Cyber surveillance in terms of coronavirus pandemic

Leonov Oleksandr [*] [A]; **Ablazov Ivan** [A]

[A] Military-Diplomatic Academy named after Yevgeniy Bereznyak, Kyiv, Ukraine

Received: August 15, 2020 | Revised: September 15, 2020 | Accepted: September 30, 2020

DOI: 10.5281/zenodo.4062366

Abstract

The scientific study describes techniques used by national governments to address the spread of the coronavirus. The focus is on the ambiguity of the decisions of the authorities, which lead, on the one hand, to an improvement in the incidence of coronavirus among the population and, on the other hand, to the disclosure of confidential information of citizens (passport details, contact numbers, location information), which in turn violates the right to privacy. The legal and regulatory framework relating to the inviolability of private information has been analysed, as well as the efforts of individual countries to amend existing legislation aimed at legitimizing surveillance at the state level. Attention is drawn to the risk of the long-term storage of private information and its access by a large number of individuals, which could lead to the leakage and misuse of data.

Key words: pandemic, tracking tools, human rights violations.

Introduction

The spread of the coronavirus has become a real challenge for the whole world, for which humanity has not been ready. Due to the high number of deaths among the sick and the lack of a vaccine to combat the disease, governments have imposed strict quarantine measures, including border closures, restrictions on movement and forced interruption of business activities. Such comprehensive measures have improved the incidence of the disease, but have hit large, medium and small businesses. This is evidenced by the economic downturn in virtually every country in the world.

However, in addition to the obvious negative economic consequences, the pandemic has resulted in a situation that has given governments much more leeway, which they use far more than just to counter the spread of the virus. In order to prevent the spread of coronavirus, the authorities of many countries are resorting to global cyber surveillance of their citizens. After all, the threat to everyone, which is Covid-19, legitimizes the level of government interference in the daily lives of citizens, which would be impossible under normal conditions [1].

Material and methods

The aim of the article is to analyze the mechanisms of pandemic control in different countries of the world, operating on the basis of cyber surveillance, as well as the possible negative consequences of using such methods.

Such scientific methods as observation, analysis, synthesis, generalization were used in the work.

Results and discussion

1.1. Over time, national governments have begun to develop mechanisms to control the spread of the disease. One of the prerequisites for overcoming the spread of the disease has become the effective detection of infected people and control over their isolation from

[*] **Corresponding author:** PhD student, e-mail 578original@gmail.com

healthy people. With this in mind, security measures have increasingly begun to include technological surveillance tools, such as the latest information technology and artificial intelligence. It is obvious that the rapid spread of the disease has increased state control over citizens. Covid-19 has conditioned interference with the privacy and provided access to personal information that may be sensitive.

The first cases of coronavirus were detected in the city of Wuhan in the People's Republic of China. The dramatic increase in the number of infected people encouraged the authorities to act decisively. The latest technologies have been used in China to fight the spread of the virus. With the help of unmanned aerial vehicles, medicines were delivered to the affected areas, disinfecting was carried out by robotic cleaners in the quarantine zone, which means robotics made it possible to help sick people without being exposed to danger [2]. Artificial intelligence technologies were used extensively: the latest diagnostic systems were introduced which were faster than human beings to distinguish normal pneumonia from coronavirus infection, which facilitated the work of medical staff greatly. In addition, various mobile applications have been created, which can track the location of infected people. With the help of the developed software and the recognition system that identifies a person, even if there is a protective mask on a face, it has become possible to detect the gathering of potentially sick people.

As we can see, the latest technologies play a significant role in the fight against coronavirus. Combined with the harsh measures taken by the Chinese authorities, this has had a positive impact, allowing the lifting of restrictive measures. On the other hand, however, it can be argued that the use of state-of-the-art technologies is gradually blurring the line between security measures and total surveillance [2].

Apps for smartphones have a wide range of features: some of them help to detect possible cases of infection, but at the same time have access to personal data and geolocation of their users. Other applications allow a registered user to access the map on which the infected areas are marked. However, when registering, the user goes through a verification process, which requires the indication of his phone number, name and even identity card. Collecting private information makes it possible to fight the coronavirus more effectively and help its citizens, but it also provides an opportunity to use it for their own benefit.

The software used in China assigns to its users a code of a certain colour: green, yellow or red. Each of the colours indicates the appropriate state of health, depending on which a person may be allowed to enter the subway, shopping centres or obliged to quarantine [3]. However, the analysis of the mobile application code indicates that the software, in addition to determining the risk of infection, sends information to the police. This precedent indicates the use of new methods of automated social control, which can be stored long after the end of the pandemic.

Similar technologies are used in other countries in terms of the spread of coronavirus, because access to confidential information is of interest to any ruling elite.

Using mobile data, the Israel authorities are able to track the movements of infected citizens and identify those who have been in contact with them. In cooperation with Vocalis Health, the Ministry of Defense of the government of Israel is developing a special program that will detect the symptoms of coronavirus using human voice analysis. If the creation of this program is successfully implemented, it will allow remote diagnostics of potentially infected people, which will significantly ease the burden on the health care system [4]. However, access to sensitive information by those who will use the software remains an open question.

In the UK, a new state medical program "Test and trace" to fight the spread of Covid-19 was implemented. It is based on the developed mobile software, which has to track the contacts of a person infected with the virus, and warn them about the necessary 14-day self-isolation and passing a test for the disease. At the same time tracking possible chains of infection will still be in manual mode. 25,000 people will be

involved [5]. And although this practice can significantly help in the fight against the disease, the access of a large number of people to private information increases the likelihood of its leakage.

In addition to daily reporting of the number of cases, the places with the highest infection rate, and recommendations to prevent virus contamination through Whattsapp application, Tracetogether software has been developed in Singapore. Using national surveillance tools, the programme tracks people who are at risk of infection. Using Bluetooth technology, the program tracks the proximity of users to each other, and if one of them has a confirmed diagnosis or a high risk of infection, it warns the other one. If the program determines that the user has already been in contact with infected people, the user's location and home address are automatically sent to the appropriate supervisory authorities [6].

With the help of special technical equipment, Taiwan authorities are able to track the mobile phone signals of infected citizens in quarantine homes. If such a person leaves his or her home or turns off his or her gadget, the device will automatically report the violation to the police [6].

In Poland, a mobile application called «Kwarantanna domowa» was developed. It is mainly used by people who are obliged to remain under 14 days quarantine. Users of the program give their mobile number and location at the time of the quarantine. From time to time, users must send their own photo with geo-location from their phone, which allows them to check compliance with quarantine requirements. The frequency at which it is necessary to send photos – from one to several times per day [6].

The Government of South Korea, using the data of its mobile operators, can track the whereabouts of any person. In addition, a digital map showing the routes of coronavirus patients has been created. Geolocation from mobile phones, credit card information and personal interviews with patients are used [7]. However, the disclosure of the routes of infected people has already been used by fraudsters as a tool of blackmail. There have been cases when unknown people demanded money from the owners of catering establishments, threatening that if they are infected, they will enter the establishment, and their stay on the map will be marked, which will lead to the closure of the establishment on quarantine.

Therefore, the use of private information, in particular location, by the authorities can have negative consequences. These examples clearly indicate, if not a lack of respect for human rights, then at least insufficient number of safeguards to ensure their observance [8].

As we can see, the nature of the response to the pandemic in different political countries has clearly demonstrated that the deep-seated nature of the state mechanism has a lot of common features [1]. In critical situations, the restrictions of rights and freedoms becomes a feature of both democratic and authoritarian political systems, and the collection of data on the citizens is an integral part of the fight against emerging dangers. The increased immersion of the state in the private lives of citizens is a matter of serious concern. Nowadays, all individual rights and freedoms are losing their meaning and this may become the norm – the state will monitor citizens through digital technology, disclose confidential information about their health, etc [9].

1.2. The European Convention on Human Rights emphasizes that public authorities may not interfere in the privacy of citizens, except in certain cases, in particular for the protection of health, in the interests of national security and public order, economic welfare of the country [10].

There is a joint statement by the Chairman of the Committee of the Council of Europe Convention on Data Protection, Alessandra Pierucci, and the Commissioner for Data Protection of the Council of Europe, Jean-Philippe Walter [11], which confirms the existence of problems with the privacy of citizens. Their statement addresses the dangers of using digital contact tracking technologies and emphasizes the introduction of safeguards to prevent risks to personal data and privacy. Therefore, in order to legitimize the fight against the pandemic through digital surveillance,

national governments are beginning to introduce massive changes in existing legislation that will allow access to sensitive information.

For example, in the Federal Republic of Germany, the authorities intend to amend the Act on Protection against Infectious Diseases which will give the opportunity to collect data on citizens by mobile phone number [12].

Slovakia, in turn, has adopted a law which allows the authorities to track people according to the mobile operators [6].

In the United States, in the framework of the Economic Stimulus Bill allocated $500 million dollars to the United States Centre for Disease Control and Prevention (CDC) for establishing a surveillance and data collection system [13]. It is not yet clear how such a system will work.

Such circumstances raise concerns that modern cybersecurity measures may become acceptable worldwide. Human rights experts believe that, without proper monitoring, even legitimized government action on global surveillance poses a risk to citizens' right to privacy and freedom of expression [14].

In any case, cyber-assisted coronavirus control can lead to massive violations of civil rights. In addition, there is concern about the centralized storage of large amounts of personal data that may be of interest to hacker groups and foreign intelligence services.

Conclusions

The massive spread of Covid-19 introduced restrictive measures such as quarantine or emergency mode. This has led to restrictions on fundamental civil rights, in particular freedom of movement, freedom and inviolability, and respect for privacy. An analysis of the security arrangements of different political systems suggests that cyber-security for the citizens has become a global policy trend in the fight against the coronavirus pandemic. Analysis of geodata from mobile phone users, tracking of contacts, setting up of cameras in cities with identity function are new realities that until recently were used only in exceptional situations In a pandemic, democratic principles are temporarily sidelined, because human life is a top priority for any state.

However, massive access to confidential information by the state is a matter of concern and requires a number of additional measures from the authorities. There is a need to legislate when it is necessary to collect confidential data from citizens, to establish the time intervals for the use of such data, the purpose of their processing and which public authorities can access it. In addition, a privacy protection algorithm should be developed to prevent leakage.

The Covid-19 pandemic has resulted in a global change in the established world order, but it should not become an excuse for mass surveillance of humanity by interested parties. During the pandemic, when state intervention in the private lives of citizens reaches the highest degree, the actions of the authorities are in greater need of objective assessment and detailed analysis than ever.

References

1. A new world order: now everyone is on his own. Ukraine's survival depends only on our efficiency. URL: https://niss.gov.ua/news/statti/noviy-svitoviy-poryadok-teper-kozhen-sam-za-sebe-vizhivannya-ukraini-zalezhit-lishe-vid (date of application: 07.05.2020).
2. Comment: How the coronavirus promotes censorship and the development of technology in China. URL: https://www.dw.com/uk/yak-koronavirus-spryiaie-vstanovlenniu-tsenzury-ta-rozvytku-tekhnolohii-v-kytai/a-52797748 (date of application: 29.03.2020).
3. As coronavirus surveillance escalates, personal privacy plummets. URL: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html (date of application: 03.06.2020).
4. Anti-infective technologies: how programs help fight the spread of coronavirus. URL: https://112.ua/statji/tehnologii-protiv-

zarazy-kak-programmy-pomogayut-borotsya-s-rasprostraneniem-koronavirusa-530782.html (date of application: 04.04.2020).
5. Coronavirus: test and trace programme launches amid reports of 'crashes'. URL: https://news.sky.com/story/coronavirus-test-and-trace-programme-launches-amid-reports-of-crashes-11996193 (date of application: 01.04.2020).
6. How a smartphone app can help fight the spread of coronavirus. URL: https://zik.ua/ru/blogs/kak_prilozhenie_v_smartfone_mozhet_pomoch_poborot_rasprostranenie_koronavirusa_964208 (date of application: 04.04.2020).
7. As a tool for tracking Covid-19 violates the rights of people around the world? URL: http://ecpl.com.ua/news/yak-instrumenty-stezhennia-za-covid-19-porushuiut-prava-liudey-u-sviti (date of application: 07.05.2020).
8. The (for) digital rights pandemic: how Ukraine and the world are responding to new challenges. URL: https://zmina.info/articles/pandemiya-dlya-czyfrovyh-prav-yak-ukrayina-ta-svit-vidpovidayut-na-novi-vyklyky (date of application: 02.05.2020).
9. Life the day after tomorrow: after the coronavirus pandemic, the old world will disappear or nothing will change? URL: https://zik.ua/article/zhyttia_pisliazavtra_pislia_pandemii_koronavirusu_znykne_kolyshnii_svit_abo_nichoho_ne_zminytsia_964958 (date of application: 10.04.2020).
10. European Convention of human rights. URL: https://www.echr.coe.int/Documents/Convention_UKR.pdf (date of application: 04.05.2020).
11. COVID-19 tracing apps: side effects on personal data protection should be avoided. URL: https://www.coe.int/en/web/portal/-/covid-19-tracing-apps-side-effects-on-personal-data-protection-should-be-avoided (date of application: 09.05.2020).