Cybersecurity and personal data protection

Maria Piątek

06.05.2021

Main points:

- During the COVID-19 pandemic the number of cyberattacks, including those targeting personal data, has increased.
- Problems associated with cybersecurity are often caused by a person "letting in" the malicious program that infects the computer or mobile device, which is the result of a lack of appropriate training in the area of cyber threats.
- In the United States, the process of gradually regulating personal data protection at the state law level has been visible for several years, which may contribute to the adoption of an act at the federal level.

Introduction

During the COVID-19 pandemic, the number of cyberattacks has grown. The reason for that is an increase in the digital activities and digitalization of processes which before required a person's presence in a given place i.e. at the office. In the first quarter of 2020, the experts from the NASK National Research Institute in Poland registered 6,893 reports and the number of analyzed incidents was 2,507[1]. In the second quarter, 9,689 reports were registered and the number of analyzed incidents equaled to 2,723[2]. For comparison, 6,484 incidents were registered in 2019, which was a record high at that time[3]. Personal data may be the target of attacks at times of increased cybercrime. For this reason, more and more voices are heard about the need to provide it with legal protection.

Cybersecurity and personal data

Cyberspace is one of the most important fields of security in the 21st century. It is worth paying attention to the features that distinguish it:

- transnational character;
- no time limits;
- greater anonymity of cybercriminals;

- low cost of use, which allows unlimited access to the network[4].

The above features are influencing the increase in crimes. Therefore, cyberattacks are inevitable and more common phenomena. The victims are companies, government offices, and individuals.

Data is stored and processed in cyberspace at a huge scale. Every activity online is registered by digital systems, which implies the fact that by using the internet every day, we leave a trace taking the form of our personal data. The increasing development of digitalization means that governmental and corporate sites, as well as social networking sites, have data on both the professional careers and private lives of citizens.

One of the human rights guaranteed and protected both by the EU constitution and treaties as well as the Charter of Fundamental Rights of the European Union is the right to privacy. It is a personal need which includes everything understood as "a reasoned isolation of an individual from the society serves them to develop their physical and mental self and to maintain their achieved social status"[5]. Even though the Polish definition seems unspecific and it is difficult to precisely establish what exactly is a right to privacy, one can undoubtedly say that it includes the right to personal data protection, which the General Data Protection Regulation (GDPR) defines as: "information about an identified or possible identification of the natural person". Such information includes i.e. name, surname, place of residence, or internet user ID.

The development of new technology systems brings not only enormous benefits but also threats. Today's solutions enable systems to analyze information and draw conclusions from it. Certainly, fast processing allows various questions to be answered. This makes it easier to identify and predict certain social behaviors. However, the fact that they are processed in a complicated way raises the question over the proper protection of privacy, democracy, and freedom of speech.

The increased processing of personal data online especially intensified during the last year due to the pandemic, implying a stronger emphasis on the protection of cyberspace. The danger exist at different levels. From the smallest entities such as individuals, to small companies and offices to large companies and entire countries. The typical forms of

cyberattacks include i.a., viruses, phishing, vishing, spyware, malware, and trojans. In 2019, phishing accounted for approximately 54% of all attacks as registered by CERT Polska[7].

Over the past few years, the way such attacks are carried out has changed. **Cybercriminals demand ransom not only for decrypting data but also for not disclosing it. In a way, their actions are caused by the regulations resulting from the GDPR.** Namely, the regulation coordinates the rules regarding the processing of personal data and sanctions their violation, imposing a fine of up to EUR 20,000,000 or 4% of the company's annual global turnover. According to the legislator, such a high penalty is to motivate entrepreneurs to invest in appropriate infrastructure which would ensure proper data protection. However, in reality, it can make entrepreneurs pay a ransom to criminals, in fear of an administrative penalty for not maintaining data security.

The problem with the defense against cyberattacks is the human factor. Usually, it is the employee, being the first line of defense, who makes the mistake and "lets in" the malicious software. This is one of the reasons why phishing, which is, e.g. sending targeted e-mails intended to encourage the recipient to click on a link redirecting to a fake website, ranks so high in popularity among cybercriminals. **Entities that store and process personal data should, in particular, put emphasis on employee training.**

The effects of a lack of a proper safety procedure and adequate education of employees can be seen in an example of the attack on the Marshal’s Office in Cracow in early February. The attackers used file encryption software which led to the loss of access to personal data, and they demanded a ransom to unlock it.

Another high-profile leakage of a huge amount of personal data was a double one from the Warsaw University of Technology in 2020. The leak was very serious, as it contained data on names, ID numbers, PESEL (a numeric symbol that identifies a specific person in the Common Electronic System of Population Register) numbers, and recruitment numbers. Additionally, it is worth noting that the attacks took place within two months. During the first attack, approx. 5,000 students and staff fell victim to it.

The last example of a serious breach of personal data protection worth mentioning is a data leak of over 50,000 judges, prosecutors, trainees, assessors, and officials, which were stored

in the servers of the National School of Judiciary and Public Prosecution in Krakow (KSSiP) [8]. Information revealed by the criminals includes i.e. telephone numbers, addresses, and ICQ numbers. Following the incident, law enforcement officials were intimidated. It is worth looking at this problem more broadly - the KSSiP is an institution supervised by the Minister of Justice, which has the data of all judges and prosecutors, who are public officials. A situation in which the data of individuals exercising judicial power in the state and the only institution dealing with their training are in the wrong hands could lead to far-reaching negative consequences for the functioning of the entire state.

International aspect

As it was mentioned before, one of the fundamental rights guaranteed and protected by the EU treaties is the right to privacy and the protection of one's personal data. For several years, the Union has been taking steps to become a leader in the field of secure, digital transformation, where the protection of personal data will be ensured. It is worth noting that no other international entity has regulated and provided such a high level of protection for the right to privacy.

Building a digital economy is to be based on:

- EU values and fundamental principles;
- protection of fundamental rights, including the right to privacy and personal data;
- the right to a secure internet which will ensure an unrestricted flow of information;
- democratic and efficient management of cybersecurity policies that involve various social groups;
- a shared responsibility for ensuring safety[9].

The European Union notices the problem of cybercrimes which is why a specialized European Cybercrime Centre, operating within Europol, was established. Cybercrimes include the following illicit activities:

- taking over the control of personal devices using malicious software;

- theft or exposure to violation of personal data and intellectual property for the purpose of committing online fraud;
- disseminating illegal content through the use of the internet (with an emphasis on the importance of social media);
- using the dark web to sell illegal goods or hacking services[10].

In 2007, Estonia fell victim to a large-scale DDoS cyberattack, i.e. distributed denial of service consisting in blocking of server or the entire infrastructure. **As a result of the incident, the public lost access to banking and e-mail, and the websites of the government and the State Assembly were blocked.** The Estonian Ministry of Defense stated that the purpose of the attack was to undermine the functioning of public and private information systems. These events are very important as they constituted the first massive attack against a state as a whole. Estonia was already a digitally developed country at that time, which clearly shows how necessary it is for states to secure their cyberspace infrastructure.

The GDPR regulates the transfer of personal data from the countries of the European Economic Area (EEA) to other countries and international organizations. The condition for the transfer is that the European Commission recognizes the entity as providing adequate protection. Such transfer does not require special authorization. At present, the European Commission has recognized 12 countries as providing an adequate levels of data protection[11].

Due to the non-compliance with European requirements on the protection of personal data by the United States, but taking into account the strong ties between the EU and the US, in 2016 the Commission's decision establishing the EU-US Privacy Shield Program was issued. It enabled the transfer of data to US entrepreneurs provided that they process it in accordance with the regulations. If any entity breached the rules and requirements, the European Commission had the power to remove such an enterprise from the list.

The operation period of the Privacy Shield lasted only four years because in 2020 the Court of Justice of the European Union (CJEU) issued a ruling in which it annulled the contract. The CJEU's decision resulted, i.a., from a different understanding of the value of personal

data protection. For the EU, it is one of the fundamental rights that can only be limited on the basis of proportionality, i.e. when the scope and form of the Union's actions do not exceed what is necessary to achieve within the objectives of the treaties[12]. **However, the way this problem is regulated in American law is not equivalent to EU law. The American legal norms do not provide sufficient protection from the authorities' interference in the transferred personal data[13].**

Despite the differences in the approaches towards protecting the personal data between the US and EU, it should be noted that there are many different legislative initiatives overseas. Individual states have been working on legislation regulating the problematic areas for several years. Even though many initiatives got stuck in heated discussions within the legislative bodies, there were some which resulted in the development of an act. In particular, two regulations from the states of California and Virginia are worth paying attention to.

On March 2, 2021, the Virginia Consumer Data Protection Act (VCDPA) was signed by State Governor Ralph Northam. This document is very important compared to other regulatory acts because it is the second - after the document signed in California - that regulates the issue of personal data protection in such a broad and comprehensive manner[14]. It guarantees consumers (defined as natural persons residing in Virginia, acting individually, whose activities are not related to business or professional activity) the possibility of accessing, correcting, and deleting personal data. It obliges companies to seek the consumer's direct consent to collect and use his sensitive data, which includes, inter alia, race, sexual orientation, health, and immigration status. In addition, only the Attorney General of Virginia will have the power to sue companies that fail to comply with the law[15].

At the beginning of 2023, the California Privacy Rights Act (CPRA) is to take effect, which is a "revised" version of the California Consumer Privacy Act (CCPA), which took effect on January 1, 2020. The purpose of the document is to extend the protection of privacy of those living in California. The CPRA introduces rules similar to the GDPR standards, including, for example, the category of sensitive data, and extends the scope of activities covered by the obligation to obtain consumer consent. It should be emphasized that the aforementioned acts regarding the protection of personal data are state law acts. **More and more states undertake legislative activities, which may result in the emergence of large legal**

discrepancies between the acts. American companies and industry organizations more frequently point to the need for federal regulations. Such regulations from the federal authorities are probable to come soon.

	VCDPA	CCPA, as amended by the CPRA	GDPR
Right to opt-out of sale	✓	✓	✗
Opt-in or opt-out for processing of sensitive information	Opt-in	Opt-out	Opt-in
Statutory cure period for violations	✓	✓	✗
Right to appeal denials of requests	✓	✗	✗
Express obligations regarding de-identified data	✓	✗	✗
Requirement to perform data protection impact assessments	✓	✓	✓
Private right of action	✗	✓	✓
Governmental enforcement entities	Attorney General	CPPA, Attorney General	DPAs
Penalties	Up to $7,500 per violation	Up to $2,500 per violation and up to $7,500 per intentional violation or violation involving minors	Up to €10 million, or 2% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of less severe violations. Up to €20 million, or 4% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of more serious violations.
Operative date	January 1, 2023	January 1, 2023	May 25, 2018

Source: Kornbacher, Devika. Falcon, Briana. 2021 „Virginia Is For Lovers Of Data Privacy – UPDATED March 2021" https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3509049/

The aforementioned legislative discrepancies between states may lead to legal chaos. "The one thing that might create the political pressure [for federal privacy legislation] is more individual states coming up with crazy draconian laws," said Alan Chapell, president of privacy law firm Chapell and Associates[16].

American politicians are mostly in agreement with each other about the enactment of a federal law answering this issue. However, there are some major differences between them. Democrats want to give natural persons the power to sue companies that violate their law, while Republicans want to give this power to the attorney general.

Another cause which increases the chances of creating uniform regulations is the problem of China. The protection of the privacy of US citizens should be viewed as an element of

national security. The growth of Chinese companies on the American market, with the simultaneous technological development and implementation of new solutions to the functioning of the economy, implies easier access to huge data resources by Chinese actors. The lack of appropriate security standards allows the data to be used in a manner contrary to the principles of the economy, national security, and democratic values e.g. human rights.

The aforementioned development of new technologies, including mainly the development of artificial intelligence, influences the likelihood of cyberattacks. It should be remembered that technologies are used in both civilian and military matters. Algorithms work on the basis of data collected from the environment – including personal data. In a situation where digitalization is proceeding so rapidly, which results in an increase in cyberattacks, countries should take steps to ensure the best possible data protection rules. An example of cybercrime where the victim was an American company was data theft from Equifax (which is a rating company). From May to July of 2017, when the breach was discovered, Chinese hackers stole the personal data of over 147 million American citizens. As a result of this incident, the US charged four Chinese military officers, but China denies the allegations. Announcing the indictments, the Attorney General called the hack "one of the largest data breaches in history"[17].

Conclusion

Undoubtedly, one of the most important challenges that today's societies and international entities have to face is cybersecurity. Every day, mankind produces roughly 1.145 trillion megabytes of data[18]. Among the various data processed by networks, there are also those most related to natural persons - personal data. Many entities have taken steps to regulate and protect them against undesirable or even illegal activity. Among them are the European Union with its data protection regulation and some US states. In the United States, there are attempts to unify the law at the federal level, but one will certainly have to wait for the outcome of these efforts.

During the COVID-19 pandemic, a huge amount of people switched from traditional to remote working. As a result of the lack of adequate preparation, there have been cases when

an employee performs business activities on a private computer. Such a situation increases the probability of a data breach. The lack of awareness among employees is the result of insufficient or low-quality training. There will be more and more cyberattacks, which is why an increased effort of increasing public awareness over how to behave and how to protect oneself from dangerous actions is needed.

References:

[1]NASK, „Dane CERT Polska za pierwszy kwartał 2020 roku pokazują, że w okresie pandemii liczba zagrożeń wzrasta. <https://www.nask.pl/pl/aktualnosci/3835,Dane-CERT-Polska-za-pierwszy-kwartal-2020-roku-pokazuja-ze-w-okresie-pandemii-li.html>

[2]*NASK*, „Co pokazują dane CERT Polska za drugi kwartał".<https://www.nask.pl/pl/aktualnosci/3888,Co-pokazuja-dane-CERT-Polska-za-drugi-kwartal-2020-roku.html>

[3]*NASK*. 2019"Krajobraz Bezpieczeństwa Polskiego Internetu Raport Roczny 2019 Z Działalności CERT Polska". 2019. <https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.>

[4]Stępień, Agnieszka. 2018. „Bezpieczeństwo zintegrowane współczesnej Polski" s. 57 <http://piz.san.edu.pl/docs/e-XIX-2-3.pdf>

[5]Kopff, Andrzej.1982. „Ochrona sfery życia prywatnego w świetle doktryny i orzecznictwa", Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace Prawnicze, nr 100 (1982): 37.

[6]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[7]*NASK*. 2019 "Krajobraz Bezpieczeństwa Polskiego Internetu Raport Roczny 2019 Z Działalności CERT Polska". 2019. <https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.>

[8]tvn24, 2020. „Już ponad 400 prokuratorów i sędziów otrzymało groźby po wielkim wycieku danych osobowych". <https://tvn24.pl/polska/wyciek-danych-z-krajowej-szkoly-sadownictwa-i-prokuratury-ponad-400-prokuratorow-i-sedziow-otrzymalo-grozby-4937550>

[9]Wspólny Komunikat Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów – Strategia Bezpieczeństwa Cybernetycznego Unii Europejskiej: Otwarta, Bezpieczna I Chroniona Cyberprzestrzeń (JOIN(2013) 1 Final Z 7.2.2013). 2013.

[10]Rada Europejska, Rada Unii Europejskiej. „Cyberbezpieczeństwo: Jak UE Radzi Sobie Z Cyberzagrożeniami" <https://www.consilium.europa.eu/pl/policies/cybersecurity/.>

[11]European Comission. „Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection." <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents>

[12]Treaty on European Union

[13]Shoper.pl „Koniec Tarczy Prywatności UE-USA, co to oznacza dla twojego sklepu?" <https://www.shoper.pl/blog/koniec-tarczy-prywatnosci-ue-usa-co-to-oznacza-dla-twojego-sklepu/>

[14]Kornbacher, Devika. Falcon, Briana. 2021 „Virginia Is For Lovers . . . Of Data Privacy – UPDATED March 2021" <https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3509049/>

[15]Senate Bill No.1392 2 Amendment in the nature of substitute. <https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf>

[16]Kaye, Kate. 2021. „Cheat sheet: What to expect in state and federal privacy regulation in 2021" <https://digiday.com/media/cheatsheet-what-to-expect-in-state-and-federal-privacy-regulation-in-2021/>

[17]Corera, Gordon. 2020. „Equifax: US charges four Chinese military officers over huge hack" <https://www.bbc.com/news/world-us-canada-51449778>

[18]Bulao, Jacquelyn. 2021. „How Much Data Is Created Every Day in 2020?". <https://techjury.net/blog/how-much-data-is-created-every-day/#gref>

ABOUT THE AUTHOR

Maria Piątek. Graduate of BA in European Studies at the European Centre of the University of Warsaw, currently a fourth year law student at the Faculty of Law and Administration of the University of Warsaw. Her research interests include integration and disintegration processes in Europe, diplomacy, technological development and geopolitics.

IF YOU VALUE THE INSTITUTE OF NEW EUROPE'S WORK, BECOME ONE OF ITS DONORS!

Funds received will allow us to finance further publications.

You can contribute by making donations to INE's bank account:

95 2530 0008 2090 1053 7214 0001

with the following payment title: „darowizna na cele statutowe"