Saint-Petersburg State University

TURILINA Polina Yurievna

Master’s thesis

The potential and risks of digital surveillance during pandemic policy: cases of Russia, USA and South Korea

Education level: master's degree

41.04.04 «Political science»

Main educational program SV.5660*

«Political Governance and Public Policy (in English)»

Scientific adviser: Associate Professor of the Department of Theory
and the philosophy of politics of St. Petersburg State University,
PhD in Political Science
Maltseva Daria Alexandrovna.

Reviewer: Professor of the Department of Theory and
history of politics at Moscow State University,
Doctor of Political Science
Kuznetsov Igor Ivanovich.

Saint-Petersburg

2021

Санкт-Петербургский государственный университет

ТУРИЛИНА Полина Юрьевна

Выпускная квалификационная работа

Политические риски цифрового наблюдения в условиях COVID-19: кейсы России, США и Южной Кореи

Уровень образования: магистратура

Направление 41.04.04 «Политология»

Основная образовательная программа ВМ.5660*

«Политическое управление и публичная политика (на английском языке)»

Научный руководитель: доцент Кафедры теории
и философии политики СПбГУ,
Кандидат политических наук
Мальцева Дарья Александровна.

Рецензент: профессор Кафедры теории и
истории политики МГУ,
Кузнецов Игорь Иванович.

Санкт-Петербург

2021

CONTENTS

INTRODUCTION

The COVID-19 pandemic has caused a forced digitalization of information technology and changed the methods and forms of government surveillance, which is a source of risks and dangers. The more COVID-19 spreads and the number of deaths from the virus grows, the more governments are introducing information technology into their policies to combat COVID-19. Of course, this can be seen as a positive thing if it really helps to reduce the rate of morbidity and mortality. But in the context of the rapid growth of technologies, society must pay attention to what measures are being taken "for its benefit", what technologies are being developed and implemented, what functions they perform and what will happen to them after the pandemic ends.

It is also necessary to think about clarifying these technologies in order to understand who will benefit and who will suffer. This study will examine the potential and risks of such technologies, as well as how these technologies will be used to repress and oppress populations.

Several international organizations (Privacy International, Project Plowshares) have noticed the proliferation of digital tracking technologies during the COVID-19 pandemic. A large number of countries (China, Ecuador, Germany, India, Israel, Italy, Poland, South Korea, Taiwan, and Thailand) use GPS on mobile phones to track people in quarantine and infected people in contact with another.

Israel uses historical data to track the movement of people in recent weeks. South Korea has combined mobile phone monitoring data with CCTV recordings and credit card purchases to track the routes of infected people. In Hong Kong, bracelets are issued to all arrivals to ensure compliance with mandatory quarantine. Several countries are working with commercial companies to develop new technologies (TraceTogether in Singapoore, Home Quarantine in Poland). Some governments use drones to spray disinfectants in public places and to transport medical equipment to quarantine areas. Saudi Arabia has already deployed drones to measure people's body temperature. [1] However, this research will focus only on one type of surveillance - digital tracing.

Questions concerning these technologies has sparked many questions: How much online surveillance is ethical? When is privacy more important than public safety and health? Who has the right to use personal data of others, and for what reasons?

While answers to these questions are complex and subjective, one thing is clear; the choices policymakers make in times of crisis will shape the future and will likely remain in force post-COVID-19. Navigating issues of surveillance during the crisis requires realising and recognising three critical things.

Altogether, many countries have been developing or using digital tracing to combat COVID-19, therefore, it is destined to be an extremely important topic for discussion in the coming months and years (Attachment A).

There are a lot of research works concerning theoretical aspects of government surveillance.

L.V. Smorgunov prove that types of control and surveillance are manifested in all modern high-tech societies, regardless of democratic or authoritarian regimes. Democratic regimes cannot resist the expansion of techno-social assemblies of control because of security and efficiency needs. Authoritarian regimes legitimize their intentions of dominance with the same technocratic argument for security and efficiency provided by the new industrial revolution.[2]

Based on the work "Engaging Privacy and Information Technology in a Digital Age" by National Research Council, it is possible to trace the evolution of government surveillance from the early 19th century to the present day.

It is impossible also to not mention theoretical works of Torin Monahan («Surveillance in the Time of Insecurity», «Surveillance and Security: Technological Politics and Power in Everyday Life»), David Lyon («Theorizing Surveillance: The Panopticon and Beyond», Surveillance Studies: An Overview) and Sarah Brayane («Predict and Surveil: Data,

[1] Acheson R. COVID-19: The Risks of Relying on Technology to “Save Us” from the Coronavirus // Women’s International League For Peace&Freedom. 2020. URL: https://www.wilpf.org/covid-19-the-risks-of-relying-on-technology-to-save-us-from-the-coronavirus/. (03.03.2021).

[2] Smorgunov L.V. Institutionalization of Governability and the Problem of Veillance in the Space of Digital Communications // South-Russian Journal of Social Sciences. 2019. Vol. 20. Issue 3. 63 pp.

Discretion, and the Future of Policing») which all contribute in theoretical investigation of such concept as «state surveillance».

There are also researches concerning current situation with digital surveillance. One of the first meaningful scientific work in this field – article of Yuval Noah Harari - the author of the popular science bestsellers «Sapiens: A Brief History of Humankind». His article «The world after coronavirus» published in Financial Times journal aware that many short-term emergency measures implemented during pandemic will become a fixture of life. The main idea of article is that even when the number of cases of coronavirus infections has dropped to zero, some governments that need data argue to maintain a biometric surveillance system, because they are afraid the second wave of coronavirus, or because a new Ebola virus is spreading in Central Africa. «A big battle has been raging in recent years over our privacy. The coronavirus crisis could be the battle's tipping point. For when people are given a choice between privacy and health, they will usually choose health»[3]. The author conclude: «If we choose disunity, this will not only prolong the crisis, but will probably result in even worse catastrophes in the future. If we choose global solidarity, it will be a victory not only against the coronavirus, but against all future epidemics and crises that might assail humankind in the 21st century».[4]

Ray Acheson in her article «COVID-19: The Risks of Relying on Technology to "Save Us" from the Coronavirus» touches upon such important topics use of informational technologies, and justifications for them, in the context of militarism and political economy in order to fully understand who will benefit and who will suffer. There is also consideration of the potential for weaponisation of some of this technology, or how it can be used to repress and oppress populations. Also the author writes about what actions we can take now to prevent the dystopian future that otherwise awaits us.[5]

[3] Harari Y. N. The world after coronavirus // Financial Times. URL: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. (11.02.2021).

[4] URL: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

[5] URL: https://www.wilpf.org/covid-19-the-risks-of-relying-on-technology-to-save-us-from-the-coronavirus/.

But there is a lack of research which focuses on different approaches to implementing such policies and identifies the risks and potential of each approach.

So, the *goal* of this research is to specify the potential and risks of digital surveillance implementation as a part of government's policy during COVID-pandemic.

This goal is achieved by solving a number of interrelated *tasks:*

1. Review of scientific approaches to government surveillance definition.

2. Determination of the main stages of state surveillance systems' development in the context of digital state evolution.

3. Review of modern digital state surveillance methods, as well as the risks they accumulate.

4. Research of tracing as one of the most efficient type of state surveillance, determination of it's specifics.

5. An overview of the technical capabilities of tracing, as well as the strategies of it's implementation.

6. Development of unique methodology of comparative analysis of public policy in terms of the introduction of tracing systems on the example of 3 countries (justification of the choice of countries and the development of criteria for analysis and comparison).

7. Comparison of the obtained results of conducted policy analysis, the division of tracing systems' implementation policies into three types.

8. Research of the advantages and risks of each policy type.

9. Formulation of recommendations for government authorities in the field of efficient digital surveillance systems' implementation to manage coronavirus.

Object of research – strategies of digital surveillance systems' implementation in the context of COVID-19.

Subject of research - determination of the potential and risk assessment of the introduced systems (on the example of tracing tools).

Research design. The methodology of this research is a combination of 2 approaches - policy analysis and comparative analysis in case-study frame.

The policy analysis approach was chosen for analysis of existing government policies, it aims to explain their development. The areas of research are policies of three countries that implemented digital surveillance during the COVID-19 pandemic. This research puts focus onto political processes and the stakeholders involved. The aim is to determine what processes, means and policy instruments (e.g., regulation, legislation, sanctions) are used. Countries for policy analysis will be categorized into three types based on their reaction speed on pandemic. A fast time value indicated that the infections were quickly suppressed in a country; hence, it would be categorized under ‘fast reaction’. Therefore, for the Pandemic indicator, this research categorized the countries into three groups: fast, medium, slow (Table 1).

Comparative analysis here is for comparative research where contextual interrogation precedes any analysis of similarity and difference. It will help determine which logical conclusions a data set resulting from policy analysis supports. The analysis will provide list of variables observed in policy analysis, followed by applying the rules of logical inference to determine which descriptive inferences or implications the data supports.

The results will be grouped into three categories based on the data that will be identified in the analysis, highlighting three types of policy. The focus of the definition will be laid on determining the main resource of a policy.

The combination of these approaches is carried out in the context of a case study, that involves an up-close, in-depth, and detailed examination of a particular case or cases, within a real-world context. The research design is described in more detail at the beginning of paragraph 2.2.

CHAPTER 1. THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF GOVERNMENTAL SURVEILLANCE IN THE CONTEXT OF MODERN POLITICAL REALITY

1.1 Concept of surveillance: operationalization and development issues

Surveillance is an important issue in Western societies due to increased awareness and an increase in types of surveillance technologies. During the second half of the 20th century, not only the types and technologies of observation increased, but also the number of people and spaces being monitored have been increasing as well. This sparked the emergence of a scientific discipline called surveillance studies, but the concept of surveillance is increasingly found in different contexts and disciplines, making it more complex to focus debates across disciplines.[6]

The term "surveillance" could be decomposed into etymological parts "sur" (above) and "veillance" (to watch). Although the first associations with the term surveillance are often associated with closed-circuit television (CCTV) cameras located in city centers and other locations, the term was debated before the ubiquitous electronic eyes in public places. Due to the enormous technological changes that have taken place since 1960s, the term "surveillance" gained popularity both in meaning and in substance, and was theoretically based on a wide range of disciplines.[7]

Due to vast and seemingly radical technological changes that information and communication technologies (ICTs) have brought about since roughly the 1960s, the term surveillance has been spreading both in meaning and substance and has been theorised on from a large range of disciplines. One point of departure for understanding surveillance could be found in Lyon's explanation of surveillance as being about both caring and controlling.

[6] Galič M., Timan T., Koops B-J. Bentham, Deleuze and Beyond: An Overviewof Surveillance Theories from the Panopticonto Participation // Philosophy & Technology. 2017. Vol. 30. P. 9-37.

[7] In the same source.

In a recent article, Ross Bellaby writes that, ‘Surveillance’ can cover a wide range of activities from CCTV cameras and ‘covert surveillance’ to dataveillance and datamining. At the same time, the scope should not be narrowed down too much. According to David Lyon, surveillance is “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered”.[8] Furthermore, Kevin Macnish observes, this excludes too much, both in requiring the specific purposes of influencing or managing, and in requiring surveillance to collect data. Presumably there should be allowed for surveillance in cases of e.g., voyeuristic interest, and attempted but unsuccessful data collection.[9]

Moreover, there are useful informal definitions of surveillance provided by K. Macnish. He writes that, “Surveillance involves paying close and sustained attention to another person. It is distinct from casual yet focused people-watching, such as might occur at a pavement cafe, to the extent that it is sustained over time. Furthermore the design is not to pay attention to just anyone, but to pay attention to some entity (a person or group) in particular and for a particular reason. Nor does surveillance have to involve watching. It may also involve listening, as when a telephone conversation is bugged, or even smelling, as in the case of dogs trained to discover drugs, or hardware which is able to discover explosives at a distance”.[10]

In another recent article, there has been written that, surveillance could be used in referring to the monitoring of a competent adults over a specific time period, without their consent.[11] Finally, in “The Ethics of Surveillance”, Macnish recognizes the difficulties of defining surveillance, but adopts “for the purposes of [the] book” the understanding that surveillance is “the sustained monitoring of a person or people”.[12] These definitions are explicitly stipulatory – they are intended only to provide a definition suitable for a particular purpose.

[8] Bennett C. J. Surveillance Society: Monitoring Everyday Life // The Information Society. 2003. Vol. 19. P. 335-336.
[9] Macnish K. The Ethics of Surveillance – An Introduction. Routledge, New York, 2017. P. 216.
[10] Macnish, K. Surveillance Ethics // The Internet Encyclopedia of Philosophy. URL: https://iep.utm.edu/surv-eth/. (28.04.2021).
[11] Macnish, K. An Eye for an Eye: Proportionality and Surveillance // Ethical Theory and Moral Practice. 2015. Vol. 18. Issue 3. P. 537.
[12] Macnish K. The Ethics of Surveillance – An Introduction. Routledge, New York, 2017. P. 128.

The world is entering a new stage of digital development, which is characterized by an active transformation of institutions and mechanisms of public administration. The use of new electronic platforms and digital technologies creates preconditions for the transformation of public policy functions, the development of institutional forms that allow for more effective interaction between government bodies and society. In addition, digitalization leads to the creation of prerequisites and demand for the active use of information and communication technologies, for the purpose of increasing the efficiency of partnership institutions and the quality of public services provided.[13] As a result of the digital shift, many aspects of life are now stored in digital form. On that note, concern has been expressed concerning the fact this information could be used by governments to carry out mass surveillance on their populations.

Technological shift, public demand for security, new risks posed by the pandemic caused increasing of digital surveillance systems by government. Furthermore, government surveillance is concerned with the collection of information through ongoing observation of individuals or groups. In the context of cybersecurity, surveillance is conducted by observations of networks and information processing and communication systems in general. Government surveillance could be used for intelligence collection or law enforcement investigation, for counterintelligence monitoring, for political intelligence, or even for social control.

Government surveillance is often cited as essential to struggle with terrorism, prevent crime, control the population and protect national security. Conversely, mass surveillance has been equally frequently criticized for violating privacy rights, restricting civil rights and freedoms.[14] Another point of critique is that, increased surveillance can lead to the development of a surveillance state or an electronic police state in which civil liberties or political dissent are violated.[15]

[13] Smotritskaya I. State administration in conditions of development digital economy: strategic challenges and risks // STAGE: economic theory, analysis, practice. 2018. Vol. 4. P. 51.

[14] Watt E The right to privacy and the future of mass surveillance // The International Journal of Human Rights. 2017. Vol. 21. Issue 7. P. 789.

[15] Giroux H. A. Totalitarian Paranoia in the Post-Orwellian Surveillance State // Cultural Studies. 2015. Vol. 29. Issue 2. P. 108-140.

One another important thing in context of surveillance development is the growth of smart cities. The main purpose of surveillance there is to use information technologies to control the urban environment. The implementation of such technologies by different cities, has led to the increase of efficiencies in urban infrastructure, as well as improved community participation. Apart from that, with the use of sensors and systems, the infrastructure, operations and activities of a smart city are monitored to increase their efficiency. For example, the city could use less electricity; its traffic would run more smoothly with less delays; its citizens use the city with more safety; hazards could be dealt with faster; citizen infractions of rules could be prevented, and the city's infrastructure; power distribution and roads with traffic lights for example, dynamically adjusted to respond to differing circumstances.[16]

In addition, the development of smart city technology has also led to an increase of potential unwarranted invasions of privacy and limited autonomy. The widespread adoption of information technologies in the daily life of urban citizens is increasing the surveillance capacity of states - to the point where people may not know what information is being accessed, when it is being accessed, and for what purpose. It is possible that in such conditions an electronic police state can develop. Shanghai, Amsterdam, San Jose, Dubai, Barcelona, Madrid, Stockholm and New York are use different smart city technologies nowadays.

1.2 Surveillance systems in the context of modern digital states

Currently, the scientific substantiation and development of approaches to the digital transformation of public administration institutions are based on a change in the fundamental understanding of the essence of the state.[17] «The concept of Digital Government evolves towards more complexity and greater contextualization and specialization, similar to evolution-like processes that lead to changes in surveillance methods and systems» - following Thomas Janowski, - «digital Government Evolution Model have three increasingly complex phases in the evolution of the concept:

[16] DeAngelis S. Smart Cities and the Big Brother Syndrome [Electronic resource] // Enterra Solutions. 2018. URL: https://enterrasolutions.com/blog/smart-cities-and-the-big-brother-syndrome/. (20.01.2021).

[17] Smotritskaya I. State administration in conditions of development digital economy: strategic challenges and risks // STAGE: economic theory, analysis, practice. 2018. Vol. 4. P. 6-72.

Digitization (Technology in Government), Engagement (Electronic Governance) and Contextualization (Policy-Driven Electronic Governance)» [18]. In the next part, the stages of digital state development (Janowski, 2015) will be discussed and compared with the stages of surveillance development.

Stage 1. Digitalization (Technology in Government). In the first stage, the focus is primarily laid on modernization, and secondly at internal efficiency and access. The Digitization Stage includes the development of the technological environment, including the availability of technological capabilities, services and infrastructure within and between government organizations. Based on this environment, Stage entails the presentation of data, documents and other information in digital formats, if they were previously owned by government organizations in physical or analog form; automation of existing processes, services and the entire office based on digitized information and its exchange through digital networks; and making services available to citizens digitally and over digital networks where they were previously available in physical and analogue forms.[19]

Examples of initiatives and investigations during this stage according to T. Janowski:

- «Access to government information in electronic formats
- Developing, analyzing and operating government websites: securing the content and analysis of web vulnerabilities.
- Technological infrastructure for digital government: technological, sharing and knowledge services»[20].

It possible to conclude that this stage does not involve redesigning, improving or any modification of existing processes, services or practices, but simply digitizing and automating what already exists and delivering the results to the same stakeholders and customers through digital networks. Thus, the Digitization Stage is not improving government internal operations, adapting to changing working conditions and social

[18] Janowski T. Digital government evolution: From transformation to contextualization // Government Information Quarterly. 2015. Vol. 32. Issue 3. P. 221-236.

[19] In the same source.

[20] In the same source.

expectations, and delivering value to the public, but it is a necessary step towards the subsequent stages of the evolution of digital government.[21]

Surveillance on this stage is characterized by rapid technological growth, an increased reliance of government on surveillance, and the initial formulations of privacy as a legal right. From the late 1950s onwards, the computer became a central tool of organizational surveillance; it addressed problems of space and time in the management of records and data analysis and fueled the trend of centralization of records. The power of databases to aggregate information previously scattered across diverse locations gave institutions the ability to create comprehensive personal profiles of individuals, frequently without their knowledge or cooperation. During the 1960s, the possibility of the use of such power for authoritarian purposes awakened images of Orwellian dystopia in the minds of countless journalists, scholars, writers, and politicians, drawing wide-scale public attention to surveillance and lending urgency to the emerging legal debate over privacy rights.[22]

Stage 2. Engagement (Electronic Governance) revolves around the transformation of the relationships between government and citizens, businesses and other non-government actors using digital technologies. The transformation aims at increasing access, convenience and effectiveness of public service delivery systems, engaging citizens in political and civil affairs, developing knowledge-based society and economy, and pursuing other high-value public policy goals. Apart from that, the Engagement stage is also part of a larger trend towards implementing the Digital by Default and Open Government principles.[23]

Examples of initiatives and investigations undertaken at the Engagement Stage, according to T. Janowski:

- «Increasing adoption by citizens: applying communication and marketing strategies to lead citizens to electronic channels and thus increase the usage of e-

[21] Janowski T. Digital government evolution: From transformation to contextualization // Government Information Quarterly. 2015. Vol. 32. Issue 3. P. 221-236.
[22] Waldo J., Lin H. S., Millet L. I. Engaging Privacy and Information Technology in a Digital Age. Washington, DC: The National Academies Press, 2007. P. 450.
[23] Janowski T. Digital government evolution: From transformation to contextualization // Government Information Quarterly. 2015. Vol. 32. Issue 3. P. 221-236.

government services; the impact of technology knowledge – knowledge about and ability to operate specific technologies – on citizen engagement and the use of e-government services.

- Increasing participation and engagement: citizen coproduction and a unified typology or existing coproduction models along the “citizen sourcing”, “government as a platform” and “do-it-yourself government” categories; and applying electronic rulemaking and its ancillary activities from the early stages of legislative and policymaking processes to increase public interest, involvement and commitment.
- Transparency, accountability and open government: the use of digital technology by parliaments and their members to support accountability and greater engagement with citizens and their communities».[24]

As previously outlined, the Engagement Stage is concerned with improvements in the relationships between government, including executive, legislative and judicial branches, and its constituencies, including citizens, businesses, civil society organizations and other non-state actors.

During the Engagement Stage, surveillance becomes centralized and more computerized. All financial transactions became electronic, which made it possible to track and register them in computer databases.

In addition, advances in science have made the human body the primary tool for the practice of observation. Cameras have appeared in many public places with the aim of fighting crime. «In the 1990s, the development of biometrics, a method of automatic identification based on body characteristics, offered the ability to identify people without the need for documents. The advent of DNA analysis and the subsequent mapping of the human genome promised revolutionary opportunities for identification and medical testing».[25]

The observation became deeper and deeper. The need for national data centers disappeared as computer networks came into play. In the meantime, tracing systems

[24] In the same source.

[25] Waldo J., Lin H. S., Millet L. I. Engaging Privacy and Information Technology in a Digital Age. Washington, DC: The National Academies Press, 2007. P. 450.

began to permeate absolutely all sectors of society: ATMs, airports, highways and a large number of other points of contact transmitted data automatically.[26]

Stage 3. Contextualization (Policy-Driven Electronic Governance) aims at supporting the self-development of specific territorial and social units (countries, regions, cities, communities), namely the implementation of the goals of state policy and sustainable development. «At this stage, the government uses electronic technology to record, collect, store, organize, analyze, search and disseminate information about its citizens. In addition, states are also involved in massive government surveillance of landline and cell phone traffic, mail, e-mail, web surfing, Internet searches, radio and other forms of electronic communications, as well as extensive use of video surveillance».[27]

There are seventeen factors to describe the development of a surveillance on Contextualization Stage:

- Government surveillance orders: punishment for disclosing the existence of government surveillance agencies;
- Cash flow tracking: registration of financial transactions (checks, credit cards, money transfers);
- Fight against cryptocurrency: prohibiting or limiting encryption technologies;
- Tracking identity and registration documents issued by the state;
- Movement control: border control at borders, checking computers and phones, tracking travel within the country;
- Retention of data: the state assumes the obligation to store all data.

To sum up, there are three stages of development of state surveillance in accordance with the stages of digital state evolution. It is possible to trace that each stage of surveillance is characterized by certain factors (political, legal and

[26] In the same source.

[27] Janowski T. Digital government evolution: From transformation to contextualization // Government Information Quarterly. 2015. Vol. 32. Issue 3. P. 221-236.

technological). These factors highlight the main trends in institutional information collection by satate.

The first stage is characterized by technological growth, increasing government dependence on surveillance, and the first formulation of privacy issues.

During the second stage, surveillance can be defined as computerized and centralized, as well as to the first concerted social efforts to develop the legitimate right to privacy as an effective countermeasure.

In the third period, technological components are widely developed, as well as the political component of the issue. Wireless technologies are helping to develop surveillance to the highest level. Authoritarianism begins to figure as the primary justification for observation. To sum up, history of government surveillance can be divided into three stages in context of digital state development, each characterized by particular political, legal, and technological developments. While these divisions are arbitrary, they highlight some of the main trends that have characterized the institutional collection of information and the corresponding moral and legal responses.[28]

In the course of the evolution of the electronic and digital state, the logic of surveillance is also changing: the interaction between the state and citizens is increasing; the control technology becomes more complicated: from observation "from above" it becomes personal observation; responsibility for the behavior of citizens increases.

1.3 Surveillance systems’ instruments and new risks

The response to COVID-19 has seen an unprecedented rapid scaling up of technologies to support digital contact tracing and surveillance. We are witnessing how government prepares to leave the risk society and soft risk governance of conduct for a more radical securitization path while still protecting democracy thus far. In this paragraph these technologies will mention in relation with government policy. To

[28] Waldo J., Lin H. S., Millet L. I. Engaging Privacy and Information Technology in a Digital Age. Washington, DC: The National Academies Press, 2007. P. 450.

emphasize the problematics of these technologies for governments, it will be understood as part of pandemic policy «institutions».

It is widely believed in society that surveillance is represented as physical components, for example, drones or cameras with face recognition. But this is not the case. Surveillance is how these physical components collect and use data. For example, the face recognition function itself does not pose any threat. It becomes problematic when information obtained in the course of its use is misused. And this is already a problem of policy, including the government one.

The technologies used to better understand the nature of the COVID-19 pandemic include mobile phone tracing, biometric technologies and data scraping, and have been employed to carry out two main forms of tracing: digital proximity tracing and location tracing.[29]

Digital tracing proximity: determines the proximity (distance) between devices and the movement history of an infected person. This technology can be used to find out if a person has come into contact with carriers of COVID-19. This technology includes the use of bluetooth, so digital tracing proximity can be carried out without any centralized data collection and / or can be achieved by collecting anonymized data without violating personal privacy.

Location tracing: aims to locate people to ensure that social distancing measures and isolation orders are effective. This technology uses GPS from the mobile phone network to detect potential congestion and prevent it from happening. In most cases, location tracing requires centralized data storage and access. However, the aggregate data can be used to determine the geographic area in which people do not adhere to social distancing,

Data scraping / collation (artificial intelligence): This technology collects data from social media posts to predict disease incidence.

Facial recognition may be used to: identification of a person who violates the isolation regime, control of the movement of known infected people, control of persons

[29] Srivastava V. Surveillance, COVID-19, and the unexpected problems of a new normal // Policy Forum. 31.07.2020. URL: https://www.policyforum.net/surveillance-covid-19-and-the-unexpected-problems-of-a-new-normal/. (18.04.2021).

in self-isolation (by uploading a selfie from home and recognizing a face on it). This technology poses the greatest number of risks, as it requires centralized storage and poses a number of privacy issues.

Today, mobile operators remain the main source of data on citizens for the state. Tens of millions of subscribers send a signal to base stations approximately every 5 minutes. By overlaying geolocation data on a city map, you can get the user's travel routes. In this case, the error is 50–100 meters, which are added by the systems themselves. This technology is called trilateration. The three nearest base stations transmit the distance to the subscriber, and the person's location is calculated from the signal strength. Basically, it is calculating the coordinates of a point in space using three other points and the distance from them to it. [30]

Given the popularity of mobile communications, collecting data seems like an easy task. But the task can sometimes be complicated by the proliferation of anonymous SIM-cards. In such cases, surveillance systems can go for tricks: for example, create a mobile application for video surveillance recording. In Iran, the AC19 app has recently become popular, which was supposed to help determine if a user is infected with COVID-19. A message with a recommendation to install the application came on behalf of the country's Ministry of Health. In fact, the application recorded data, including videos from users' phones.

The question is what the long-term implications will be if the government moves towards stricter securitization, with extensive bans and fines, and a form of governance that increases the government's power.

The COVID-19 situation raises many questions regarding risk and risk science, including how to mitigate the risks caused by the introduction of such tracing systems.

It is possible to see how different countries adopt different policies, from lockdown to non-binding public health guidelines for social distancing, all claiming to be based on scientific evidence and often referring to the precautionary principle, but end up using different strategies to combat the virus. Obviously, a balance needs to be

[30] Mobile Location Data and Covid-19: Q&A // Human Rights Watch. 13.05.2020. URL: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa. (06.02.2021).

found between different issues. Society is facing a health crisis, but the implications of society blackouts are enormous, and when considering what to do next, it is clear that the risks associated with the coronavirus pandemic must be seen in conjunction with all the relevant aspects - and risks - involved. [31]

Surveillance systems are becoming complex political systems supported by the principles of the digital state. They work on the principle of very high personalization. The increasing complexity of these systems is associated with new risks for the ideal society, including COVID-19.

[31] Giritli Nygren K., Olofsson A. Managing the Covid-19 pandemic through individual responsibility: the consequences of a world risk society and enhanced ethopolitics // Journal of Risk Research. 2020. Vol. 23. P. 1031.

CHAPTER 2. DIGITAL TRACING IMPLEMENTATION IN CONTEMPORARY STATE POLICY

The common elements in all surveillance policies employed by states today include the identification of individuals and the collection, storage, tracing, and analyzation of data concerning their health status, movements, and relationships.[32] The goal of this chapter is concerned with the aforementioned method, which includes a combination of digital proximity tracing and location tracing (as previously mentioned in paragraph 1.3.) and determine the policies of implementation of this technology used by Russian, South Korean and American governments. Next, these policies will be analyzed from different perspectives, using a case-study methodology to evaluate the risks posed by such systems.

2.1 Digital tracing technology: definition and types

This research defines "digital tracing of people" as geolocation and proximity information from mobile phones and other devices. Governments presenting individualized tracing as a reliable way to trace the movement of people who are infected and identify individuals with whom they came into contact during the period in which they are contagious. Individualized tracing can also be used to determine whether people are complying with social distancing and quarantine measures. Analysis of aggregate location data, on the other hand, might provide insight into the effectiveness of social distancing measures, model the potential for transmission, and identify potential "hot spots" of transmission. Examples of how governments are using technology to respond to Covid-19 include:

Contact tracing: Contact tracing is concerned with the process of the identification of individuals who may have been in contact with an infected person. The goal of contact tracing is to prevent transmission through the rapid identification

[32] Turner J. S, Baxenberg S.M. Track, Trace, and Quarantine: The Role of Mobile Data in Managing the COVID-19 Pandemic // Wiley Rein LLP. 2020. URL: https://www.wiley.law/newsletter-Apr-2020 PIF_Track_Trace_and_Quarantine_The_Role_of_Mobile_Data_in_Managing_the_COVID-19_Pandemic. (15.03.2021).

of individuals who have been in close contact with someone who is infected, within 6 feet of someone for approximately 10 or more minutes (United States Centers for Disease Control and Prevention (CDC), YEAR). The idea is to stimulate these individuals to self-isolate and seek testing and treatment. Due to the fact that the coronavirus is primarily transmitted through person-to-person contact, via respiratory droplets when an infected person coughs, sneezes, or talks, mobile location data has been described as a helpful method for the identification of potentially exposed individuals. Next, the technological specifics of each of the subspecies of digital tracing will be given, taken from the study of Humans Rigts Watch «Mobile Location Data and Covid-19»:

«Enforcing quarantine and social distancing orders: Governments have been imposing quarantines and other restrictions on movement; broad lockdowns, closures of business, public spaces, and institutions, orders for the isolation of individuals infected, and requests for voluntary social distancing. In addition, governments have been using mobile location data to monitor compliance with restrictions, for example, by encouraging people to install an app that uses location data to identify people who violate these restrictions.

Big data analytics: Companies and governments have also been examining location data in an aggregated form to better understand general patterns of people's movements and behaviors and how these have changed over time. This sort of analysis aims to forecast in what way the virus might spread and the effectiveness of public health interventions such as social distancing measures and identify ways to better allocate testing and medical resources.

Hot spot mapping: Hot spot mapping is a type of big data analysis that includes the use of location data to piece together the movement or location history of individuals who have tested positive. Hot spot mapping could be used to send out public health warnings about specific locations, or close down or disinfect particular locations.»[33]

[33] URL: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

As already explained in paragraph 1.3 - data for digital surveillance (including digital tracing) can come from various sources, such as cell towers, GPS and Bluetooth technology. Further in the text, different data sources will be analyzed in more detail.

Cell site location information: mobile phones connects to internet networks through cell towers. When the phone moves with the person, the phone communicates with the nearest cell towers. This process generates information about the location of people, which is later stored by cellular operators. Governments may require cellular operators to provide this information to track someone's movements.

Global positioning system (GPS): This technology is more accurate than the one described above. It can determine the location with an accuracy of 3 meters. Many applications for smartphones (social networks, games, maps, shops) collect GPS data and then transmit it to the government. During COVID-19, a large number of new applications appeared designed specifically for tracing contacts and tracing the movement of people. GPS technology is different in that it can be used to track not only the current location, but also movements in the past.

Bluetooth beacons: bluetooth is a wireless set of protocols used by devices to transfer data on small devices. This technology can only communicate with devices located in the vicinity (10 meters). This technology has been proposed for contact tracing by detecting the proximity of a phone to other devices. Unlike GPS technology, bluetooth does not track the actual location, but only the fact of interaction with other devices. Hence, it is best understood as an engagement tracing tool.[34]

2.2 Comparative analysis of tracing technology’s implementation (on the example of pandemic policies of Russia, USA and South Korea)

In this paragraph, there will be looked at responses used by governments and tech companies to help contain the spread of COVID-19. Also there will be analysis of a very specific case study, but in the hopes that it will lend insights into how digital tracing of people can and should, be used in crises response situations.

2.2.1 Research design

[34] Mobile Location Data and Covid-19: Q&A // Human Rights Watch. 2020. URL: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa. (06.02.2021).

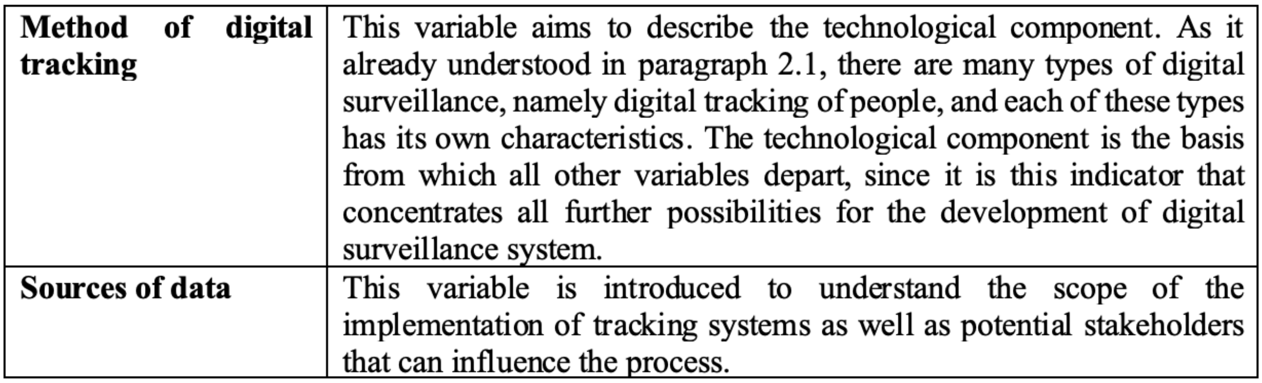
The following steps were taken to analyze the policy reaction of three governments in coping with the COVID-19 pandemic, with the use of digital tracing systems: Russia, USA and South Korea:

1. During the first step, countries were categorized into three types based on their reaction speed on pandemic. A fast time value indicated that the infections were quickly suppressed in a country; hence, it would be categorized under «fast reaction». Therefore, for the Pandemic indicator, this research categorized the countries into three groups: fast, medium, slow. This plan postulated that the country categorized under «fast reaction» should have a good reaction to the pandemic compared with countries categorized as «medium reaction» or «slow reaction». As a metric of the effectiveness of the implemented policy and its illustration, the number of infected people and death in a population, as this roughly reflects the duration that a country is experiencing a pandemic will be evaluated (Table 1).

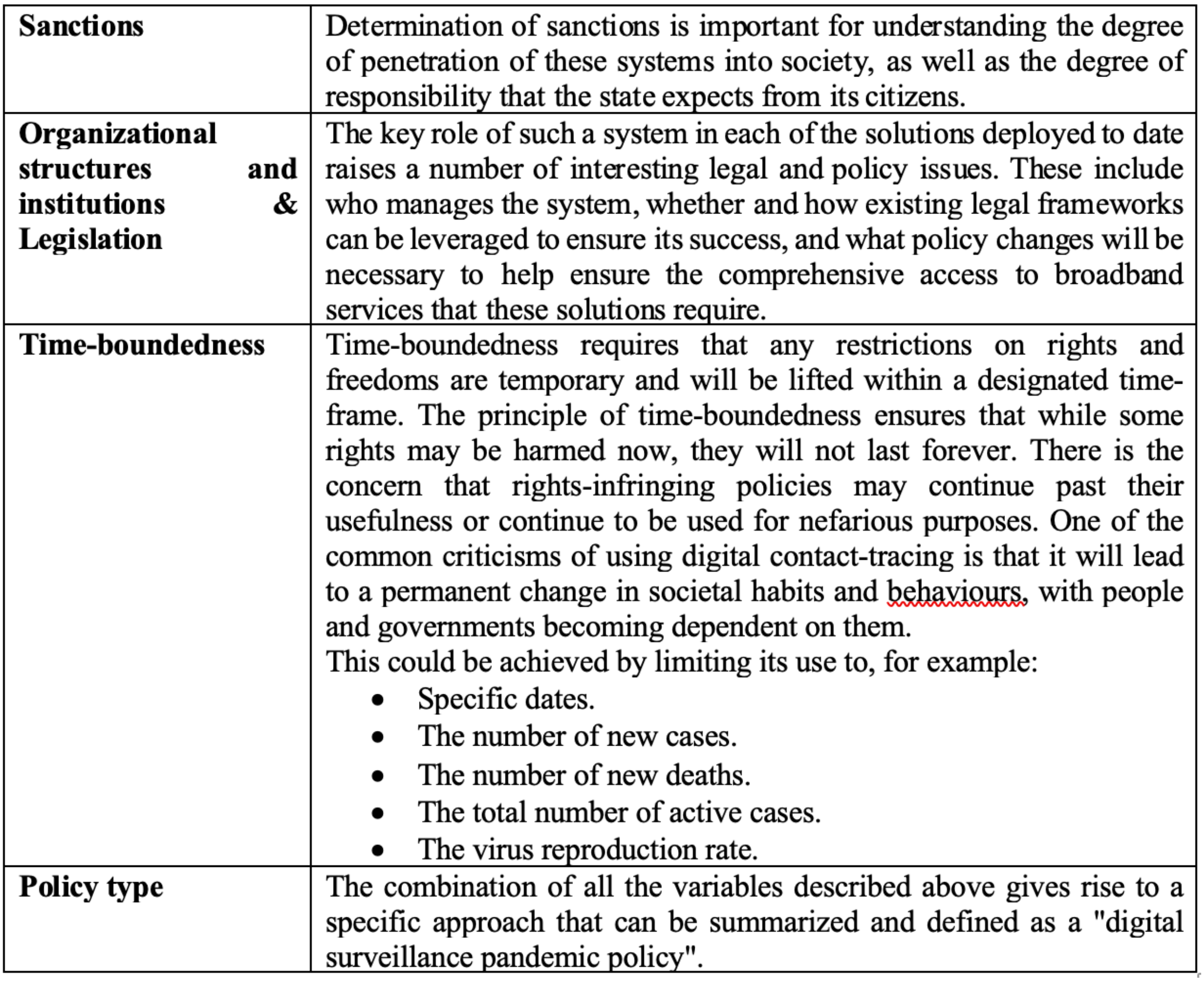
	South Korea	Russia	USA
Reaction	fast	medium	slow
Infected people (% per population)	0,28	3,16	9,60
Deaths (% per infected people)	1,58	2, 22	1,75

Table 1. Country selection

2. The aim of the second stage is to determine government policy reactions with regards to digital surveillance in dealing with the COVID-19 pandemic, based on the comparison of seven criteria:



Method of digital tracking	This variable aims to describe the technological component. As it already understood in paragraph 2.1, there are many types of digital surveillance, namely digital tracking of people, and each of these types has its own characteristics. The technological component is the basis from which all other variables depart, since it is this indicator that concentrates all further possibilities for the development of digital surveillance system.
Sources of data	This variable is introduced to understand the scope of the implementation of tracking systems as well as potential stakeholders that can influence the process.



Sanctions	Determination of sanctions is important for understanding the degree of penetration of these systems into society, as well as the degree of responsibility that the state expects from its citizens.
Organizational structures and institutions & Legislation	The key role of such a system in each of the solutions deployed to date raises a number of interesting legal and policy issues. These include who manages the system, whether and how existing legal frameworks can be leveraged to ensure its success, and what policy changes will be necessary to help ensure the comprehensive access to broadband services that these solutions require.
Time-boundedness	Time-boundedness requires that any restrictions on rights and freedoms are temporary and will be lifted within a designated time-frame. The principle of time-boundedness ensures that while some rights may be harmed now, they will not last forever. There is the concern that rights-infringing policies may continue past their usefulness or continue to be used for nefarious purposes. One of the common criticisms of using digital contact-tracing is that it will lead to a permanent change in societal habits and behaviours, with people and governments becoming dependent on them. This could be achieved by limiting its use to, for example: • Specific dates. • The number of new cases. • The number of new deaths. • The total number of active cases. • The virus reproduction rate.
Policy type	The combination of all the variables described above gives rise to a specific approach that can be summarized and defined as a "digital surveillance pandemic policy".

Table 2. Criteria for comparison.

3. The results will be grouped into three categories based on the data obtained from the analysis of the selection of the three types of policies. The resource will be put at the center of policy making. Today, we are aware of many different strategies of policies to combat COVID-19, from attempts to create herd immunity and not change the old life to strict measures to control every aspect. Countries in the Asian region took strict measures early in the spread of the virus, while Western countries took more cautious measures and more slowly. Some cared about the least damage to the economy, others put privacy issues at the center of attention, and some tried to organize herd immunity. Nevertheless, despite the different approaches, the goal is the same - to prevent infection and reduce the number of deaths. [35]

[35] Ryan M. In defence of digital contact-tracing: human rights, South Korea and Covid-19 // International Journal of Pervasive Computing and Communications. 2020. Vol. 16. Issue 4. P. 390.

2.2.2 Russian case

In Russia, the prime minister ordered the communications ministry to design a national system to track people who have been in contact with coronavirus patients, using location data provided by individuals’ mobile phone provider. The communications ministry confirmed it had designed the system. The communications ministry has demanded that regional authorities provide lists of mobile phone numbers of people infected with coronavirus, as well as the phone numbers of citizens who are quarantined at home either because they had traveled abroad or had contact with infected people.

In April 2020, the city government of Moscow launched an app to track the movement of coronavirus patients. The app is mandatory for all patients who have been ordered to stay at home. It requests access to the user’s calls, location, camera, storage, network information, sensors, and other data to ensure people do not leave their home while contagious. This app is in addition to the installation of one of the world’s biggest surveillance camera systems equipped with facial recognition technology to ensure that everyone placed under self-quarantine stays off the streets. Moscow also introduced a digital permit system for non-essential travel, both on public transport and private vehicles.

Method of digital tracing. In accordance with the Provisional Regulations, medical organizations, territorial bodies of Russia, within two hours after the hospitalization of a patient with a new coronavirus infection, the information is entered into the regional segment of the COVID-19 Information Resource.

The Situation Center of the Ministry of Telecom and Mass Communications of the Russian Federation daily uploads information about the sick (phone numbers) to the tracing system. Further, in the automatic mode, the list of sick phone numbers is compared with the database of ported numbers, the mobile operator is determined, lists of sick subscribers' phone numbers are formed for each operator.

The Situation Center of the Ministry of Telecom and Mass Communications of the Russian Federation receives daily information about cellular subscribers, in terms of preventing the spread of a new coronavirus infection, summarizes, analyzes it and presents it to the Ministry of Telecom and Mass Communications of Russia in the form of references, tables and in visualized form in the following areas (according to the project of law «Regulations for information and organizational and technical interaction of the tracing system with information systems of interested executive authorities and operational headquarters of the constituent entities of the Russian Federation»[36]):

1) Information on compliance by cellular subscribers of the self-isolation (quarantine) regime.

The coordinates of the base station to which the subscriber device is connected when it is at the isolation site are recorded, and its compliance with the self-isolation regime is monitored for 14 days. The subscriber is tracked by his geolocation during the first night (the place of self-isolation), moving outside the zone for a distance of more than 500 m (for some operators, 2000 m).

For the constituent entities of the Russian Federation, a list of telephone numbers of subscribers that violate the self-isolation regime is formed.

2) Information about cellular subscribers who may have contacted sick subscribers.

For each sick subscriber of cellular communication within 14 days from the date of entry into the Information resource COVID-19 of the Ministry of Health of Russia: using the geolocation method, the coordinates of the location and movement of the subscriber are determined before being placed in a medical hospital or isolated at the place of residence; the identification of subscribers with whom the sick subscriber contacted by phone (calls / sms) is carried out; a filter is implemented, according to the joint location of subscribers in the same geolocation for 5 minutes or more.

A list of telephone numbers of subscribers in the constituent entities of the Russian Federation, who may have personally contacted sick subscribers, is formed.

To sum up: the data of the Ministry of Health on the mobile phone number of the infected with the coronavirus infection will be used to compile a list of people who

[36] Russian Federation. Laws. (2020). Regulation of information and organizational and technical interaction of the tracking system with information systems of interested executive authorities and operational headquarters of the constituent entities of the Russian Federation. P. 1-7.

have been in constant direct contact with him over the past 14 days. As a result, a list of numbers of those who were most likely to be infected should be formed. This data will be transmitted to the information systems of the Ministry of Telecom and Mass Communications, the Ministry of Health, the Ministry of Internal Affairs, the National Guard and the headquarters of the constituent entities of the Russian Federation.

The system will also be used to detect cases of violation of the quarantine regime by coronavirus patients and people who came from abroad. Special algorithms will detect the movement of subscribers beyond the isolation site.[37] Thus, Russian systems solve 2 problems: track contacts of patients and monitor compliance with the self-isolation regime.

Sources of data. The system uses data from the Ministry of Health on the numbers of subscribers infected with COVID-19.

The regulations of the Ministry of Telecom and Mass Communications assume participation in the developed interaction scheme of the “Big Four” mobile operators - Megafon, MTS, VimpelCom (Beeline) and T2 Mobile, as well as Yekaterinburg-2000 LLC (Motiv brand). The Situation Center of the Ministry of Telecom and Mass Communications will receive from them information about subscribers on a daily basis and summarize it in several directions: information about subscribers who have contacted the sick, about subscribers' compliance with the self-isolation (quarantine) regime, about the number of cellular subscribers of the Russian Federation on the territory of foreign states and about subscribers crossing border of Russia. The lists of phone numbers of these people will be uploaded to the cloud resource of the situation center of the Ministry of Telecom and Mass Communications and will become available to officials of the Ministry of Health, the Ministry of Internal Affairs, the National Guard and operational headquarters for combating coronavirus infection of the constituent entities of the Russian Federation for taking the necessary measures. And they have already provided information on citizens' compliance with the isolation regime.

[37] Milyukova M. Will a new contact tracing system for COVID-19 patients lead to violation of the rights of Russians? // Lawyer Newspaper. 2020. URL: https://www.advgazeta.ru/ag-expert/advices/novaya-sistema-otslezhivaniya-kontaktov-zabolevshikh-covid-19-privedet-k-narusheniyu-prav-rossiyan/. (17.02.2021).

Sanctions. Prior to the entry into force of the regulations proposed by the Ministry of Telecom and Mass Communications, the data received from mobile operators cannot become the basis for holding a person accountable for violating the quarantine regime. The use of this information for the imposition of fines after the entry into force of the regulation is also questionable, since the current Administrative Code of the Russian Federation and regional codes of administrative offenses (with the exception of the Moscow one) do not provide for the possibility of fixing violations on the basis of these systems that make it possible to establish the location of citizens.

If the regulation enters into force, the data obtained using the tracing system will rather be used not as independent evidence, but as additional confirmation of the person's guilt in violating the quarantine regime. But if we nevertheless assume that amendments will be made to federal and regional legislation, the question arises of how to protect your rights when prosecuted due to a technical error in the system. And here everything will depend on how they will prosecute citizens based on geolocation data.

Organizational structures and institutions. Responsibility for ensuring the smooth functioning of the tracing system rests with the Situation Center of the Ministry of Telecom and Mass Communications of the Russian Federation (Attachment B).

The Ministry of Telecom and Mass Communications of Russia is responsible for the organization of information and organizational and technical interaction of the tracing system with information systems of interested federal executive bodies and operational headquarters of the constituent entities of the Russian Federation. This ministry has developed a regulation for tracing persons who have come into contact with citizens infected with coronavirus.

But here there is an interesting fact: the authority of the Ministry of Telecom and Mass Communications does not include the collection of information about citizens in order to protect health or ensure a safe epidemiological situation.[38]

Legislation. The Russian Ministry of Telecom and Mass Communications has developed a system of rules for tracing contacts of people infected with the COVID-

[38] URL: https://www.advgazeta.ru/ag-expert/advices/novaya-sistema-otslezhivaniya-kontaktov-zabolevshikh-covid-19-privedet-k-narusheniyu-prav-rossiyan/

19 coronavirus. The Ministry considered the new rules in the draft order posted on the portal of draft regulatory legal acts on July 6, 2020. The project was named "On the regulation of information and organizational and technical interaction of the tracing system with information systems of interested executive authorities and operational headquarters of the constituent entities of the Russian Federation." His ID on the portal is 01/02 / 07-20 / 00105648, and the document attached to it is dated May 27, 2020.

Many questions have arisen about the legality of the proposed contact tracing measures. The Russian tracing system establishes that the identification of persons in contact with a sick person is carried out on the basis of call details and SMS. However, access to information about such detail is limited to secret correspondence, telephone conversations, postal, telegraphic and other messages in accordance with the Constitution and is allowed only on the basis of a court decision. The automatic transmission of information by operators without obtaining a court sanction only on the basis of the assumption that a person is infected with COVID-19 does not meet the requirements established by the Basic Law for protecting the secrecy of correspondence and negotiations.

In addition, the legality of the processing of subscriber data raises questions. The Chairman of the Government of the Russian Federation Mikhail Mishustin, when discussing the considered tracing system, noted that the processing of personal data will not be carried out at all, since only information about the mobile phone of the sick person is collected. However, in accordance with the Law on Personal Data, they mean any information relating directly or indirectly to a specific or identifiable individual. A mobile phone number is not personal data only as long as it is just a set of numbers that are not tied to any subscriber, and if, based on such a number, information about a specific person is not obtained or determined.

In this case, other questions arise: on what legal basis and within what limits the processing of personal data is carried out, what are its purposes, whether citizens will be informed about the beginning of the processing of those data that are not received directly from such persons. In the Russian case, it is unclear whether the data obtained in this way will be secured, stored and not leaked. The question also arises about the transparency of the mechanisms for collecting such data by state structures.

Time-boundedness. The regulation for tracing the contacts of infected citizens, developed by the Ministry of Telecom and Mass Communications, involves the processing of personal data of a person without his consent. Article 6 of the Russian Law on Personal Data allows their processing in order to protect life and health or other vital interests without consent, if it is impossible to obtain it. That is, in this case, data processing should serve to prevent the spread of coronavirus infection and be limited in time by its spread. Further processing of data in the framework of epidemiological research will require the consent of the individual, and processing for commercial or law enforcement purposes is not permitted.

Policy type. In this case, there is a state monopoly on the regulation of the problem. Regulation policy is centralized and the focus is on state security. This approach can be characterized as centralized «government – driven» policy.

2.2.3 Case of USA

More than 32 million confirmed cases have been reported since January 2020, resulting in more than 571,000 deaths, the most of any country, and the sixteenth-highest per capita worldwide. The U.S. has about one fifth of the world's cases and deaths. More Americans have died from COVID-19 than died during both World Wars and the Vietnam War combined.[39]

State and local responses to the outbreak have included mask mandates, prohibition and cancellation of large-scale gatherings (including festivals and sporting events), stay-at-home orders, and school closures.

Congress has allocated $631 million for state and local health surveillance programs, but the Johns Hopkins Center for Health Security estimates that $3.6 billion will be needed. The cost rises with the number of infections, and contact tracing is easier to implement when the infection count is lower.[40]

[39] Carter A. More Americans Have Died Of COVID-19 Than In World War I, 9/11 & Vietnam War Combined // NowThisNews. 2020. URL: https://nowthisnews.com/news/more-americans-have-died-of-covid-19-than-during-world-war-i-911-vietnam-war-combined. (24.01.2021).

[40] Setzer E. Contact-Tracing Apps in the United States // Lawfare. 2020. URL: https://www.lawfareblog.com/contact-tracing-apps-united-states. (09.03.2021).

Method of digital tracing. In the United States, not only the government, but also business, represented by technology companies, was engaged in the development of digital tracing systems. American companies Apple and Google have developed a unique bluetooth-based contact tracing technology and made this technology available to the government. This technology is based on a decentralized system - data is stored on people's phones, not on government servers. At the same time, you do not need to install any applications to use this technology, you just need to have Apple or Android phone. The system will use short-range bluetooth communication and create a voluntary contact tracing network by storing data on phones.

In addition to this technology, the government of 3 states has already begun work on digital tracing on their own. North Dakota, South Dakota and Utah have created a voluntary contact tracing app to help contain the coronavirus pandemic. These states are using alternative technology, unlike what Apple and Google have created. The focus here is on GPS data, which allows officials to manually call places where users may have spread the virus and request the names and details of others who were there at the same time. This data allows the authorities to decide which business to close due to the spread of the virus and to prioritize contacts for testing.[41]

Sources of data. Government apps take location data based on WI-FI, and GPS. Unlike the government method, Bluetooth does not track the physical location of people. It picks up the signals of nearby phones and stores the connection between them in the database. If one person tests positive for COVID-19, he/she will be able to inform the application about infection, and the application, will notify everyone who has come into contact with this person.

The system cannot identify people even after they have shared data. This is because the phones themselves perform the cryptographic calculations needed to

[41] Bradford L., Aboy M., Liddell K. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes // Journal of Law and the Biosciences. 2020. Vol. 7. Issue 1. P. 1-21.

protect privacy. The central servers only support the public key database, not the interactions between those keys.[42]

Sanctions. Administrative measures against citizens will be taken only in case of violation of one ban, introduced immediately after the start of the pandemic. All Americans returning to the country from China, Iran and the EU countries are required to undergo a medical examination and comply with a two-week quarantine. Violation of it could face a fine of up to US $ 100,000 or one year in prison.

Moreover, in each state for these violations, their own penalties can be established. For example, in Wisconsin, if a person knows that he is infected and violates quarantine, he can be fined $ 500 or taken into custody for up to 30 days. In Wyoming, isolation violations can be fined $ 10,000 or sent to jail for a year. And in Texas, the same violation can be imprisoned for up to six months and a fine of $ 2,000.[43]

Organizational structures and institutions. The federal government, through the Centers for Disease Control and Prevention, and state and local governments. CDC is a federal agency of the US Department of Health created in Atlanta in 1946 to fight malaria. The agency employed only 400 people and had a budget of $ 10 million. With this money, the CDC campaigned and organized anti-mosquito treatment throughout the country. Over time, it took over all new powers, and one department after another was transferred to it from the Ministry of Health. For example, during the outbreak of the Hong Kong flu in 1957, the CDC acquired the former ministerial department for the control of sexually transmitted infections. In 1960, the same story happened with the Department of Tuberculosis Control. The CDC is now a 10,000-employee agency with budgets that have fluctuated between $ 7.2 billion and $ 7.7 billion over the past five years. It is led by 68-year-old virologist Robert Redfield.

[42] Brandom R., Robertson A. Apple and Google are building a coronavirus tracking system into iOS and Android // The Verge. 10.04.2020. URL: https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app. (27.02.2021).

[43] Akopyan D. How quarantine violators are fined in the world. Table // RBC. 2020. URL: https://www.autonews.ru/news /5e8738d89a 79470dd14d03b6. (07.02.2021).

Legislation. The U.S. government has broad authority to request personal data in the case of a national emergency but does not have the legal authority, except in criminal investigations, to insist that companies turn it over.

With appropriate safeguards, the potential use of location data to combat coronavirus is "a real opportunity to do something positive with the technology and still protect people's privacy." But currently there are no legal controls on how the federal government might use data once it has been collected, so location information collected for a health emergency could later be acquired by the FBI or the IRS.

As of May 22, 2020, three bills have been introduced that address privacy issues related to digital contact tracing apps, one proposal from the Senate and a second proposal that has been introduced in both the House and the Senate:

- The Public Health Emergency Privacy Act (H.R. 6866, S. 3749) was introduced in the House by Representative Anna Eshoo on May 14, 2020, and referred to the Committee on Energy and Commerce the same day. The bill was introduced in the Senate by Senator Richard Blumenthal the same day and referred to the Committee on Health, Education, Labor, and Pensions.
- The COVID-19 Consumer Data Protection Act of 2020 (S. 3663) was introduced in the Senate by Senator Roger Wicker on May 7, 2020, and referred to the Committee on Commerce, Science, and Transportation the same day. A House version has not been introduced.

The three bills aimed at securing the data collected by digital contact tracing apps differ significantly in their approaches, such as:

- how and to what extent the legislation would ensure government transparency and consumer privacy;
- the scope of entities covered (private, or public and private);
- whether to preempt state laws that might require more robust consumer protections; and

- whether to provide a private right of action to individuals against companies if their data is used in an unauthorized manner.[44]

Time-boundedness. An official excerpt from the state application sites says: «Users own their data and can delete their data at any time. The use of your data is limited to COVID-19 response efforts. Any location data will be automatically deleted after 30 days». As we can see, the main restrictive measure is efforts to combat COVID-19. However, this is a very vague wording that the authorities can use for their own purposes.

Policy type. United States have left key policy choices to state governments, or even municipalities—allowing for individualized measures. This approach can work if sub-national governments receive sufficient support and there is adequate coordination across levels of government. United State's response to the COVID-19 outbreak could be characterized as decentralized, uncoordinated, slow, and it focused on educating citizens and enhancing social and human capital (the "human-driven" approach). Also, the US approach had another unique feature - multistakeholderism - the cooperation of many participants to manage the problem (cooperation between the state and business).

2.2.4 South Korean case

South Korea was one of the first countries to have COVID-19 outbreak. The government closed schools and churches, but did not impose strict restrictions. Instead of massive bans, the country has deployed an extensive contact tracing and testing system. Patient monitoring was carried out through a special digital application.[45]

Method of digital tracing. In South Korea, the government is tracing individual people using cell phone location data and using that information to compile public maps of infection zones.[46]

[44] Digital Contact Tracing Technology: Overview and Considerations for Implementation // Congressional Research Service. 2020. URL: https://fas.org/sgp/crs/misc/IF11559.pdf. (25.01.2021).

[45] Khimshiashvili P., Lindell D., Atasuntsev A., Pudovkin E. Which countries have chosen alternative strategies to combat coronavirus // RBC. 02.04.2020. URL: https://www.rbc.ru/politics /02/04/2020 /5e846ad19a79474fd1d6c01a. (02.05.2021).

[46] Turner J. S., Baxenberg S. M. Track, Trace, and Quarantine: The Role of Mobile Data in Managing the COVID-19 Pandemic // Wiley Rein LLP. 2020. URL: https://www.wiley.law/newsletter-Apr-2020PIF_Track_Trace_and_Quarantine_The_Role_of_Mobile_Data_in_Managing_the_COVID-19_Pandemic. (15.03.2021).

A technological feature of the digital tracing system in Korea is a publicly available map created by the authorities. This map used shared data from infected people to allow other people to check if they had crossed paths with infected people (Attachment C). Health authorities send phone notifications based on this card. The notifications contain very detailed information about the confirmed cases (age, gender, daily routes). The purpose of such large amounts of information disclosure is to enable people to recognize and prepare for infection.[47]

The legislation governing these tracing systems allows for the rapid disclosure of information about the movement of people. The details published may vary from building to floor and room number.

Thus, in South Korea, a centralized public database of infected persons and their movements was created, which was used by application developers not only by the state but also by the private sector.

The implementation of these applications was relatively easy, as South Korea has a very high technological enlightenment (9 out of 10 Koreans have a smartphone). But this system also has disadvantages: in some cases, the general public participated in a thorough background check and disclosed infected individuals. Some of these people suffered from unwanted invasions of privacy and even became the subject of public scorn. In restaurants, shops and other commercial premises visited by the infected, the number of visitors was often dramatically decrease.[48]

Sources of data. South Korea's IDCPA allows authorities to assess the data of infected individuals from 27 public and private organizations as follows: 22 credit card companies, 3 telecommunications companies, the National Police Agency and Credit Finance Association of Korea.

The KCDC (Korea Disease Control and Prevention Agency) can exclusively request information from cellular operators to determine the routes of infected people and determine who may be infected with the virus. This data is mapped to determine

[47] URL: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

[48] Ryan M. In defence of digital contact-tracing: human rights, South Korea and Covid-19 // International Journal of Pervasive Computing and Communications. 2020. Vol. 16. Issue 4. P. 383-407.

the routes of the infected people and the vehicles they use. To do this, the government uses cell phone data and satellite technology.[49]

Sanctions. South Korea's digital surveillance uses law enforcement and fines to sanction individuals who violate quarantine or social distancing orders. The country also begin strapping electronic wristbands on those who ignore home-quarantine orders. A refusal to use the band would result in the person being moved to a shelter, which they will have to pay for themselves.[50]

Organizational structures and institutions. South Korea's Centers for Disease Control and Prevention (KCDC) runs COVID-19 Smart Management System (SMS), a contact tracing system that runs through smartphone apps and helps the authorities analyze the movement of affected patients and those in quarantine.[51]

Legislation. Privacy violations Korea has stringent privacy protection laws, such as its 2011 Personal Information Protection Act (PIPA). This bans the collection, use and disclosure of personal data without the prior informed consent of the individual whose data are involved. PIPA was altered after the Middle East respiratory syndrome (MERS) outbreak in 2015 to allow authorities to override some of these provisions in future epidemics. The government realized that the strict criteria found within PIPA were a barrier to their response during the MERS outbreak. As a result, Korea "established a clear legal basis for collecting personal data during disease outbreaks that align with general data protection regulation guidelines"

«Following the MERS outbreak in 2015, the government amended their Infectious Disease Control and Prevention Act (IDCPA) to provide authorities with greater ability to collect and analyse data from infected individuals during outbreaks, whereby, private companies had to provide data to the Korea Centre for Disease Control and Prevention (KCDC) about their customers». [52]

[49] In the same source.

[50] Au A. Ubiquitous Gaze: Privacy Protection in the Era of COVID-19 // The MIT Computational Law Report. 2020. URL: https://law.mit.edu/pub/theubiquitousgaze/release/2. (26.03.2021).

[51] Hood L. How South Korea flattened the coronavirus curve with technology // The Conversation. 2020. URL: https://theconversation.com/how-south-korea-flattened-the-coronavirus-curve-with-technology-136202. (11.04.2021).

[52] Park S., Choi G. J., Ko H. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea - Privacy Controversies // Jama Network. 2020. URL: https://jamanetwork.com/journals/jama/fullarticle/2765252. (07.03.2021).

Thus, under the current CDPCA, public agencies including the Ministry of Health and Welfare (MOHW) and Korea Centers for Disease Control and Prevention (KCDC) can, at the outbreak of a serious infectious disease, collect, profile, and share 7 categories of data (Attachment 2) that pertain to infected individuals or those suspected to be infected. Specifically, the data that can be collected include location data (including location data collected from mobile devices); personal identification information; medical and prescription records; immigration records; card transaction data for credit, debit, and prepaid cards; transit pass records for public transportation; and closed-circuit television (CCTV) footage.[53]

Time-boundedness. All digital surveillance systems used by Korea had clear timelines. For example, people arriving in Korea had to download the application for 14 days (self-isolation period), and then they could delete it. As for digital tracing: an official statement from the Korean authorities claims that "The platform is working on a temporary basis and all personal data stored on it will be deleted after the completion of the official response to COVID-19." But it possible to see that only the storage of personal data is mentioned here, and does not in any way relate to the use of the technology itself. Therefore, there is a risk that the use of such technologies will continue after the pandemic.

Policy type. South Korea adopted centralized, coordinated, rapid, and comprehensive approaches that involved smart technology (the “techno-driven” approach). South Korea’s tracing strategy relies heavily on its digital infrastructure. The authorities did not monopolize the approach, and provided open access for all citizens as well as for the private sector, which was able to integrate these opportunities into their daily life.

[53] Park S., Choi G. J., Ko H. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea - Privacy Controversies // Jama Network. 2020. URL: https://jamanetwork.com/journals/jama/fullarticle/2765252. (07.03.2021).

2.2.5 Comparative analysis

	Russia	USA	South Korea
Method of digital tracing	Contact Tracing, Enforce Quarantine and Social Distancing Orders	Apps and Bluetooth technology	Big Data Analytics: Hot spot mapping
Sources of data	4 Telecommunications Providers and Avia companies	Government apps use WiFi data from advertising industry, cell tower data. Bluetooth technology database it's a signals from phones, so That's because the phones themselves are performing the cryptographic sources of data.	27 companies of different spheres
Sanctions	Fines for violating the quarantine regime. But current Administrative Code of the Russian Federation and regional codes of administrative offenses do not provide for the possibility of fixing violations on the basis of these systems that make it possible to establish the location of citizens.	Violation of quarantine could face a fine of up to US $ 100,000 or one year in prison. In each state for these violations, their own penalties can be established.	Law enforcement and fines for violation quarantine or social distancing orders.
Involved institutions	Federal government body - Situation Center of the Ministry of Telecom and Mass Communications of the Russian Federation.	The federal government (Centers for Disease Control and Prevention), state and local government and Business companies.	State government body - Korea Centers for Disease Control.
Legislation	No specially taken acts but there is draft order: «Regulations of information and	Currently there are no legal controls on how the federal government	Infectious Disease Control and Prevention Act (IDCPA) with

	organizational and technical interaction of the tracing system with the information systems of the interested executive bodies»	might use data once it has been collected. 2 bills have been introduced that address privacy issues related to digital contact tracing apps, on project stage: • The Public Health Emergency Privacy Act • The COVID-19 Consumer Data Protection Act of 2020	extended tracing of people abilities, redesigned due to the Korean MERS pandemic in 2015.
Time-boundaries	Article 6 of the Russian Law on Personal Data allows their processing in order to protect life and health or other vital interests without consent, if it is impossible to obtain it. That is, in this case, data processing should serve to prevent the spread of coronavirus infection and be limited in time by its spread.	An official excerpt from the state application sites says: «Users own their data and can delete their data at any time. The use of your data is limited to COVID-19 response efforts. Any location data will be automatically deleted after 30 days».	South Korean official announcement in April 2020 stated: “The platform operates on an interim basis, and all the personal data stored in it will be deleted once an official response to COVID-19 is complete”.
Policy type	Centralized «government – driven» approach	Decentralized «human-driven» approach	Centralized «techno-driven» approach
Infected people (% per population)	3,16	9,60	0,28
Deaths (% per infected people)	2, 22	1,75	1,58

Table 3. Comparative analysis

This analysis allows to conclude that there are three models for implementing surveillance policies that are unique for each country. It consists of certain type of centralization / decentralization of power, as well as the key values around which the policy is built (human / technology / state security stability).

3 contrasting approaches to digital contact tracing have emerged: a more centralized approach favored by governments in South Korea (technology-driven) and Russia (state security-driven), and decentralized, human-driven approach supported by USA and the joint Apple-Google system. Russia and South Korea demonstrated early responses that were centralized, coordinated, rapid, comprehensive. Although these regions shared borders with China, received high volumes of travelers from Wuhan, and became involved in the pandemic very early, their infected people rates were miniscule compared to that in USA.

2.3 The potential and risks of using digital tracing technology

According to the Table 3 it is possible to assume that each policy type can provide specific risks and benefits. For example, in Russian case there is a question about the legality of data collection - for example, the Ministry of Telecom and Mass Communications does not include the collection of information about citizens in order to protect health or ensure a safe epidemiological situation. The second is the risks caused by technical reasons. For example, a situation is quite likely when citizens, one of whom is sick with a coronavirus infection, live in one, but in fact they rarely see each other or do not meet at all, but at the same time they know each other regularly using communication means. As follows from the project, the likelihood of including such a neighbor in the list of controlled persons and inconveniences arising from this is high.

In case of USA - U.S. smartphone ownership rates will affect the ability to reach the estimated number threshold needed for effective digital contact tracing. The Pew Research Center found that in 2019, 81% of Americans had a smartphone, but that figure is lower for the elderly and those making less than $50,000. Those without smartphones will not benefit from public health interventions enabled by digital tracing apps.

In South Korea case - the information published on the government’s website from digital contact tracing is detailed and has the potential for privacy infringements. If information is too specific, it may allow individuals to be identified and outed, causing psychological harm to the individual, harassment or create relationship problems. Early in the outbreak, Korea’s National Human Rights Commission (NHRC) stated that some of the KCDC’s notifications were unnecessarily intrusive and their methods of disclosure should be amended.

But there are some common features that are represented in each system. For example, all analyzed models are characterized by an unlimited nature of regulation, and this can provide risks and potential both: expansion of opportunities for use for non-public purposes, a change in the degree of control over the population, the emergence of new data sets about citizens for the purposes of public regulation but there are risk of citizens' resistance to excessive control, risk of confidential information security and risks of information leakage.

These systems also have technical limitations. Firstly, even the most detailed mobile phone data may not be accurate, which complicates the use of this data to establish contacts with infected people. Even an ordinary tree or roof can become a hindrance to GPS technology.

Another important question is how technology will be able to determine whether people have been in close contact with an infected person. Technology researchers have found that GPS cannot provide such a high level of accuracy. In such cases, it is possible to use Bluetooth technology, which is designed to achieve more accurate measurements, but also has limitations: the accuracy decreases in areas with high levels of interference, such as high-density buildings or parks (especially in big cities).

All countries have different requirements for digital tracing and a different approach to implementation, which complicates the process of reaching the required number of people across the country.

Many epidemiologists have stated that such technologies will be effective if they are used by 60-80% of the population of the entire country.[54] It is very difficult to reach even the lower limit of this indicator.

To sum up, the main technological risks of digital tracing systems can be highlighted:

1. Requires all users to have high technological and Internet education: you must know how to install the application, be able to use the navigation of the application.

2. Apps may not be effective against COVID-19 unless at least 60% of the population uses them.

3. Requires people always to keep their devices with them and depends on whether the user gives permission to collect this or that information.

4. Different data formats from different tracing systems can be incompatible and can make it difficult to integrate data into common contact tracing systems.

5. Requires a lot of effort to address ethical and legal issues related to digital surveillance.

6. Data leakage or hacker attack and break-in can threat the safety of a large number of people using these systems.

Also, there is a possibility that digital tracing will be misused to monitor citizens and lead to round-the-clock monitoring. Digital tracing can be repurposed for other activities for which it was not originally intended. Confirmation of this fear can be found in history: many methods of observation in the past were initially applied in specific cases, but later grew into something more and were used for other purposes. This ability to globally control the movement of citizens can allow people to be influenced. For example, you can easily track the environment of any oppositionist and influence him.

There is also a risk of fraudsters using information. In the event of a data leak, fraudsters will be able to use information about a person's movements and contacts to their advantage.

[54] Holmes A. M., Charlton A., Derby B., Ewart L., Scott A., Shy W. Rising to the challenge: applying biofabrication approaches for better drug and chemical product development // Journal «Biofabrication». 2017. Vol. 9. P. 1-8.

In terms of potential, in the case of Covid-19, the most obvious benefit of implementing digital human tracing is to contain the virus, avoid isolation and, most importantly, protect human life. Despite the scientific uncertainty, digital systems can make a significant contribution to reducing the spread of SARS-CoV-2 infection if they are widely adopted and integrated into comprehensive public health strategies. Ultimately, there may be a trade-off between public health efficiency and privacy enhancement functions.

CONCLUSION

Through this study, one can see all the risks associated with the implementation of digital surveillance systems. Location information can hide sensitive data, hiding information not only about the location, but also about the behavior, personality, associations and actions of a person. The use of such data enables governments to place people in forced quarantine as well. So lee suppression of the population and even discrimination. If this technology ends up in the hands of "unscrupulous" governments, for which surveillance of people is already the norm, it could lead to an increase in the number of reprisals.

The main risk of all the technologies and policies described above is a lack of transparency and the fact that governments collect and store data in excess of what is required. This prevents society and researchers from assessing the problem of the intervention.

Other risks and concerns include restrictions on the movement of people based on opaque applications, lack of consent to the use of personal data (as in the case of South Korea), and the combination of digital tracing with other surveillance systems such as face recognition cameras (as in the case of Moscow). Nearly all of these technologies involve the transfer of large amounts of data to governments, many of which have a history of repression and discrimination against political dissidents. Excessive interference with confidentiality can lead to unjustified restrictions on human rights. Disclosing information can cause fear, panic, and discrimination in people.

Thus, the COVID-19 pandemic is a global public health and policy emergency that requires a lot of government effort and attention. But these efforts by states should not be used to cover up the expansion of digital surveillance systems.

Technology can help save lives, for example, by spreading information and educating people and ensuring equal access to health care. But expanded government powers over digital surveillance threaten privacy, free speech and freedom of association, undermining the effectiveness of any policy that seeks to "provide a response to the threat".

This research recommends governments not to respond to the COVID-19 pandemic with increased digital surveillance unless the following conditions are met:

1. Restrictive measures taken in connection with the pandemic, including digital tracing systems, must be regulated by law and be proportionate. The government needs to maintain transparent policies so that all citizens can study the policies and, if necessary, revise or cancel them.

2. If governments implement digital surveillance tools, then this should be strictly limited in time and only last as long as the fight against the pandemic requires.

3. The government must ensure the safe use of the data it collects. Data collection should also be limited in time. The data should not be used further for political or commercial purposes.

4. All data should be collected anonymously and the government should be responsible for this.

5. Digital surveillance technologies should be used with care and should not discriminate and discriminate against social groups.

6. If the government exchanges data with other organizations or government agencies, such exchange must be justified and regulated.

This research can also be used to better understand other aspects of the system, such as managing policy in the face of other pandemics. It can also be used to choose between feasible policy alternatives and to put them into practice based on different and even conflicting goals of the stakeholders.

Furthermore, this research made it possible to see the interactions between policies in elemental form. This gives the policy- maker more room to modify and improve the pre-existing methods for handling pandemics. First, it answers the question of which digital surveillance policies can be implemented together efficiently. Some policies are complementary. Technology-driven approach, for instance, will reduce the chance for infection without introducing new consequences to the economy. There are also policies that are inefficient when implemented in basic form, yet have great potential after being modified (human-driven approach). In particular, the education people in field of cooperation with social monitoring limits infection and also reduces the impairment of the economy resulting from complete quarantines. Rather than investing much in a single policy, multiple policies can leverage on one another to improve the state of a country under the pandemic. From this point, this research can be considered to identify the best parameters for implementation. Impactful parameters include duration or time-boundedness, technological specifics, privacy issues among other specifics that need to be defined when implementing a policy. By understanding the dynamics of the digital surveillance system, it becomes possible to finetune the best solution through the combination of best parameters.

SOURCE OF LITERATURE

Laws

1. Russian Federation. Laws. (2020). Regulation of information and organizational and technical interaction of the tracking system with information systems of interested executive authorities and operational headquarters of the constituent entities of the Russian Federation. – P. 1-7.

Books and periodicals

1. Bennett C. J. Surveillance Society: Monitoring Everyday Life // The Information Society. – 2003. – Vol. 19. – P. 335-336.
2. Borradori, G. Between Transparency and Surveillance: Politics of the Secret // Philosophy and Social Criticism. – 2016. – Vol. 42. – Issue 4–5. – P. 456-464.
3. Bradford L. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes // Journal of Law and the Biosciences / L. Bradford, M. Aboy, K. Liddell. – 2020. – Vol. 7. – Issue 1. – P. 1-21.
4. Chalmers R. Orwell or All Well? The Rise of Surveillance Culture // Alternative Law Journal. – 2005. – Vol. 30. – Issue 6. – P. 258-261.
5. Galič M. Bentham, Deleuze and Beyond: An Overviewof Surveillance Theories from the Panopticonto Participation // Philosophy & Technology / M. Galič, T. Timan, B-J. Koops. – 2017. – Vol. 30. – P. 9-37.
6. Ganascia J.-G. The Generalized Sousveillance Society // Social Science Information. – 2010. – Vol. 49. – Issue 3. – P. 489-507.
7. Giritli Nygren K. Managing the Covid-19 pandemic through individual responsibility: the consequences of a world risk society and enhanced ethopolitics // Journal of Risk Research / K. Giritli Nygren, A. Olofsson. – 2020. – Vol. 23. – P. 1031-1035.
8. Giroux H. A. Totalitarian Paranoia in the Post-Orwellian Surveillance State // Cultural Studies. – 2015. - Vol. 29. Issue 2. – P. 108-140.
9. Holmes A. M. Rising to the challenge: applying biofabrication approaches for better drug and chemical product development // Journal «Biofabrication» / A. M Holmes1, A. Charlton, B. Derby, L. Ewart, A. Scott, W. Shu. – 2017. – Vol. 9. – P. 1-8.
10. Janowski T. Digital government evolution: From transformation to contextualization // Government Information Quarterly. – 2015. – Vol. 32. – Issue 3. – P. 221-236.
11. Klimburg A. Pandemic Mitigation in the Digital Age: Digital Epidemiological Measures to Combat the Coronavirus Pandemic / A. Klimburg, L. Faesen, P. Verhagen, P. Mirtl – Hague Centre for Strategic Studies, 2020. – 26-31 pp.
12. Macnish K. The Ethics of Surveillance – An Introduction - Routledge, New York, 2017. - 216 pp.

13. Macnish, K. An Eye for an Eye: Proportionality and Surveillance // Ethical Theory and Moral Practice. – 2015. Vol. 18. - Issue 3. - P. 529-548.
14. Ryan M. In defence of digital contact-tracing: human rights, South Korea and Covid-19 // International Journal of Pervasive Computing and Communications. - 2020. – Vol. 16. – Issue 4. – P. 383-407.
15. Smorgunov L.V. Institutionalization of Governability and the Problem of Veillance in the Space of Digital Communications // South-Russian Journal of Social Sciences. – 2019. – Vol. 20. – Issue 3. – P. 62-75.
16. Smotritskaya I. State administration in conditions of development digital economy: strategic challenges and risks // STAGE: economic theory, analysis, practice. – 2018. – Vol. 4. – P. 6-72.
17. Waldo J. Engaging Privacy and Information Technology in a Digital Age / J. Waldo, H. S. Lin, L. I. Millett – Washington, DC: The National Academies Press, 2007. – 450 pp.
18. Watt E The right to privacy and the future of mass surveillance // The International Journal of Human Rights. – 2017. – Vol. 21. – Issue 7. – P. 773–799.

Electronic resources

1. Acheson R. COVID-19: The Risks of Relying on Technology to “Save Us” from the Coronavirus [Electronic resource] // Women’s International League For Peace&Freedom. – 2020. – URL: https://www.wilpf.org/covid-19-the-risks-of-relying-on-technology-to-save-us-from-the-coronavirus/. – (03.03.2021).
2. Akopyan D. How quarantine violators are fined in the world. Table [Electronic resource] // RBC. – 05.04.2020. URL: https://www.autonews.ru/news /5e8738d89a 79470dd14d03b6. – (07.02.2021).
3. Au A. Ubiquitous Gaze: Privacy Protection in the Era of COVID-19 [Electronic resource] // The MIT Computational Law Report. – 20.05.2020. URL: https://law.mit.edu/pub/theubiquitousgaze/release/2. – (26.03.2021).
4. Brandom R. Apple and Google are building a coronavirus tracking system into iOS and Android [Electronic resource] / R. Brandom, A. Robertson. – The Verge. – 10.04.2020. – URL: https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app. – (27.02.2021).
5. Carter A. More Americans Have Died Of COVID-19 Than In World War I, 9/11 & Vietnam War Combined [Electronic resource] // NowThisNews. – 22.09.2020. – URL: https://nowthisnews.com/news/more-americans-have-died-of-covid-19-than-during-world-war-i-911-vietnam-war-combined. – (24.01.2021).
6. DeAngelis S. Smart Cities and the Big Brother Syndrome [Electronic resource] // Enterra Solutions. – 02.04.2018. – URL: https://enterrasolutions.com/blog/smart-cities-and-the-big-brother-syndrome/. – (20.01.2021).

7. Digital Contact Tracing Technology: Overview and Considerations for Implementation [Electronic resource] // Congressional Research Service. – 29.05.2020. – URL: https://fas.org/sgp/crs/misc/IF11559.pdf. – (25.01.2021).
8. Hamilton I.A. Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus, and it's part of a massive increase in global surveillance [Electronic resource] // Business insider. – 14.04.2020. – URL: https://www.businessinsider.com/ countries-tracking-citizens-phones-coronavirus-2020-3. – (07.03.2021)
9. Harari Y. N. The world after coronavirus [Electronic resource] // Financial Times. – 20.03.2020. – URL: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. – (11.02.2021).
10. Holmes A. The CDC will set up a coronavirus 'surveillance and data collection system' as part of the $2 trillion stimulus bill, which President Trump just signed into law [Electronic resource] // Business insider. – 28.03. 2020. – URL: https://www.businessinsider.com/cdc-coronavirus-surveillance-and-data-collection-stimulus-package-2020-3. – (17.02.2021).
11. Hood L. How South Korea flattened the coronavirus curve with technology [Electronic resource] // The Conversation. – 21.04.2020. – URL: https://theconversation.com/how-south-korea-flattened-the-coronavirus-curve-with-technology-136202. – (11.04.2021).
12. Jo E. A. South Korea’s Experiment in Pandemic Surveillance [Electronic resource] // The Diplomat. – 13.04. 2020. – URL: https://thediplomat.com/2020/04/south-koreas-experiment-in-pandemic-surveillance/. – (07.02.2021).
13. Khimshiashvili P. Which countries have chosen alternative strategies to combat coronavirus [Electronic resource] / P. Khimshiashvili, D. Lindell, A. Atasuntsev, E. Pudovkin. – RBC. – 02.04.2020. – URL: https://www.rbc.ru/politics /02/04/ 2020/5e846ad19a79474fd1d6c01a. – (02.05.2021).
14. Kim M. J. A «travel log» of the times in South Korea: Mapping the movements of coronavirus carriers [Electronic resource] / M. J. Kim, S. Denyer. – The Washington Post. – 13.03. 2020. – URL: https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html. – (23.04.2021).
15. Kim N. «More scary than coronavirus»: South Korea's health alerts expose private lives [Electronic resource] // The Guardian. – 06.03. 2020. – URL: https://www.theguardian.com/world/2020/mar/ 06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives. – (05.03.2021).
16. Macnish, K. Surveillance Ethics [Electronic resource] // The Internet Encyclopedia of Philosophy. – URL: https://iep.utm.edu/surv-eth/. – (28.04.2021).
17. Milyukova M. Will a new contact tracing system for COVID-19 patients lead to violation of the rights of Russians? [Electronic resource] // Lawyer Newspaper. – 15.07.2020. – URL: https://www.advgazeta.ru/ag-expert/advices/novaya-

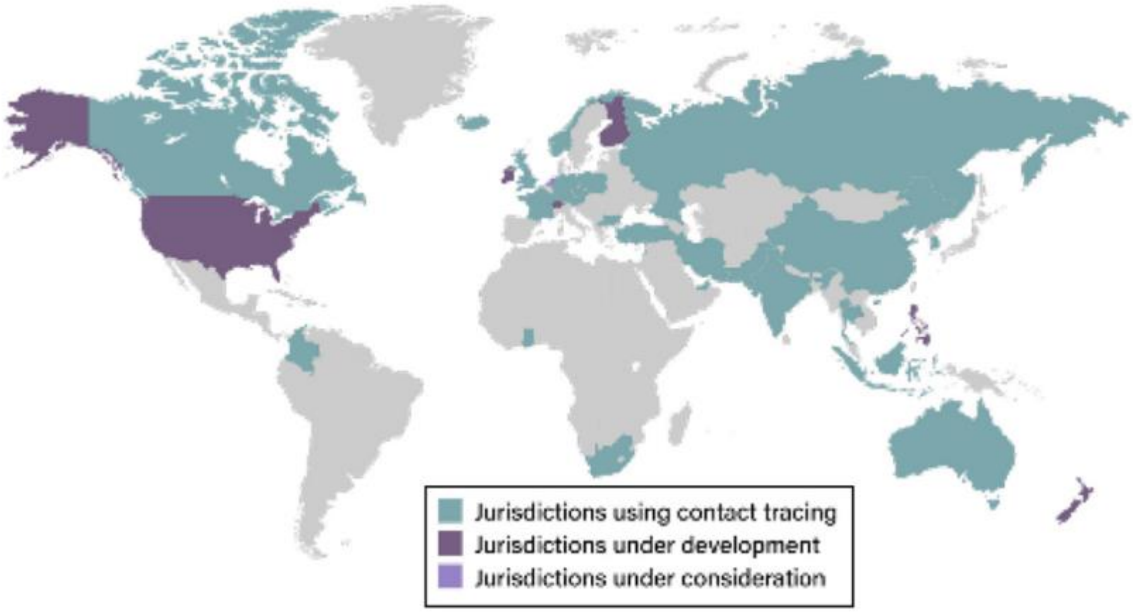
sistema-otslezhivaniya-kontaktov-zabolevshikh-covid-19-privedet-k-narusheniyu-prav-rossiyan/. – (17.02.2021).

18. Mobile Location Data and Covid-19: Q&A [Electronic resource] // Human Rights Watch. – 13.05.2020. – URL: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa. – (06.02.2021).
19. Onoprienko O. Potential carriers of coronavirus will be tracked by phone [Electronic resource] // Lawyer Newspaper. – 15.07.2020. – URL: https:// www.advgazeta.ru /ag-expert/news/potentsialnykh-nositeley-koronavirusa-budut-otslezhivat-po-telefonu/. – (16.02.2021).
20. Park S. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea - Privacy Controversies [Electronic resource] / S. Park, G. J. Choi, H. Ko. – Jama Network. – 23.04.2020. – URL: https://jamanetwork.com/journals/jama/fullarticle/2765252. – (07.03.2021).
21. Setzer E. Contact-Tracing Apps in the United States [Electronic resource] // Lawfare. – 06.05.2020. – URL: https://www.lawfareblog.com/contact-tracing-apps-united-states. – (09.03.2021).
22. Sooriyakumaran D. Surveillance will not save us from COVID-19 [Electronic resource] // Aljazeera. – 21.05. 2020. – URL: https://www.aljazeera.com/opinions/2020/5/21/surveillance-will-not-save-us-from-covid-19. – (25.03.2021).
23. Srivastava V. Surveillance, COVID-19, and the unexpected problems of a new normal [Electronic resource] // Policy Forum. – 31.07.2020. URL: https://www.policyforum.net/surveillance-covid-19-and-the-unexpected-problems-of-a-new-normal/. – (18.04.2021).
24. Tau B. Government Tracking How People Move Around in Coronavirus Pandemic [Electronic resource] // The Wall Street Journal. – 28.03.2020. – URL: https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202. – (30.04.2021).
25. Turner J. S. Track, Trace, and Quarantine: The Role of Mobile Data in Managing the COVID-19 Pandemic [Electronic resource] / J. S. Turner, S. M. Baxenberg. – Wiley Rein LLP. – 2020. – URL: https://www.wiley.law/newsletter-Apr-2020 PIF_Track_Trace_and_Quarantine_The_Role_of_Mobile_Data_in_Managing_the_COVID-19_Pandemic. – (15.03.2021).

ATTACHMENTS

Attachment A.

Picture 1. Spread of digital tracing systems over the world


Jurisdictions using contact tracing
Jurisdictions under development
Jurisdictions under consideration

Attachment B.

Picture 2. The scheme of Russian digital tracing system’ interaction

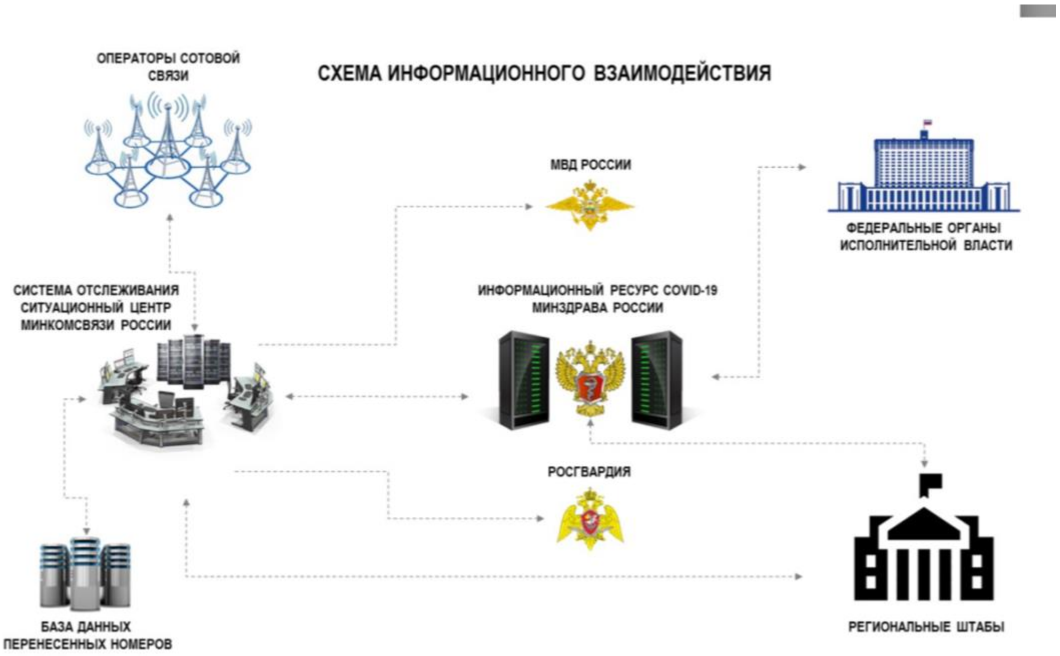
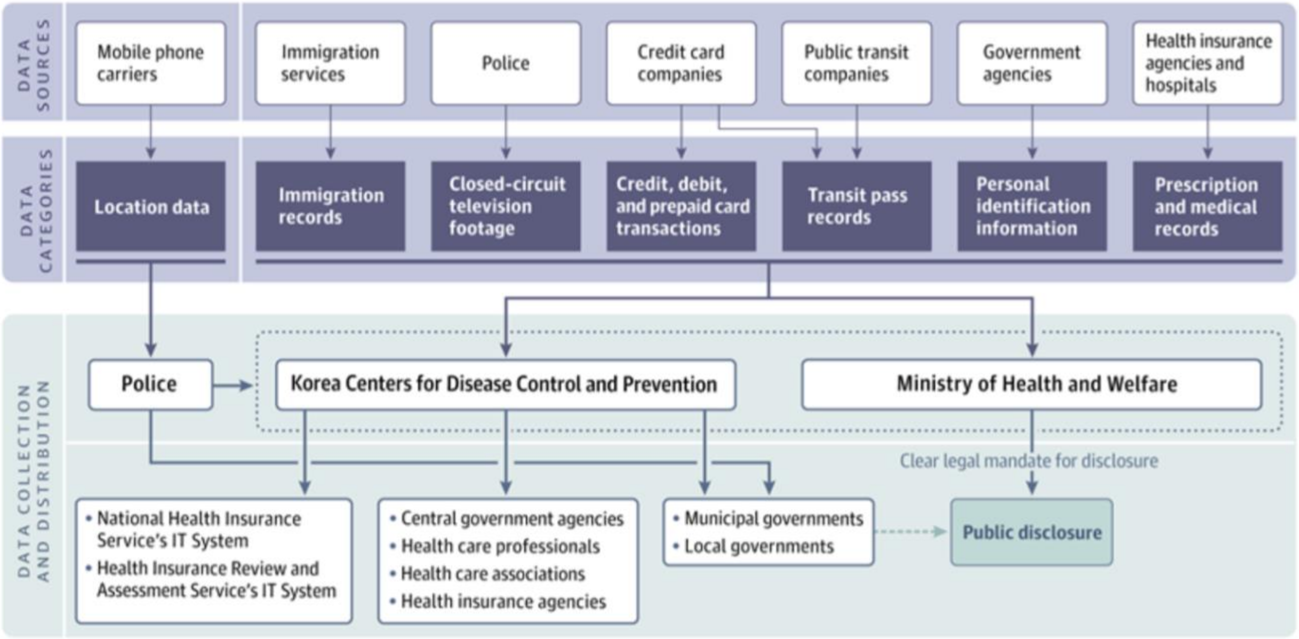


СХЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ
ОПЕРАТОРЫ СОТОВОЙ СВЯЗИ
МВД РОССИИ
ФЕДЕРАЛЬНЫЕ ОРГАНЫ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ
СИСТЕМА ОТСЛЕЖИВАНИЯ СИТУАЦИОННЫЙ ЦЕНТР МИНКОМСВЯЗИ РОССИИ
ИНФОРМАЦИОННЫЙ РЕСУРС COVID-19 МИНЗДРАВА РОССИИ
РОСГВАРДИЯ
БАЗА ДАННЫХ ПЕРЕНЕСЕННЫХ НОМЕРОВ
РЕГИОНАЛЬНЫЕ ШТАБЫ

Attachment C.

Figure 2. Coronavirus Disease 2019 Contact Tracing in Korea: Sources, Categories, Collection and distribution of data


DATA SOURCES
Mobile phone carriers
Immigration services
Police
Credit card companies
Public transit companies
Government agencies
Health insurance agencies and hospitals
DATA CATEGORIES
Location data
Immigration records
Closed-circuit television footage
Credit, debit, and prepaid card transactions
Transit pass records
Personal identification information
Prescription and medical records
DATA COLLECTION AND DISTRIBUTION
Police
Korea Centers for Disease Control and Prevention
Ministry of Health and Welfare
Clear legal mandate for disclosure
• National Health Insurance Service's IT System
• Health Insurance Review and Assessment Service's IT System
• Central government agencies
• Health care professionals
• Health care associations
• Health insurance agencies
• Municipal governments
• Local governments
Public disclosure