ESI Preprints **Not Peer-reviewed**

Surveillance in the Digital Age

Anri Nishnianidze
Ph.D. Student, Grigol Robakidze University, Georgia

Doi: 10.19044/esipreprint.12.2023.p80

Approved: 01 December 2023
Posted: 06 December 2023

Copyright 2023 Author(s)
Under Creative Commons CC-BY 4.0
OPEN ACCESS

Cite As:
Nishnianidze A. (2023). *Surveillance in the Digital Age*. ESI Preprints.
https://doi.org/10.19044/esipreprint.12.2023.p80

Abstract

Purpose: With technological progress, electronic devices have become available to almost all people. They use mobile phones, computing devices and other electronic devices every day for both personal and work purposes. The purpose of the research is to analyze how people are being monitored in the digital world and what is needed to protect citizens from mass surveillance. Design/methodology/approach: In the process of developing the research, using scientific methods, both the opinions of scientists about surveillance in the digital age and the past cases of mass surveillance of people's actions in the digital world were analyzed. Findings: In the modern era, almost everyone uses devices for various purposes. Most often they use search engines, social networks, or other means of the digital world. But, they don't realize that not every piece of data they put into cyberspace "disappears." The purpose of the study is to show how the said data is acquired, how they are used, and what dangers humanity is facing if people's private life is not protected from surveillance in the digital age. Research limitations/implications: The research aims to analyze the existing scientific works, studies and articles about the dangers of surveillance in the digital age and to show the problems that exist in the process of fighting against surveillance. In the final part of the study, a minimum of recommendations will be presented, which are important to follow, so that the constitutional rights of people are not violated in the conditions of the possibility of simplified surveillance. Originality/value: There is hardly a person who does not use an electronic device to communicate in cyberspace. They use cyberspace for both work and personal purposes. In many cases, the data that is shared in cyberspace is not secured and through automated

surveillance models, certain individuals, groups of individuals or states get hold of people's data, thereby successfully conducting surveillance. Due to the mentioned reasons, the research is of special relevance and it is important to show the means of surveillance and the ways of fighting them to protect fundamental human rights in the digital age.

Keywords: Surveillance; Digital Age; Cybersecurity; Privacy; Civil liberties

I. Introduction

With technological progress, various types of electronic devices, be it mobile phones, personal computers, or others, have become available to almost the entire population of the earth. Not only millions, but billions of people use electronic devices every day and will always carry them in their pockets, because, in modern times, existence without said devices is unthinkable. People use them for personal purposes (personal correspondence, education, listening to music) and work purposes (company management, remote software troubleshooting, financial transfers) - and for all of these, even one mobile phone is enough to achieve all of the above goals. Moreover, with the functional capabilities of modern mobile phones, many more activities are possible. Attention should be paid to one detail - all of the said activities have a place, in the new - digital world.

It is important to understand that every action that a person performs with the help of his electronic devices in the digital world leaves a digital trace, following which trace it is possible to find out for what purposes a person used this or that device (64,14-19). It is noted that such traces, like other human activities in the digital world, do not disappear easily and are stored by large companies on their servers. For their part, large companies assure users that their information is securely stored, but in practice, Data leaks have shown, in many cases the words of large companies are not true - eg. Yahoo(62,1-2), Linkedin(24,777-782), Facebook(10,22). It is a fact that the listed companies are the giants of today's digital world, however, they have failed to protect the security of their users. Therefore, a completely logical question arises in society – Are users' private data protected in the digital world? There is no exact and convincing answer as of today.

In the twentieth century, the world witnessed many local and international scandals (6,199-204), when there were cases of surveillance not on a specific person or group of persons, but on the entire population (15,25-34). Various agencies of the state, in concert or independently, conducted surveillance of the entire population. In such cases, it is easy to understand that fundamental human rights and freedoms were not being protected. The intelligence and counterintelligence services of the state explained such cases

by saying that surveillance was of special importance to prevent crimes against the interests of the state and the population - whether it was to prevent the work of the intelligence services of a hostile country or other activities (60,101-125). It is important to protect the interests of the population and the state, especially from the work of such dangerous organizations as groups of hostile intelligence services. But if, in the process of fighting the enemy, the relevant structures and agencies of the state themselves violate fundamental human rights, and the frequency of violation of rights increases, it will be impossible to have a healthy society. Where the basic rights of the population are violated, there will be nothing left to protect and democracy will no longer exist.

This study will discuss what surveillance is, how and for what purposes it was used by various government agencies, and what systems existed in the twentieth century to track the population - individually or en masse.

At the end of the twentieth century and in the twenty-first century, in the wake of technological progress, a new territory appeared - the digital world, a world where each person has found his own place. Technological progress does not stand still, and there will be many more ways to make people more comfortable in the digital world, e.g. The concept of a smart city, where almost everything will be connected to the digital world (18,12-19) - or the development of artificial intelligence, which will help people in many fields (3,928-938) and many other technologies that will accompany the progress. In such conditions, the surveillance of the population will be much easier, and the temptation for the relevant agencies of the state to monitor what activities this or that person is doing in the digital world will increase. In order to prevent such temptations, it is important to have relevant legal bases, frameworks and other acts and their active implementation, which will protect citizens not only from cybercriminals but also from the work of relevant state agencies.

The main goal of the research is to show how the surveillance methods and mechanisms have changed along with technological progress and what tools different state agencies have today in the process of surveillance of individuals or the entire population. The surveillance systems that exist in the modern world and whose main and only purpose is surveillance will be analyzed. By analyzing surveillance systems, it will be much easier for readers to understand what capabilities states have to analyze anyone's digital activity.

The final part of the study will summarize what opinions exist on surveillance in the digital world and based on the analyzed literature, recommendations will be made which are important to be processed and understood by the states in order to protect the fundamental rights and

freedoms of people in the digital world. If human rights are not protected in the real and digital worlds and their rights are ignored, such an action will be a step away from democracy and a step forward towards a dystopian reality.

II. Surveillance in the Twentieth Century and its Meaning

In the history of mankind, one of the oldest mechanisms used in the process of fighting against crime, to prevent conspiracies or for other similar purposes is surveillance (32,17-25). Since ancient times, the letters of certain persons were opened and read, so that the relevant structures of the state had information about the goals of the person of interest to them. Population surveillance was used to control whether a revolution was being prepared or not. Also, surveillance of the activities of various persons coming from abroad - that they did not commit certain actions against the interests of the state (20,291-299). Surveillance was such an accepted and well-known practice that there were also methods of combating it, e.g. Julius Caesar used a cypher when writing letters, and if the person who had the letter fell into his hands and did not know the cypher, he would have a piece of paper on which there would be a meaningless arrangement of Latin letters without any content (38,2-17). Therefore, humanity has known the importance and role of surveillance since ancient times and thought about what importance it could have in the process of protecting state interests.

Of course, as the centuries passed, methods, mechanisms and strategies were developed on how to carry out the tracking so that the desired results for the state were easily achieved. Considering the international definition of surveillance (77), it is possible to distinguish two different types:

A. Covert surveillance. This surveillance is a type of pursuit where the object or objects are unaware of the surveillance. Such tracking is carried out in the background - searching for information, opening private correspondence, listening to conversations, and more.

b. Active surveillance. Active surveillance is when a person or persons know they are being watched. The tracker is in direct contact with the object. e.g. Monitoring the location of the object openly (when the object knows that it is being monitored), meeting the object directly with hidden recording equipment, etc.

Of course, this is a general summary of what surveillance is and how it is carried out (40,9-69).

At the beginning of this research chapter, it was noted that tracking is one of the oldest mechanisms, but it is rightly noted that tracking reached its highest point of development in the twentieth century, especially during the Cold War (27,1-30). During the mentioned period, the means of tracking in the real world were raised to the highest level - as it was necessary for

twenty-four-hour surveillance of the citizens of the rival state on the territory of the country so that they did not carry out harmful intelligence activities of the state (60,101-125). However, it is important to note here that surveillance was not only used to control intelligence activities, e.g. Tracking mechanisms have caused irreparable damage to organized crime groups (41,23-25).

For research purposes, it is important to analyze practical cases. One of the well-known facts, when not only individuals, but the entire population was actively secretly watched, was the Ministry of State Security of the German Democratic Republic - the so-called Stasi activity (15,25-34). After the fall of the Berlin Wall, when Germany was reunified and the Stasi archives became public, it became known that Stasi agents monitored the activities of almost every citizen: who they wrote to, who they met, what they wrote, what they read, what they listened to, etc. Such mass surveillance is one of the most widespread surveillance systems of the twentieth century (37,741-789). Of course, the activity of the Stasi had nothing to do with the protection of human rights, and such surveillance had no legal basis. The model of surveillance mentioned is active surveillance - because virtually every citizen of East Germany knew that there was some service monitoring their every activity(8,142-161).

In contrast to the overt activities of the Stasi, the US National Security Agency's Project SHAMROCK is a classic example of covert surveillance (6,199-204). The mentioned project was implemented in the 60s of the twentieth century, and almost no one knew about its existence, when it became known about the existence of the mentioned project, the project was immediately closed. In particular, in the 70s of the same century, it became known that there was a SHAMROCK project and that within the framework of the project, all telegrams going abroad and coming from abroad were read by the National Security Agency of the United States of America (61,67-76). It is mentioned that during the existence of the project, for a certain period, the contents of 150,000 letters were analyzed monthly (48,33-34). After the information about the project was made public, there was an opinion that in the conditions of the Cold War, the existence of such a project was of special importance, since there were many intelligence officers or agents of opposing countries in the American territory, whose activities could cause great harm to the United States of America. Accordingly, it was necessary to analyze outgoing and incoming letters in order to provide a timely response if necessary. Of course, the mentioned motivation is important, but, in contrast to East Germany at that time, the fundamental human rights and freedoms protected by the country's constitution and amendments were and are especially important for the United States of America (50).

After the Watergate scandal (54,49-53), when it became known about the illegal activities of the intelligence and counter-intelligence services of the United States of America on the territory of the USA, on the initiative of Senator Frank Church, the committee, „United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities", was organized. It is simply known as the Church Committee (29:3-14). The purpose of the Church Committee was to investigate abuses of power by the Internal Revenue Service, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency. In the end, the commission identified the cases when the activities of the mentioned services did not comply with the requirements of the American Constitution and legislation, and the services used unlimited opportunities at their disposal (55,270-297). Finally, in the report of the commission, it was indicated that it was necessary and important to have a legal framework that would limit the unlimited possibilities of the aforementioned services, so that they, in the process of protecting the state and citizens, would not violate the fundamental human rights (30,198-225).

The twentieth century is rightly considered as the century of raising surveillance to the highest point. Of course, the activities of the Stasi and Project SHAMROCK were not the only surveillance programs implemented in the twentieth century. It was important to present the mentioned cases in order to make it easy for the reader to understand how surveillance worked in the real world and how much power the relevant services had to carry out surveillance. The situation has changed significantly at the end of the twentieth century and into the twenty-first century because a new area - the digital world - has become available to many people.

III. Surveillance in the Digital World

With the development of the digital world, many new tools and opportunities have appeared. What used to be complicated has become easier in the digital world. It became possible to send letters without leaving home, contact any person anywhere in the world, etc. Technological progress has simplified the lives of many people and given many people opportunities that were unimaginable and impossible in reality before progress.

The development of the digital world, along with many positive moments, also brought negative moments. In particular, a new type of criminal appeared in the digital world - cybercriminals, whose goal is to use the opportunities of the digital world to achieve their own criminal goals, using their special knowledge and computer devices (25,13-20). It should be noted here that the goal of the vast majority of cybercriminals is to obtain some financial gain (47,965-986). For this, they use various methods and

mechanisms - cyber extortion (44,105-125), cyber fraud (28,21-68) and other ways.

Based on the goals of the research, it is important to talk about several groups of cybercriminals. In particular:

A. Cyber terrorists. Part of the terrorist groups, when they realized what opportunities exist in the digital world, partially moved to cyberspace. In particular, cyber terrorists have the ability to cause significant and irreparable damage from the digital world to the real world. e.g. They can disrupt the work process of agencies of the state and damage critical infrastructure facilities in the real world (for example, cause interruption of electric power supply(36,317-318), damage a metallurgical facility(34,1-15)) and others(35,1-12).

B. Cyberespionage. In previous years, in order to carry out espionage activities, a person needed direct contact with an object in order to intercept it or to penetrate a certain facility to steal information desired by the country and other methods, which were associated with many difficulties and time. Along with the development of the digital world and the digitization of data, a new type of spies appeared - cyber spies, whose activities are radically different from classical espionage activities, in particular, they do not need direct contact and similar actions - but it is enough to have the appropriate knowledge, computer equipment and connection to the digital world (14,5-49).

C. Cybercriminals under the control of state agencies. One of the most dangerous phenomena mentioned is in the digital world because they perform any activity desired by the state. Starting from elementary massive propaganda, ending with hacking websites of various agencies of foreign countries and posting desired information. Therefore, they are cybercriminals, but, to other cybercriminals, everything they do in cyberspace is for orders from state agencies(65,347).

Therefore, it can be said that with the development of the digital world, the dangers arising from it have also increased (7,9-38). Accordingly, there is an opinion that tracking the activities in the digital world is especially important so that the relevant structures of the state can respond in time and prevent the criminal activities of cyber criminals (53,3-17). But, a fair question arises, in the process of fighting cybercriminals, to what extent will fundamental human rights and freedoms be protected? (5,183-207)

For research purposes, and to see, what surveillance systems can do in the digital world, and why fundamental human rights and freedoms protection are under question, it is first important to analyze the programs by which surveillance was carried out in the digital world.

IV. Surveillance Programs in the Digital World

1. PRISM (United States). One of the most famous surveillance programs is PRISM(58,1-6). It first became known in June 2013, when whistleblower Edward Snowden released classified files about the program. According to the files, PRISM was a National Security Agency program designed to collect and analyze information about online activity, including emails, chat messages, and communications data(2,121-144). However, the greatest possibility that the program had was that it could access data stored on the servers of such large companies as Google, Facebook and Apple(26,1-43). The disclosure of the mentioned program caused a great debate in society and the question arose about the extent to which a person's personal life is protected in the digital world. The last information about the program was available in 2013. Since then, the program has been canceled, changed, or serves other purposes - it is unknown.

2. Tempora (United Kingdom): Tempora is a UK Government Communications Headquarters program (56,1-2). It became known after Edward Snowden made classified files public. It is noted that the purpose of the program is to collect Internet traffic data - including emails, phone calls, browsing history and other activities of people in cyberspace(9,23). Of course, the existence of such a program has also led to a debate in society about how acceptable it is to have such a program that can collect and analyze such personal data. The debate continues to this day as to the extent to which such a program is necessary (33,1-5). It should be noted here that the European Court of Human Rights found that the actions taken by using the Tempora program were against fundamental human rights and freedoms(70).

3. Echelon (Multinational): Echelon is a program managed by the cooperation of several countries, namely the United States of America, Great Britain, Canada, Australia and New Zealand (66,198-215). Their main purpose is to control the network in those countries and collect any electronic information, such as e-mails, phone calls, and faxes, also, the main purpose of the program is to control the traffic of public communications and obtain relevant information for their common purposes (45,9-42). Of course, the program was kept secret for many years and they tried to keep the information about the existence of the program from becoming known, however, as a result of many investigative journalistic activities and the activities of whistleblowers, the information about the existence of the program became known (4,10-14).

4. MUSCULAR (United States): MUSCULAR was a joint surveillance program managed by the United States National Security Agency and the United Kingdom's Government Communications Headquarters. The main purpose of the program was to extract data from

companies such as Google and Yahoo, therefore, it was possible to obtain any user data that was located on the servers of the mentioned companies, including emails, documents and any other information that the user stored in his account (23,1). The mentioned program became known after the secret files made public by Edward Snowden (22,1-3). It should be noted here that the program obtained the desired information without Yahoo and Google knowing anything about it. Since then, both companies have decided to strengthen safety standards (43,1-3).

5. SORM (System for Operative Investigative Activities): The SORM program is a set of technical means and measures, with the help of which operative-investigative activities are carried out in the Russian Federation - telephone connections, Internet connections and any other activities are controlled by SORM (49, 1-22).

SORM developed in three stages.

SORM 1 - was created with the purpose of being able to listen to phone conversations.

SORM 2 - replaced SORM 1 and, in addition to telephone conversations, it became possible to analyze and monitor Internet traffic.

Sorm 3 - is the last phase of Sorm development. In the presence of SORM 3, any information can be analyzed, processed and stored for a long time. (57,23-30)

It should be noted here that according to the decision of the European Court of Human Rights in 2015, the court unanimously determined that under the conditions of the activity of the SORM program, the protection of human rights is not guaranteed, and people are not protected. The European Court of Human Rights found that the SORM program violates Article 8 of the Convention on Human Rights(71).

6. Central Monitoring System (CMS): CMS is the surveillance program of India(51,41). As noted, through the program it is possible to analyze telephone communications, as well as read e-mails, and read the correspondence on social platforms, such as Twitter, Facebook, and LinkedIn, and it should be noted here that within the framework of the program, it is possible to monitor the activities of people in the Google system, e.g. Analyzing activity such as user searches on Google (76). There are opinions that the system has much more extensive capabilities, and it can be considered an analogue of the PRISM program of the National Security Agency of the United States of America. According to one of the conclusions of Human Rights Watch, it is noted that the system may endanger fundamental human rights and freedoms(73).

7. Unit 8200: Unit 8200 is an intelligence unit of the Israeli Army, also referred to as the Central Collection Unit of the Intelligence Corps, under AMAN, Israel's Directorate of Military Intelligence (19,111-123). The

subdivisions are numerous and their activities refer to many areas, counter-intelligence, military intelligence, etc. (52,1-5) and surveillance is also among their functions (59,56). The main purpose of their surveillance is the surveillance of any kind of communication - be it phone calls or communication in the digital world. Unit 8200 is considered to be one of the strongest units in the world in a similar field, and its successful operations are still considered exemplary operations (13,4-10).

8. The Great Firewall: China's The Great Firewall, also known as the Golden Shield Project, is one of the largest systems with the dual purpose of censorship and surveillance (11,111-119). As part of the first objective, the Great Firewall blocks a number of foreign websites and applications that are considered by the authorities of the People's Republic of China to be sensitive and inappropriate, e.g. Democratic information websites, human rights websites, etc. Within the scope of censorship, search words are blocked, as a result of which it is possible to obtain censored information (16,61-76). As part of the surveillance, all Internet activity is controlled so that the potential threat to the People's Republic of China can be eliminated in time (1,442-469). Also, social media platforms such as Facebook, Twitter, Instagram, and YouTube are blocked in the People's Republic of China, and instead, the government offers the Chinese people alternatives in the form of WeChat and Weibo, which are subject to censorship and surveillance (31,1-6). Of course, there are efforts to circumvent censorship and surveillance (12,20-35) but work on the Great Firewall continues to prevent people in China from accessing the global Internet and its content (17,445-458).

The presented eight surveillance programs or systems are, of course, not a complete list of what projects exist today. Of course, it should also be understood that today there are systems about which there is no information and the existence of which is strictly confidential. Until the information about them becomes accessible to the general public as a result of active investigative activities of journalists or information disclosure by whistleblowers.

By purpose, the existence of such surveillance systems is important because, as already mentioned in the research, in the modern digital world, there are many criminal syndicates whose main and only goal is to cause significant damage to individual institutions or objects with their criminal activities. In such a reality, surveillance is essential. But, as mentioned in this chapter of the research, around two surveillance systems, the European Court of Human Rights has ruled(70) that it is against the Convention of Human Rights(71), and around the rest, there is still an active debate on how justified the existence of such surveillance systems is.

For research purposes, in order to fully understand the importance of surveillance in the digital world, it is important to present those legal and

ethical considerations that are particularly relevant today and around which active debates are taking place in various scientific fields.

V. Ethical and Legal Aspects of Surveillance

Research has repeatedly noted that the vast majority of the population today uses electronic devices, whether it is a mobile phone, a personal computer, a smart TV or other devices. In many cases, such devices are used to share various intimate details between different people - be it in a romantic or sexual context(42,15-36). At the moment of sharing such information, most people do not know that, even if they delete the chats, the information about the conversations is stored on the servers for a certain period of time, so that, if necessary, the messages can be recovered by the relevant government agencies and used for their lawful purpose (for example, if there are signs of crime in the Facebook conversations, and the alleged perpetrator deleted the messages does not mean that this chat cannot be recovered (10,22)). But, a completely logical question arises - how ethical is it to store such information, which can be accessed by surveillance systems without any problems? If citizens massively realize that their private life is known not only to them but also to surveillance systems (46,14-15), how much will it be possible to maintain public order? Of course, the ethical questions presented in the research are a very small part of the ethical and moral dilemmas that exist in the era of surveillance systems (21,15-35). However, even these minor problems lack answers from the respective states and agencies that manage surveillance systems.

All democratic states of the modern world protect the right of a person to have a private life, e.g. the Fourth Amendment of the Constitution of the United States of America (69). Basic human rights and freedoms are protected by the international declaration (78) and a number of other international acts (72). One of the most important questions that is in the order of the day is how much is the right to the private life of a person protected in the era of strengthening surveillance programs and systems? The word of the law is supreme and everyone should be subject to it, both ordinary citizens and states, government agencies, agencies and intelligence officers.

But if in any case, when the question arises around surveillance systems, whether the right to private life is protected in the process of surveillance, the answer will be that surveillance is necessary in order to fight against hypothetical and probable threats. At a certain point, if surveillance continues at such a tempo, the constitutions themselves and international agreements protecting fundamental human rights and freedoms will become hypothetical laws, because a law that cannot protect a person

from the state, and cannot guarantee human rights and freedoms - it is only a logical arrangement of words on paper and nothing else.

It is easy to understand that, where the value of the law is lost, where the rule of law is not protected, society moves away from the fundamental principles of democracy and approaches a totalitarian regime. And under totalitarian rule, no one questions whether their private life is protected, because they already know that the answer is – no, human rights are not protected. As noted in the study, a similar situation existed in post-World War II East Germany. Every citizen knew that there was some agency monitoring them and watching their every activity. Historically, it is known how East Germany and the head of surveillance, the Ministry of State Security – Stasi - ended their existence (15,25-34).

In terms of security, the manner in which the information obtained by the surveillance systems is protected is also of particular importance. It is a fact that every year, as a result of the activities of cybercriminals, the information of tens of millions of accounts is made public (24,777-782). They can steal information from powerful banking systems such as the Caymanian banking system(67). able to break into the Washington, D.C. Police Department and obtain officers' personal information(68). A completely logical question arises - To what extent they can protect the personal, intimate data obtained through the surveillance system? Of course, it is possible to say that the world's strongest protection is provided by the relevant surveillance services, but as history has shown, the action of one person is enough to call into question their security systems - we are talking about the activities of Edward Snowden, who introduced such classified information to humanity, which many states do not have similar top-level secrets (63,14-20). If Snowden was not a whistleblower, but an evil criminal whose goal would be to make public the intimate data in the system, how would the events develop? There are many questions surrounding cyber security, and as of today, no one can say that cyber security is guaranteed and that data cannot be accessed. Because, as already mentioned, millions and tens of millions of personal data are leaked on the Internet every year.

Of course, there are a number of international acts(74) whose purpose is to protect people's personal data in the digital world(75), but there is one important problem surrounding such legal acts. The pace of technology development nowadays is very fast and new and new tools are emerging every day. The legislator, who wrote the law to protect basic human rights and freedoms in the digital world, took into account the challenges and problems of reality when the law was written - It is impossible to determine what will happen, not in the next ten years, but in the next year, in the next months. e.g. A few years ago, it was unthinkable that artificial intelligence would reach the level of development it has reached in 2023. Using AI, it’s

possible to carry out censorship and propaganda, as well as surveillance, at the level of automation. The issue surrounding the encroachment of human rights and freedoms by new technologies has not been thoroughly resolved as of today.

Technology is progressing and the digital world is evolving. Many criminals use the mentioned progress to achieve their criminal goals, and the challenges facing the relevant structures and agencies of the state are very large and important. They need to respond in a timely manner to both cyber criminals and real-world criminals, but if the ethical, legal, and security issues analyzed in this chapter of the research come to the fore, the consequences of these issues will be far more destructive to a healthy society, rather than the consequences of the criminal activities of any digital or real-world criminals. Any democratic state should understand that its surveillance systems should be aimed at protecting fundamental human rights and freedoms, not the other way around.

Conclusion

It's rightly noted that the twenty-first century is a century of unprecedented technological progress, where technologies are developing at such a tempo that it is difficult to control the progress. The twenty-first century has offered humanity many innovations and many means to simplify its daily life and existence. But, as noted in the research, along with positive moments, there were also moments when the gifts of technological progress were used for negative, criminal purposes (25,13-20).

To fight crime in the digital world, both states and international communities have developed a number of strategies and mechanisms through which they successfully fight crime. One such mechanism is a surveillance system. Using it, states or international communities control human activity in the digital world. Around surveillance systems, many questions have arisen that have led to many debates and raised questions for which there are no answers to this day. One of the main unanswered questions is whether fundamental human rights and freedoms are protected in the digital world.

Everyone agrees that with technological progress, similar surveillance programs and systems must exist to protect statehood, state structures, and citizens. But it is also a fact, as the European Court of Human Rights found, that in certain cases (in the cases of Great Britain and the Russian Federation) surveillance programs are used in such a way that human rights are violated, that is, instead of protecting people from cybercriminals, the state directly violates their fundamental rights and freedoms.

Based on the literature, scientific opinions and other ideas introduced in the process of developing the research, the following recommendations are presented so that surveillance programs serve people and protect their rights and freedom, not the other way around. Namely, the following recommendations:

1. Legal basis. The first and foremost is the renewal of the legal bases. As research has repeatedly noted, technology is advancing at a rapid pace. Both international and local legislators should create special working groups to analyze technological progress and its impact on fundamental human rights and freedoms. It is easy to understand that the legislation, which was created in the period when there were no specific technologies that exist today, can no longer respond to the dangers that accompany progress. It is important to frequently update the legal bases so that fundamental human rights and freedoms are guaranteed and protected from both cyber criminals and international and state surveillance programs and systems.
2. Transparency. The study noted that the existence of today's famous surveillance programs became known, not because the state decided to tell citizens about existing surveillance programs and systems, but as a result of the investigations of journalists and the activities of whistleblowers. When an ordinary citizen receives a newspaper one morning, or while surfing on a social platform, discovers that there is some kind of surveillance program through which the state has access to both his personal communications on the social network and the information stored on his Google account, one automatically feels fear and feeling, That no one can protect his rights, because the one who should ensure the protection of his rights, on the contrary, violates his rights. It is important to have a minimum burden on the part of the state bodies so that the citizens know why the surveillance programs exist, for what purpose they function and why their work is important. When a citizen knows that there is some program PRISM or ECHELON or whatever, and when he knows that it exists so that he can live in the free world, he will not be afraid, but on the contrary, he will feel safer because he will know that the state will protect his rights and freedoms, and citizen will be Protected both in the real world and in the digital world.
3. Encouraging digital education. States should ensure that citizens have access to special courses, training or other means through which they can increase their knowledge and understand what the digital world is and what dangers arise from it. Also, courses should be encouraged that explain at a basic level what cybersecurity is and what minimum

security norms need to be met in cyberspace so that people can be safe in the digital world.

4. Protection of digital rights. States should encourage and help organizations that are narrowly specialized in the protection of human rights in the digital world. People with a specific profile of education, who are familiar with both the digital world and fundamental human rights and freedoms, will manage to protect human interests more effectively and successfully. With appropriate assistance, it will be possible to protect more victims in the digital world.
5. Development of the ethical artificial intelligence systems. The rapid progress in the development of artificial intelligence in recent years is remarkable. Many companies or surveillance systems use artificial intelligence to collect and accumulate data massively, in an automated manner, which further threatens the protection of fundamental human rights and freedoms. States and the international community must ensure the development of ethical artificial intelligence systems that protect citizens and their personal data in the digital world.

The recommendations presented in the study are a minimum basis for how states and international communities should act so that the existence of citizens in the digital world is connected with security and the protection of fundamental human rights and freedoms.

Technological progress will not stop, and in the coming years, humanity will see many unique inventions and great achievements, using which the daily life of each person will be easier. But if technological progress is accompanied by the violation of human rights, both by cybercriminals and state agencies - instead of humanity waking up to a simplified and safe future as a result of technological progress, it will wake up in a totalitarian and dystopian world.

Funding Statement: The authors did not obtain any funding for this research.

Data Availability: All the data are included in the content of the paper.

Conflict of Interest: The authors reported no conflict of interest.

References:

1. Akduman, B., 2023. From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance. Uluslararası Sosyal Bilimler Dergisi, 7(28). 442-469.
2. Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., Walker, R.B., 2014. After Snowden: Rethinking the impact of surveillance. International political sociology, 8(2). 121-144.
3. Berman, D.H., Hafner, C.D., 1989. The potential of artificial intelligence to help solve the crisis in our legal system. Communications of the ACM, 32(8). 928-938.
4. Bowden, C., 2013. The US surveillance programmes and their impact on EU citizens' fundamental rights. 10-14.
5. Bronitt, S., 1997. Electronic surveillance, human rights and criminal justice. Australian Journal of Human Rights, 3(2). 183-207.
6. Brennan, B., Gilbert, K., 1983. The Puzzle Palace: A Report on America's Most Secret Agency. In The Fletcher Forum, Vol. 7, No. 1. 199-204.
7. Brenner, S.W., 2010. Cybercrime: criminal threats from cyberspace. Bloomsbury Publishing. 9-38.
8. Bruce, G., 2010. The firm: The inside story of the Stasi. Oxford University Press. 142-161.
9. Bump, P., 2013. The UK Tempora Program Captures Vast Amounts of Data–and Shares with NSA. The Atlantic Wire 21(06). 23.
10. Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17(1). 22.
11. Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., Zhipeng, Z., 2019. The Golden Shield Project of China: A decade later—an in-depth study of the Great Firewall. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 111-119.
12. Clayton, R., Murdoch, S.J.,Watson, R.N., 2006. Ignoring the great firewall of China. In International Workshop on Privacy Enhancing Technologies. Springer Berlin Heidelberg. 20-35.
13. Cordey, S., 2019. The Israeli Unit 8200–An OSINT-based study: Trend Analysis. ETH Zurich. 4-10.
14. Deibert, R., Rohozinski, R., Manchanda, A., Villeneuve, N., Walton, G., 2009. Tracking ghostnet: Investigating a cyber espionage network. 5-49.
15. Dennis, M. and Laporte, N., 2014. The Stasi: Myth and Reality. Routledge. 25-34.

16. Ensafi, R., Winter, P., Mueen, A., Crandall, J.R., 2015. Analyzing the great firewall of China over space and time. Proc. Priv. Enhancing Technol., 2015(1). 61-76.
17. Ensafi, R., Fifield, D., Winter, P., Feamster, N., Weaver, N., Paxson, V., 2015. Examining how the great firewall discovers hidden circumvention servers. In Proceedings of the 2015 Internet Measurement Conference. 445-458.
18. Eremia, M., Toma, L., Sanduleac, M., 2017. The smart city concept in the 21st century. Procedia Engineering, 181. 12-19.
19. Fiegenbaum, A., 2007. Elite Units of the Israeli Defense Forces-The Story of Unit 8200. In The Take-off of Israeli High-Tech Entrepreneurship During the 1990s. Emerald Group Publishing Limited. 111-123.
20. Foucault, M., 2023. Discipline and punish. In Social Theory Re-Wired. Routledge. 291-299.
21. Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R., Peissl, W., 2017. Surveillance, privacy and security. Taylor & Francis. 15-35.
22. Gellman, B., Soltani, A., 2013. NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. The Washington Post. 30. 1-3.
23. Gellman, B., Soltani, A., Peterson, A., 2013. How we know the NSA had access to internal Google and Yahoo cloud data? The Washington Post. 10(30). 1.
24. Gibson, B., Townes, S., Lewis, D., Bhunia, S., 2021. Vulnerability in massive API scraping: 2021 LinkedIn data breach. International Conference on Computational Science and Computational Intelligence (CSCI). 777-782.
25. Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. Journal in computer virology, 2. 13-20.
26. Greenwald, G., MacAskill, E., 2013. NSA Prism program taps into user data of Apple, Google and others. The Guardian, 7(6). 1-43.
27. Holden, R.H., 1999. Securing Central America against communism: The United States and the modernization of surveillance in the Cold War. Journal of Interamerican Studies and World Affairs, 41(1). 1-30.
28. Howard, R., 2009. Cyber fraud: tactics, techniques and procedures. CRC press. 21-68.
29. Johnson, L.K., 2004. Congressional supervision of America's secret agencies: The experience and legacy of the Church Committee. Public Administration Review, 64(1). 3-14.

30. Johnson, L.K., 2008. The Church Committee investigation of 1975 and the evolution of modern intelligence accountability. Intelligence and National Security, 23(2). 198-225.
31. Kalathil, S., 2017. Beyond the great firewall: How China became a global information power. Washington, DC: Center for International Media Assistance. 1-6.
32. Laidler, K., 2008. Surveillance Unlimited: How we've become the most watched people on Earth. Cambridge. 17-25.
33. Lanchester, J., 2013. The Snowden files: Why the British public should be worried about GCHQ. The Guardian, 3. 1-5.
34. Lee, R. M., Assante, M. J., Conway, T. 2014. German steel mill cyber attack. Industrial Control Systems, 30(62). 1-15.
35. Lewis, J.A., 2002. Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: Center for Strategic & International Studies. 1-12.
36. Liang, G., Weller, S. R., Zhao, J., Luo, F., Dong, Z. Y. 2016. The 2015 Ukraine blackout: Implications for false data injection attacks. IEEE transactions on power systems, 32(4). 317-318.
37. Lichter, A., Löffler, M., Siegloch, S., 2015. The economic costs of mass surveillance: Insights from Stasi spying in East Germany (No. 9245). IZA Discussion Papers. 741-789.
38. Luciano, D., Prichett, G., 1987. Cryptology: From Caesar ciphers to public-key cryptosystems. The College Mathematics Journal, 18(1). 2-17.
39. Lyon, D., 2001. Facing the future: Seeking ethics for everyday surveillance. Ethics and information technology, 3. 171-180.
40. Lyon, D., 2007. Surveillance studies: An overview. 9-69.
41. Martin, J., 2014. Mafia in Florida and Cuba: FBI Surveillance of Meyer Lansky and Santo Trafficante, Jr. The Charleston Advisor, 16(1). 23-25.
42. Miguel, C., 2018. Personal relationships and intimacy in the age of social media. Springer. 15-36.
1. 43.Miller, C.C., 2013. Angry Over US Surveillance, Tech Giants Bolster Defences. New York Times, 31. 1-3.
43. Minnaar, A. 2019. Cybercriminals, cyber-extortion, online blackmailers and the growth of ransomware. Acta Criminologica: African Journal of Criminology & Victimology, 32(2). 105-125.
44. Mombelli, I., Piodi, F., 2014. The Echelon Affair: The EP and the global interception system 1998-2002. European Parliament History Series. 9-42.
45. Moran, S., 2015. Surveillance ethics. Philosophy Now, 110. 14-15.

46. Nicholls, J., Kuppa, A., Le-Khac, N.A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9. 965-986.
47. Owen, M.D., 2012. A review of intelligence oversight failure: NSA programs that affected Americans. Military Intelligence Professional Bulletin. 33-34.
48. Polyakova, A., Meserole, C., 2019. Exporting digital authoritarianism: The Russian and Chinese models. Policy Brief, Democracy and Disorder Series. 1-22.
49. Ponder, J., 2006. Operation Shamrock: NSA's First Domestic Spying Program Was Revealed by Congress in 1975. Pensito Review.
50. Reddy, J., 2014. The Central Monitoring System and Privacy: Analysing What We Know So Far. Indian JL & Tech., 10. 41.
51. Reed, J., 2015. Unit 8200: Israel's cyber spy agency. Financial Times, 10. 1-5.
52. Reveron, D.S., 2012. Cyberspace and national security: threats, opportunities, and power in a virtual world. Georgetown University Press. 3-17.
53. Ritchie, D.A., 1998. Investigating the Watergate scandal. OAH Magazine of History, 12(4). 49-53.
54. Schwarz Jr, F.A., 2007. The Church Committee and a new era of intelligence oversight. Intelligence and National Security, 22(2). 270-297.
55. Shubber, K., 2013. A simple guide to GCHQ's internet surveillance programme Tempora. Wired UK, 24. 1-2.
56. Soldatov, A. and Borogan, I., 2013. Russia's surveillance state. World Policy Journal, 30(3). 23-30.
57. Sports, P.O.L., 2013. NSA slides explain the PRISM data-collection program. 1-6.
58. Tawil-Souri, H., 2016. Surveillance sublime: The security state in Jerusalem. Jerusalem Quarterly, (68). 56.
59. Taylor, S.A., Snow, D., 1997. Cold War spies: Why they spied and how they got caught. Intelligence and National Security, 12(2). 101-125.
60. Theoharis, A.G., 1984. Researching the intelligence agencies: The problem of covert activities. The Public Historian, 6(2). 67-76.
61. Thielman, S., 2016. Yahoo hack: 1bn accounts compromised by biggest data breach in history. The Guardian, 15. 1-2.
62. Verble, J., 2014. The NSA and Edward Snowden: surveillance in the 21st century. ACM Sigcas Computers and Society, 44(3). 14-20.
63. Weiss, A., 2009. A digital trail is forever. NetWorker, 13(2). 14-19.

64. Weissbrodt, D., 2013. Cyber-conflict, cyber-crime, and cyber-espionage. Minn. J. Int'l L., 22. 347.
65. Wright, S., 2005. The ECHELON trail: An illegal vision. Surveillance & Society, 3(2/3). 198-215.
66. BBC News. 2019 "Cayman National suffers Manx bank 'data hack,'". 19 November, Available at: https://www.bbc.com/news/world-europe-isle-of-man-50475734 (Accessed: September 1, 2023).
67. CNN. 2021 "DC Police Personnel Files Obtained by Hackers in Recent Ransomware Attack, Acting Police Chief Says". 29 April, Available at: https://www.cnn.com/2021/04/29/politics/dc-police-ransomware-attack-personnel-files/index.html (accessed September 1, 2023).
68. Constitution of the United States: Fourth Amendment. Available at: https://constitution.congress.gov/constitution/amendment-4/ (Accessed: September 1, 2023).
69. ECHR (Big Brother Watch and Others v. United Kingdom) HUDOC - European Court of Human Rights, Coe. int. Available at: https://hudoc.echr.coe.int/eng?i=001-186048 (Accessed: September 1, 2023).
70. ECHR (CASE OF ROMAN ZAKHAROV v. RUSSIA) HUDOC - European Court of Human Rights, Coe. int. Available at: https://hudoc.echr.coe.int/eng?i=003-5246347-6510358 (Accessed: September 1, 2023).
71. European Convention on Human Rights. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed: September 1, 2023).
72. HRW "India: New monitoring system threatens rights". 7 June, Human Rights Watch. Available at: https://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights (Accessed: September 1, 2023).
73. The Data Protection Directive. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046 (Accessed: September 1, 2023).
74. The General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed: September 1, 2023).
75. Time. 2013 "In India, prism-like surveillance slips under the radar.". 30 June, Available at: https://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/ (Accessed: September 1, 2023).

76. Surveillance definition & meaning. Dictionary.com. Available at: https://www.dictionary.com/browse/surveillance (Accessed: September 1, 2023).
77. Universal Declaration of Human Rights. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: September 1, 2023).