Privacy protection in a digital economy

Łukasz Wróblewski
Faculty of Command and Naval Operations, Polish Naval Academy, Gdynia, Poland
E-mail address: wroblewski86@gmail.com

ABSTRACT

The author wonders, what impact on the privacy of the human being is developing ahead of us digital economy, with the acquisition of new technology. Brings forth the most important legal standards in force and outlines future European plans for digital market development. It presents the role of cyberspace in the functioning of business and society, and addresses the risks associated with it, such as exclusion, poverty and social unrest. Looking for answers to the question of what decides about behavior or loss of privacy in virtual reality.

Keywords: privacy, economy, cyberspace, market, protection

1. INTRODUCTION

Today, more and more media tell us about the digital economy, digital society and the digital single market. All these concepts function in our consciousness as a synonym of modernity and an irreversible, charitable trend.

EU documents, such as the European Digital Agenda, are intended to enable European citizens and entrepreneurs to maximize the benefits of digital technology and to revitalize the economy in Europe.

In the digital revolution that is taking place in our eyes, information is the driving force of modern economy [1], so it is not surprising that their importance and security will continue to grow. Concentrations of readily available information - like islands on the ocean of ignorance - will determine the further development of societies, their knowledge and wealth. Today, you can see that in the name of fast and easy access to information with simple applications, the user is ready to easily abandon the elements of his own privacy.
The free circulation of information in cyberspace forces such legal changes in Europe to offset the amount of acceptance needed to access devices that are increasingly becoming elements of the Internet of Things. Europeans are still more attached to their privacy than Americans, where the digital revolution has already left a trail of more free access to private data. Are we immune from the right to privacy in the name of access to information? From the point of view of the digital economy, unrestricted access to data is better, but it is not so obvious from the point of view of their security and privacy. In the next part of the article, I will try to answer the question of whether privacy protection is possible in a dynamically developing digital economy.

2. ANALYSIS AND DISCUSSION

Privacy rights are enshrined in the legal order of many states and organizations, is the law of the first generation and requires special protection. It oversees, among other things, the Convention for the Protection of Human Rights and Fundamental Freedoms in Article 8, and the Constitution of the Republic of Poland in 1997, in Article 47. In addition, the Polish Data Protection Act is applicable in the same year, and has recently been amended in 2016 [2]. It is also important to look at international regulations such as this year's Privacy Shield, which specifies the flow of personal data between the European Union and the United States.

The Shield replaced the previously applicable Safe Harbor, which did not generally restrict data collection by public authorities or institutions. Regardless of whether the data flows through a quiet port or are protected by a privacy shield, they migrate across a wide stream between the two continents, as ordinary network users may not seem to be comfortable with. But it's big companies where millions of people store and manipulate data every day, share photos, videos and locations, have their offices in the ocean, and the local institutions have the right to access all those data. The same companies where these data are collected filter them for behavior or illegal activities. In every statute we will find a clause on the right of individuals to privacy, where this privacy is subordinated to the good of the general public and does not threaten in any way public order [3-7].

The border between privacy and the good of the public can be interpreted differently depending on the context. Its characteristic feature is that it is dynamically shifted at the expense of privacy in an emergency situation and rarely returns to its former location after the threat has disappeared.

Privacy Shield, on the one hand, can force the US to better protect its personal data as recommended by European institutions, but on the other hand, there is no certainty as to how these data will be processed in the US's more liberalized system. Although an average European Internet user may feel protected by national and international standards for the transmission of his personal data, no law will prevent him from losing his data if he makes it available voluntarily and often unconsciously. This is usually done through an application that, once the rules are approved, have access to device resources such as text and multimedia, location, and more to serve the broader meaning of personalization [8-10].

Not only large companies try to acquire customers through their own applications for mobile devices. They are used by even small shops or retail chains and all who want to make life easier for the user. It would be wise to remain sensitive to the rules and knowledge of what data and to what extent they are used, processed and made available by a particular
entity. Very often mentioned above applications are very useful, and sometimes even necessary to work and are adequately protected for the needs of a particular company, have become an integral part of mobile devices.

The data centers, the so-called Big Data, where zettabytes of data are being processed are a characteristic element of the cyanide development. According to IDC’s forecasts in four years, 40 zettabytes of data are to be collected on all world servers, which is equivalent to one billion terabytes.

In parallel with the collection and digitization of the past achievements of mankind, technology is being developed to process this data in a quick and intelligent way. In this process a man is still needed as the one who analyzes and investigates. Professionals with special predispositions for information analysis are particularly sought after by companies seeking to build a digital business model. Such companies are able to offer their services faster and cheaper than their non-virtual world counterparts. We need to be prepared to completely change the business model and services that we know so far and to which we are accustomed. This does not mean, of course, that everything that is traditional will disappear, but there is a risk that people and businesses will not adapt to the new needs of the market at the right time.

This threatens to exclude particular social groups and increase poverty in uncompetitive areas of the economy. Hence, it leads to a simple way to social dissatisfaction, which can turn into a disorder, which harms public order and safety.

This is one possible scenario for the future, but not the only one. It is not my role now to conjecture about the future. Any such analysis should be supported by reliable data, which today serves data centers, facilitating analysts' tasks by quickly providing all the information needed to analyze.

How in such a situation is human privacy? Prior to the development of the network and related services, access to personal data contained in documents was difficult and often costly due to the need to physically reach those data. Today through the Internet, the consumer, the entrepreneur, but also the criminal does not have to leave his position in front of the computer and find information is faster and cheaper. In order not to be unproductive, I present an example of the hospitality industry in which I have been working for three years. In recent years, many booking portals have been created that allow you to book your stay in any of the selected properties around the world. Most of the reservations come from these booking channels, called OTA - Online Travel Agency. As an intermediary in the booking process, they are already becoming a link that can lose visitors to the hotel, becoming a convenient feature of the attack.

If the attack on the booking portal ends with a success, data such as name, address, account number or credit card number, company tax number, company name, length and place of stay, and the price of the stay will be leaked. This information may be sufficient to obtain more money or to scam the money from the appropriate institution, and even to reach the place of residence and home to steal property.

The basics would be to give you information about habits, habits, direction and time of travel, the wealth of your wallet. The premise that only OTA channels are vulnerable to data leaks would be over-use because internal hotel reservation systems and software are not free from similar threats and even contain more detailed personal information. It can be PESEL, ID card, apartment address, reservation notes or consumption while staying at the hotel restaurant. If we add hundreds of cameras, which are also present in hotel-chach, which monitor
the usable space, then the burglar knows perfectly where and with whom the person is moving [11-14].

Everyone has an individual space, which we call privacy. Some people give up easily and do not see any problem, others are not willing to accept slowly but consistently narrow field of their own freedom. Still others live in unconsciousness and what is interesting to live like this is comfortable and the only thing they have to accept is another branding agreement, trade agreement or rules of the new service.

As a consequence, the new life-enabling technology that the user accepts can be used to illegally acquire commercial information, social, behavioral and behavioral analyzes, purchasing predispositions, and real-time location. Maybe but of course not. You have to remember that there is such a technical possibility.

The average internet user uses email, obtains financial transactions via the Internet, plans vacation and vacation by making a hotel reservation through the portals prepared for this purpose. He often uses at least one social moment, book tickets for the movie or plane, shopping in many online stores, is a user of several instant messengers. All these activities involve the acceptance of the Terms and the provision of personal data. By participating in a service that he voluntarily chooses, he limits his privacy in a certain sense, moving part of his life into the virtual world. Services that can be used to automatically consume personal data are to protect the service provider from unauthorized user activity. Data entry and acceptance of the regulations is a peculiarity of the contract for the provision of services and is reflected in the relevant legislation.

Despite the rapidly growing sector of the digital economy, there are still barriers to free Internet use in Europe, the European Commission points out:

- breakdown of digital markets,
- lack of interoperability,
- cybercrime growth and the risk of network mistrust,
- lack of network investment,
- insufficient research and innovation efforts,
- lack of ability to use digital technologies,
- unused opportunities to meet social challenges.

These are obstacles to the development of the single European market outlined in the European Digital Agenda adopted in 2010. We see the efforts of companies and institutions that are increasingly aware of new challenges, increase their research and development budgets, including their telecoms sector. On the other hand, e-government administration sometimes discourages the user from illegible graphics or complicated registration procedures. According to the Central Statistical Office data, 75% of Poles have access to the Internet, and since 2012 almost all large companies have access to a global network.

In Poland, the foundations for building a digital economy, based on e-services and e-government, have developed. The latter is more popular among businessmen, and other users have been convinced in recent years of electronic tax returns. The Ministry of Digitization continues its efforts to popularize the digital environment and eliminate the barriers to its development. In the name of creating a digital single market, the European Commission adopted in 2015 a document entitled "Strategy for a Single Digital Market for Europe", which sets out the need to enhance the digital capabilities, regardless of the boundaries.
For this purpose, rigid national regulations concerning telecommunication law, copyrights, data protection, radio frequency management and the application of competition law are superfluous.

In addition to the aforementioned position of the political guidelines, Jean-Claude Juncker, President of the European Commission, said by signing the document: "Today we have laid the cornerstone for Europe's digital future. I would like to operate pan-European telecommunications networks, digital services are provided irrespective of the course of the borders and there are numerous innovative European start-up companies. I want to live in a time where every consumer is offered the best possible conditions, and every business has access to the largest market - regardless of where they are located in Europe”.

3. CONCLUSIONS

Given the pace and development of new technologies, the efforts of policy-makers focused on building a digital society and a knowledge-based economy, one can come to the conclusion that one way in which progress, if not the only, is access to the digital environment and the use of its enormous resources. Continued careful analysis of documentation, agendas and strategies, reinforces the belief that Europe and the whole of the developed world are striving for a single digital market without borders. The creation of such a market is expected to give billions of profits and increase the competitiveness of the economy, according to its calculators.

This digital economy, gaining more and more traditional market share each year, is a great opportunity and a space for development, but it also presents the threat of exclusion of those social classes or companies that do not adapt or adapt too slowly. It is a platform for attacks in the digital environment, becoming prone to phishing, material means, identity theft on a broad and unprecedented scale. The bigger the data, the more data it leaks, and the terabytes, which can be quickly taken over without leaving home.

The beginning of the 21st century is the opening to a new reality in which not the one who has the money wins, and who has reliable information. The average internet user bases his knowledge on the information contained there, shaping his worldview based on the virtual world in which he is increasingly living. In the near future, anti-competitive and privacy legislation will be modified to suit the needs of a single digital market. From individual societies will depend on which direction they will go. Will they choose privacy protection or will they be ready once again to give up a little of it in the name of facilitating the life and development of the services they use.

It is not difficult today, especially in the younger generation to observe how easily they are willing to share their data and mobile device resources by installing additional applications. The desire to use the service quickly, which in addition is very popular in the environment, makes the user accepts all conditions and does not read the provisions of the rules. The only goal is to use the application, game, communicator.

Businesses even if they are using advanced data protection systems can not afford to be prevented from attacking if they have a laid-back worker in security, using personal equipment or electronic mail in the company.

Man has one universal feature, and it is curiosity often and comfort. This is enough to become vulnerable to cyber attacks, and thus unknowingly infect other devices.
The right to privacy is very important and it is always available to man. Only from him depends on how much of this privacy will give up. In fact, in our lives, it is often difficult to determine its limits. In the face of new technology and growing market share in the Internet market, the unawareness of users who volunteer their data, photos, videos and personal life information is unsettling.

No law, even the best formulated, will prevent this kind of behavior. It would be wise to go in the direction of increasing user awareness at an early age to see the benefits, but also the risks of virtual reality. Not only about students but also about entrepreneurs, officials and everyone using the Internet. Brighten up from danger! I am afraid that only so much and so much we are able to do for them.

References


-327-