14 years ESJ
Special edition

Peer-reviewed

Surveillance in the Digital Age

Anri Nishnianidze, PhD Candidate In Law
Grigol Robakidze University, Georgia

Doi:10.19044/esj.2024.v20n37p1

Submitted: 01 December 2023
Accepted: 26 January 2024
Published: 21 February 2024

Cite As:
Nishnianidze A. (2024). *Surveillance in the Digital Age.* European Scientific Journal, ESJ. 20 (37), 1. https://doi.org/10.19044/esj.2024.v20n37p1

Abstract

Purpose: As technology advances, electronic devices have become ubiquitous among individuals of all backgrounds. From mobile phones to computing devices, people rely on these tools on a daily basis for both personal and professional purposes. The presented research seeks to investigate the extent to which individuals are being monitored in the digital realm and identify solutions to safeguard citizens from the threat of mass surveillance.

Findings: In the modern era, it is common for people to utilize various devices for a multitude of purposes, such as search engines and social networks. However, many are unaware that the information they share online is not always erased from cyberspace. This study aims to shed light on how this data is obtained and utilized and the potential risks humanity faces if privacy is not safeguarded in the digital age.

Research limitations/implications: The objective of this research is to thoroughly examine the current scientific literature, studies, and articles regarding the perils of surveillance in the digital era. The paper aims to highlight the challenges associated with combating surveillance. In the concluding section of the analysis, a concise set of recommendations will be provided, which are crucial to uphold in order to safeguard individuals' constitutional rights in the face of the potential ramifications of streamlined surveillance.

Originality/value: In today's digital age, it has become almost universal for people to communicate through electronic devices in cyberspace, whether for work or personal purposes. Unfortunately, this environment is often not secure, and automated surveillance models can be used to acquire people's data

without their knowledge or consent. This raises serious concerns about privacy and the protection of fundamental human rights. That is why it is essential to conduct research that sheds light on the means of surveillance and explores ways to fight against it.

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

I. Introduction

The fast-paced technological advancements in today's world have led to the widespread use of electronic gadgets such as mobile phones and personal computers. These devices have become an integral part of people's daily lives, and it is hard to imagine a routine without them. The versatility of electronic gadgets has made them indispensable for both personal and professional purposes, such as communication, learning, managing businesses, troubleshooting software issues remotely, transferring funds, and much more. With just a single mobile phone, one can accomplish a plethora of tasks, such as browsing the internet, accessing social media platforms, sending and receiving emails, managing their finances, and staying connected with loved ones. The remarkable advancements in modern technology have enabled people to do much more than they ever thought possible. It is worth noting that all these activities are a part of the digital world, which has revolutionized the way people live, work, and interact with the world around them.

It is crucial to understand that every action performed on a digital device generates a trace that can be used to determine for what purpose the device was used (Weiss, 2009). These traces, like other digital activities, are not immediately removed and are stored on servers by large corporations. Although these corporations assure users that their data is secure, the occurrence of data breaches has demonstrated that their claims are often misleading. Major companies such as Yahoo (Thielman, 2016), LinkedIn (Gibson et al., 2021), and Facebook (Cadwalladr & Graham-Harrison, 2018) have failed to protect the privacy of their users. This leads to the question: Is personal data safeguarded in the digital world? Currently, there is no definite or convincing response to this inquiry.

Throughout the twentieth century, numerous local and international scandals have unfolded (Brennan & Gilbert, 1983), marked by instances of surveillance on entire populations rather than specific individuals or groups (Dennis & Laporte, 2014). These operations were often conducted by state agencies acting together or on their own. Unfortunately, in such cases, it becomes clear that the protection of fundamental human rights and freedoms was not a priority. Intelligence and counterintelligence services often justified such actions by citing the need to prevent crimes against the interests of the

state and its people, such as espionage by hostile countries or other nefarious activities (Taylor & Snow, 1997). Protecting the interests of the state and its people is undoubtedly crucial, especially in the face of threats from dangerous organizations like hostile intelligence services. However, if state agencies themselves violate the fundamental human rights of their citizens in the process of combating these threats and the frequency of such violations increases, society cannot remain healthy. When the fundamental rights of the population are disregarded, democracy ceases to exist, and all that remains to protect is an empty shell.

This research aims to explore the concept of surveillance, its various applications by government agencies, and the systems that existed in the 20th century to monitor individuals or groups. The study will delve into the definition of surveillance, its purpose, and the different ways it has been implemented by government entities. Additionally, the investigation will shed light on the technologies that were used to track people, whether individually or en masse. The findings of this research will provide insights into the evolution of surveillance systems and their impact on society.

As humankind entered the new millennium, the digital world emerged as a new frontier in technological advancement. With each individual finding their own place in this digital landscape, progress continued to push the boundaries of comfort and convenience, from the concept of smart cities, where everything is connected to the digital world (Eremia et al., 2017), to the development of artificial intelligence aiding people in countless fields (Berman & Hafner, 1989), also many other cyber technologies that will accompany the progress. As a result, monitoring the population becomes more accessible, and the temptation for state agencies to monitor individuals' activities increases. To prevent such temptations, it is crucial to establish legal bases, frameworks, and other acts for the active protection of citizens against not only cybercriminals but also state agencies.

The central objective of this research is to demonstrate the evolution of surveillance methods and mechanisms in response to technological advancements, as well as to examine the tools utilized by various state agencies in conducting surveillance on individuals or entire populations. The study will focus on modern surveillance systems dedicated solely to monitoring. By delving into these systems, readers will gain valuable insight into the extent of the state's capacity to scrutinize digital activity.

The study's concluding segment will provide an overview of prevailing perspectives on digital surveillance. Drawing on the analyzed literature, the study will offer crucial recommendations intended to safeguard the fundamental rights and freedoms of individuals in the digital realm. Neglecting the protection of human rights in both the physical and digital

worlds and dismissing their significance would be a regressive move away from democratic ideals and towards an ominous, dystopian future.

II. Surveillance in the Twentieth Century and its Meaning

The use of surveillance has been recognized as an essential tool in maintaining the safety and security of the state. Over the centuries, various technological advancements have been made in the field of surveillance to improve its effectiveness and efficiency. Throughout the course of human history, the practice of surveillance has been an essential means to prevent criminal activities, expose conspiracies, and safeguard the interests of the state (Laidler, 2008). This practice of keeping an eye on individuals and groups can be traced back to ancient times when officials used to read the letters of certain individuals to gain insight into their objectives. In addition, foreign visitors were closely monitored to ensure that they did not engage in activities that could harm the state's interests (Foucault, 2023). This practice of surveillance was so widespread that methods were developed to counter it. For instance, Julius Caesar famously used a cypher to protect the contents of his letters (Luciano & Prichett, 1987).

Over the course of history, surveillance has been an integral aspect of statecraft, with various techniques, systems, and approaches being developed to conduct effective tracking activities. Due to the universally accepted definition of surveillance (Surveillance, n.d.), it is possible to categorize surveillance into two distinct types:

1. Covert surveillance - Covert surveillance is a type of surveillance that involves monitoring an individual or a group without their knowledge or consent. The objective of covert surveillance is to observe and gather information about the target's activities, conversations, and movements without alerting them. This type of surveillance is usually conducted in secrecy, making it difficult for the target to detect that they are being monitored. Covert surveillance techniques can include searching for information, opening private correspondence, listening to conversations, and other methods that allow the observer to gather information while remaining undetected.

2. Active Surveillance - Active surveillance is a type of surveillance in which the object or person being monitored is fully aware of the surveillance activity. This means that the tracker is in direct communication with the object and informs them that they are being monitored. The main aim of active surveillance is to gather information or evidence in a legal and ethical manner. Active surveillance techniques could include openly monitoring the object's location, meeting the object directly with hidden recording equipment, or any other method of surveillance that involves direct communication between the tracker and the object.

Of course, this is a general overview of how surveillance is conducted (Lyon, 2007). It is essential to keep in mind that surveillance is a complex and multifaceted concept that encompasses a wide range of practices and technologies.

In the introductory section of this research chapter, it was observed that surveillance has been a longstanding practice. Nevertheless, it is worth mentioning that the advancement of surveillance technology reached its pinnacle in the twentieth century, particularly during the Cold War era (Holden, 1999). During this time, surveillance methods in real-life situations were elevated to unprecedented levels, as it was imperative to conduct twenty-four-hour surveillance of rival state citizens within the country's borders in order to prevent them from engaging in harmful intelligence activities (Taylor & Snow, 1997). It is important to note, however, that surveillance was not solely employed for intelligence control purposes, as tracking mechanisms have also inflicted irreparable damage on organized criminal groups (Martin, 2014).

Conducting thorough research is a critical aspect of gaining a comprehensive understanding of a topic. One such example is the Ministry of State Security of the German Democratic Republic, also known as the Stasi - this organization implemented a vast and covert surveillance system that monitored not just individuals but the entire population (Dennis & Laporte, 2014). After the Berlin Wall fell and Germany was reunited, the public was allowed access to the Stasi archives. These archives revealed that the agents had been keeping a close eye on almost every aspect of citizens' lives, including their communication, reading material, meetings, written content, and even their listening habits. The scope of the Stasi's mass surveillance system was one of the most extensive of the 20th century (Lichter et al., 2015). However, it was not legally authorized, and its purpose was not to protect human rights. The type of surveillance used by the Stasi was active, meaning that nearly every citizen of East Germany was aware of being monitored, which had a significant impact on their daily lives (Bruce, 2010). The Stasi's actions serve as a stark reminder of the dangers of such mass surveillance systems and the importance of protecting human rights and privacy.

During the Cold War, the U.S. National Security Agency's Project SHAMROCK was implemented in the 1960s as a covert surveillance program aimed at monitoring all telegrams sent and received from abroad (Theoharis, 1984). The project remained unknown to the general public until the 1970s, when it was revealed that the National Security Agency was analyzing the contents of around 150,000 letters every month (Owen, 2012). However, the project was immediately shut down after it became public knowledge. The existence of Project SHAMROCK was considered crucial during the Cold War, as there were numerous intelligence officers or agents of opposing

countries operating within the U.S. territory. The project was designed to provide a timely response if necessary and to ensure the safety of the United States of America. Despite the project's significance, the United States of America is a country that upholds fundamental human rights and freedoms protected by the Constitution and amendments. The Constitution and its amendments ensure that the U.S. government respects its citizens' right to privacy and that any surveillance must be carried out in compliance with the law (Ponder, 2006). In contrast to the overt activities of the East German Stasi, the SHAMROCK project was a classic example of covert surveillance, which was not known to the public (Brennan & Gilbert, 1983). The SHAMROCK project was designed to provide a timely response to any threats to the United States of America's security, but the fundamental human rights and freedoms protected by the country's Constitution and amendments were and still are of utmost importance.

The Watergate scandal of 1972 brought to light the illegal activities of the intelligence and counterintelligence services of the United States of America within the country's borders (Ritchie, 1998). In response to this, Senator Frank Church proposed the formation of a committee known as the "United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities." This committee, commonly referred to as the Church Committee, was tasked with investigating abuses of power by various government agencies, including the Internal Revenue Service, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency (Johnson, 2004). The Church Committee's primary objective was to identify cases where the activities of these services were not in compliance with the American Constitution and legislation. The commission sought to uncover instances where these agencies had used their unlimited power and resources to violate fundamental human rights while attempting to protect the state and its citizens (Schwarz Jr., 2007). Through their investigations, the committee discovered various violations of privacy and civil liberties by these agencies. Ultimately, the commission concluded that it was necessary to establish a legal framework to regulate the extensive powers of these agencies. The report of the Church Committee recommended the implementation of measures to limit the unlimited possibilities of these services so that they could perform their duties without violating the rights of the American people (Johnson, 2008). The findings of the Church Committee were instrumental in shaping the policies and regulations of intelligence agencies in the United States, ensuring that their activities remain within the bounds of the law and the Constitution.

The twentieth century was a time when surveillance was taken to unprecedented levels. While the activities of the Stasi and Project SHAMROCK are often cited as examples of surveillance programs, there

were many others that were implemented during this time. These programs were designed to keep a close eye on citizens and gather information about their activities. By presenting these cases, it becomes easier to understand how surveillance worked in the real world, as well as the immense power that the relevant services had to carry out these operations. However, as humankind moved into the twenty-first century, the situation changed dramatically. With the advent of the digital world, a whole new area of surveillance became available to many people. This has had a profound impact on people's lives as they have become increasingly reliant on digital technologies for communication, work, and leisure.

III. Surveillance in the Digital World

In today's digital age, people are exposed to an extensive range of technological tools and opportunities that have revolutionized the way they live. The convenience of staying connected with people across the globe and sending letters from the comfort of our homes is now a reality. The advent of innovative technologies has simplified their lives, making it possible to access endless opportunities that once seemed beyond our reach. With this progress, the boundaries of what one can achieve have been pushed further, enabling them to explore and achieve what was once thought impossible.

With the rapid advancement of technology and the increasing reliance on digital platforms, the world has witnessed a surge in cybercrime. The emergence of cybercriminals has posed a significant threat to the security of the digital world. These criminals leverage their technical expertise and sophisticated computer equipment to exploit vulnerabilities in the digital infrastructure and carry out their nefarious activities. From stealing personal information to launching devastating cyber attacks, the impact of these cybercriminals can be far-reaching and damaging (Gordon & Ford, 2006). It should be noted here that the vast majority of cybercriminals aim to obtain some financial gain (Nicholls et al., 2021). They use various methods and mechanisms - cyber extortion (Minnaar, 2019), cyber fraud (Howard, 2009) and others.

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

1. Cyber Terrorists. In recent times, there has been a growing concern over certain groups of terrorists who have realized the enormous potential that the digital world holds and have consequently shifted their operations to cyberspace. These individuals, who are known as cyber terrorists, leverage various digital tools and technologies to inflict substantial and irreversible harm from the digital realm to the physical world. Through their nefarious actions, cyber terrorists can impede the functioning of governmental agencies, disrupt critical services, and cause extensive damage to crucial infrastructure

facilities in the real world. This poses a significant threat to national security as it becomes increasingly difficult to protect against such cyber threats. Cyber terrorists often use sophisticated techniques such as hacking, phishing, and social engineering to access sensitive data and exploit vulnerabilities in computer systems. They can also use malware and other forms of malicious software to disrupt operations and cause chaos. For example: Causing interruption of electric power supply (Liang et al., 2016), Damage to a metallurgical facility (Lee, 2014) and other criminal acts (Lewis, 2002).

2. Cyberespionage. In the past, espionage activities were often carried out through physical means, such as breaking into an object or facility to intercept or steal specific information. These methods were often complicated and time-consuming, requiring a lot of effort and resources. However, with the rapid advancement of digital technology and the increasing digitization of data, a new form of espionage has emerged - cyber espionage. Unlike traditional espionage, cyber espionage activities do not require direct contact or physical access to the target. Instead, cyber spies use their knowledge of computer equipment and access to the digital world to carry out their activities. They leverage various tools and techniques to gain access to sensitive information, monitor communication channels, and steal confidential data. Cyber espionage has become a significant threat to national security and the private sector, as it allows spies to operate in a completely different way compared to traditional spies. The use of sophisticated hacking tools and techniques makes it easier for cyberspies to conduct espionage activities, and the risk of being caught is relatively low. Consequently, governments and organizations need to be more vigilant and proactive in protecting their information and infrastructure from cyber espionage attacks (Deibert et al., 2009).

3. Cybercriminals Under the Control of State Agencies. The digital world has become a hub for cybercriminals that operate under the control of state agencies. This phenomenon is considered one of the most dangerous, as these cybercriminals carry out any activity desired by their respective states. Their actions range from conducting elementary propaganda on a massive scale to hacking websites of foreign agencies and posting desired information. Despite being classified as cybercriminals, they operate in a unique manner, as their every move in cyberspace is dictated by orders from state agencies. This makes them a formidable force that poses a severe threat to the digital security landscape (Weissbrodt, 2013).

Therefore, it can be said that with the development of the digital world, the dangers arising from it have also increased (Brenner, 2010). 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 (Reveron, 2012). However,

a fair question arises: to what extent will fundamental human rights and freedoms be protected while fighting cybercriminals (Bronitt, 1997)?

In order to gain a better understanding of the capabilities of surveillance systems in the digital realm and to address concerns around the protection of fundamental human rights and freedoms, it is imperative to conduct a thorough analysis of the programs used to carry out such surveillance. By delving into the technical details of these systems, it becomes possible to gain insight into their inner workings and assess their potential impact on individual privacy and civil liberties.

IV. Surveillance Programs in the Digital World

1. PRISM (United States). In June 2013, whistleblower Edward Snowden came forward with classified files that revealed details about one of the most prominent surveillance programs in history - PRISM (Sports, 2013). This revelation sparked a significant debate in society about the extent to which personal privacy can be safeguarded in the digital world. Many people were concerned that the program's existence posed a threat to their privacy and civil liberties. Despite the public outcry, no further information about the program's operations was released after 2013. It is unclear whether the program was suspended, altered, or repurposed for other uses.

According to Edward Snowden's files, PRISM was a program created by the National Security Agency that was designed to collect and analyze online activity data, including emails, chat messages, and communications data (Bauman et al., 2014). However, the most significant aspect of the program was its ability to access and retrieve data stored on the servers of large companies such as Google, Facebook, and Apple (Greenwald & MacAskill, 2013).

PRISM program was a highly controversial and secretive government surveillance initiative with the capability to collect and analyze vast amounts of personal data. The public disclosure of the program raised serious concerns about privacy and personal liberties in the digital age, and its current status remains unknown.

2. Tempora (United Kingdom): Tempora is a U.K. Government Communications Headquarters program (Shubber, 2013). In 2013, former National Security Agency contractor Edward Snowden revealed that the US government had been operating a secret program called PRISM. The program's primary objective was to gather extensive Internet traffic data from various sources, including emails, phone calls, browsing history, and other online activities of individuals. The program was reportedly designed to allow government intelligence agencies to monitor and track potential threats to national security, both domestically and abroad (Bump, 2013).

It must be noted that the creation of a program that is capable of collecting and analyzing personal data has sparked a great deal of debate within society. The discussion centers on whether or not it is acceptable to have such a program in place, and if the benefits of its use outweigh the potential drawbacks. This debate has continued to this day and has raised important questions about the extent to which such a program is necessary, as well as the ethical implications of its implementation. While some argue that such a program is necessary for the safety and security of individuals, others contend that it is a violation of privacy and a threat to personal freedom. The debate remains ongoing and requires careful consideration of all viewpoints in order to reach a consensus (Lanchester, 2013).

The Temporia program was deemed by the European Court of Human Rights to be a violation of essential human rights and freedoms. This ruling serves as a reminder of the importance of protecting individuals' privacy and personal data in today's digital age (European Court of Human Rights, 2021).

3. Echelon (Multinational): Echelon is a highly secretive intelligence-gathering program that has been in operation since the Cold War era. It is managed by the cooperation of several countries, namely the United States of America, Great Britain, Canada, Australia, and New Zealand, and its primary purpose is to monitor and control the network in those countries (Wright, 2005). The program's primary function is to intercept and collect any electronic information, including emails, phone calls, faxes, and other forms of communication, both domestic and international. The program has the ability to process vast amounts of data at high speed, using sophisticated algorithms and analytics to identify patterns and signals of interest. The program's primary purpose is to control the traffic of public communications and obtain relevant information for their common purposes, which can include intelligence gathering, counterterrorism, and national security operations (Mombelli & Piodi, 2014).

The existence of a specific program was kept confidential for a considerable number of years, with those involved in its development going to great lengths to ensure that the information pertaining to it remained undisclosed. Despite their efforts, various investigative journalists and whistleblowers eventually succeeded in uncovering the truth about the program's existence, leading to widespread awareness of its secretive operations. The program's inner workings and purpose were gradually brought to light, with many people expressing concern over its implications and the potential consequences of its continued operation (Bowden, 2013).

4. MUSCULAR (United States): MUSCULAR was a highly controversial joint surveillance program that was jointly managed by the National Security Agency (NSA) of the United States and the Government Communications Headquarters (GCHQ) of the United Kingdom. The program

was specifically designed to extract vast amounts of data from companies such as Google and Yahoo, using various methods such as tapping into the communication links between their data centers. This allowed the program to gain access to any user data stored on the servers of these companies, including emails, documents, photos, videos, and any other information the user had stored in their account (Gellman et al., 2013). It must be mentioned that the software was able to retrieve the required data without the involvement of Yahoo or Google, thus ensuring data privacy and security. Following this incident, both companies have taken measures to enhance their safety protocols and prevent similar occurrences. This includes implementing more robust security algorithms, improving data encryption techniques, and enhancing their overall safety standards to protect their users' information from any unauthorized access or breaches (Miller, 2013).

The MUSCULAR program was highly secretive and was not known to the public until it was exposed by Edward Snowden in 2013. The revelations sparked widespread outrage and criticism from privacy advocates and civil liberties groups, who argued that the program's activities violated users' privacy rights and constituted a severe breach of trust. The fact that the program was jointly managed by two of the world's most powerful intelligence agencies only added to the controversy and fueled concerns about the scope and reach of government surveillance programs around the world (Gellman & Soltani, 2013).

5. SORM (System for Operative Investigative Activities): SORM is a comprehensive program consisting of various technical tools and measures that allow for the lawful interception and monitoring of various communication channels in the Russian Federation. SORM enables the authorities to monitor telephone conversations, internet traffic, and any other communication activities in order to ensure public safety and combat criminal activities. This program is used by law enforcement agencies and other authorized government bodies (Polyakova & Meserole, 2019).

SORM has developed in three stages over the years.

The first stage, SORM 1, was introduced in the 1990s and was primarily created to intercept and record phone conversations. This system enabled authorities to monitor phone calls made by individuals suspected of criminal activity.

The second stage, SORM 2, replaced SORM 1 in the early 2000s. It expanded the capabilities of the system to include the monitoring and analysis of internet traffic in addition to phone conversations. With SORM 2, authorities could track and monitor emails, instant messaging, social media activity, and other online communications.

The latest stage of SORM development is the third phase, known as SORM 3. This iteration of the system is the most advanced and comprehensive

version yet. With SORM 3, authorities can effectively intercept, analyse, process, and store any information transmitted through communication channels. This includes not only phone calls and internet traffic but also all other forms of digital communication, such as text messages and video calls. Additionally, SORM 3 enables authorities to store this information for an extended period, allowing them to access it at any time for investigative purposes (Soldatov & Borogan, 2013).

It must be mentioned here that the European Court of Human Rights made a significant ruling in 2015 regarding the SORM program. In its unanimous decision, the court declared that the protection of human rights is not ensured under the current conditions of the SORM program's operation, leaving individuals vulnerable and unprotected. The court further concluded that the SORM program violates Article 8 of the Convention on Human Rights, which guarantees the right to privacy (European Court of Human Rights, 2015).

6. Central Monitoring System (CMS): The CMS program is a surveillance system implemented in India (Reddy, 2014) and is capable of intercepting and analyzing telephonic conversations, as well as monitoring email and social media correspondence on platforms such as Twitter, Facebook, and LinkedIn. It is worth noting that the program is designed to work within the framework of Google's system and can even monitor the activities of users on the search engine, such as analyzing their search history (In India, prism-like surveillance slips under the radar, 2013). There are some experts and individuals who hold the view that the system in question possesses an array of capabilities that are far more extensive than what is currently known to the public. In fact, comparisons have been drawn between this system and the infamous PRISM program that was run by the National Security Agency of the United States of America. Moreover, a report by Human Rights Watch has expressed concern that the system may pose a threat to fundamental human rights and freedoms. The report highlights the potential for abuse of the system and its implications on privacy and freedom of expression. The report also calls for greater transparency and oversight to ensure that the system is being used in a manner that is consistent with universal human rights standards (India: New monitoring system threatens rights, 2013).

7. Unit 8200: Unit 8200 is a highly specialized intelligence unit of the Israeli Army, which is also known as the Central Collection Unit of the Intelligence Corps. This unit operates under the Directorate of Military Intelligence (AMAN) of Israel (Fiegenbaum, 2007).

One of their primary functions is surveillance (Tawil-Souri, 2016). The surveillance carried out by Unit 8200 is not limited to any particular medium. They monitor and track all forms of communication, including phone calls,

emails, and digital communication channels, among others. Their sophisticated surveillance technology allows them to monitor these channels in real time, ensuring that they can quickly identify and respond to any potential security threats (Reed, 2015).

Due to their expertise and successful operations, Unit 8200 is widely regarded as one of the world's most robust intelligence units in the field. Their operations have been considered exemplary and have served as a model for other intelligence agencies around the world (Cordey, 2019).

8. The Great Firewall: The Great Firewall, also known as the Golden Shield Project, is a vast system that operates in China with the dual purpose of censorship and surveillance. The system is one of the largest of its kind in the world and is designed to maintain strict control over the internet within the People's Republic of China (Chandel, 2019). Its primary objective is to block several foreign websites and applications that the Chinese authorities consider sensitive and inappropriate, such as democratic information websites, human rights websites, and other sources of information that may be deemed subversive (Ensafi et al., 2015a). In addition to its role in censorship, the Great Firewall also blocks search words, which enables the system to control the information that the Chinese people can access. It is a powerful tool that the authorities use to limit the spread of ideas that they deem unacceptable.

As part of the surveillance function, the Great Firewall monitors all internet activity within China, which allows the authorities to identify and eliminate any potential threats to the security of the People's Republic of China. The system is a powerful tool that enables the government to maintain control over the internet and prevent the dissemination of information that may be considered harmful to the state (Akduman, 2023).

Social media platforms such as Facebook, Twitter, Instagram, and YouTube are all blocked in China. Instead, the government offers the Chinese people alternatives in the form of WeChat and Weibo, which are subject to censorship and surveillance. The use of these platforms is strictly controlled, and any content that is deemed unacceptable is quickly removed (Kalathil, 2017).

Despite the efforts of the authorities, there are still many people in China who seek to circumvent the censorship and surveillance of the Great Firewall (Clayton et al., 2006). However, the government's work on the system continues, and it remains a significant obstacle to the Chinese people's access to the global internet and its content (Ensafi et al.,2015b).

The eight surveillance programs or systems listed earlier are just a few examples of the many projects that currently exist. It is essential to keep in mind that there are likely many more systems in operation that are not publicly known and whose existence is kept under strict confidentiality until they are revealed through investigative journalism or whistleblowers. As technology

advances and surveillance capabilities become more sophisticated, it is possible that new systems are being developed all the time, which may be even more covert and difficult to detect.

As stated in the previous section of the research, the existence of surveillance systems serves a crucial purpose in the modern digital world. The increasing prevalence of criminal syndicates whose primary objective is to cause harm to individuals or institutions through their illegal activities necessitates such surveillance. However, it is noteworthy that the European Court of Human Rights (European Court of Human Rights, 2021) has deemed two of these surveillance systems to be in violation of the Convention on Human Rights (European Court of Human Rights, 2015). This ruling has sparked an ongoing debate on the legitimacy of other existing surveillance systems, with many questioning their justification and possible infringement on individual privacy rights. The need for surveillance must be balanced against the fundamental human right to privacy, and it is necessary to ensure that any surveillance system is implemented in compliance with the law and human rights conventions.

In the present-day digital world, surveillance has become an integral part of our lives. To fully comprehend its significance and implications, it is essential to delve into the legal and ethical considerations surrounding it. These considerations have been the subject of active debates in various scientific fields, including computer science, sociology, and philosophy. Researchers are keen on understanding the impact of surveillance on privacy, security, and freedom of expression, among other fundamental rights. This understanding can help us develop better policies and practices that strike a balance between protecting individual rights and ensuring the safety and security of society at large.

V. Ethical and Legal Aspects of Surveillance

This research repeated many times that in today's world, the vast majority of people use electronic devices such as mobile phones, personal computers, smart TVs, and other similar gadgets. These devices are often used to share intimate details between individuals, whether in a romantic or sexual context (Miguel, 2018). However, many people are unaware that even if they delete their chats or conversations, the information is still stored on servers for a certain period. This means that, if required, government agencies can access and recover deleted messages for lawful purposes. For instance, if there are signs of criminal activity in Facebook conversations and the alleged perpetrator has deleted messages, it does not mean that the chat cannot be recovered (Chandel et al., 2018).

While it is understandable that such measures are necessary for maintaining public safety, ethical concerns arise regarding the storage of such

sensitive and personal information. Citizens may feel uncomfortable knowing that their private lives are accessible by surveillance systems. This realization may ultimately lead to a loss of trust in the authorities and the government, which, in turn, could have significant implications for public order (Moran, 2015). It is crucial to note that the ethical concerns highlighted in studies are only a small part of the more significant ethical and moral dilemmas surrounding surveillance systems (Friedewald, 2017).

In the modern world, democratic states uphold the right of individuals to have a private life. This right is enshrined in the Fourth Amendment of the Constitution of the United States of America (Constitution of the United States: Fourth Amendment, 1791). Also, Fundamental Human rights and freedoms are protected by the international declaration (Universal Declaration of Human Rights, 1948) and several other international acts (European Convention on Human Rights, 1950). However, with the increasing prevalence of surveillance programs and systems, the extent to which the right to privacy is safeguarded has become a pressing issue. It is crucial that the law be upheld and enforced for all individuals, including ordinary citizens, government agencies, and intelligence officers. The protection of individual privacy is a critical matter and must be taken seriously in our fast-paced and ever-changing technological landscape.

The issue of surveillance systems and their impact on the right to privacy is a complex and sensitive topic (Lyon, 2001). Many argue that surveillance is necessary to ensure public safety and prevent potential threats, both real and hypothetical. However, others argue that excessive surveillance can infringe upon an individual's fundamental human rights and freedoms, such as the right to privacy. If surveillance continues at an alarming pace, it could lead to a situation where even the constitutions and international agreements that are in place to protect these rights become meaningless. A law that cannot protect individuals from the state or guarantee their fundamental rights and freedoms is essentially just a collection of words on paper.

The concept of rule of law is central to the functioning of a democracy. When the rule of law is not upheld, it can lead to a society moving away from democratic principles and towards a totalitarian regime. In such a regime, the protection of human rights and individual freedoms is often nonexistent. This was evident in post-World War II East Germany, where citizens were constantly monitored by the Ministry of State Security, also known as Stasi. They knew that their private lives were not protected and that they were being watched at every moment. The Stasi was infamous for its surveillance and its ability to infiltrate every aspect of citizens' lives. This is a stark reminder of the dangers of a society without the rule of law and the importance of upholding democratic values. The fate of East Germany and the end of the

Stasi serve as historical lessons for the world to learn from (Dennis & Laporte, 2014).

As our society becomes increasingly reliant on surveillance systems to monitor and protect our physical and digital spaces, it is crucial to consider the security of the information obtained by these systems. Cybercriminals pose a significant threat to the confidentiality of sensitive data, as evidenced by the annual exposure of tens of millions of accounts due to their activities (Gibson et al., 2021). Even powerful banking systems like the Caymanian banking system are not immune to the danger of data breaches (Cayman National suffers Manx bank' data hack, 2019). In fact, cybercriminals have even managed to infiltrate the Washington, D.C., Police Department and acquire officers' personal information (D.C. Police Personnel Files Obtained by Hackers, 2021).

In light of the widespread use of surveillance systems, a logical question arises regarding the protection of personal and intimate data obtained through these systems. While it is true that relevant surveillance services often claim to provide the world's most vital protection, it is worth considering the possibility of security breaches. As history has shown, the action of a single individual can be enough to call into question the effectiveness of the security systems employed by these services.

A prime example of such an occurrence is the case of Edward Snowden, who famously revealed classified information that many states do not have similar top-level secrets. This raises concerns about the extent to which these surveillance systems are actually capable of protecting sensitive information and whether their current security measures are sufficient (Verble, 2014). The scenario of Edward Snowden not being a whistleblower but rather an evil criminal with the intention of making private and confidential data public raises several questions about cybersecurity.

Despite the advancements in technology, cyber threats continue to pose a significant challenge in guaranteeing the safety of digital information. As already mentioned, every year, millions of personal data records are exposed on the internet, highlighting the need for robust cybersecurity measures to safeguard sensitive information.

In today's digital world, the protection of personal data is a crucial issue that several international acts (The Data Protection Directive, 1995) aim to address (The General Data Protection Regulation, 2016). However, the constantly evolving technological landscape presents a significant challenge to lawmakers. The pace of innovation is so rapid that it is difficult to predict what new tools and capabilities will emerge in the near future. Even a year from now, people may see significant changes that they cannot anticipate today. While legal frameworks have been established to protect fundamental

human rights and freedoms in the digital world, they were created with an understanding of the challenges and problems of the past.

As technology continues to advance at an unprecedented pace, it is becoming increasingly difficult to ensure that these protections remain relevant and effective. Artificial intelligence (AI) is one area of technology that has advanced rapidly in recent years. With the help of AI, it is now possible to carry out censorship, propaganda, and surveillance on a scale never before seen. This presents a significant threat to individual rights and freedoms, and it is a challenge that lawmakers and society as a whole must address. Despite the efforts of international organizations to protect individuals' rights in the digital world, the issue surrounding the encroachment of new technologies on human rights and freedoms has not been thoroughly resolved.

The world is becoming increasingly digital, and technology is advancing at an unprecedented pace. As a result, criminals are exploiting the progress to achieve their malicious intentions. This poses a significant challenge to the relevant structures and agencies of the state, which must respond swiftly to both cyber criminals and real-world criminals. However, this issue is not without consequences. The ethical, legal, and security issues involved in this matter are vast and complex. If these issues are not addressed adequately, the consequences could be far more damaging to our society than the criminal activities of digital or real-world criminals. It is crucial for any democratic state to ensure that its surveillance systems are designed to protect fundamental human rights and freedoms rather than being used to infringe upon them. This is the only way to ensure a healthy and prosperous society for all.

Conclusion

It is 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 mean to simplify its daily life and existence. However, as noted in the research, along with positive moments, there were also moments when the gifts of technological progress were used for harmful, criminal purposes (Gordon & Ford, 2006).

States and international communities have developed strategies and mechanisms to fight crime successfully in the digital world. One such mechanism is a surveillance system. States or international communities use it to 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 similar surveillance programs and systems must exist with technological progress to protect statehood, state structures, and citizens. However, 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 cyber criminals, 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 importance of updating legal bases in response to technological advancements cannot be overstated. As new technologies emerge and impact fundamental human rights and freedoms, it is critical for legislators at both the local and international levels to create specialised working groups to analyse these developments. Laws crafted before the existence of these specific technologies are no longer adequate to address the risks that come with progress. To safeguard against cyber criminals and international or state surveillance programs, it is essential to frequently revise legal bases to guarantee and protect fundamental human rights and freedoms. By doing so, humankind can ensure that their society's values remain intact while keeping pace with rapid technological advances.

2. Transparency. The study highlighted an important fact that the general public is often uninformed about the existence of surveillance programs until they are brought to light by journalists and whistleblowers. These programs allow the state to access the communications and information of its citizens, which can be a cause of concern for many individuals as they may feel that their privacy and rights are being violated. Therefore, it is crucial for the state to provide a comprehensive and transparent explanation of these surveillance programs, including their purpose, necessity, and rationale for their existence. When citizens understand the need for such programs, they can have confidence that the state is protecting their rights and freedoms both in the physical and digital world. Programs such as PRISM or ECHELON, when understood to be necessary for maintaining a free society, can help alleviate citizens' apprehensions and foster trust that their rights are being safeguarded. Additionally, it is essential for the state to ensure that these programs are being conducted in a manner that is ethical, lawful, and proportionates to the threats they are designed to address. This can be achieved through regular oversight, accountability measures, and transparency in

reporting. By doing so, the state can strike a balance between protecting national security and preserving individual liberties, thereby promoting a just and democratic society.

3. Encouraging Digital Education. Governments must place a high priority on equipping their citizens with the necessary knowledge of the digital world and its associated risks. To achieve this, it is crucial to establish specialised courses and training programs that cater to the specific needs of individuals. Moreover, it is essential to focus on promoting cybersecurity education at a fundamental level, which includes teaching the basic principles and minimum security standards required to ensure online safety. Such measures will go a long way in ensuring that individuals are equipped to navigate the digital world securely and protect themselves against potential threats.

4. Protection of Digital Rights. In today's world, where almost every aspect of our lives is governed by digital technology, protecting human rights in the digital realm has become an absolute necessity. Governments must ensure that organisations dedicated to safeguarding these rights are provided with adequate support and resources, enabling them to carry out their duties effectively. Individuals with specialised education and a deep understanding of digital technology and fundamental human rights are essential to lead these organisations. By providing the proper backing, more individuals can be protected from harm online, and their right to privacy and freedom of speech can be upheld.

5. Development of the Ethical Artificial Intelligence Systems. In the last few years, humankind has witnessed unparalleled progress in the field of artificial intelligence. Today, AI systems are being extensively used by various companies and surveillance systems to gather and analyse a vast amount of data. However, the uncontrolled collection and storage of personal data by AI systems pose a significant threat to fundamental human rights and individual freedoms. Hence, it has become crucial for governments and the global community to prioritise the development of ethical AI systems that ensure the protection of personal data and safeguard the rights and freedoms of citizens in the digital realm.

The conclusion of the presented research provides a set of essential guidelines that states and international communities should follow to ensure the safety and protection of citizens in the digital world. The recommendations aim to establish a strong link between digital security and safeguarding fundamental human rights and freedoms. By implementing these guidelines, citizens can enjoy a secure and protected online experience while exercising their fundamental rights and freedoms without fear of infringement or violation.

As technological advancements unfold, humankind can expect to witness remarkable inventions that will undoubtedly enhance their daily lives. However, if the infringement of human rights accompanies these advancements, be it by cybercriminals or state agencies, people's future will be far from the simplified and secure utopia they envision. Instead, humankind may wake up to a bleak, totalitarian, and dystopian world.

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

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

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

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 A.C.M., 32(8). 928-938.
4. Bowden, C., 2013. The U.S. surveillance programmes and their impact on E.U. 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 N.S.A. 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. Analysing 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. N.S.A. 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 N.S.A. 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. N.S.A. 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 modernisation 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. C.R.C. 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). I.Z.A. 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: F.B.I. 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 U.S. 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 E.P. 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: N.S.A. 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: N.S.A.'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 J.L. & 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. O.A.H. 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 U.K., 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. N.S.A. 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 N.S.A. and Edward Snowden: surveillance in the 21st century. A.C.M. 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. B.B.C. 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: January 1, 2024).
67. CNN. 2021 "D.C. 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 January 1, 2024).
68. Constitution of the United States: Fourth Amendment. Available at: https://constitution.congress.gov/constitution/amendment-4/ (Accessed: January 1, 2024).
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: January 1, 2024).
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: January 1, 2024).
71. European Convention on Human Rights. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed: January 1, 2024).
72. H.R.W. "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: January 1, 2024).

73. The Data Protection Directive. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046 (Accessed: January 1, 2024).
74. The General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed: January 1, 2024).
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: January 1, 2024).
76. Surveillance definition & meaning. Dictionary.com. Available at: https://www.dictionary.com/browse/surveillance (Accessed: January 1, 2024).
77. Universal Declaration of Human Rights. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed: January 1, 2024).