STUDIA NAD BEZPIECZEŃSTWEM

Nr 7 ss. 159–173 2022

ISSN 2543–7321
© Instytut Bezpieczeństwa i Zarządzania, Akademia Pomorska w Słupsku

Przyjęto: 11.06.2022
Zaakceptowano: 11.06.2022

Oryginalna praca badawcza

DOI: 10.34858/SNB.7.2022.013

Dawid Czerw
War Studies University
in Warsaw
dawid.czerw@icloud.com
ORCID: 0009-0006-8345-173X

SMART SOCIETY, EDUCATION. NEW FORMS OF "INFORMATION SOCIETY" EDUCATION IN THE LIGHT OF POLISH AND EU LAW

INTELIGENTNE SPOŁECZEŃSTWO, EDUKACJA. NOWE FORMUŁY EDUKACJI „SPOŁECZEŃSTWA INFORMACYJNEGO" W ŚWIETLE PRAWA POLSKIEGO I UE

Abstract: This issue concerns the reality of new technologies and services of the information society, which provide society with many professional and social advantages, but which also bring with them a wave of various risks. Nevertheless, as an information society we are happy to use these solutions to an unimaginable extent. It is therefore necessary to ask whether, as a society aspiring to become a 5.0 society, we are sufficiently, or not at all, educated about these technologies, both in terms of their benefits and potential dangers, e.g. cyber threats or impacts on us and our environment? The article presents an analysis of the current forms of education in Poland in 2021 in primary and secondary schools and questions whether, with the development of a reality filled with new technologies and in an era of information overload, we are placing sufficient emphasis on education in the dimension indicated?

Zarys treści: Kwestia ta dotyczy rzeczywistości nowych technologii i usług społeczeństwa informacyjnego, które zapewniają społeczeństwu wiele korzyści zawodowych i społecznych, ale które niosą ze sobą również falę różnych zagrożeń. Mimo to, jako społeczeństwo informacyjne chętnie korzystamy z tych rozwiązań w niewyobrażalnym zakresie. Należy zatem zadać pytanie, czy jako społeczeństwo aspirujące do miana społeczeństwa 5.0 jesteśmy dostatecznie lub w ogóle wyedukowani w zakresie tych technologii, zarówno pod kątem płynących z nich korzyści, jak i potencjalnych niebezpieczeństw, np. cyberzagrożeń czy wpływu na nas i nasze otoczenie? Artykuł przedstawia analizę obecnych form edukacji w Polsce w 2021 r. w szkołach podstawowych i ponadpodstawowych i stawia pytanie, czy wraz z rozwojem rzeczywistości wypełnionej nowymi technologiami i w dobie przeładowania informacyjnego kładziemy wystarczający nacisk na edukację we wskazanym wymiarze?

Keywords: education, information society, new technologies, cyber threats, robotisation, computerisation, cyberspace, artificial intelligence

Słowa kluczowe: edukacja, społeczeństwo informacyjne, nowe technologie, cyberzagrożenia, robotyzacja, komputeryzacja, cyberprzestrzeń, sztuczna inteligencja

Introduction

In the middle of the 20th century, the Polish writer of the hard science fiction geno.e, philosopher and futurologist, and eminent figure, Stanisław Lem, in his publications conveyed messages concerning the digital reality that has already materialised today. The guru of fantasy, and visionary thinker, made bold and accurate assumptions about the development of society with the advent of information technology development. A no less visionary approach was put forward by Karel Capek in a 1920 publication titled "*Rossum's Universal Robots,*" in which he used and popularised the word ROBOT for the first time.

Both authors presented, at the time, seemingly fantastic and surreal visions about new technologies and their application. They wrote about automation, robotisation, computerisation, the internet, cyberspace and virtual reality, creating original ideas of fantasy literature. In doing so, they warned of phenomena that could be dangerous to humans and even to humanity as a whole.

The hypotheses set out in the literature of the last century are currently materialising in many aspects of life, to the extent that many of us would not be able to function if these tools were not present. While technologically literate societies are happy to enjoy the benefits of technology in everyday life, which provide many advantages on both professional and social grounds, their awareness, responsibility and education in terms of potential dangers seems to be insufficient, at least in terms of formal education.[1]

Outline of the problem of using ICT services – results of a statistical survey

Publicly available statistics from 2021 show the current scale of our dependence on the Internet, which is on an upward trend. The Digital 2021 report series,[2] published in collaboration between *We Are Social* and *Hootsuit,* shows that over the past year web-based services such as e-commerce and social media etc. have become an indispensable part of people's lives. Of a population of 7.83 billion people, 5.22 billion use a mobile phone today, representing 66.6 per cent of the world's total population. 4.66 billion people worldwide used the Internet in January 2021, 316 million more compared to the same period in the previous year. Social media currently has 4.20 billion users worldwide. This number has increased by 490 million in the last 12 months, showing year-on-year growth of more than 13 per cent.[3]

The same report shows that the average user now spends 2 hours and 25 minutes on social media each day. In total, social media users worldwide spent *3.7 trillion*

[1] *On the Integrated Qualification System* Act of 22 December 2015, Dz. U. (Journal of Laws) 2020, item 226, as amended.

[2] https://datareportal.com/reports/digital-2021-global-overview-report, [accessed: 08.12.2021].

[3] *Ibidem*.

hours on social media in 2021, which equates to more than 420 million years of connected human existence. These comparisons may evoke different emotions, although it is the statistical number of hours per day spent "online" by a user that is astonishing.

In total, the average internet user now spends almost seven hours a day using the internet across all devices, which equates to more than 48 hours a week online – that's a full two days out of the week. Assuming the average person sleeps between seven and eight hours a day, this means that we now spend around 42 per cent of our lives awake and spend almost as much time online as we do sleeping.

According to the Business Insider website, during an average eight-hour working day, an employee works productively for only three hours.[4] They vary the rest of their working time with pleasures such as mentally moving to the online world and browsing social networks etc.

One of the reasons why we use the internet so much is the widely available information society services,[5] which enable us to work remotely, to entertain ourselves, to carry out many activities and needs (which are e.g. shopping, obtaining information, communication, etc.). Services are also defined in Article 4(25) of RODO,[6] which refers us to Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council, and means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of the recipient of the service. In Poland, an information society service is defined as a service provided electronically.[7] In other words, it is a service provided without the simultaneous (physical) presence of the parties at the time the service is provided (service provided at a distance).

Provision of a service by electronic means means that the service is sent and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data and is entirely transmitted, routed and received by wire, radio, optical or other electromagnetic means. An information society service must furthermore be provided at the individual request of the recipient of the service, e.g. use of a social networking site, sending of e-mails or video on demand.

An information society service should (but not necessarily) be provided for remuneration, but this is not just about situations where the service provider receives remuneration expressed in money, but remuneration understood as economic value. This is therefore of all kinds:

- online newspapers;

[4] https://businessinsider.com.pl/twoje-pieniadze/praca/psychologia-pracy-efektywna-praca-jak-dlugo/xc545sz, [accessed 14.12.2021].

[5] The concept of "information society" is formulated, [in:] Krzysztofek, K*., Understanding the development from traditional to information societies*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2005, p. 169; Goban-Klas, T., *Media and mass communication. Teoria i analizy prasy, radia, telewizji i Internetu*, Wydawnictwo Naukowe PWN, Warszawa–Kraków 1999, p. 286.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons in relation to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC.

[7] *On provision of electronic services* Act of 18 July 2002, Dz. U. (Journal of Laws) 2020, item 344, as amended.

- email;
- online TV;
- social networks;
- communicators, auction portals;
- dating apps;
- e-libraries;
- medical e-visits;
- restaurants providing a meal delivery service;
- car rental companies;
- hotel booking portals;
- banking;
- discussion portals;
- advertising portals
- online shops;
- e-training;
- e-advice and many others (omitted here).

It would seem that in Poland we use the Internet mostly for private purposes and less frequently for work. Nothing could be further from the truth. Due to technological possibilities and "public health" conditions in Poland, many employers have decided to enable remote working.[8] According to the Central Statistical Office, in 2020, 14.2% of all working people in Poland will work remotely, using the Internet, which is a considerable number of 2,317,700 people.

Taking the above data into account, it can be concluded that, apart from sleep and active web surfing, the real world is only a sideline for us, which we have to use for everyday hygiene, a meal, walking the dog or shopping. The amount of time we devote to surfing the web every day, both privately and professionally, means that we, as an information society, are confronted with considerable challenges and threats in various forms.

Each of us, because of the influence of the development of technology, the internet of things[9] and artificial intelligence, is becoming more and more dependent and less cautious in our daily activities, after all, it is "the good itself," and any risks concern other users, not us. Thus, we become completely defenceless in the face of the impact of the internet. We are affected, for example, by social media algorithms and automated scripts for commercial, social or political purposes and factors that shape our behaviour, perception and absorption of information, knowledge, intellectual development, and the online identity we create online, very often without realising how wrong we are about its anonymity.

In the digital world, we can never be fully anonymous or safe. Each of our online activities leaves a kind of digital footprint that we leave behind us by visiting

[8] *Labor Code* Act of 26 Juni 1974, Dz. U. (Journal of Laws) 2020, item 1320, 2021, 1162, as amended, art. 67.

[9] Ashton, K., *That "Internet of Things*", 2009.

various websites, filling in forms, sending e-mails, adding various attachments, videos, photos, comments, etc., thus sharing our emotions, views, preferences, problems, location, finances, needs, family situation, health data, data about our address, marital status and information about our absence from home. It is clear that the information we leave about ourselves on the web can become subject to, for example, hacking attacks or targeted algorithms.

Current forms of training

It seems natural that as a society aspiring to become society 5.0[10] with the development of technology we should acquire knowledge, shape and develop our awareness, responsibility, skills, e.g. information and cognitive skills, which are the foundations for the functioning of the information society and the knowledge society.[11] There is a mutual correlation between these two types of societies, because having an amount of data implies the need to be able to manage it, transform it, build logical relationships from it, to have knowledge, understood as the totality of human skills or a given mind, but also a body of knowledge in a certain field and consisting of information systematised and placed in context, processed through the prism of our experience, i.e. it is an appropriate analysis and synthesis of information.

It should be noted that having information is not the same as having knowledge. Knowledge implies, among other things, that, with knowledge, we can judge which information is true or not. So, given the direction we are going in, and that information technology allows us to absorb information more efficiently, can we conclude that we are becoming better at using the information we have? Is it possible to uphold the assumption of social philosophers that free access to information on any subject is a sufficient condition for forming opinions and making judgements, and consequently for making informed decisions and being a responsible Internet user?

According to some researchers, the fact that information has such important functions in modern society also has negative consequences. No society has suffered from such an overabundance of information and T. H. Eriksen, for example, argues that the basic skill to be developed in today's world is to be on guard against 99.99% of the information reaching us and to focus on the reliable use of the remaining 0.01%.[12]

It is worth remembering that it is people who decide how to dispose of information and in this their role is irreplaceable. It is not in the use of technology that the main source of danger lies, the problem is that people may stop wanting to think, e.g. due to so-called "information overload."[13] The lack, or rather the low level of information culture and education, and the implementation of concepts of social development that are

[10] Society 5.0 – a human-centred society in which economic progress containing solutions to social issues is balanced by a system offering high integration of digital and real space, https://sektor3-0.pl/blog/japonski-czlowiek-nowej-ery-czyli-spoleczenstwo-5-0/, [accessed: 03.01.2022].

[11] Toffler, A., Toffler, H., *Budowa nowej cywilizacji*, Wydawnictwo Zysk i S-ka, Poznań 1996.

[12] Eriksen, T.T., *Tyranny of the Moment*, Państwowy Instytut Wydawniczy, Warsaw 2003, p. 33.

[13] Toffler, A., *Future shock*, Wydawnictwo Zysk i S-ka, Poznań 1998, p. 41 .

not always accurate, means that society in the age of the Internet, instead of becoming more and more reflective, is becoming more and more algorithmic, and therefore more and more "like" the computer to a degree beyond its real needs. The world moving towards total openness and the public's desire to consciously share personal information with the world is also a significant problem, and thus the value of privacy is being eroded. Sometimes we ourselves do not even realise that we are accepting widespread surveillance**.**

We are surrounded by information, our everyday life is based on its production, dissemination and use. We want to be up to date, so we do it quite uno.eflectively. As defined by *Dr Hanna Batorowska, Professor at UP, "Information literacy is the responsibility of the information society."* These duties should not only concern the essence of information, but mainly the moral dilemmas related to its use, dissemination, sharing, selection, evaluation and management.

In view of the above, it must be recognised that the scale of the penetration of the Internet into our daily lives and the ocean of information available means that the elements that should keep up with it, or even surpass it, are the education of society, multi-level development, humanism and the interdisciplinarity of the fields of life. It is therefore important to pay attention to current forms of education and to create awareness in this area.

The declaration,[14] made on 12 October 2020 by the Association of Data Protection Officers within the framework of a commemorative letter in view of the 4th anniversary of the Association, that *Information* + *Knowledge* + *Wisdom* will balance the imbalance between privacy and today's high technology, is the essence expressing the needed educational trend.

It is not without significance that a new value for the respect of privacy is expressed in the activities of the SIODO, the "Data Protection Culture." Developed in a multi-level manner, it will arouse the need to respect one's own privacy, as well as allow for the skilful acquisition, evaluation and application of information, and thus contribute to raising awareness of the constitutional right to informational autonomy and the protection of one's personal rights.

How, then, is the aforementioned education implemented in Poland in 2021? Well, the basis for consideration is the Ordinance on the core curriculum of formal education in Poland[15] and the Ordinance of the Minister of National Education of 30 January 2018 on the core curriculum of general education for general secondary school, technical school and industry secondary school.

In terms of the analysis of the curriculum for grades I–VIII, at least the content related to the essence and understanding of privacy as a fundamental human right, its value and potential sources of its threat are overlooked.

[14] https://siodo.pl/2020/10/, [accessed: 28.12.2021].

[15] Regulation of the Minister of National Education of 14 February 2017, on the basis of the program of preschool education and the program basis of general education for elementary school, including for students with intellectual disabilities of a moderate or severe, general education for secondary school, general education general education for a special school for special preparation for work and general education for a post-secondary school post-secondary school Dz. U. (Journal of Laws) 2017, item 356.

Also overlooked in the analysed core curriculum is content related to building information management skills, which, in an age of information overload, as Alvin Toffler wrote about in "Future Shock" as early as 1920, is fundamental to navigating through the thicket of information and assessing its value and sources.

The only subject that thematically comes close to the area in question is Safety Education. This subject has been taught since 1 September 2009 as one hour per week per school year in the then lower secondary school. Since 1 September 2012, it has been taught for the same amount of time in upper secondary (post-primary) schools. Safety education has completely replaced the previously known defence przysposobieczenie obronne. With the introduction of the new core curriculum from 1 September 2017, Safety education was introduced in primary schools. As of 2018, it is taught in class VIII as one lesson per week.

This subject focuses primarily on general aspects of state security and civil defence. In the form of truncated theory, it prepares students for emergency situations such as disasters, mass accidents or terrorism. It also develops first aid skills and attitudes that promote health in a broad sense.

Although Education for Safety does not teach about the problems indicated in the article, some educational materials at individual schools include lesson topics that address cyberbullying and the use of resources available on the Internet. These may amount to several lesson hours over the entire eight years of primary education, but their implementation depends on the teacher's initiative. This seems to be an insufficient amount of hours devoted to education when juxtaposed with the results of a consumer survey of children and parents carried out by the Office of Electronic Communications,[16] which shows that in 2020 97% of school-age children were using the Internet.

It cannot reasonably be considered that the fault lies with the school principals, as the lack of introduction of content into the programmes and adequate preparation of the teaching staff will not happen "overnight." It is an action that should be planned and systematically implemented over years with the addition of content.

According to the above-mentioned report, almost 60% of the teachers participating in the survey consider that there is too much inappropriate content on the Internet, including manipulation, violence, swearing, pornography and material that may have an impact on the demoralisation of the youngest generation, who, in retrospect, will be responsible for the further education of younger generations. So why is there so little focus on education about perceived problems?

Attention to the aspects in question is given in the Regulation of the Minister of National Education of 30 January 2018 on the core curriculum of general education for general secondary, technical and upper secondary schools.

The above programme indicates that one of the most important skills acquired by a student in the course of general education at upper secondary and technical schools is the ability to efficiently use modern information and communication technologies, including respect for copyright and safe navigation in cyberspace. Well, a specific skill is acquired by a student in 3 subjects.

[16] https://www.uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html, [accessed: 05.01.2022].

One of these is Education for Safety, already discussed, which in its subject area includes, among other things, the task for the instructor to explain the meaning of cyberbullying and knows the procedures to follow in the event of its occurrence, and identifies inappropriate behaviour regarding cyberbullying and knows what the appropriate response to it should be.

Another subject, which thematically touches upon the problems indicated in the article, is Ethics, which deals with the identification and analysis of selected moral problems associated with scientific and technological progress (e.g. the problem of privacy protection, copyright protection, cyberbullying, the development of artificial intelligence, transhumanism).

The third element of the curriculum in question is also Information Technology, which covers with its thematic scope a truly important issue, i.e. "*respecting the law and security rules. Respecting information privacy and data protection, intellectual property rights, etiquette in communication and norms of social coexistence, assessing the risks associated with technology and taking them into account for the safety of oneself and others*." It is puzzling, however, that the legal aspect is taught as part of a subject whose most important aim is to develop computational thinking skills, focused on creative problem solving in various fields with the conscious and safe use of methods and tools derived from computer science. In its basic and extended scope, the subject focuses, among other things, on technical and IT aspects of information security, and this is not conducive to bringing users closer to information awareness and developing the necessary skills.

Another interesting element of reference is the framework curriculum[17] for a four-year general secondary school and the minimum number of hours of compulsory education classes and tutor classes indicated therein, which for the subjects indicated above is respectively:

1) Safety Education – 1 hour per week, implemented only during the education period of Class I
2) Ethics – at least 1 hour per week – although the final decision on the number of hours of ethics is taken by the principal
3) Computer science – 1 hour per week implemented during the education period of grades I–III

I agree with the assumption included in the core curriculum,[18] i.e. "*An important task of school is to prepare students for life in an information society. Teachers of all subjects should create conditions for students to acquire the skills of searching, organising and using information from various sources and documenting their work, taking into account the correct composition of the text and the principles of its organisation, with the use of information and communication technologies*." However, the success of this task is in doubt:

[17] Regulation of the Minister of National Education of 3 April 2019, on framework educational plans for public schools, Dz. U. (Journal of Laws) 2019, item 639.

[18] Regulation of the Minister of National Education of 14 February 2017, op. cit.

a) Minimalist approach to issues in the core curriculum;
b) too few hours dedicated to their implementation;
c) lack of system orientation.

Within the framework of the subject matter under discussion, the shortcomings of the systems approach are discernible in both core curricula presented above. By this I mean a curriculum based on a structured and logically structured range of topics, forming a whole. Such an approach, together with continuing education, would influence the interdisciplinary development of the pupil, providing him or her with the necessary knowledge appropriate to the stage of life in question. This would allow for a balanced flowering of wisdom in the broadest sense. The systematic acquisition of knowledge, the development of awareness, intelligence, maturity and the gaining of experience at further stages of education, combined with commercial education would allow for a number of individual benefits.

It would also provide an opportunity in building specialist human resources, future managers or managers of organisational security and state security in this area. Commercial education could play a significant role here, contributing to the specialisation of these individuals. However, there are few such pro-social activities, to say the least, that I see in the field of continuing education. With certain "periodic booms", such as the entry into force of the General Data Protection Regulation,[19] commercial education offers appear to be aimed at the most profitable customer segment, which in this case can "create" an expert in information security management in a few days.

The dilemma, however, is that they lack in-depth knowledge of, for example, information security systems, the methodology used in audit activities, or even the subject of information society threats in the security system of organisational units. Instead, content concerning the creation of registers, records, the so-called information clauses (which, in fact, should not be called that), the "implementation of RODO" in the organisation, with the help of sample documents, prevails.

Admittedly, some are saturated with knowledge that is highly cumulative, both practical and theoretical, but which cannot be taught effectively in a day or two, or often even a year, of postgraduate study. However, it would not be an exaggeration to say that no one would risk hiring a head of human resources or a chief accountant after this level of training, even if he or she had regulations and model letters at their disposal; what is needed here is well-established knowledge and skills.

The remodelling of current and the creation of new forms of education requires, above all, qualitative changes in the interpretation and conceptualisation of specialised knowledge in confrontation with increasing technological development and the scale of its penetration into everyday life and the resulting new challenges for society. Curricula and all forms of education should be built on a systems approach, which will force issues to be treated as open systems, interlinked to form a coherent whole.

[19] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, op. cit.

Risks

It should realised that it is not the information itself that is at risk, but rather its unskilful and irresponsible use. There are many dangers, for example, psychological dangers (inner compulsion to be online, escape from the real world into an artificial virtual world, access to pathological cultural groups, alienation), technical dangers (loss of confidentiality and integrity of data), medical dangers (dangers to human health caused, for example, by work at a computer or the harmfulness of radiation from a computer monitor) and legal dangers (dangers to human health caused, for example, by work at a computer or the harmfulness of radiation from a computer monitor). The risks are also linked to the development of modernity (excessive information, disparity of information, problematic value of information, information noise, information stress and ethical dilemmas).

The scarcity or non-existence of the indicated educational elements in educational programmes and the lack of a systemic approach to teaching makes an unaware society fall prey to the threats indicated above and contributes to the vulnerability of the individual. Recognising the scale of the potential challenges that lie ahead, and given the range of forms of education discussed above, it is also worth drawing attention to cyber threats such as:

- Cyberbullying – bullying by sending and posting harmful content or images via online communication tools. Cyberbullying occurs when a child or adolescent is bullied, intimidated, harassed, humiliated, shamed or otherwise harmed by another child or adolescent using the internet, interactive or digital technologies, or mobile phones.
- Deepfake – image editing, which involves combining images of the human face via artificial intelligence. The resulting images offer the possibility of manipulating, blackmailing or compromising the person whose image has been used.
- Fake news – the large-scale dissemination of false information.
- Flaming – the so-called "insult war", which involves sending hostile and vulgar messages to one or more members of a community.
- FOMO – an acronym for fear of missing out, meaning a paranoid fear of what is passing us by while we are offline. It involves constantly keeping track of what is happening online.
- Child Grooming – actions taken to befriend and emotionally bond with a child in order to reduce the child's resistance to later sexual abuse.
- Heyt – involving destructive criticism using online posts in a public forum.
- Patostream – consisting of "online" webcasts during which behaviour widely regarded as social deviance is presented, for which viewers pay so-called donations.
- Pharming – a more dangerous form of phishing for the user and more difficult to detect. Characteristic of pharming is that even after entering a valid website address, the victim will be redirected to a fake (although it may look the same)

website. The aim is to intercept passwords, credit card numbers and other sensitive data entered by the user on trusted sites.

- Phishing – a method of deceptively obtaining passwords to a user's online bank accounts via e.g. emails, including phishing for sensitive personal information (e.g. passwords or bank account details) by impersonating a trustworthy person or institution.
- Ramsonware – malware that causes data on devices to be encrypted until a ransom is paid by the victim. Infection most commonly occurs via emails, pop-ups and social media.
- Scam – a scam to induce trust in someone and then use that trust to defraud them of money or other assets, popular on dating sites, charity ads, advertisements for a win, super offer or quick way to make money, etc.
- Sexting – sending photos, videos or messages of a sexual nature via mobile phones.
- Skimming – the illegal copying of the contents of a bank card's magnetic strip without the cardholder's knowledge in order to perform unauthorised transactions.
- Stalking – persistent and repeated harassment, solicitation of a person using new technologies.
- Trolling – unfriendly behaviour towards other internet users that is intended to disrupt an ongoing discussion.
- Vishing – a method of fraud, with its basis in phishing and social engineering methods, whereby fraudsters use internet telephony to impersonate financial institutions.

The above dangers are just a few examples. Every victim of these dangers will find himself or herself in an extremely difficult situation. Will he or she be able to cope? Will a teenager who wants to conceal a situation (e.g. embarrassing photos) from his or her parents find help from those close to him or her, when his or her parents are not even aware of it? Ridiculous content shared within a community (e.g. a class or school) can lead to anger, sadness, fear, lowered self-esteem or even a suicide attempt within seconds. Every day 160,000 children in the United States of America do not go to school because of cyberbullying (online bullying). Unfortunately, we are also dealing with this phenomenon more and more often in Poland.[20]

When we reply to an e-mail in a hurry, will we each time spot a form of phishing and recognise an attempt to defraud us by impersonating an institution in order to obtain personal data or other information from us?

Will we uno.eflectively dispose of our data for the range of proof of identity requirements placed on us?

Without reflection, do we share our material possessions on social media, e.g. a beautiful house, also sharing information about a holiday stay?

[20] https://www.gazetaprawna.pl/wiadomosci/artykuly/1097364,michal-wroczynski-w-rozmowie-z-magdalena-rigamonti-dzis-sztuczna-inteligencja-nie-wie-nawet-ze-w-grze-pokonala-czlowieka.html, [accessed: 06.01.2022].

Will we securely dispose of company information as part of our professional activities?

In view of the above, insufficiently or inadequately developed ethical values and information competences of Internet users will lead, among other things, to addictions, a range of psychological and social effects, cyber-bullying, to a loss or withdrawal of one's own privacy and even to a decrease in respect for one's own privacy in relation to others, and, when faced with too much information, may lead to information overload, which will distort the information evaluation system.[21]

It is impossible not to draw attention to threats involving information security of private and state organisations and state security. The available forms of education and the applicable legal regulations treat very openly, for example, the obligations of[22] Administrators to appoint functional people responsible for supervising, monitoring and advising on the management of the information security system, i.e. Data Protection Officers.

They are appointed pursuant to Article 37 of the RODO, on the basis of their professional qualifications and, in particular, their expertise in data protection law and practice and their ability to fulfil the tasks incumbent upon them.[23]

This seems to be an insufficient regulation, which is devoid of standards supporting the decision to appoint a Data Protection Officer after prior verification and confirmation of relevant qualifications (e.g. obtained through formal education[24]) and experience within the defined specificity of the organisation. The lack of such regulation in practice translates into the appointment of people to the position of Data Protection Officer who often have completed short preparatory courses lasting a few hours in preparation for this function. In most cases, the only criterion that influences the selection of a candidate, especially in the public sector, is the lowest price, which obviously translates into the quality of the service provided. Thus, finances are prio ritised over real benefits and acting in accordance with the law, or simply over the responsible disposal of other people's personal data.

This aspect requires, above all, an understanding of the correlation between financial issues and the losses caused by negligence in this area. It is also important to change the attitude of entity managers and company boards to the issue of information protection and the application of legislation. Their lack of awareness in this regard very often results in them equating and making the Data Protection Officer responsible for fully relieving the management of their tasks and dealing with the unprepared area comprehensively, preferably without interfering in the day-to-day operation of the entity.

Ultimately, the road we are heading down, which is devoid of elementary assumptions for education and the formation of an information culture, instead of creating attitudes of an informed consumer of information, active, selective, critical and ready

[21] Babik, W., *W natłoku informacji i związanym z tym przeciążeniu informacyjnym*, Kraków 2010.

[22] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, op. cit., art. 4 (7).

[23] *Ibidem*, art. 37.

[24] *On the Integrated Qualification System* Act of 22 December 2015, op. cit.

for the daily technological development of the surrounding world, will lead to information illiteracy and the "dumbing down" of society.

Videos and pictures, memes and emoticons are ubiquitous. The image has become a source of information and a vehicle for emotions, a medium that shapes our perception of the world. We read less and less, and if we do, we prefer to listen to an audiobook instead of a traditional book. In addition, however, we prefer to relax with a phone in our hand, scrolling for hours on a smartphone or tablet screen. A society that does not see the real world, only the digital.

Any form of public transport is a case in point; on buses most passengers use their smartphones or tablets. The same happens among pedestrians and, horror of horrors, among car drivers in traffic jams. They derive satisfaction and fulfilment from winning the games offered by the online world, to which young people devote a significant proportion of their time.

Conclusions

Noticing the deepening knowledge deficit in relation to the increasing scale of the use of new technologies, social deviations and relativism in the field of information security management, I believe that the current "trends" and attitudes to the essence of the discussed area, if deprived of some kind of sobriety, in the long run will lead to many pathologies, psychological problems and destruction of social relations. It will also lead to a lot of negligence, backlogs and absurd solutions in the field of information security management and problems in the application of legal regulations in organisations obliged to do so.

How can this be prevented? We absolutely need an appropriate supplement to the core curriculum and a thorough remodelling of the educational assumptions. These should include an outline of the protection of society's privacy and its potential dangers, criminal liability for the use of high-tech devices, anonymity on the web, the impact of social media on disruptions in social interaction (electronic aggression, pathostreaming, manipulation, hejt, etc.) and many others.

The education of society in this regard should be based on lifelong learning. According to this concept, the initial years of primary education should be regarded as one of the first links in a demanding educational process that will prepare the individual for further educational activity.

A systems approach could dramatically change this state of affairs and could be implemented on the basis of the following exemplary pillars, which represent the direction of the core issues:

Pillar I – Right to privacy

Pillar II – Right to the protection of personal data

Pillar III – Cyber security

Pillar IV – Public information

To do this you need staff with both knowledge and experience. Admittedly, this knowledge can be gained in-house, based on private experience and indeed this is the case, but it is not sufficient. However, our goal, as an information-conscious society striving for constant evolution, should be to further educate the current workforce and to build the future workforce on the basis of an educational programme developed through a public discussion in which the relevant scientific communities and state organisations would be involved and, by extension, the creation of new institutionalised forms of education for children, young people and adults.

We are talking here about starting work on integrating the subject into formal education because it is not being addressed to a sufficient extent. This reveals a number of neglected issues, if only due to the fact that the information civilisation is a civilisation of rapid changes, and this implies the necessity to react efficiently to new conditions, for example work focusing on legal standards covering artificial intelligence, the Internet of Things and virtual reality. In a perspective of years, this would allow building an information society aware of both opportunities and threats and deliberately aspiring to be the 5.0 society.

Bibliography

Ashton, K., *That "Internet of Things*", 2009.

Babik, W., *O natłoku informacji i związanym z nim przeciążeniu informacyjnym*, [in:] *Człowiek-Media-Edukacja*, J. Morbitzer (ed.), Kraków 2010.

Eriksen, T.T., *Tyranny of the Moment*, Państwowy Instytut Wydawniczy, Warsaw 2003.

Goban-Klas, T., *Media and Mass Communication. Theories and analysis of the press, radio, television and the Internet*, Wydawnictwo Naukowe PWN, Warszawa–Kraków 1999.

Krzysztofek, K*., Understanding development from traditional societies to information societies*, University of Silesia Publishing House, Katowice 2005.

Toffler, A., Toffler H., *Budowa nowej cywilizacji*, Wydawnictwo Zysk i S-ka, Poznań 1996.

Toffler, A., *Future shock*, Wydawnictwo Zysk i Ska, Poznań 1998.

https://datareportal.com/reports/digital-2021-global-overview-report, [accessed: 08.12.2021].

https://businessinsider.com.pl/twoje-pieniadze/praca/psychologia-pracy-efektywna-praca-jak-dlugo/xc545sz, [accessed: 14.12.2021].

https://sektor3-0.pl/blog/japonski-czlowiek-nowej-ery-czyli-spoleczenstwo-5-0/, [accessed: 03.01.2022].

https://siodo.pl/2020/10/, [accessed: 28.12.2021].

https://www.uke.gov.pl/akt/badanie-konsumenckie-dzieci-i-rodzicow-oraz-nauczycieli-2020,372.html, [accessed: 05.01.2022].

https://www.gazetaprawna.pl/wiadomosci/artykuly/1097364,michal-wroczynski-w-rozmowie-z-magdalena-rigamonti-dzis-sztuczna-inteligencja-nie-wie-nawet-ze-w-grze-pokonala-czlowieka.html, [accessed: 06.01.2022].

Legal acts

On the Integrated Qualification System Act of 22 December 2015, Dz. U. (Journal of Laws) 2020, item 226, as amended.

On provision of electronic services Act of 18 July 2002, Dz. U. (Journal of Laws) 2020, item 344, as amended.

Labor Code Act of 26 Juni 1974, Dz. U. (Journal of Laws) 2020, item 1320, 2021, 1162, as amended.

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons in relation to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC.

Regulation of the Minister of National Education of 14 February 2017, on the basis of the program of preschool education and the program basis of general education for elementary school, including for students with intellectual disabilities of a moderate or severe, general education for secondary school, general education general education for a special school for special preparation for work and general education for a post-secondary school post-secondary school Dz. U. (Journal of Laws) 2017, item 356.

Regulation of the Minister of National Education of 3 April 2019, on framework educational plans for public schools, Dz. U. (Journal of Laws) 2019, item 639.