarre statement on the existence of the COVID-19.[124] Also, media minimised the risks related to the pandemic and as of today state authorities continue report unreliable information about the limited risks of COVID-19. As a result, the official figures of cases and deaths in the country are not accurate and they generally lack of any scientific credibility. Yet, some unofficial data report that the undocumented cases are among the highest in Europe and in the world[125].

As a result, the COVID-19 response policy in Belarus was totally insufficient and almost non-existent as the authorities provided very little information to Belarusian citizens[126]. It is therefore not a surprise that public institutions did not develop any COVID-19 tracing instrument and digital service to fight the virus. Nevertheless, within the context of this study, a focus group was organized to evaluate the level of trust in state agency and in a hypothetical tracing strategy developed by the Belarusian government.

Most of the respondents in the focus groups recognized the importance of COVID-19 tracing apps but the great majority of them were against its application in Belarus. The reasons reported were different and included the specific political situation that Belarusians faced in 2020-2021. Also, some of the respondents mentioned that the poor health management of Belarus in general and the people's understanding of the dynamic of the virus would have prevented the app to be useful. For instance, the lack of economic assistance provided by the government would have made a hypothetic tracing app totally not effective and people would not had followed the information provided within the app.

Also, the repressive atmosphere would had contributed to not trusting tracing digital instruments or any kind of informative digital services. Belarusian respondents claimed that a COVID-19 tracing app could potentially be used to track people's location and collect data about their political opinions and views on Lukashenko's regime. Thus, the risks related to a tracing app were very well understood by the civil society and citizens participating in focus groups. Moreover, citizens and civil society members interviewed in Belarus pointed out to possible misuse of data collected by COVID-19 tracing apps in a non-democratic political context.

123. Radio Free Europe 'Damage Was Done': Belarus, Where Lukashenka Dismissed COVID-19, Now Struggles To Vaccinate June 28, 2021
124. Ibid.
125. East Center Project, September 15, 2021
126. UNDP 3 lessons we learned from our COVID-19 response in Belarus January 15, 2021

Conclusions

10

Conclusions

COVID-19 and its consequences for public health, digital human rights, and democracy were an enormous challenge for the whole world, including the EaP countries. The countries in the region has certainly adopted different strategies to deal with the consequences of the pandemic but digital tools were certainly one of the main way adopted to inform citizens, provide services and track cases of infections. The comparative analysis of this report has shown that there are serious issues related to digital human rights and democracy caused by tracing apps and e-services in EaP countries introduced during COVID-19.

The EaP countries experienced major difficulties in the development of tracing app instruments. In particular, the effectiveness and security of many digital instruments adopted in EaP countries are questionable as it is not clear if they could be used exclusively for managing COVID-19 pandemic and are proportional to its purpose. Moreover, most COVID-19 tracing apps and other e-services developed during COVID-19 pay little or no attention to personal data protection, transparency, cyber security and possible abuse of sensitive data for undemocratic purposes. The issues related to tracing apps in the EaP countries are only partially related to COVID-19. Indeed, tracing app are not negative instruments per se. However, the amount and quality of data that they collect require public authorities to ensure a good level of transparency and accountability, particularly within public institutions. However, in the EaP region abuses related to law enforcement and lack of transparency remain significant. The specific situation of the EaP region in terms of legislation and practices in the public sectors (e.g. corruption, lack of transparency etc.) make extremely problematic to persecute any kind of exploitation of personal data.

First of all, the adoption of data protection legislative instruments such as GDPR in the EaP countries is still insufficient or incomplete. While enhancing the right to data protection in Eastern Partnership countries remain a key top priority for many governments in the region, the pandemic and the adoption of tracing apps have shown that in emergency situations national authorities struggle to fully implement or enforce data protection instruments. The lack of shared and transparent standards has obviously strong negative consequences on the level of citizens' trust in new technologies adopted by state authorities including tracing apps and e-health services.

Second, the lack of information about potential risks related to data breach and digital personal information is quite high in the EaP countries. In particular, both citizens and state authority largely ignore the risks of not having elevated standards for data protection within state authorities. This situation contributed to many issues related to tracing apps during the pandemic. For example, the requests of public opinion to ensure transparency and accountability of tracing app's data processing were quite low in every country that adopted such app. One could argue that the emergency situation related to COVID-19 was something totally unexpected and thus it is understandable that tracing apps were not perfect. However, governments in EaP should aim at developing a cyber-resilient society, where the level of information provided to citizens and the tools adopted by state authorities are always meeting certain standards. In particular, its governments' responsibility to ensure that citizens are both ready to prepare and prevent adverse cyber events and personal data leaks. Thus the adoption of apps and instruments that are not compliant with transparency and accountability standards contribute to the lack of achieving a cyber-resilient society. Moreover, considering the emergency situation, it also crucial that citizens have the opportunity during the COVID-19 crisis to engage with a public authority acting as data controller which has the

Conclusions

responsibility to keep and process their digital records and data. In this way, citizens can also be sure that the principle of accountability is fully respected.

Third, data collected by COVID-19 tracing apps could be used in purposes other than COVID-19 especially in countries with weak institutions. Most experts and citizens interviewed or surveyed in EaP countries pointed out that they do not trust the governments in storing their personal data, especially data related to health. Such data could be used to trace citizens' whereabouts not related to COVID-19 or in other political purposes. Therefore, COVID-19 tracing apps should have a strict time and scope limits and should be dismantled as soon as the pandemic is over.

Last, the level of engagement between state authorities and civil society is very low and only a small number of experts and civil society members in the EaP region have raised the concerns posed by digital instruments, including COVID-19 tracing apps during COVID-19. However, it crucial that civil society and governments engage more on these topics. Indeed, civil society should both provide more information to general public about potential risks on data protection, cyber security and democracy as well as monitor potential threats related to the implementation of digital solutions of any kind, including tracing apps. Also, national and regional governments must put in place adequate measures to ensure that citizens can effectively express their concerns or report potential issues related to their data protection or privacy. Indeed, providing transparent information on any digital tools adopted at the state level should be a key priority for any government interested in creating a cyber-resilient and democratic society that can effectively overcome unexpected challenges such as COVID-19.

Recommendations

11

Recommendations

Following the comparative analysis of the EaP countries in relation to digital solutions and tracing apps during the COVID-19 outbreak and subsequent lockdown policies, there are a number of recommendations to different stakeholders:

Recommendations to the EaP countries' governments:

1. Harmonize national and local legislation to EU Standards, in particular EU's ePrivacy Directive (Directive on Privacy and Electronic communications (Directive 2002/58/EC)), and the General Data Protection Regulation.

2. Engage with EU partners in order to get adequate support to implement positive and transparent reforms in the field of data protections and e-services.

3. Provide clear and accessible information on any digital tools used during the COVID-19 pandemic, including tracing apps. As for the tracing apps, the data provided should include number of downloads, number of current active users, number of tracked cases.

4. Ensure an appropriate level of security by technical and organizational measures in implementing any COVID-19 tracing systems.

5. Put in place adequate measures to ensure the principle of lawful processing of data. In particular, the data collected with COVID-19 related instruments should be processed lawfully, fairly and in a transparent manner and only in relation to explicit and legitimate health related issues.

6. Ensure mechanism by which data collected by tracing app cannot be further processed by third parties, or in a way that is incompatible with the specific COVID-19 purpose the app or the tool has been developed.

7. Designate a data controller (e.g. the relevant authority) who is obliged to keep a record of all the data processing activities and provide channels by which citizens can access their own data during the COVID-19 emergency period.

8. Engage with citizens and civil society in order to keep a transparent and positive approach when introducing new digital instruments of any kind in order to address potential issues related to privacy, data protection and accountability of body structure.

9. Provide training and information to law enforcement bodies and officers about data protection and cybersecurity issues

10. Publish periodic reports on the cyber security, e-privacy and data protection measures adopted, implemented or improved in the country.

Recommendations

Recommendations to civil society:

1. Provide information to general public about potential risks on Data Protection and Cyber security, with a specific focus on vulnerable groups and other categories that might face significant issues in case of abuses of personal data from public authorities.

2. Advocate for harmonization of national and local legislation to EU Standards, in particular EU's ePrivacy Directive (Directive on Privacy and Electronic communications (Directive 2002/58/EC), and the General Data Protection Regulation.

3. Engage in constructive dialogue with public authorities vis-à-vis the specific needs and challenges faced by citizens during COVID-19 and how to address them with digital tools (including tracing apps).

4. Monitor potential threats related to the implementation of tracing apps and other COVID-19 related issues and publish periodic reports in order to raise awareness among general public and international community.

5. Share good practices in the field of data protection with both public and private companies in order to create a general positive environment based on cyber resilience.

Recommendations to the European Union:

1. Provide expertise and support for the harmonization of data protections, cyber security and e-privacy to EaP governments, particularly in the fields related to e-health and COVID-19.

2. Support civil society through material and non-material support in EaP countries in order to create a resilient society that is aware of potential challenges related to GDPR and misuse of data.

3. Create training opportunities for elected officials and civil servants to learn more about potential threats and opportunities related to data protections and engagement with citizens through digital tools such as tracing apps and e-services.