European Research Studies Journal
Volume XXIII, Special Issue 3, 2020

pp. 287-301

Divergence of Security and Right to Privacy in Light of Measures Taken during COVID-19 Pandemic

Submitted 03/08/20, 1st revision 12/09/20, 2nd revision 20/10/20, accepted 11/11/20

Jakub Adamkiewicz[1], Luiza Trzcińska[2]

Abstract:

Purpose: *The paper aims to assess methods and information technologies used to control and surveil citizens in light of measures taken to combat the spread of the COVID-19 virus outbreak. That assessment pays particular attention to the right to privacy, which seems not to be observed by both private market entities and state authorities. The paper attempts to determine the importance of privacy concerning civil liberties and in the context of building a democratic society.*
Design/Methodology/approach: *The paper is based primarily on research conducted using the desk research method. The subject of analysis is data available, inter alia, in scientific papers and special reports regarding opportunities and practices used to obtain information about Internet users and mobile communication device holders concerning combating the spread of the COVID-19 epidemic. Materials covering the pandemic period will be juxtaposed with documents showing the relevant periods before the outbreak began.*
Findings: *Analysis results are presented in the context of a broader discussion regarding the relation between security and civil liberties.*
Practical implications: *The issue of correlation between security and freedom (including the extent of intrusion into privacy) allows us to determine boundaries for developing various technologies connected with ensuring security under ethical principles and in the spirit of international human rights.*
Originality/Value: *Among publications devoted to the difficult relation between security and civil liberties, only a small number pertains to the current COVID-19 pandemic. Besides, the epidemic period has revealed to an even greater extent, the tendency to impose greater control over society through various information technology tools and new technologies.*

Keywords: *Security, right to privacy, surveillance, COVID-19.*

JEL: *H55, D82, D83.*

Paper type: *Research in Security Studies.*

[1] *Wojskowa Akademia Techniczna, Wydział Bezpieczeństwa, Logistyki i Zarządzania.*
E-mail: jakub.adamkiewicz@wat.edu.pl;
[2] *Wojskowa Akademia Techniczna, Wydział Bezpieczeństwa, Logistyki i Zarządzania.*
E-mail: luiza.trzcinska@wat.edu.pl;

1. Introduction

The issue of the relationship between security and freedom is one of the most important contemporary ethical dilemmas. The discussion on this topic contributes to defining the limits of the development of technologies for ensuring protection and comfort in the context of moral norms and, in the spirit of international human rights, recognized as a key value in democratic states. This dilemma is especially important in the era of technological transformations affecting all areas of human life. Our everyday, biological reality is constantly intertwined with functioning in the digital world (in the Internet network). We are constantly accompanied by electrical devices that record activity, interests, social relationships, or where we are. The collected data is used to create profiles of their users, based on which private companies prepare individual commercial offers.

Most of the highly developed countries agree to this state because the services offered through this information exchange significantly improve the quality of life and even help make decisions (e.g., consumer decisions). Our tendency to openness is therefore used by private entities interested in profit. Nevertheless, this data can also be and is often used by internal and external security services. The argument that justifies this practice is the increase in the effectiveness of protecting citizens against danger. Such a motive is often organized crime and terrorism, and recently also the threat resulting from the spread of the Covid-19 epidemic.

The purpose of this article is to present and evaluate the methods and information technologies used for the control and surveillance of citizens, in the light of, inter alia, measures taken to combat the development of the Covid-19 pandemic. As part of this assessment, the aspect of the right to privacy will be considered, which seems not to be respected by both private market entities and public services. The article attempts to indicate the importance of privacy for civil liberties and in the context of building a democratic society. The methods used to track Internet users' actions and owners of mobile communication devices will also be presented here. New solutions in this area that have emerged with the expansion of the global pandemic will be indicated. Their presentation will take place in the context of the effectiveness of the fight against the threat and the context of potential social consequences.

2. Understanding the Concept of Privacy

"Privacy" is a difficult term to define. While we understand this word's idea, we often fail to express its utilitarian scope and meaning comprehensively. Privacy is multidimensional. It covers many spheres of life - including psychological, social, and legal. The term is also understood differently depending on regions or countries, shaped differently from the historical and cultural perspective.

Its modern European understanding can be derived from antiquity when the civilization of the old continent was formed. At that time, it was understood as an attribute of free persons. Here is the ancient Roman adjective "private" (private) denoted personal property or a person not performing a public function. Its etiology, however, was the concept of prices, meaning "free from one's own, single" (Lewis and Short, 1879). The French philosopher Benjamin Constant, who developed the interpretation of this issue in modern times, also linked "privacy" to freedom. According to him, human life should be divided into public and private spheres. Furthermore, it is the right of an individual to have this space free from interference by authorities or other persons based on human freedom. This privacy is supposed to result in the freedom to dispose of one's own political and religious beliefs or the possibility of association.

According to Constant, privacy understood in this way should be guaranteed to every citizen (Lumowa, 2010). Similarly, Samuel Warren and Louis Brandeis (1890) were the first to formulate the "right to privacy" principle in an identically titled article published in 1890 in the Harvard Law Review. They demanded every human be granted the right to "be let alone".

The idea of the legal protection of privacy was finally reflected in the legal provisions in the past century, becoming one of the fundamental norms enjoyed by human beings. Here it was made one of the Universal Declaration of Human Rights principles, in which article 12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation." Moreover, "everyone has the right to the protection of the law against such interference and attacks." Likewise, in the International Covenant on Civil and Political Rights, Article 17 indicates that "no one shall be exposed to arbitrary or unlawful interference with his private life, family, home or correspondence, or to any unlawful attacks on his honor and reputation."

In turn, according to the Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8), "everyone has the right to respect for his private and family life, his home and his correspondence". Following international law, the principle of privacy protection has also become present in the regulations of supranational institutions such as the European Union (EU Charter of Fundamental Rights) and democratic rules of law. Thus, the right to privacy concept gained importance as one of the fundamental attributes of a free man, universally recognized in the world.

3. Contemporary Depreciation of the Importance of Privacy

The very need for privacy manifests itself inconsistently, depending on cultural influences and individual preferences. It can also take many forms. A specific manifestation of privacy protection is the decision to cover its own body and select its parts that can be exposed. In the still recent past, it was considered that almost every part of the body's exposure, perhaps excluding the face and neck, was too bold. Even the hair - especially women - should remain covered (Morris, 2004). To this day, some cultures

include in the privacy zone, the appearance that is almost completely hidden - as in the case of, e.g., some factions of Islam or Judaism (e.g., Hasidism).

More often, however, privacy was associated with keeping strangers from entering houses and preventing outsiders from accessing their correspondence. In both cases, violation of these spheres was unacceptable - both by ordinary citizens and by institutions and services representing the state. This was expressed in numerous legal provisions. The persistent violation of our personal rights has become a stalking offense (Sheridan and Arianayagam and Chan, 2019).

Furthermore, to gain access to private correspondence or the interior of the taxpayers' house, the services had to obtain the consent of independent judicial authorities after prior exhaustive justification of such a need (primarily for the sake of the public good). The United States, in particular, had become famous, over the past century, for respecting these principles, especially when they applied to its citizens. Simultaneously, there was a strong need to protect this privacy among the population, manifested, for example, by the general care for securing postal items and letters, while ensuring their confidentiality by courier companies (Desai, 2007).

However, an attitude towards privacy has changed significantly over the past five decades. The transformation took place with the development of the idea of liberalism and technological progress. At first, it started with a loosening of the approach to clothing and reduced subsequent elements considered unnecessary. This is the acceptance of freeing the body from the clothes that cover it, has evolved along with the emergence of subsequent moral and fashion revolutions - from hippie freedom in the sixties and seventies, through breaking new barriers by music and film stars in the last two decades of the last century, to the almost abolition of the taboo undress in the present age. This process was accompanied by a change in other levels of morality.

There was a tendency to make information about personal and family life public. The popularity of reality TV programs increased people's natural tendency to spy on them and created a fashion for a kind of social exhibitionism. This was accompanied by the emergence of a new category of idols - celebrities are known only for being publicly visible. These personalities were followed by many imitators who wished to become famous by showing their interests and everyday life to strangers. The development and dissemination of Internet technologies strongly supported this process. Thanks to portals such as YouTube, Facebook, and Instagram, it has become possible to report on one's own life. On the other hand, mobile phone development into a miniature computer allowed interested parties to keep track of such information.

This openness and tendency to social exhibitionism have become a permanent element of the still shaping of global culture. Attitudes towards privacy vary from generation to generation, but there tends to be more open in this aspect among young people.

They cannot imagine life without a mobile phone by the side, without a personal profile on Facebook (or another social networking site), without connections via instant messaging, or without platforms where you can share private photos or videos. It is a sign of the overwhelming influence of technology on our lives and culture. However, this openness on the Internet is accompanied by numerous threats resulting from an unauthorized violation of privacy and the use of the information obtained against its owners. Threats - it should be mentioned - are not always aware of and often accepted as a kind of payment for the facilities resulting from the possibility of using new technologies and information solutions.

4. Privacy towards Websites

In fact, the price we pay for "free" access to websites is our data. However, technological progress allows us to "be online" around the clock, which is associated with the continuous sharing of personal information. Such a situation brings both benefits and threats. In the age of the Internet, most matters can be done with one click - paying bills, contacting friends, or buying a ticket. However, this comes at a price. Applications installed on smartphones collect, among others, information such as location, sent SMSes, call list, friends list, interests, traveled routes, or visited places. Using popular social networking sites allows applications to create our personal profile that can both serve and harm users. According to Megapanel PBI / Gemius data from November 2019, in Poland, "23.4 million internet users have accessed the network via personal computers and laptops. 23.8 million used mobile devices for this purpose, while 23.4 million internet consumers used smartphones, and 3.1 million browsed the web using tablets" (Gemius / PBI, 2019.

One of the popular Internet portals collecting information about users on a large scale is Facebook. It turned out to be a leader among the most visited websites in Poland (Juza, 2019) and in the world. In its regulations, it lists, inter alia, the following data that it collects: "... We collect content, messages and other information received from you when using our products (...) We collect information about people, pages, accounts, tags, and groups with which you are connected (a) and your interactions with them in our products, e.g., which people do you communicate most or which groups you belong to (...) We collect information about how you use our products (...) when you use and when you last used our products, and what posts, videos, and other content you display on our products. We also collect information about how you use features such as the camera (…) we collect information from computers, telephones, TVs connected to the Internet and other devices connected to the network". Simultaneously, ensuring that the collected information is used, inter alia, to personalize functions and content. The provision regarding using data such as name, surname, and profile photo is very controversial. According to chapter 3, point 2, "You give us consent to use your name and profile picture and information about your Facebook activities in advertising, offers and other sponsored content that we display in or in connection with our products without compensation." This is how - in the age of the information society - private data has become a commodity.

This principle, adequately applied to Facebook, is used by another internet portal - Google. The corporation behind processes exorbitant amounts of data users, assuming that it is collected to catalog the world's information resources and make them universally available and useful. Currently, Google is not only a search engine for terms but the following related services:

- Google apps, websites, and devices, such as Search, YouTube, and Google Home;
- Platforms such as the Chrome browser and the Android operating system;
- products integrated into third-party apps and sites, such as ads and embedded Google Maps.

The data we provide when creating an account include your first name, last name, and password. Optionally, you can add a phone number or payment card details. However, Google also collects data such as: "written and received emails, saved photos, and videos, created documents and spreadsheets, comments on YouTube videos (...) information about the applications, browsers and devices with which you use Google services (...) a browser type and settings, a device type and settings, operating system, cellular data (...) searched terms, watched movies, ads and viewed content together with performed interaction, information related to voice and audio while using audio functions, purchases, people with whom contacts or materials are shared, activities on third-party websites and applications that use Google's services, browsing history in chrome synchronized with a Google account". This website's software allows users to influence the transfer of information about themselves to some extent; after all, it is possible to manage the data to which Google has access. However, in practice, people rarely limit the browser's surveillance potential because it also limits the scope of its services and the related advantages. At the same time, it does not protect users against the potential and real dangers of collecting information.

5. Threats to Privacy on the Internet

Therefore, social networks and applications are collections of data about their users. The portals cited above to ensure that they store information about us only to provide and improve the services offered, adjust the displayed ads, measure results, or contact users. Profiles of website users are created in two ways - with the use of explicit and implicit profiling. "Explicit profiling (direct profiling) consists of obtaining information directly from the user by filling in a questionnaire. "Implicit profiling" (implicit, indirect) consists of observing user's behavior and reactions" (Olszak and Olszówka, 2007). Many users are unaware of what information they share with social networks and how it is later used. Furthermore, even after deleting the accounts, we are unsure whether the data is not further stored and processed.

The information itself is not a threat, but it is not always used as it should be. Especially its careless dissemination becomes a problem. "The intensive development of

information technologies has revealed or intensified numerous negative phenomena, which are induced by the ease of obtaining and distributing information using electronic devices" (Tomczyk and Mider and Grzegorczyk, 2019). Information collected and used is applied by hackers, private companies, and secret services. The most serious threat seems to be its theft and use to our disadvantage. Moreover, even the largest websites (Facebook, Google) could not avoid losing the information they collected, as evidenced by the examples below.

One of the largest data leaks from Facebook took place in 2014 when the website disclosed information to Cambridge Analytica, an analytical company without users' consent. The sale of data reached even 87 million people. It was not the only data leak. In October 2018, a security vulnerability allowed hackers to steal information such as names, contact details, locations, and 29 million people's birthdays. Another example of a data release from Facebook is purchasing information about one million users for $ 5 by the Bulgarian blogger Bogomil Shopov in 2012 (Shopov, 2012). The last large data leak from this portal took place in December 2019. At that time, information related to over 267 million accounts. Access to the database was quickly blocked, but information about users was duplicated and made available on one of the hacker forums.

In turn, Google struggled with one of the largest data leaks in 2015-2018. At that time, data on half a million people, such as user's name and surname, email addresses, date of birth, gender, profile picture, place of residence, profession, and relationship status, could have been released from the Google + portal (currently available only for business accounts). Another data loss took place shortly after this incident. This time it concerned 52.5 million users of the aforementioned portal.

In early 2019, there was another significant data leak, this time from other Internet service providers. One of the hackers' forums could buy a database with 21 million passwords and 773 million email addresses from over 2,000 websites. With regular updates, the database called "Collection # 1" was available for $ 45. However, in October 2019, there was a leak of the popular music application's user base - Spotify. There were 25 thousand people in the publicly available database, email, and account passwords.

So, it is easy to see that the Internet is not a safe place. To complete the picture of threats resulting from criminal activity within it, it is enough to quote statistical data on offenses in a selected country, e.g., Poland. In 2018, CERT Polska operators received 19,439 notifications of security incidents. 431 of them concerning offensive, illegal content, 862 - malware, 101 - information gathering through scanning, wiretapping, social engineering, and others, 153 - intrusion attempts, 125 - intrusions, 49 - resource availability, 46 - information security attack, 1,878 - computer frauds such as identity theft, spoofing or phishing, 69 - vulnerable services, 25 - other (NASK / CERT Polska, 2019). The scale of these activities shows how our private data can get

into the possession of unwanted people. Nevertheless, not only criminals are interested in information about Internet users.

In addition to numerous data theft cases collected by websites, there have been cases of its deliberate sharing - primarily with government services and institutions. It is worth mentioning here, for example, the PRISM program, under which the National Security Agency of the United States collects Internet data about users. PRISM began operating in 2007 after the Protect America Act of 2007 was passed under the administration of President George W. Bush. The project's availability was not disclosed to the public, and information about it was leaked after nearly 6 years of operation. Edward Snowden contributed to that occurrence. The Theesystem's participants out to be such forms as Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype, and Apple - most of the portals issued statements contradicting their cooperation with PRISM. According to the scope of the program, it can supervise live communication and stored information. This includes, but is not limited to, emails, video conferences, voice chats, photos, and file transfers.

Most countries' intelligence services show the will to perform surveillance over citizens by collecting and analyzing information about them. China, where omnipresent surveillance is carried out openly and ruthlessly, is the farthest in this respect. The project of this oversight was perversely called the Social Credit System. Hence, each resident is constantly assessed for his/her daily activity, receiving a certain number of points that can be lost or gained depending on his/her actions. The number of points rises along with taking actions determined by the authorities as desirable, while any offenses against the established order will reduce it.

These points significantly impact the quality of life - they determine the ability to move, the conditions for obtaining loans from banks, taking up education, or a professional or political career. Data collected on followed people is stored through digital technology. The system sucks information from social networks and assesses the overall activity on the Internet (e.g., based on IP), documents the use of payment cards and bank accounts, applications on communication devices, and even collect information (based on biometric features) from a network of cameras located in various parts of the country.

The Social Trust System serves to increase the security of the state and its citizens (e.g., economic security through improved checking of creditworthiness). In fact, however, it is a solution that increases control over the inhabitants and subordinates them to the authorities, strengthening their integrity. Although this solution is widely criticized, many states, to some extent, seek similar control over the citizen. The pretext of security has become the best argument to justify violating people's freedom and privacy. It is especially useful in situations of fear caused by a real threat. Recently it was terrorism, and now this function is performed by the SARS-CoV-2 virus pandemic.

6. Privacy in Times of Pandemic - Digital Methods of Controlling the Development of the Disease

Here, along with the development of the COVID-19 pandemic, it was decided to use the potential of mobile applications to control the spread of the virus. In stores such as the App Store or Google Play, applications whose main task was to control and track the pandemic's development began to appear. Depending on the needs of a given country, the application has various defined tasks and rights. Some of them monitor the health condition, warn about a potential threat, control compliance with the imposed quarantine, check users' movement, or possible contact with infected people.

One of the first countries to use technological advances to fight the pandemic was the aforementioned China, which applied existing social control models for this purpose. They use both city monitoring systems and drones and robots that use detection and identification technology to track down people who do not wear masks and show symptoms of virus infection (Mehta, 2020). One of the mobile applications operating in China is Alipay Health Code. It contains a QR code specifying the user's health by giving him/her one of three colors: green, yellow, and red.

Healthy people are marked with the first of these colors. The yellow means the user that may be asked to stay home for a week. Red color indicates those who are in a two-week quarantine. Yellow or red color can be assigned if the user had contact with an infected person, stayed in a high-risk zone, or reported the disease's symptoms in the form during registration. In a way, this application is obligatory - whoever does not have it has certain restrictions: he/she cannot enter offices, use public transport, move freely around the city, go to work, go shopping in shopping centers, or use restaurants. However, this program raises concerns for its users, as the collected data is transferred to the police. This, in turn, raises the suspicion that the application - under the pretext of ensuring health safety - is implementing the next stage of public surveillance.

Another Asian country that has introduced digital social control methods, motivated by fighting the pandemic, is South Korea. Its Corona100m enables ongoing monitoring of people quarantined by the authorities. Each user of the application can check whether infected people have broken the quarantine rules, and if an infected person is within 100m, an alarm is triggered. Another application operating in the country is the Self-quarantine safety protection implemented by the government. It is intended to make it easier for quarantined users to contact social workers. At the same time, it uses GPS to monitor compliance with the imposed quarantine. The app is a must for Koreans and foreigners (Lee and Lee, 2020).

One of South Korea's ideas to facilitate the fight against COVID-19 was also the intention to implement a system using data such as camera recordings or cashless transactions. The Korean Alert System for Potentially Infected People is as controversial as the Chinese. Messages sent to Koreans allow the identification of infected persons

and information about where and when they have been. In many situations, this involves stigmatizing people who have tested positive for COVID-19 while using the application because the data disclosed relates to users' personal matters, such as hospital stays or private meetings.

The COVIDSafe application, in turn, operates in Australia, the main tasks of which are identifying people at risk of becoming infected with the virus and slowing the spread of the coronavirus. From the very beginning, the application aroused controversy in terms of privacy protection. However, the authorities ensure that all data is encrypted, the application does not record the location, and that data on contacts with other people is only stored for 21 days (Moses *et al*., 2020).

Discussion on the digital possibilities of supporting the fight against the spread of the SARS-CoV-2 virus was also undertaken in Europe. Due to a certain commitment to the protection of privacy and human rights, this debate ended with the resolution of the European Parliament of April 17, 2020, on coordinated EU action to combat the COVID-19 pandemic and its consequences, which allowed the development of applications to control the spread of disease.

However, under point 52 of this document, their use "shall not be mandatory and that the generated data are not be stored in centralized databases". Furthermore, "demands that all data storage be decentralized to ensure full transparency of the (non-EU) commercial interests of the developers of these applications and those clear projections be demonstrated as regards how the use of contact tracing applications by a part of the population, when combined with other specific measures, will lead to a significantly lower number of infected people. 'Whereas point 53 notes that "data on the location of mobile devices may only be further processed in compliance with the e-Privacy Directive and the GDPR; stresses that national and EU authorities must fully comply with data protection and privacy legislation, and national data protection authorities must provide oversight and guidance."

On May 14, 2020, a plenary debate was held in which it was emphasized that the most important thing is that the personal data collected by mobile applications should be well secured, and the applications themselves should be non-discriminatory, transparent, and voluntary (Lietzén, 2020). In response to this provision, many European Union countries have decided to launch mobile applications. They were, among others, Germany, Poland, France, Italy, and Denmark.

The Federal Republic of Germany has therefore launched the Corona-Warn-App, which was developed in Berlin by the Institute of Robert Koch (RKI). Its main task is to monitor the spread of COVID-19 symptoms throughout the country (Lasarov, 2020). Installing the program is voluntary, and owners of wristbands and watches that monitor health can use it. This application tracks, among other things, the quality of

sleep, resting pulse, physical activity, and temperature, informing its user about significant changes in RKI. All data is encrypted and stored under pseudonyms Corona-Warn-App. This function has been very successful. Within two weeks of its premiere, it was downloaded by 16.6 million users.

There are two applications in Poland Kwarantanna domowa (Home Quarantine) and ProteGo Safe. The first is to facilitate quarantine at home. Installing it is obligatory for every person who has been officially quarantined. The application allows us to confirm the user's location, assess its health, quickly contact the indicated services, and report urgent needs to a social welfare center. It also sets out daily tasks, e.g., taking a photo proving that a person is in the declared place of quarantine. Data from the application is to be stored for a period of 6 years.

The second application - ProteGo Safe - is installed without obligation, and the collected data is used, according to the provider, only to "counter the SARS-CoV-2 virus pandemic; profile to counter the SARS-CoV-2 virus pandemic; use the Application by a person under the Regulations; to do analysis, organization, and improvement of ProteGO Safe". The data collected by the program is encrypted and, according to the assumptions, cannot be made available in a form that allows the identification of the user. Therefore, this solution was created - as its producer announces - mainly to facilitate self-monitoring of health (e.g., keeping a health diary). The application also collects up-to-date data on the pandemic situation.

Another European country that has developed an application to help to counter the COVID-19 virus in France. The main task of its StopCovid France was to warn against contact with an infected person, which would allow for a quick test and early treatment. The application was released on June 2, 2020. During the first three weeks, 1.9 million users downloaded it, while only 68 people entered the virus infection data. However, according to the available data, the StopCovid France application did not achieve the expected effect of mass control of society in the context of the epidemic. It was downloaded by only 2% of the population, and during the first three weeks, it sent only 14 notifications.

One of the most affected countries in Europe - Italy - has introduced the Immuni application that does not rely on a centralized database. During the first ten days of operation, it was downloaded by nearly 2.2 million people (Bogacki, 2020), and after a month, this number reached 4 million. The application works by sending information to users about the fact that they have had contact with an infected person, which means that isolation and testing are recommended. The Italian government ensures that the transmitted data is anonymous.

Denmark is another example of a country that has decided to introduce a mobile application, in this case, called Smittestopp (Sandvik, 2020). The latest data published on June 30, 2020, proves that it was downloaded 619 thousand times. Its main goal is

to prevent the spread of the COVID-19 virus. The data collected by the program concern contacts with particular persons, their duration, date, and strength of a signal between the phones on which it is stored. However, both users of mobile devices and the Danish authorities do not have access to this information. All collected data is stored on these devices for 14 days. There is, however, a specific problem with this application. This is because Denmark keeps the source code of this program secret, giving an excuse to distrust potential users.

All of the above-mentioned applications aimed at strengthening the state in preventing the spread of the COVID-19 epidemic contain mechanisms of violating their users' privacy. They collect data on people's behavior, places of stay, health, relationships with other people, and many other aspects of everyday life, which under normal circumstances, many people still would not want to disclose. There are currently no indications that these programs could be used for commercial purposes (e.g., in the field of marketing). However, for the institutions of power of individual countries, they remain a valuable source of information about the vast number of citizens. These data may tempt governments in the future, for example, to use it to strengthen internal security (including intelligence or investigative activities) or even oversight a society.

It is not difficult to imagine when a user of one of these applications will be accused of terrorist or criminal activity. Why, in the face of the current trend towards security, should the legislative authorities refuse to pass a resolution allowing the use of these programs to profile wanted persons and the executive authorities to implement procedures for their use in the prosecution process? After all, there is already an intrusion into the privacy of the Internet and mobile devices users, even to a greater extent than the potential possibility of using data from the presented COVID-19 applications. Examples of such surveillance include the US Security Agency's aforementioned PRISM program, or the Social Trust System operated in China. Therefore, any violation of privacy nowadays should give rise to a reflection, in what direction the development of digital technologies is going and how dangerous for an individual is our cultural attitude to public exposure of our private life? Our main concern is the theft of our data because of hacking. However, we do not see any threats in gathering personal information obtained legally.

7. Threats of the Contemporary Depreciation of the Importance of Privacy in the Light of Security Needs - Summary

Undoubtedly, the loss of our defining data to unauthorized persons can be fearful. First, we imagine the danger of using this information to deprive us of real goods and property. After all, hackers can rob us of funds collected in bank accounts, obtain loans under our names, or determine when we are away from home without taking care of our property. We often lack the awareness that apart from economic threats, there are also other, perhaps even more severe ones.

To some extent, users of websites or mobile applications (including those used in the combat against COVID-19) also know that making public hidden private information may have serious social and personal consequences. In many countries worldwide, there have been cases of tragic disclosures of hidden secrets leading to depression, alienation, or even self-abuse (Lopez-Agudo, 2020). Especially young people and teenagers - not always sure of their value and susceptible to the social environment's influence - easily become victims of the so-called "Internet haterage". The more they are exposed to the risk of violating their privacy when, in their loneliness, they seek contact with other people on social networks. Psychologists have already noticed that presence on the Internet causes disturbing personality consequences, such as "internal compulsion to be online; escape from the real world to the artificial virtual world; access to pathological cultural groups; alienation (e.g., telework alienates)" (Furmanek, 2014).

However, after all, disclosing private information can be used to damage the reputation of just anyone. Even if not by publishing real hidden secrets, it is through the skillful manipulation of falsehood and creating an untrue, but the victim's equally destructive image. Information and disinformation management may, in fact, translate into a more serious threat because of its mass dimension.

After all, it is rarely noticed that threats to our privacy violations on the Internet also have a political or even philosophical context. The latter is primarily related to the considerations quoted at the beginning of this text and related to the reflections of Benjamin Constant. After all, if privacy - as the thinker claimed - is the mainstay of freedom, then isn't the consent to function in a reality in which this privacy is so easily lost or even voluntarily given up, in fact, being forced into a kind of virtual bondage? If government services, private corporations, or hackers gain access to our most hidden secrets, they can easily force us to act against our will. We do not even have to be aware of it. We already know the case of using social networking sites to manipulate information and direct numerous recipients to make political choices in line with the manipulator's intention. This is the case of the aforementioned scandal involving Cambridge Analytica, which cataloged and imposed on its users' content via Facebook that was to influence their decisions during the last presidential election in the United States.

Thus, the ultimate principle of freedom of choice, a fundamental feature of democratic states, was violated. Will such manipulations become a permanent element in the process of electing democratic authorities in the future? In the face of this, can we still talk about ourselves as free people if we do not make our own decisions due to the influence of technology supported by information about ourselves?

In this context, it is also worth considering whether private companies have tools to influence citizens; why should not governments use similar solutions? Especially when it is an authoritarian or tending towards authoritarianism power. The prerequisite for such concerns is, for example, China's surveillance activities as a part of the

Social Trust System they have implemented. This project proves that the world already has the technology of multi-level surveillance of society. Some states decide to a greater or lesser extent to introduce similar solutions to social control. For now, the pretext for this is primarily security and public order. However, how far will we go in this way to eliminate the threats? Today, it is the pandemic of a dangerous disease that causes deeper surveillance of societies to, e.g., faster detect pathogen transmission sources? However, it is worth remembering that every time we agree to give up some part of our privacy - even for the noble purpose of improving general security - we are giving up a little bit of our freedom and freedom of choice. Therefore, we should constantly ask ourselves how willing are we to waive our right to privacy?

References:

Bogacki, K. 2020. Kraje Unii Europejskiej coraz bliżej powszechnego stosowania aplikacji śledzących rozwój epidemii. Przykłady z Włoch i Niemiec. ITReseller, 15.06.2020, https://itreseller.com.pl/kraje-unii-europejskiej-coraz-blizej-powszechnego-stosowania-aplikacji-sledzacych-rozwoj-epidemii-przyklady-z-wloch-i-niemiec/.

Charter of Fundamental Rights of The European Union. 18 December 2000, 2000/C 364/01. https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Council of the Europe. Convention for the Protection of Human Rights and Fundamental Freedoms. 341.24(4): 0(C'E. Col/C.E. https://www.echr.coe.int/Documents/Archives_1950_Convention_ENG.pdf.

Desai, A.C. 2007. Wiretapping before the wires: the post office and the birth of communications privacy. Stanford Law Review, 60(2), 554-594.

European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences. 17 April 2020, (2020/2616(RSP)).

Furmanek, W. 2014. Zagrożenia wynikające z rozwoju technologii informacyjnych. Dydaktyka informatyki. T. 9, Uniwersytet Rzeszowski, Rzeszów, 23.

Gemius/PBI. 2019. Polscy internauci w listopadzie 2019. http://pbi.org.pl/raporty/polscy-internauci-w-listopadzie-2019/.

Juza, M. 2019. Między wolnością a nadzorem. Internet w zmieniającym się społeczeństwie. Wyd. Naukowe SCHOLAR, Warszawa, 284.

NASK/CERT Polska. 2019. Krajobraz bezpieczeństwa polskiego internetu. Raport roczny z działalności CERT Polska 2018. Warszawa, 11-12.

Lasarov, W. 2020. Im Spannungsfeld zwischen Sicherheit und Freiheit. Eine Analyse zur Akzeptanz der Corona-Warn-App. HMD Praxis der Wirtschaftsinformatik.

Lee, D., Lee, J. 2020. Testing on the move: South Korea's rapid response to the COVID-19 pandemic. Transportation Research Interdisciplinary Perspectives, 5. https://doi.org/10.1016/j.trip.2020.100111.

Lewis, C.T., Short, C. 1879. A Latin Dictionary. Oxford: Clarendon Press.

Lietzén, I. 2020. COVID-19 tracing apps: MEPs stress the need to preserve citizens' privacy. News European Parliament, 14.05.2020. https://www.europarl.europa.eu/news/pl/press-room/20200512IPR78915/covid-19-tracing-apps-meps-stress-the-need-to-preserve-citizens-privacy.

Lopez-Agudo, L. 2020. The association between Internet searches and suicide in Spain. Psychiatry Research, 291, DOI: 10.1016/j.psychres.2020.113215.

Lumowa, V. 2010. Benjamin Constant on Modern Freedoms: Political Liberty and the Role of a Representative System. Ethical Perspectives, 17, 389-414.

Mehta, I. 2020. Baidu open sources AI to identify people without face masks. TNW2020, 17.02.2020, https://thenextweb.com/neural/2020/02/17/baidu-open-sources-ai-to-identify-people-without-face-masks/.

Morris, D. 2004. Naked Woman. Study of the female body. Wydawnictwo Jonathan Cape, London, 19-34.

Moses, L., Churches, G., Zalnieriute, M., Byrnes, A., Scully, J., Kemp, K., Greenleaf, G. 2020, COVIDSafe App - Submission to the Parliamentary Joint Committee on Human Rights, SSRN Electronic Journal.

Olszak, C.M., Olszówka, K. 2007, Gromadzenie danych o użytkownikach na potrzeby personalizacji portali internetowych, Systemy wspomagania organizacji SWO 2007, 274.

Sandvik, K.B. 2020. 'Smittestopp' if you want your freedom back, download now. Big Data & Society, 7(2), DOI: 10.1177/2053951720939985.

Sheridan, L., Arianayagam, J., Chan, H.C. 2019, Perceptions and experiences of intrusive behavior and stalking within a culture. Psychology, Crime & Law, 25(4), 394.

Shopov, B. 2012. I just bought more than 1 million …Facebook data entries. OMG!, Talkweb.eu, http://talkweb.eu/openweb/1819/.

Tomczyk, P., Mider, D., Grzegorczyk, J. 2019. Inwigilacja elektroniczna jako metoda pozyskiwania informacji – ewaluacja i prognozy, Studia politologiczne, 54, 259.

UN General Assembly. International Covenant on Civil and Political Rights, 16 December 1966, 2200A (XXI). https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217A (III), http://www.un-documents.net/a3r217.htm.

Warren, S.D., Brandeis, L.D. 1890. The Right to Privacy, Harvard Law Review, 4(5),15, 1890, 193-220.