Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2021, Volume 53, Number 1(199), Pages 164-177
DOI: 10.5604/01.3001.0014.8118

Review article

Personal data in the aspect of IT usage – the end of anonymity

Katarzyna Zawierucha

Faculty of Management and Command, War Studies University, Warsaw, Poland,
e-mail: zawieruchakatarzyna@wp.pl

INFORMATION

Article history:
Submited: 04 October 2019
Accepted: 25 January 2020
Published: 15 March 2021

ABSTRACT

Information technologies are now a vital element of social life. Their task is to introduce people to a better tomorrow, catch up with the most developed countries, broaden horizons, and increase the standard of living. However, the rapid development of technology, access to data, and the possibility of managing it are still dependent on the human being, who determines whose data, when, and for what purpose it will be obtained and utilized. Nonetheless, indeed, all the data once found on the Internet remains there forever.

Huge data banks are built based on personal data and account profiling. Besides, these banks are strongly guarded and secured with the most modern alarm systems, and only a small group of trained IT specialists has access to them. By information provided on own preferences, purchases made, applications downloaded, shared information, photos, and likes on social networks, one can specify the sexual preferences, education, political and religious views, evaluate assets, or determine the marital status of the user. Even small amounts of information shared reveal the deeply hidden interests of online account users, and the benefits of information technology are designed to share personal information while forgetting about the risks automatically.

KEYWORDS

information technologies, personal data, security, GDPR

Introduction

The progress of the contemporary world caused the place where humanity was supposed to feel safe, where it was supposed to be able to be anonymous, namely, virtual reality, became anonymous only for criminals. Information technology is continually evolving, changing, adapting to a changing world, bringing many opportunities, and many threats. The inevitable development of everything related to human existence, including technology that creates today's reality, gave rise to the idea of analyzing technology used in relation to personal data. It is the technology that has the most significant impact on social reality. The importance and topicality of the issue are the most important arguments for taking it up.

Time, human work, research, and discoveries have caused social life changes to take place diametrically. Decades ago, it would have been hard to believe in today's possibilities of a telephone or computer connected to the Internet. Technology unanimously made it easy to communicate information using various instant messengers and direct access to knowledge and culture. Information technology is also all kinds of applications that make everyday life more comfortable, making payments, and making reservations without leaving homes, managing activities over time, or navigating the journey.

It is worth noting that technological changes that have occurred over the years enabled faster development in all branches of the economy. However, it is vital to make proper usage of what modernity offers. As mentioned, new technologies recognized as development trends guarantee unlimited data flow in all parts of the world, while taking technical requirements into account. If used correctly, artificial intelligence allows for surprising and fast development, access to entertainment, various fields of knowledge, efficient work, networking, medical care, and maintaining the length and quality of life.

However, there is also the other side of information technology, which is conducive to the spread of dangers, surveillance, the creation of existential threats, and going beyond the already largely augmented reality. The dangers of technology can have serious consequences. Humanity needs to protect itself from possible threats, but it also needs to set human evolution on a genuinely crazy pace. At what point to limit technological novelties and when to stop controlling them?

The article aims to generally analyze the issue of personal data in the aspect of the application of information technology, currently playing an essential role in human life. It is also an attempt to show the direction of development and autonomy of systems with still faulty intelligence in interdependence with social security.

Taking up issues related to personal data obtained and stored technology is very important. Information technology helps to create long-term ventures, supports the functioning of any activity, including human activity, and influences an effective response to rapidly occurring changes and the entire reality. At the same time, it leads to an endless race between people and the machines they create.

To achieve the assumed goal, personal data, information technologies, risks related to the violation of natural persons' rights or freedoms, and the security measures used to protect personal data were defined, and their essence was presented. Moreover, the problem was analyzed, and the direction of the impact of information technology on society was defined. The attention was also paid to the speed of said development and the ease of losing personal data using information technology.

1. The concepts of personal data and information technology

The era of information and technology falls in the 20th and 21st centuries, and its development is closely related to information-based computerization. Computerization having a relationship with the use of computers to process information, creates a scientific discipline called computer science. Informatics, in Latin *informatio*, means image, picture, idea, and deals with the methods of presenting, transmitting, and processing information as well as technical measures serving this purpose [1, p. 341]. The word information comes from the Latin word *informare*, which means to form. Initially, only the concept of information was created, without its general definition, by Claude Shannon in the late 1940s. M. Mazur defined information most consistently with its intention in the book entitled *Jakościowa teoria informacji* (*Qualitative information theory*). He describes information as transforming one informational association message into another message of this association [2, p. 72]. It mainly concerns sequences and connecting associations.

The word *technology* is a combination of two words *techne* – proficiency, and *logos* – knowledge. Technology is a field of technical knowledge aimed at processing raw materials and producing semi-finished and finished products. It is a way of using technical means. Technology is the use of technical means while a technique is only technical means [3]. When analyzing the underlying origin of the above words, it should be considered that information technology is a combination of practical skills, knowledge of devices, and messages that favor data processing.

Information technology is the method of obtaining and processing and distributing information through electronic devices, e.g., computers, telephones, radio, and television. The information is searched and selected using IT tools, mainly computers and web browsers, to obtain, process, store, secure, and transmit information. Information technology is a tool for information processing; it is the application of computer science in society [4, p. 179]. Information technology has radically been changing how people learn, communicate, and work (Fig. 1).

Information technology, i.e., architecture and production of technical IT means for information processing, is combined with communication technology that directly affects the transmission of information, and with information technology as the combination of IT applications with communication techniques [5, p. 90]. Information technology allows the processing of information between devices and users of these devices. Additionally, it stores and secures the obtained information for later analysis and presentation to deliver the right information to people. The information technology market, in cooperation with ICT (*Information and Communication Technology*), is developing at an alarming pace. A human can identify most technologies but is not fully aware of them.

Due to the high level of development of science, technology, and computer science, the information civilization is permanently connected with computers. However, the rapid development of technology, access to data, and the possibility of managing it are still dependent on the human being, who determines whose data, when, and for what purpose will be obtained and used. The information technology usage may contribute to the protection of personal data, but may also threaten it. The feeling of security after losing such data also

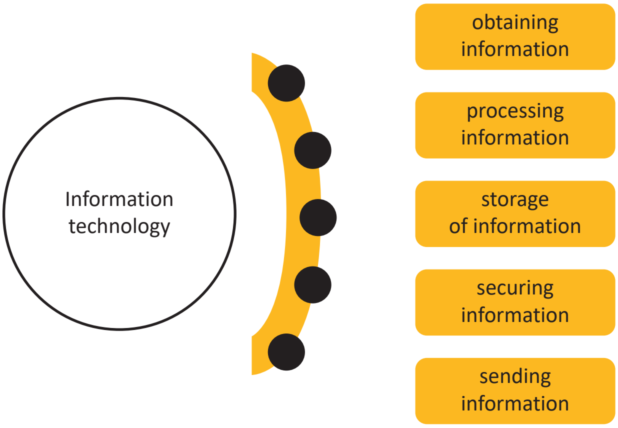

Fig. 1. Functions of information technology
Source: Own study based on [4, p. 179].

seems essential; although it may only constitute a meaningless incident for the person whose data is leaked, it is a breach of privacy and the occurrence of a threat. Is the data processed with the use of information technology safe? Where and for what purpose are they used? How to increase the effectiveness of personal data protection? Is it true that everything that is shared on the Internet stays there forever?

The protection of personal data, which is significantly influenced by information technologies used for activities violating personal data and/or privacy, is defined in the Regulation of the Minister of the Interior and Administration as *legal regulations related to the creation and use of personal data sets, as well as other data, aimed at the administrative and legal protection of the right to privacy as well as the rights and freedoms of the data subject* [6, Art. 48]. The Regulation definition is the same as the general concept of personal data protection included in the Dictionary of the Polish Language. However, it does not raise issues related to freedom and privacy *data protection – data security, the sum of all undertakings of a technical and organizational nature, undertaken to protect the collected data against destruction or damage* [7, p. 25]. What is personal data in principle? According to Article 4 (1) of the GDPR (European Data Protection Regulation), *personal data means information relating to an identified or identifiable natural person (data subject), an identifiable natural person is a person who can be directly or indirectly identified, in particular, based on an identifier such as name and surname, identification number, location data, internet identifier or one or more specific factors describing the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person* [8, p. 29-30] (Fig. 2, 3).

There are two types of personal data: ordinary personal data and personal data falling into special categories. Ordinary data includes [9, p. 163-186]:

– name and surname,
– home address (city, street, building number, apartment number),
– age,
– date of birth,
– PESEL number,
– education.

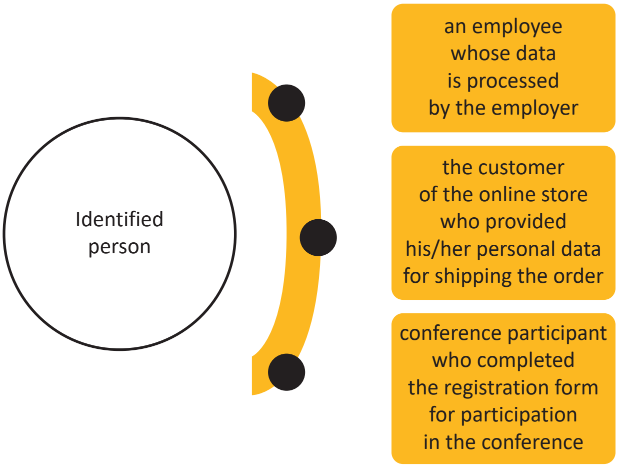
Identified person
an employee whose data is processed by the employer
the customer of the online store who provided his/her personal data for shipping the order
conference participant who completed the registration form for participation in the conference

Fig. 2. Examples of identified people
Source: Own study based on [9, p. 163-186].

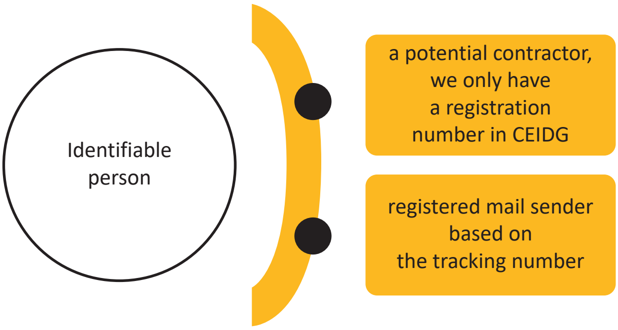
Identifiable person
a potential contractor, we only have a registration number in CEIDG
registered mail sender based on the tracking number

Fig. 3. Examples of identifiable people
Source: Own study based on [9, p. 163-186].

Personal data falling into special categories are:

- racial or ethnic origin,
- political views,
- religious or philosophical beliefs,
- membership of a trade union,
- genetic data,
- biometric data,
- health data,
- sexual orientation.

Personal data is data about natural persons. Legal persons do not have personal data, but employees of legal persons may have such data, e.g., information about the name of the company, as well as the name and surname of the person who works for it or represents it, it is possible to identify such a person.

To identify a natural person, in some cases it is only possible to have one piece of information about a given person, which is personal data. This type of information includes [9, p. 163-186]:

- PESEL number,
- car VIN number,
- e-mail address in the form of the name, surname, and the name of the company where the person works.

There are exceptions where the provisions of the GDPR do not apply. These provisions do not apply to the processing of personal data [9, p. 163-186]:

- by a natural person as part of a purely personal or household activity,
- by competent authorities for the purposes of crime prevention,
- of deceased people,
- during an activity which falls outside the scope of EU law,
- by the Member States when carrying out activities falling under Title V, Chapter 2, TEU (international agreement).

Legal regulations are intended to unify the law in all European Union countries. The public is not aware that many of the personal data protected by the GDPR may be generally available in countries outside the European Union, e.g., when a given company provides services inside and outside the EU. It is the institution's responsibility to inform about the attempted or theft of data, but many organizations forget about it.

GDPR (Regulation of the European Parliament and the EU Council on the protection of individuals concerning the processing of personal data and on the free movement of such data) is an act that has been adopted by the European Union and is intended to regulate the principles of personal data protection. The GDPR has replaced the Directive 95/46/EC of 195 and the Personal Data Protection Act of 1997. The GDPR is not implemented, which means that its provisions did not have to be introduced in Poland through the act, but all the provisions contained therein must be strictly complied with from May 25, 2018. The supervisory body, in accordance with the provisions and proper processing of personal data, is the President of the Personal Data Protection Office (UODO), replacing (in Poland) the Inspector General for Personal Data Protection (GIODO).

The development of technology has been hugely significant, especially today, when the population cannot imagine life without social networking sites, applications, and mobile devices. Each person builds a second reality, often unconsciously. Through the scraps of shared information, people manifest themselves ultimately and transmit data classified as confidential information. Due to information technology, society has lost its vigilance of the credibility of signals and messages from the world of cyberspace, i.e., the illusion of the real world, the world created with the use of ICT tools [10, p. 55-58]. Therefore, is it worth publishing personal data or private information in a world that is only a tool, often used by criminals for their benefit? Does society mindlessly live in an imaginary world that is slowly becoming a second life? The reality, which was to improve security, communication, cooperation, and human comfort around the world, became useful primarily to criminals and contributed to the decline of human intelligence, the escalation of terrorism, and future cyber wars.

2. Risks related to the violation of the rights and freedoms of natural persons

Information technologies have closed human to the surrounding world and other people. It mainly affects young people who are online every day. Social ties disappear in favor of loneliness or admiring what is happening in virtual reality. Probably 6 hours and 2 minutes a day are devoted to Internet use by the average Pole. If the average sleep time (8 h) is deducted, a Pole spends 1/3 of the day using the Internet. Along with the growing interest in being online, the risk of violating natural persons' rights or freedoms increases. Natural person means any person from birth to death [1, p. 341].

The lack of anonymity has become a permanent feature of information technology. In the past, the society using the Internet was anonymous, now there are non-anonymous social networking sites where one can find out everything about the other person based on the first and last name, place of residence, or preferences. In addition, all applications potentially serving to facilitate functioning, despite the designated function, continuously monitor people's position.

The increase in the development of information technology made it possible to steal or break the password to access websites, e-mail accounts, social networks, and applications. Despite this, the prospect of the inability to exchange information via Internet access generates considerable problems. Why can society no longer function without the Internet, and why does it surf the Internet unskillfully? Total surveillance and the loss of privacy is a massive flaw in information technology that is difficult to counter and, in principle, cannot be opposed to. The continuous development of information technology has made it available to an increasing number of recipients. As the research results show, households with Internet access, which include the type of household with children, constitute over 99% of the Polish population at the end of 2018, i.e., 0.4% more than at the end of 2017. The increase in Internet users is also visible, taking such factors as the class of place of residence and the degree of urbanization into account (Fig. 4).

All kinds of facilities, synchronization of devices and accounts, automatic saving of passwords, or restoring the login after logging in once is a considerable danger limiting the human freedom. Besides, it is joined by applications and devices that collect data about who is in which place, thematically sending profiles of potential friends or similarly displaying thematic websites or products that are likely to be of interest to the Internet user. Also, the devices changed, and applications always control the user's location, they know who they are meeting with, who their friends are, based on the frequency of correspondence, what they are interested in, based on the pages they browse or giving likes, how they like to spend their free time, based on marking places at shared photos, what music they like to listen, what they read, what watch, where eat, what time they get up and fall asleep, based on the lack or frequency of the phone display lighting up.

All this data is analyzed and can be applied in the process of identity theft or extortion. Additionally, all IT devices can cooperate to transmit the desired data. We are talking about the Internet of Things, where devices and objects collect or exchange the information obtained and processed. It is possible thanks to their sensors and via the computer network to which they are connected. The Internet of Things is mostly communication without human intervention. Devices, applications, etc., connected to the network, communicate in their language. These items can also be controlled by a human using a smartphone.

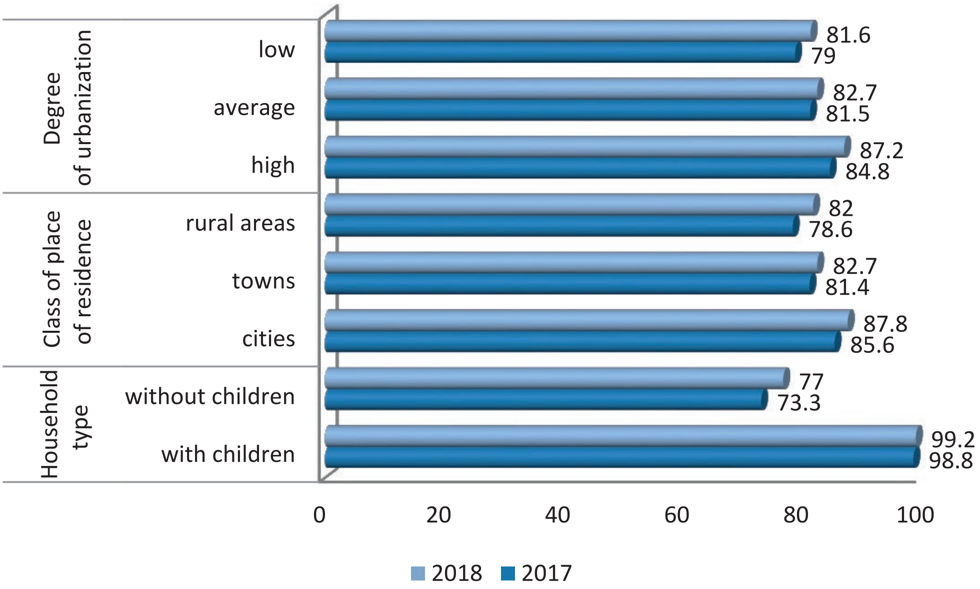

Fig. 4. Households with Internet access at home (data expressed in %)
Source: Own study based on [11].

The ease of access to data by third parties is also the possibility of modifying or removing them, preventing access to certain services, or blocking them entirely. While technology cannot be stopped, it can be limited or used consciously, so that it does not cause more harm than good. If the development of technology is implemented as quickly as it is happening today, it seems likely that soon every person will have a personalized chip in the form of a tattoo that will take over the functions of an identity card, credit/debit card, and apartment or car keys, and it will all be connected to one network. The amount of data to be analyzed will be huge but also easy to steal.

3. Personal data breaches

The risk related to violating rights and freedoms mentioned in the previous chapter is an inherent part of the life of the modern, digital Generation Z. Using only likes, someone can infer what sexual preferences the other person has, what their education is, what their political and religious views are, based on photos, they can appraise assets or determine the marital status of the observed person. Theft of a password is also no problem for a determined person. What to do in the event of password theft and access to personal data using information technology? In the above situation, the President of the Personal Data Protection Office should be notified immediately (up to 72 hours from finding the violation).

For activities involving a high risk of the possibility of violating freedoms, rights and loss of personal data include:

- profiling of the unemployed as a result of electronic application to a given job offer and entering their small address by selecting the location and nature and field of work, as well as by entering information about the applicant’s age, subsequent job offers will be sent thematically and will be adapted to a specific age group,
- creditworthiness assessment – bank systems in synchronization with cards or payment devices may, e.g., based on the amount of alcohol purchased or on the basis of frequent hotel room reservations, recognize that a given person will not be able to repay the loan because, for example, he/she divorces or falls into alcoholism, obviously one can appeal against the system’s decision, but then the request is decided by a bank employee (it means a decision change is unlikely). China is the country that monitors its society in this way. The Chinese government has the ability to analyze the purchasing history of citizens, thanks to payment devices, assess activity in social media, and analyze the group of friends or places that a given citizen visits (online and in real life). If a person wants to get a loan, they should follow the expectations of the ruling party. Impeccable behavior of a citizen may be rewarded with a promotion at work, a place in a privileged queue in a state office, a place in a better school for children, and higher creditworthiness,
- extensive public space monitoring systems, cameras at road intersections that monitor the location, speed, registration numbers, current location and time, and the brand of the car used by a specific person, as well as information about the presence of passengers,
- mobile monitoring system, the importance of which is like that of extensive monitoring systems, but is carried out by patrolling or photographing by uniformed services,
- data collection on the Internet, as the most dangerous activity connected with the risk of losing personal data by profiling Internet users’ accounts, observing with the help of a built-in camera in mobile devices, impersonating other people to build

trust, and sending viruses to the victim's e-mail. There are very often situations where the offender, to achieve the intended goal, influences the victim's emotions, e.g., by sending a message with the content to see what his wife, daughter, husband or other family member is doing and adding a link to it. If a person opens the link, their computer will be infected. The danger increases when the person using the work computer is the victim. In this case, the criminal gains access to all company data. The danger is increasing as companies increasingly use social media in running a business, both for marketing purposes, as well as for cooperation and communication with the client. It is worth noting that the number of enterprises using social media is systematically increasing. In 2013, this percentage was 19.1%, while in 2018 it increased by 11.2% and is 30.3% (Fig. 5),

- data processing in which people are classified or assessed relates to personalized offers, where the searched items, age range, or gender are taken into account,
- central data sets supporting the management of a specific group of people for purposes related to the implementation of public tasks, applies to data collected by offices in order to obtain, for example, statistical data.

The current number of data protection breaches is very large. Society should be sensitive to the activities of criminals, fraudsters, and hackers. The possibilities offered by information technology are huge. Data collected on the Internet may also be gained through ordinary, non-suspicious telephone calls. Often the caller introduces himself/herself as a bank employee, talks about a recent attempt to steal money from the caller, and mentions the possibility

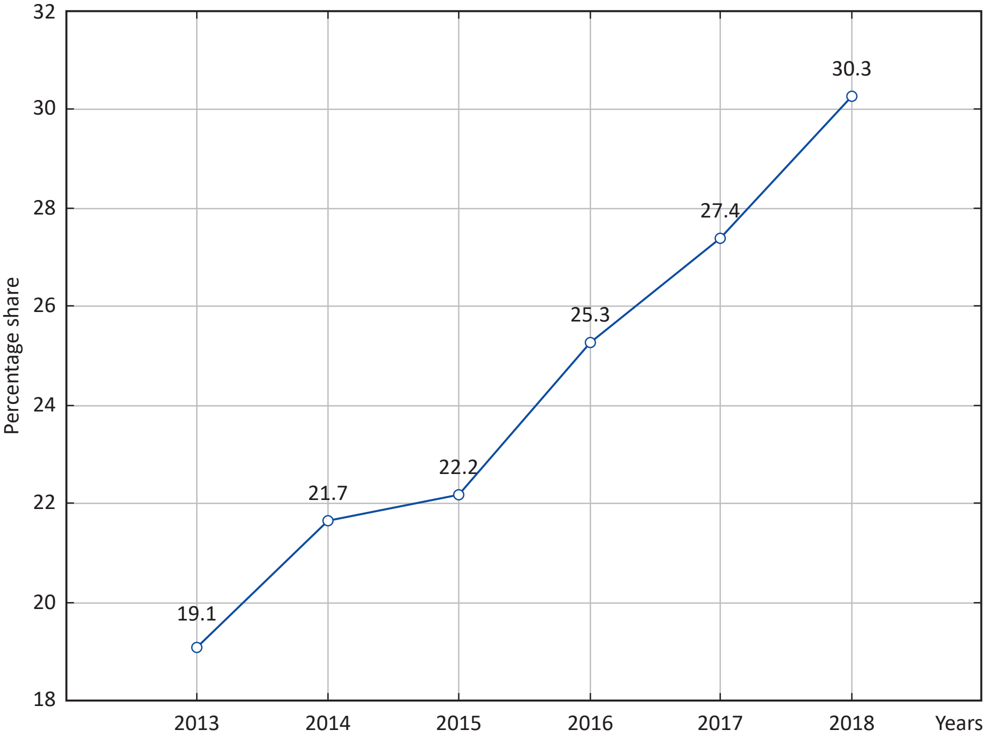

Fig. 5. Enterprises using social media (in % of total enterprises)
Source: Own study based on [11].

of introducing new security features. The bank's customer decides to use new security and provides the necessary data to protect his/her property. Ultimately, however, he/she becomes a victim of data loss and loss of property.

When agreeing to the processing of personal data, one should carefully read and analyze the content of the signed document beforehand. The privacy policy of many companies is based on cooperation between many other enterprises. If the data subject consents to the processing of data, other partner companies will also have access to the data. Despite a subsequent request to stop using the data, only the binding company will cease to process it. However, if a given person decides that other companies should also stop using their personal data, they must individually report such a reservation. Unfortunately, in practice this may prove problematic. Because one can meet with a lack of information about cooperating companies or this cooperation may have a more extensive structure and it will become completely impossible to reach all data processing companies. It should be said that functioning in today's reality is extremely difficult. Undoubtedly, more importance should be attached to signing documents or disclosing information on personal data.

4. Security used to protect personal data

It is worth noting that if a person rationally approaches modern technologies and is not consciously susceptible to the evil brought about by some technological creators' inventions, they can derive many benefits from some methods, systems, or techniques. However, it is essential to protect the information about themselves further and not succumb to imaginary opportunities or, consequently, to false chances of gaining profits. Many dangers may result in the loss of personal data or any other relevant information. Nonetheless, there are also many options for securing data against such loss. To protect privacy, one should:

- use an anti-virus program that provides protection against malware,
- introduce multi-stage login, most often double login to verify the account owner,
- cyclically change the password in order to limit the possibility of logging in to someone else's account after theft or observation of the password characters of a potentially affected person,
- use secure passwords containing 12 characters, capital letters, numbers, special characters,
- do not protect all accounts with the same password,
- use codes logged in via SMS to up-to-date verification of the owner of a portable multimedia device,
- install an authentication application to validate user details,
- turn on the function of notifying about unrecognized draws to detect data theft early,
- check the session logging sites on social networking sites to verify that no unauthorized person is logging into the account, and if so, check the location, log out of all sessions, report data theft and change the access password.

For additional data protection, one should always check security features in specific websites and control whether the website processes data correctly. According to the research, most Polish society (634 respondents, i.e., 57%) follow the standard registration instructions and do not read its conditions. That is the fundamental problem of the present day. The public striving to have an account on a given site often swears at all consents to implement the plan, frequently at the cost of their personal data. A relatively small percentage, i.e., 17% (187 respondents), check the quality of security. On the other hand, the remaining 26% (286 respondents) verify information on the privacy policy. It happens that the public wishing to join a specific website cannot opt out of data processing by enterprises cooperating with the website that enjoys interest. If a person wants to use a given website, it seems reasonable to pay fees, even if they are personal data. However, it is crucial to use the most reliable websites with a favorable quality policy (Fig. 6).

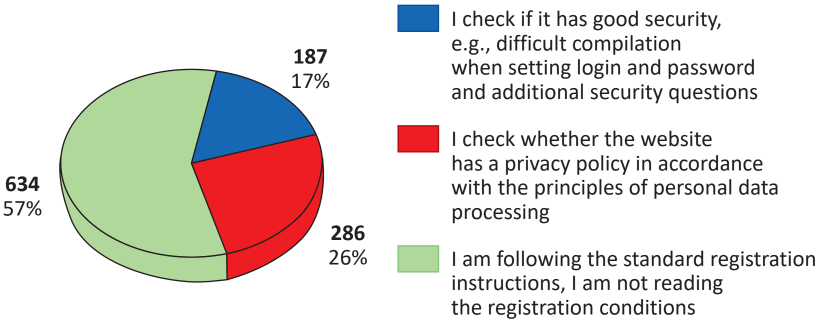

Fig. 6. During registration in the electronic service…
Source: Own elaboration based on [12].

Information or data about a specific person shared on the Internet should be superficial and well-thought-out. It is worth noting that information once it reaches the Internet remains there forever. According to most respondents, their identity appears as soon as they enter their first and last name in the Google browser. Five hundred sixty-four respondents (51%) are convinced about that. It mainly applies to younger people who use information technology from childhood or parents who make their children's image public from birth. Another example of unskillful use of the Internet is a part of the society which, at the time of popularizing the Internet, set up accounts on newly created social networking sites, and then, due to forgetting the password, did not delete the accounts, thereby they continue to function to this day. If the search results are narrowed down to the locality, it is straightforward to find information about the person one is looking for, as well as their photos. The situation is similar if the results are narrowed to the workplace. Unfortunately, sometimes using all possible security measures and resigning from life in the virtual world, some people post photos or information about others. The data of elderly people, who use the Internet ineptly or do not function in virtual reality, often cannot be identified on the Internet (Fig. 7).

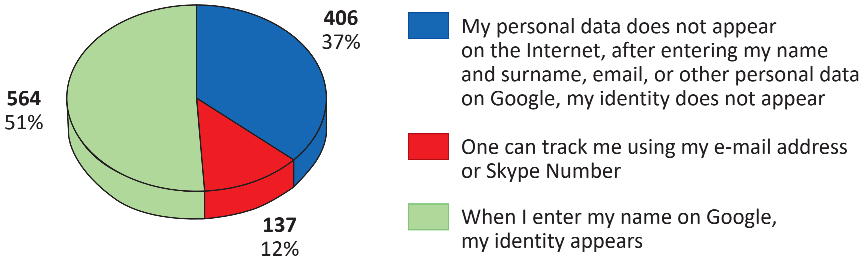

Fig. 7. How easy is it to track me on the Internet?
Source: Own elaboration based on [12].

There are many security features used to protect data. It is also prevalent to block cameras on laptops, tablets, or smartphones with special covers. It is often heard that criminals are connected to several devices and remotely watch the behavior of observed people, their apartments, equipment, or friends. However, it should be stated that by applying all the described safeguards, there is still a risk of data loss. Increasingly new threats can cause much damage, so it is so essential to navigate the virtual world skillfully.

Conclusions

The reality of information technology, which was supposed to improve security, communication, cooperation, and human comfort around the world, has turned out to be more useful to criminals, influenced the loss of human intelligence, and security risk. Besides, it violated information integrity, blocked the possibility of operation, as well as led to the theft of confidential information, access to passwords, e-mail addresses, identity theft, profiling, manipulation, and lack of knowledge of what is happening with the obtained data. Virtual reality, which was supposed to be an anonymous stepping stone from real life, was turned into an under-surveillance space, no longer anonymous.

Acknowledgement

The work was created as part of a research task included in the *Plan zadaniowo-finansowy działalności naukowej ASzWoj na rok 2018* (*Task and financial plan for scientific activity of ASzWoj for 2018*).

Conflict of interests

The author declared no conflict of interests.

Author contributions

The author contributed to the interpretation of results and writing of the paper. The author read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Katarzyna Zawierucha https://orcid.org/0000-0002-9439-5589

References

1. Sajko M (ed.). *Mała encyklopedia PWN*. 2nd rev. ed. Warszwa: PWN; 1996.
2. Mazur M. *Jakościowa teoria informacji*. Warszawa: WNT; 1970.
3. Furmanek W. *Kluczowe umiejętności technologii informacyjnych (eksplikacja pojęć)*. In: Furmanek W, Piecuch A (eds.). *Dydaktyka informatyki. Problemy teorii*. Rzeszów: Wydaw. Uniwersytetu Rzeszowskiego; 2004, p. 250-264.
4. Collin SMH, Głowiński C. *Słownik komputerów i Internetu*. United Kingdom: Peter Collin Pub.; 1999.
5. Juszczyk S. *Dydaktyka informatyki i technologii informacyjnej jako element przestrzeni edukacyjnej*. In: Furmanek W, Piecuch A (eds.). *Dydaktyka informatyki. Problemy teorii*. Rzeszów: Wydaw. Uniwersytetu Rzeszowskiego; 2004, p. 85-103.

6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024).
7. Fajgielski P. *Kontrola i audyt przetwarzania danych osobowych*. Wrocław: Presscom; 2010.
8. Szostek D (ed.). *Bezpieczeństwo danych i IT w kancelarii prawnej*. Warszawa: Wydawnictwo C.H. Beck; 2018.
9. Bielak-Jomaa E, Lubasz D (eds.). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa: Wolters Kluwer; 2018.
10. Retkiewicz W. *Cyberprzestrzeń w geograficznych badaniach środowiska człowieka*. Łódź: Wydawnictwo Uniwersytetu Łódzkiego; 2013.
11. *Społeczeństwo informacyjne w Polsce w 2018 r.*, [online]. Główny Urząd Statystyczny. 22.10.2018. Available at: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-wyniki-badan-statystycznych-z-lat-2014-2018,1,12.html [Accessed: 30 July 2019].
12. *Nie daj się okraść. Chroń swoją prywatność*, [online]. SCANN.R Available at: http://www.scanner.com.pl/wiadomosci/warto-wiedziec/366-vi-edycji-kampanii-nie-daj-sie-okrasc-chron-swoja-tozsamosc [Accessed: 1 August 2019].

Biographical note

Katarzyna Zawierucha – graduate of the War Studies University, Master of Logistics with specialization in transport, Master of Management and Command, specialization: quality management; winner of a doctoral scholarship and the Rector's scholarship for the best doctoral students. Her research interests include personal data, application of information technology, data protection on the Internet, artificial intelligence, and new technologies. Author of several publications related to transport, forwarding, storage, personal data protection, and modern technology. She actively participated and organized doctoral conferences, International Public Management Scientific Conferences and the National Scientific Conference on the arms industry.

Dane osobowe w aspekcie zastosowania technologii informatycznych – koniec anonimowości

STRESZCZENIE

Technologie informatyczne stanowią obecnie bardzo istotny element życia społecznego. Mają one za zadanie wprowadzać ludzi w lepsze jutro, dorównywać krajom najbardziej rozwiniętym, poszerzać horyzonty i zwiększać standard życia. Szybki rozwój technologii, dostęp do danych i możliwość zarządzania nimi są jednak ciągle zależne od człowieka, to od niego zależy czyje dane, kiedy i w jakim celu będą pozyskane i wykorzystane. Pewne jest jednak, że wszystkie dane, które raz trafią do Internetu pozostają tam na zawsze.

Ogromne banki danych są tworzone na podstawie danych osobowych oraz na podstawie profilowania kont. Dodatkowo banki te są silnie strzeżone i zabezpieczone najnowocześniejszymi systemami alarmowymi, a dostęp do nich ma jedynie mała grupa przeszkolonych informatyków. Poprzez określenie własnych preferencji, dokonywanych zakupów, pobieranych aplikacji, udostępnianych informacji, zdjęć, polubień na portalach społecznościowych można określić, preferencje seksualne, wykształcenie, poglądy polityczne i religijne, wycenić majątek użytkownika, czy też określić stan cywilny. Nawet małe ilości udostępnianych informacji ukazują głęboko ukryte zainteresowania użytkowników kont internetowych, a korzyści oferowane przez technologie informatyczne mają na celu automatyczne udostępnianie danych osobowych przy równoczesnym zapominaniu o zagrożeniach.

SŁOWA KLUCZOWE technologie informatyczne, dane osobowe, bezpieczeństwo, RODO

How to cite this paper

Zawierucha K. *Personal data in the aspect of IT usage – the end of anonymity*. Scientific Journal of the Military University of Land Forces. 2021;53;1(199):164-177.

DOI: http://dx.doi.org/10.5604/01.3001.0014.8118