Europejski Przegląd Prawa i Stosunków Międzynarodowych
Europejska Wyższa Szkoła Prawa i Administracji w Warszawie
nr 1–2/2023/65–66

Urszula Staśkiewicz*
Leszek Kołtun**
Grzegorz Kostyra***

Challenges and Threats to Safety Education in the Age of Digital Society. Analysis and conclusions based on the Polish education system

[Wyzwania i zagrożenia dla edukacji o bezpieczeństwie w dobie społeczeństwa cyfrowego. Wnioski z analizy polskiego systemu edukacyjnego]

Abstrakt
W artykule przedstawiono wyzwania stojące przed edukacją z zakresu bezpieczeństwa w świecie zagrożeń wynikających z pojawienia się społeczeństwa cyfrowego. Jak już wskazywali liczni badacze, współczesne zmiany związane z rozwojem technologicznym dotyczą wszystkich dziedzin życia, w tym sposobów dokonywania transakcji (upowszechnienie płatności bezgotówkowych) oraz pozyskiwania i ochrony danych. Artykuł definiuje pojęcie społeczeństwa cyfrowego oraz omawia kilka wybranych zagrożeń z nim związanych. W tym kontekście autorzy odnieśli się do potrzeby edukacji społeczeństwa w celu przygotowania go na nowe wyzwania i zagrożenia. Szczególny nacisk położono na program nauczania w szkołach podstawowych i średnich w Polsce.

Słowa kluczowe: społeczeństwo cyfrowe, phishing, polski system edukacji, skimming, sharenting, media społecznościowe, superconnected.

Safety is a state and process that necessitates complex legal, institutional, and organizational actions. It is not given once and for all, and the whole system of preparing for threats must be adequate to the changes occurring in the security environment. In the Polish scientific thinking, safety education is defined as "the education and development of defence awareness of youth, so that they can not only quickly and accurately

* **Urszula Staśkiewicz** – PhD, Europejska Wyższa Szkoła Prawa i Administracji w Warszawie.
** **Leszek Kołtun** – MA, Akademia Wymiaru Sprawiedliwości.
*** **Grzegorz Kostyra** – MA, Akademia Wymiaru Sprawiedliwości.

predict various threats, but also define them and actively participate in projects related to ensuring safety in social environments" (Pieczywok, 2011: 70), as well as "a specific system of didactic and educational activity provided by the family, school, army, mass media, social organizations and associations for the dissemination of ideas, values, knowledge and skills directly relevant to maintaining the external and internal security of the state" (Lorek, 2018: 65). Safety education is also a subject taught in Poland in primary and secondary schools, the core curriculum of which is outlined in the Regulation of the Minister of National Education of 30 January 2018 *on the core curriculum for general education in general secondary schools, technical secondary schools and stage II sectoral vocational schools* (Regulation 2018) and the Regulation of the Minister of National Education of 14 February 2017 *on the core curriculum for pre-school education and the core curriculum for general education in primary schools, incl. for pupils with moderate and severe intellectual disability, and for general education in stage I sectoral vocational schools, general education in special schools preparing for employment, and general education in post-secondary schools* (Regulation 2017).

The article presents the challenges faced by safety education in the world of threats posed by the emergence of digital society. As many researchers have already pointed out, the present-day changes associated with technological development affect all areas of life, including social behaviour and development of identity (Molotokienė, 2020: 32), ways of making transactions (widespread use of cashless payments) (Rabong, 2013: 262), as well as the acquisition and protection of data (and the phenomenon called disinformation) (Majdan, 2018: 145).

Modern society seems to live in two parallel worlds – the real and the virtual one. The advancement of the Internet has made everything faster, closer and more accessible. However, it has also brought new threats – cybercrime, which develops in cyberspace – a world that is fundamental for the existence of digital society. People need to learn to live and navigate in these worlds.

In recent years there have been many publications dealing with issues of digital society, which suggests that researchers, especially sociologists and psychologists (e.g. Mary Chayko and Tom Redshaw quoted in this publication), recognize that technological development changes human life and carries both opportunities, challenges and threats. However, the

analysis of the Polish education system has led the Authors to put forward the hypothesis that safety education in Poland (understood both as a school curriculum and as a process of shaping awareness, preparedness for various threats and acquiring skills to counteract them) is somehow lagging behind the changes occurring in the world.

The article will define the notion of digital society, as well as identify and discuss a few selected threats related thereto. The authors will also give a thought to safety education – suggest paths of development and ways to educate society to prepare it for the new challenges and threats. However, due to the limitations of this research paper, the study only addresses the issues of preparation of students in primary and secondary schools. Other forms of education in Poland were not analysed. The authors acknowledged that it is school that is the place where the most part of the education of young people takes place, and for this reason it was decided to examine how the curriculum and syllabus in Poland prepare the youth for the threats associated with digital society. At the stage of conceptualization of the research it was also recognized that the process of safety education is particularly relevant to young people, who are just developing their attitudes but already constitute a large part of the digital society – as early as in 2010 71% of 9–16 year olds in Poland had a profile on a social networking site (Livingstone, Haddon, 2011: 41), with another study conducted in 2018 showing that 10% of Facebook users were aged 13–17, while their percentage among Instagram users was 17% (www.mobirank.pl).

Despite addressing only a part of the issue, the article may serve as an introduction to further, in-depth research. For, as noted by M. Lorek, "New challenges in the context of safety linked with cyberspace must be taken into consideration in the curricula of safety education. This will allow for effective building of safety and security system and translate into the proper level of sense of security of citizens living in modern societies. It is essential to keep a close eye on new threats and respond to them, especially in building the security system at its core" (Lorek, 2018: 67).

Digital society – characteristics of the phenomenon

Digital information technology is becoming more and more deeply and dynamically ingrained in our society. It will probably not be long before every-

one is permanently connected to each other via the Internet. What remains clear is that widespread digitization will radically transform virtually every aspect of society. As pointed out in a report prepared by a group of Dutch universities, "digitisation will have major consequences for the way people live, work and learn, how we promote health and fight disease, how we deal with freedom and security, and for the role of information and knowledge, of industry, safety and mobility, of cultural identity and social equality, of consumption and sustainability, and of governance and democracy" (VSNU, 2016). A number of scholars note that digital society is a new type of society, different from that of the 20th century – the digital society, where information technology has led to fundamental societal shifts, is a carrier of particular characteristics. It got new organizing principles (relations and arenas) for public institutions and private agents, and it has also altered the relation between public and private. In digital society, information technology has become something more than a tool for communication, storage, and sharing of information (Svalastog, Donev, Jahren Kristoffersen, Gajović, 2018: 432).

In order to characterize digital society, it is necessary to point out, after T. Redshaw, that "digital society is characterised by information flowing through global networks at unprecedented speeds" (Redshaw, 2018: 28). It is also worth to mention that there are various attributes of digital society, among which are the following:

- Digital society deals with tools and technologies.
- The technologies and tools of digital society may be change.
- Some of the common technologies of digital societies are – network technology, software technology, communication technology, database technology, multimedia technology.
- All the emerging areas are – IOT, 5G, Cloud computing, big data.
- Digital society has for many passages such as digital divide, information divide (Paul, Aithal, 2018).

The concept of digital society is inextricably linked with the concept of "superconnected" introduced by M. Chayko (Chayko, 2017: 53). Quoting T. Redshaw: "Embodying this process are the growing array of devices which comprise the 'internet of things' and 'smart cities', linking mundane objects to networks of data analysis and in the process making our everyday lives ever more 'superconnected'. This new 'techno-social' arrangement is the backdrop of digital society, against which various social issues must be understood" (Redshaw , 2018: 28). Super connected is also

a multitude of threats and phenomena that create digital society – 'fake news' and online 'echo chambers' (that threaten the functioning of democracies), new forms of addiction that permeate digitally mediated forms of gambling and consumption (Chayko, 2017: 57).

Selected risks associated with the phenomenon of digital society

Threats related to e-banking – transactions with payment cards

E-banking and cashless payments using payment cards, as its integral part, play a n extremely important role both on the Polish and global markets for banking services. The use of modern information and telecommunication technologies is constantly growing, which is reflected in more and more innovative solutions in the field of electronic payments. Electronic payments, also known as e-payments, are payments made over the internet. They comprise all financial transactions made at a distance using electronic devices such as computers, cell phones or tablets. Electronic payments can be made through a variety of channels: credit transfers, credit cards or through electronic payment providers. In most cases, they replicate traditional payment methods – such as payment by bank transfer or credit card – adapted to the specifics of the Internet. The basis of their operation is a payment service provider (PSP), mediating between the bank of the customer making the purchase and the merchant, or mediating only between the parties to the transaction (Chinowski, 2013: 10).

A *payment card*, according to the European Parliament and Council Regulation, is defined as "a category of payment instrument that enables the payer to initiate a debit or credit card transaction" (UE 2015/751).

It is usually issued in the form of a plastic card. Each payment card specifies its issuer (precisely indicates the name of e.g. the bank) and its authorised holder. A cardholder may be a natural person, a legal person or any other entity that makes transactions using the card for its own account on the basis of the payment instrument agreement. The payment card agreement is a bilateral agreement between the card issuer and the cardholder. The card issuer undertakes to settle transactions made by the cardholder

with the use of the card. The cardholder, in turn, undertakes in the agreement to pay the amounts of the transactions or, in the case of a loan, to pay its liabilities together with interest and additional fees (Wójcicka K.).

Currently on the market there are several types of payment cards and several methods of their classification. Following the view of M. Zajda, payment cards can be divided according to the issuer, the cardholder, the function of the card, technical features, the nature of the agreement between the holder and the issuer and according to customer segmentation (Zajda, 2003: 13). It is also worth to point out the division of payment cards according to their construction – the technology of recording data on the card (technical features). According to this typology we can distinguish: embossed cards, magnetic cards, microprocessor cards and hybrid cards (Kuchciński, 2013: 111). Currently, according to data from the National Bank of Poland (NBP), the basic category of cards in Poland are debit cards (82.2%). The second most common category of cards in Poland are credit cards (12.7%) (NBP, 2021).

At the end of Q3 2020, there were 43.279 million payment cards issued on the Polish market, which is 30 thousand fewer cards than in June 2020 (a minimal decrease of 0.1%). A total of 37.9 million contactless cards were in circulation in Poland at the end of September 2020. Over the quarter this number increased by 261,000 cards. The share of contactless cards in the total number of payment cards amounted to 87.5% (86.8% in the previous quarter) (NBP, 2021). For comparison, at the end of Q4 2018, there were 41.2 million payment cards on the market in Poland and in Q4 2018 there were 1.445 billion transactions (cash and non-cash) made using payment cards for a total amount of PLN 191.7 billion, according to data received by the NBP from banks (NBP, 2019).

In the past decade in Poland an increasing number of users were inclined to use payment cards instead of the previously commonly used cash. The development of a functioning payment infrastructure is clearly visible. The number of available ATMs is increasing, as is the number of retail outlets where payment cards are accepted. On the other hand, against the background of the European Union, our country is still far behind in the rankings comparing the main indicators of the development of payment infrastructure, much below average parameters for the whole Union (Rabong, 2013: 280).

Payment card is one of the oldest electronic payment instruments. An unquestionable advantage for its users is not having to carry large sums

of money, which is also a form of protection against possible theft. A payment card does not limit its holder only to making transactions in the country of issue, as it is accepted by many others. In addition, numerous service networks offer additional discounts for card payments (Kukulski, 2002: 52).

When analysing the positive aspects of payment card transactions, one cannot help but notice that the development of the payment card market has been possible thanks to a kind of cooperation between all participants involved in card transactions. This cooperation would not be possible if individual groups were not convinced of the benefits they gain from such a form of payment. In order to better illustrate these profits, it may be useful to present them in bulleted form, broken down into individual groups of beneficiaries:

1. Banks:
- revenue from interchange fees charged to merchants,
- revenue from exchange rate differences in the situation of settlement of transactions made in foreign currencies,
- access to a tool enabling granting short-term loans and thus profiting from interest,
- strong customer loyalty to the bank,
- possibility of offering cardholders additional services (cross selling),
- possibility of gathering detailed information about the clients based on their transactions.

2. Merchants:
- increase in turnover as a result of customers making transactions for amounts greater than the value of the cash they currently have,
- increase in turnover as a consequence of taking advantage of the psychological effect of people's natural inclination to make a larger number or more expensive transactions when they do not see the amount due in cash,
- reduction or elimination of problems related to keeping and transporting cash.

3. Holders:
- prestige associated with certain types of cards,

- easy and quick method of settling liabilities and access to funds accumulated on the account connected to the card at different times and in different countries,
- safety related to the lack of necessity to transport cash and possibility to block the card in case of its loss or theft,
- access to quick credit in case of credit and charge cards,
- additional services and privileges related to the cards,
- promotions and price discounts for customers making payment card transactions.

It should be noted, however, that a payment card does not only mean facilitations regarding cashless payments, but also threats connected with crimes. The data published on the official website of the Polish Police (www.policja.pl) reveals that the most popular and the most serious e-banking offences involving payment cards in Poland are: skimming, phishing and counterfeiting of payment cards (www.policja.pl).

Skimming is a crime that involves illegal copying of information from a magnetic strip of a bank card (ATM, credit card, etc.) in order to make a duplicate of the original card, which will behave identically to the original card in an electronic environment. Transactions made using such copies of cards are charged to the legitimate cardholder, with the cardholder often unaware. It is possible to copy the entire contents of the strip and save it on another card with the help of commonly available devices. Cards can be copied in stores, restaurants, gas stations, basically anywhere where card payments can be made. A dishonest seller is able to copy a card strip in the backroom, under the counter, or even in front of an unsuspecting customer (www.policja.pl).

According to experts on the subject of skimming, in order to protect the card against being copied, the cardholder should always have it in view when making transactions in order to watch for additional (illegal) scanning (Szymczykiewicz: 3). Nevertheless, there is also another type of skimming – the so-called "ATM skimming". "ATM skimming is a crime involving illegal modification of the construction of an ATM to capture the PIN code and magnetic stripe data of a payment card in order to make a duplicate card that will be used to withdraw funds from the bank account to which the card is linked. The modification of an ATM is mainly done by placing a card-scanning device, called a skimmer, over the card slot. Professional attachments are miniature devices that can both trans-

mit data by radio and store it on a built-in memory card" (Mikołajczyk, 2014: 14).

Banking specialists suggest that in order to protect yourself from this type of skimming you should protect (gently cover) the keyboard with your hand while entering the PIN number. Additionally, "one should always make sure that bystanders are not standing too close. When making a withdrawal, pay attention to the appearance of the ATM itself: check it for any additional, non-standard equipment, e.g. unusual strips with small holes drilled in them, elements acting as magnets, a keyboard in the form of a glued-on or not very firmly attached fake keypads, elements that can be torn off or peeled off, etc. If something raises your doubts, you should immediately notify your bank, the company that operates the ATM (appropriate information is placed on each device), or the police" (https://bankomania.pkobp.pl).

Another crime is phishing. According to the generally accepted characteristics, "in a broader sense, phishing is a form of fraud where the person deceiving the victim uses a trustworthy entity (bank, municipality, post office, etc.). [...] A classic phishing scam attempt begins with an email from a bank, email service provider or another known entity. These messages usually require you to click on a link to verify your personal data. Failure to confirm such information leads to suspension or deletion of the account. In order to gain veracity, phishing emails contain logos and images related to the business the criminal claims to be. Instead of taking you to the website of the bank or other business you expect to see from the email, the link takes you to the scammer's website. Anything typed there will be sent to the author of the site, along with a login and password to the trusted website. Once able to access the account, the attacker can use it in various ways, depending on the type of account. In the case of an e-banking account, the scammer can purchase whatever they want and make a money transfer from our account: the email address can be used to log into forums, review email correspondence, send spam to other users" (https://bitdefender.pl). As a way to protect against this form of scam, IT professionals recommend SPAM filtering, installing a special anti-phishing module, as well as setting up two-factor authentication on important accounts (https://bitdefender.pl).

The third type of payment card crime outlined is counterfeiting. Payment card counterfeiting is, under the Polish Penal Code, a crime against

trade in money and securities. In line with art. 310 of the Code, "§ 1. Whoever counterfeits or forges Polish or foreign money, a Polish or foreign medium of exchange that has been designated as legal tender but has not yet been introduced into circulation, another legal tender or a document authorizing to receive a sum of money or containing an obligation to pay capital, interest, a share in profit or a declaration of participation in a company, or removes a sign of removal from circulation from money, another legal tender or such a document, shall be subject to the penalty of deprivation of liberty for a minimum term of 5 years or the penalty of 25 years of deprivation of liberty. § 2. Whoever enters money, other legal tender or medium of exchange or a document specified in § 1 into circulation or accepts it for such purpose, stores, transports, transfers it or assists in its disposal or concealment, shall be subject to the penalty of deprivation of liberty for a term of between 1 and 10 years. § 3. In cases of lesser importance, the court may apply extraordinary mitigation of punishment. § 4. Whoever makes preparations to commit the offense specified in § 1 or 2, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years" (Journal of Laws of 1997 No. 88, item 553).

In conclusion, the widespread use of e-payments is a major change for financial institutions, cardholders and merchants alike. Undoubtedly, the use of payment cards is convenient, and the card cannot get damaged as easily as a note. However, the revolution in payments has also brought threats that did not exist before, and unaware users may become victims of theft crime. It is therefore worth to consider methodical education of the public in connection with the increasingly widespread use of payment cards. Perhaps this would protect many payers from losing their savings.

Threats posed by social media

Social media is the term often used to refer to new forms of media that involve interactive participation. An apt description of the specifics of social media was presented by J. Manning: "All social media involve some sort of digital platform, whether that be mobile or stationary. Not everything that is digital, however, is necessarily social media. Two common characteristics help to define social media. First, social media allow some form of participation. Social media are never completely passive, even if sometimes social networking sites such as Facebook may allow passive viewing of what

others are posting. Usually, at bare minimum, a profile must be created that allows for the beginning of the potential for interaction. That quality in and of itself sets social media apart from traditional media where personal profiles are not the norm. Second, and in line with their participatory nature, social media involve interaction. This interaction can be with established friends, family, or acquaintances, or with new people who share common interests or even a common acquaintance circle. Although many social media were or are initially treated or referred to as novel, as they continue to be integrated into personal and professional lives they become less noticed and more expected" (Manning, 2014: 1160).

Social media have become a place where everyone can find a group of people sharing similar interests, problems or needs. Profiles are also created by companies seeking to attract customers or individuals to earn money from "followers". However, it is important to keep in mind that social media are a source of many threats.

One of them are cyber attacks, e.g. in the form of hacking into a user's account and acquiring data from private conversations, e.g. photos sent between friends and the content of conversations that should not be made public (including passwords and codes sometimes sent by users not aware of the threats).

Another threat is the fact that social media are a rich source of open source intelligence (OSINT). OSINT is all information that is not secret and that has been made available. It is also a sort of reconnaissance and a form of intelligence that involves gathering information from publicly available sources. Robert David Steele emphasises that OSINT is "unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question" (Steele, 2006: 129–147). In order to fully comprehend the value of OSINT, it is of crucial importance to point out the American view of it, according to which "information does not have to be secret to be valuable" (CIA, 2019).

In the context of discussion on safety education in digital society, it is worth mentioning how much information is made available by users of social media. Often it is the whole network of relationships (both family and business), information about the place of work, place of study and of residence. These details provide a source of knowledge for many criminals.

Another major threat comes from so-called sharenting – publishing photos of one's child. According to research, as many as 75% of parents who regularly use the Internet publish materials involving their children (London School of Economics, 2018). In Poland, this percentage amounts to about 40%. Interestingly, children may have digital footprints even before they are born. This is a result of parents publishing photos from ultrasound examinations. It even happens that, children who are not even born yet have their own profile on a social media site. It should be noted, however, that publishing their image may expose the child to cyberbullying, e.g. hate speech. Peers may easily find someone's childhood photos on profiles of their parents, download and share them, or alter them as they like. The photos can also be used by paedophilia websites. Users (parents) should be aware that such a situation may occur, especially if they post photos of children at the beach and information about the kindergarten or school they attend. Moreover, it is worth noting that posting large numbers of photos taken in one's own home only makes the task easier for possible thieves. After all, with the right number of resources, it is easy not only to reconstruct the floor plan of your home, but even the exact location of your valuables.

Information obtained from social media serves also as materials facilitating identity theft. As noted by the authors of the publication entitled *Identity theft, identity fraud and/or identity-related crime*: "There are many things you can do with identities. Not only can you use someone else's or a non-existing identity, but people can also swap identities or destroy identities." What is important here is that identity is not something that is typically stolen. This is because the defining characteristic of theft is that the owner no longer possesses the stolen item, yet with an identity, this is usually not the case: the victim of identity theft still retains it (Koops, Leenes, 2006: 25).

It should be borne in mind that identity on the Internet is very vulnerable, as data shared once can quickly be transferred to different places in the world, and identity thieves can use it while physically residing on another continent. According to research conducted by Fellowes in cooperation with the Credit Information Bureau (Pol. *Biuro Informacji Kredytowej*), the majority of Poles poorly secure their identity online.[1] Only

[1] The study was conducted from October 22, 2013 to October 4, 2014. During one year the survey was completed by 1107 people.

37% of respondents are anonymous in the web – the user's identity does not appear in Google after entering their name and surname. The second group (12%) consists of people whose identification is possible through their e-mail address or GaduGadu/Skype number. And even though this seems to be a safe solution, it actually exposes the user to a number of threats. This is because the e-mail address is assigned in the network to a particular individual and allows, for example, to gain access to private data on social networking sites or learn about one's the place of work. Half (51%) of respondents share all their personal information with any Internet user, thus exposing themselves to many dangers associated with identity theft. 79% of respondents have accounts on Facebook, Twitter or Nasza Klasa. People using these functions of the Internet declare frequent sharing of data on their profiles. Respondents most often publish their photos (78%) and information about hobbies or leisure activities (58%). Most participants protect the privacy of their families – 68% of them declare that they never publish family photos. However, as many as 27% of respondents post them several times a year (Wilk, 2014).

Summing up, social media is one of the primary tools for staying in touch in the world of digital society. It is where we meet new friends, share memories with family and establish business contacts. Yet, it is important to remember to use the Internet wisely and safely. Therefore, we should consider making the awareness of the threats posed by social media a part of safety education.

Analysis of the Polish education system in terms of safety education

As mentioned at the beginning of the paper, safety education is a subject taught in Polish primary and secondary schools.[2] However, there are also elements of safety education (in its broader sense) that can be found in other subjects. In the context of digital society, an important role is played by computer science. In their analysis, the authors decided to focus on the curricula of these two subjects.

[2] In the Polish educational system, a student who graduates from primary school goes on to attend either a general secondary school or a technical secondary school. There is also the possibility of attending a vocational school, but the curriculum of vocational schools was not subject to analysis as part of this publication.

Computer science in classes 4–8 of elementary school is taught for 45 minutes per week (1 lesson per week) (Regulation, 2019). According to legal regulations, the purpose of computer science classes at school is to "provide students with conditions for acquiring knowledge and skills needed to solve problems using methods and techniques derived from computer science, including logical and algorithmic thinking, programming, using computer applications, searching and using information from various sources, using computers and basic digital devices, as well as applying these skills during classes in other subjects, e.g. when working on texts, performing calculations, processing information and presenting it in various forms. School is also expected to prepare them to make conscious and responsible choices when using resources available on the Internet, to critically analyse information, to navigate safely in digital space, including establishing and maintaining respectful relationships with other online users." (Regulation 2017). Among the specific requirements there is work with a word processor, spreadsheet and graphics editor, as well as work on the Internet (to find necessary information and educational resources, as a communication medium). It is also worth pointing out that the curriculum contains classes on safety, and in line with this approach it is expected that at the end of elementary school the Student:

1) uses technology in accordance with generally established rules and the law; observes the principles of health and safety at work;
2) recognizes and respects the right to privacy of data and information and the right to intellectual property;
3) names threats associated with widespread access to technology and information and describes methods of protecting against them;
4) applies anti-virus prevention and knows how to protect a computer and the information stored therein from threats;
5) identifies ethical issues related to the use of computers and computer networks, such as: security, digital identity, privacy, intellectual property, equal access to information, and sharing information;
6) acts ethically when working with information;
7) distinguishes between types of licenses for software and web resources.

It should be added, however, that the entire computer science curriculum consists of five sections, of which the section on security is at the end

and is also the shortest. Thus, on the one hand the program contains elements of raising users' awareness of the threats posed by the Internet, but on the other this issue is given less importance than other topics.

In general secondary schools (and technical secondary schools), computer science is taught for three years at the rate of one hour per week. In line with the law (Regulation 2018), the most important goal of computer science education for students is the development of computer thinking skills, focused on creative problem solving in various fields while consciously and safely using methods and tools derived from computer science. Such approach, initiated in the primary school, is continued in the general secondary school and technical secondary school at both the basic and extended levels. The subject of computer science is taught to all students in every grade, starting from grade 1 of primary school, and is continued in general and technical secondary schools. The detailed content is divided (as in [primary] school curricula) into five sections:

I. Understanding, analysing and solving problems.
II. Programming and problem solving using computer and other digital devices.
III. Using a computer, digital devices and computer networks.
IV. Developing social skills.
V. Observance of the law and safety rules.

In the context of these considerations, the most important is point V, under which the Student:

1) complies with netiquette rules and legal regulations regarding: personal data protection, information protection, copyright law and intellectual property protection in access to information; is aware of the consequences of breaking these rules;
2) respects current laws and ethical standards regarding the use and distribution of computer software, others' and own applications, as well as electronic documents;
3) applies good practices in protecting sensitive information (e.g. passwords, PIN codes), data and operating system security; explains the role of information encryption;
4) describes the damage that online piracy activities can cause to individuals, selected institutions, and general public;
5) explains the role of authentication techniques, cryptography and electronic signature in protecting and accessing information;

6) explains the importance of encryption and electronic signature algorithms.

Therefore, similarly to the primary school curriculum, students are introduced to the threats associated with various aspects of cyberspace, yet that section is at the very bottom of the list of topics covered in class.

Another subject, safety education, is designed to prepare students to behave appropriately and to respond appropriately in situations that pose a threat to health and life. The subject comprises various educational contents from the field of national security, contents concerning the organization of rescue operations, health education and first aid. The primary school curriculum provides one hour per week in one year (eighth grade) and comprises four sections:

I. Understanding the nature of national security.
II. Preparing students to act in situations of extraordinary threats (disasters and mass accidents).
III. Developing skills in basic first aid.
IV. Shaping individual and social attitudes promoting health.

The general secondary school (or technical secondary school) curriculum similarly provides for one hour per week in one year and the curriculum likewise includes four sections:

I. National security.
II. Preparation for rescue operations in emergency situations (mass accidents and disasters).
III. Basic first aid.
IV. Health education. Individual and collective health. Health-promoting behaviour.

The analysis of the safety education curricula in primary and secondary schools leads, therefore, to the conclusion that this subject prepares students for threats related to the real world, not the world of cyberspace.

In conclusion, it should be acknowledged that the authors of the Polish educational programme have recognised the threats associated with cybercrime, but given the time allocated to providing students with the information on how to characterise and counteract them, as well as the fact that the curriculum covers only a part of the issues, the hypothesis posed at the beginning of the research has been partially confirmed. This is because digital society is a much broader issue carrying more threats than those discussed at school.

Conclusions

The 21st century is characterized by rapid technological changes that have more and more impact on all areas of life. However, it is important to remember that technology, although making life easier on the one hand, poses enormous challenges on the other. The skills and possibility to use them directly translate into efficiency, functionality and quality. Technologies facilitate solving specific problems and support achieving operational and strategic goals. However, improper use of modern technology (or failure to take advantage of it) can lead to a decrease in the level of security, lower efficiency or emergence of new, previously unknown problems.

The financial market is not spared from these changes either, as it is taking advantage of these developments to introduce new methods of payment. The development of electronic payment instruments is inextricably linked to the growing popularity of banking financial instruments. The rate of growth in the number of payment card users allows us to predict that in the future they will replace cash in everyday transactions. However, it has to be kept in mind that using payment cards does not only bring benefits but may also become a source of serious threats (Jakubski, 2006: 36). It is worth noting, for instance, that according to statistics from the National Bank of Poland, about PLN 15 million was stolen using payment cards in the second half of 2014, of which almost 42% of forgeries were made in the category of online transactions (the value of theft is almost PLN 6 million), 29% were transactions with stolen cards, and 18% of detected crimes were related to the use of counterfeit cards. Other types of payment card crimes mentioned in the NBP report include thefts using undelivered and lost cards and thefts committed using forged data (e.g. false ID) – but these types of thefts are rather marginal (www.nbp.pl).

In summary, the changes that led to the development of digital society resulted in emergence of new threats to the safety of people and the community they live in. Safety education must respond to such situations so that a satisfactory level of citizen safety can be guaranteed. As observed by many researchers, including Professor Inald Lagendijk, "the digital society must be based on a fundamental understanding of the interaction between information technology, people and society. A solid foundation of ICT education and science is essential in this regard" (VSNU, 2016). It must not be forgotten that safety is not only a state, but also a process of

becoming secure, and safety education should be transformed in parallel with the changes taking place in the field of security. Therefore, Poland faces a challenge of better preparing its citizens for the threats related to the emergence of the digital society. Particular attention should be paid to educating young people. Indeed, it is no secret that younger generations tend to be more enthusiastic about using new technologies (such as smartphones) and to underestimate the risks they carry.

In conclusion, the issue of safety and safety education in the age of digital society is a great challenge. This is because not only threats need to be identified, but also curricula need to be adapted in order to educate citizens effectively and adequately.

Abstract
The article presents the challenges faced by safety education in the world of threats posed by the emergence of digital society. As many researchers have already pointed out, the present-day changes associated with technological development affect all areas of life, including ways of making transactions (widespread use of cashless payments) and the acquisition and protection of data. The article defines the notion of digital society, and discusses a few selected threats related thereto. In this context, the authors referred to the need to educate the society in order to prepare it for those new challenges and threats. Special emphasis was placed on the curriculum of primary and secondary schools in Poland.

Keywords: digital society, phishing, Polish education system, skimming, sharenting, social media, superconnected.

BIBLIOGRAPHY

Chayko M. (2017), Superconnected: the Internet, digital media, & techno-social life, Thousand Oaks, CA, Sage.

Chinowski B. (2013), Elektroniczne metody płatności. Istota, rozwój, prognoza. Poradnik klienta usług finansowych, Komisja Nadzoru Finansowego, Warszawa.

CIA, INTellingence: Open Source Intelligence, available: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html [20.05.2021].

Gospodarowicz A.(2005), Bankowość elektroniczna, PWE, Warszawa.

http://www.policja.pl/pol/aktualnosci/11364,Co-to-jest-skimming.html [25.02.2021].

https://bankomania.pkobp.pl/finanse-na-co-dzien/bezpieczenstwo/skimming-jak-sie-przed-nim-chronic/ [12.02.2021].

https://bitdefender.pl/phishing-co-to-jest-i-czy-potrafisz-go-rozpoznac/ [02.02.2021].

https://mobirank.pl/2018/06/08/kim-sa-uzytkownicy-social-mediow-w-polsce-maj-2018/ [04.02.2021].

https://www.nbp.pl/ [28.02.2021].

https://www.nbp.pl/systemplatniczy/karty/q_04_2018.pdf [15.02.2021].

Jakubski K. J., *Bezpieczna karta*? [in:] J. Kosiński (ed.): Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych (2006), Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno.

Koops Bert-Jaan, Leenes Ronald (2006), ID Theft, ID Fraud and/or ID-related Crime. Definitions matter, Datenschutz und Datensicherheit – DuD, September.

Kuchciński A. (2013), *Rynek kart płatniczych w Polsce*, Akademia Finansów i Biznesu Vistula – Warszawa, „Kwartalnik Naukowy Uczelni Vistula", 4 (38).

Kukulski J. (2002), Aspekty prawne bankowych kart płatniczych w polskim systemie pieniężnym, Wyd. Kodeks Sp. z. o. o., Warszawa.

Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings. LSE, London, EU Kids Online.

London School of Economics, Livingstone S., Blum-Ross A., Zhang D., (2018), What do parents think, and do, about their children's online privacy? Parenting for a Digital Future: Survey Report 3, London School of Economics, http://eprints.lse.ac.uk/87954/1/Livingstone_Parenting%20Digital%20Survey%20Report%203_ Published.pdf [05.05.2021].

Lorek M. (2018), *Wyzwania stojące przed edukacją dla bezpieczeństwa w dobie społeczeństwa informacyjnego*, „Edukacja – Technika – Informatyka" no. 2 (24), Wydawnictwo UR.

Majdan P. (2018), *Wpływ dezinformacji i propagandy na geopolitykę w regionie Europy Wschodniej* [in:] Paulina Szymczyk, Kamil Maciąg (eds.), Człowiek a technologia cyfrowa – przegląd aktualnych doniesień, Wydawnictwo Naukowe TYGIEL, Lublin.

Manning, J. (2014), *Social media, definition and classes of* [in:] K. Harvey (ed.), Encyclopedia of social media and politics, Thousand Oaks, CA: Sage.

Mikołajczyk K. (2014), *Przestępstwa z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego", 6 (10).

Molotokienė E. (2020), *The transformation of narrative identity into digital identity: challenges and perspectives*, „Colloquium", 2 (38).

NBP (2021), National Bank of Poland, Information on payment cards Q3 2020, Payment Systems Department, Warszawa.

NBP (2019), National Bank of Poland, Information on payment cards IV quarter 2018, Payment System Department, Warsaw.

Paul P. K., Aithal P. S. (2018), Digital Society: It's Foundation and Towards an Interdisciplinary Field, Advances in Information Technology, Management, Social Sciences and Education December.

Pieczywok A. (2011), Wybrane problemy z zakresu edukacji dla bezpieczeństwa. Konteksty, zagrożenia, wyzwania, AON, Warszawa.

Rabong M. (2013), *Stan rozwoju obrotu bezgotówkowego w Polsce na tle innych krajów UE* [in:] Helena Żukowska, Marian Żukowski (eds.), Obrót bezgotówkowy w Polsce, Wydawnictwo KUL Lublin 2013.

Redshaw T. (2018), What is digital society? Reflections on the aims and purpose of digital sociology, University of Salford, UK, SAGE Publications.

Steele R.D. (2006), Open Source Intelligence. // Handbook of Intelligence Studies / Johnson, Loch K. (ed.). New York, Routledge.

Svalastog A., Donev D., Jahren Kristoffersen N., Gajović S. (2017), *Concepts and definitions of health and health-related values in the knowledge landscapes of the digital society*, Croat Med. J., Dec. 58(6).

Szymczykiewicz R., Czym jest skimming, available: https://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298321,Czym-jest-skimming.html [19.02.2021].

VSNU, The Digital Society – September 5, 2016, available: https://www.thedigitalsociety.info/wp-content/uploads/2018/04/VSNU-The-Digital-Society.pdf [10.02.2021].

Wilk A., Kradzież tożsamości. Research report, Fellowes, Biuro Informacji Kredytowej, https://archiwum.giodo.gov.pl/pl/file/6594 [01.06.2021].

Wojciechowska-Filipek (2010), Technologia informacyjna w usługach bankowości elektronicznej, Difin, Warszawa.

Wójcicka K., Karty płatnicze w Polsce, available: https://www.knf.gov.pl/knf/pl/komponenty/img/Wojcicka_Karty_platnicze_w_Polsce.pdf [10.02.2021].

Zajda M. (2003), Prawno-kryminalistyczne aspekty przestępczości z użyciem elektronicznych instrumentów płatniczych, Szkoła Policji w Słupsku, Słupsk.