Education – Relationships – Play

Multifaceted Aspects of the Internet and Child and Youth Online Safety

KEY CONCEPTS SERIES

Edited by
Agnieszka Wrońska, Rafał Lew-Starowicz, Anna Rywczyńska

FRSE Publications

Education – Relationships – Play

Multifaceted Aspects of the Internet
and Child and Youth Online Safety

Education – Relationships – Play

Multifaceted Aspects of the Internet and Child and Youth Online Safety

Areas:

- The Internet – social and legal contexts
- The Internet – selected aspects of child and youth protection

Edited by
Agnieszka Wrońska
Rafał Lew-Starowicz
Anna Rywczyńska

FRSE Publications

Warsaw 2020

KEY CONCEPTS SERIES, VOL. 6

Education – Relationships – Play

Multifaceted Aspects of the Internet and Child and Youth Online Safety

Areas:
The Internet – social and legal contexts
The Internet – selected aspects of child and youth protection

Scientific Editors:	dr Agnieszka Wrońska, Rafał Lew-Starowicz, Anna Rywczyńska
Cooperation:	Agnieszka Rybińska
Reviewer:	prof. dr hab. Mirosław Grewiński
Chief editor:	Tomasz Mrożek
Translation into English:	Poliglota
Cover design:	Artur Ładno
Design:	Diana Makulska/Podpunkt
DTP:	RZECZYOBRAZKOWE
Print:	TOP DRUK Łomża
Publisher:	Foundation for the Development of the Education System National Agency of the Erasmus+ Programme Al. Jerozolimskie 142a, 02-305 Warsaw www.frse.org.pl | kontakt@frse.org.pl

ISBN: 978-83-66515-08-6

This publication has been developed with the financial support from the European Commission in the framework of the Erasmus+ programme. The information and views set out in this publication are those of the authors and the European Commission may not be held responsible for the use, which may be made of the information contained herein.

Special thanks you to the NASK for contribution to this publication.

Free copy

Citation: *Education – Relationships – Play. Multifaceted Aspects of the Internet and Child and Youth Online Safety* (ed.), Foundation for the Development of the Education System, Key Concepts Series, vol. 6, Warsaw 2020.

More FRSE publications: www.czytelnia.frse.org.pl

FRSE Publishing House periodicals and portals:

CZASOPISMO DLA NAUCZYCIELI [języki:obce w szkole] europa eurodesk Polska EUROPEJSKI PORTAL MŁODZIEŻOWY

Table of Contents

2 The Internet – selected aspects of child and youth protection

Home

Home

Introduction

Ensuring children and young people's safety when they use information and communication technologies and inspiring them to use digital tools in a creative and responsible manner are the main challenges carers and educators face today. As youngsters have their first online experiences at ever younger ages, parents and educators of very young children need to confront these issues, too. Young people cannot imagine their lives without access to the Internet, which they perceive as a fundamental right.

A growing number of schools, acting in cooperation with external stakeholders, take prevention measures to this end. These are accompanied by a noticeable increase in the number of initiatives reported each year as part of events like Safer Internet Day. However, new Internet challenges and the system of values promoted by bloggers and extremely popular portals, whose only goal is to achieve a maximum number of visits, are phenomena that lessen the influence of families and schools on how children perceive the world.

Cooperation of international teams, public awareness campaigns and the use of research findings aim at developing students' digital competences and skills, while respecting the rights and dignity of Internet users. The issue of cybersecurity is also extremely important for teachers and students involved in eTwinning and Erasmus+ projects run by the Foundation for the Development of the Education System (Fundacja Rozwoju Systemu Edukacji, FRSE). These undertakings promote the young generation's responsible behaviour on the Internet, indicating proven ways of online functioning and methods of dealing with threats.

This publication aims to help readers better understand the virtual world, which is steadily entering our daily lives, and discuss selected aspects of this dynamically changing space. It presents social research on the phenomenon of the World Wide Web.

Home

It is thanks to this research that we can attempt to analyse the current situation relating to children's and young people's use of new media. We can also look back to the past and try to anticipate trends, opportunities and threats that may become part of online activity in the near future. An excellent example of research that allows us to trace the path of ever--changing online reality is the international research network which aims to raise awareness of the opportunities, risks and safety of European children online. It uses a wide variety of methods to map the Internet experiences of young people and their parents and to engage in dialogue with national and European political stakeholders. This project funded by the European Commission has made it possible to follow developments in Internet use since 2006. On the Polish market, similar goals are pursued by the "Nastolatki 3.0" [Teenagers 3.0] research carried out cyclically since 2014.

This publication presents both risks and opportunities brought about by the Internet. Its contributors are major figures in educational circles in Poland and abroad. They have made a significant contribution to research into phenomena occurring online and created models and recommendations in the field of media education.

Due to the chosen perspective and the complexity of issues presented here, the publication is divided into two parts. The articles featured here present structured information on risks and on the role which media education should play in monitoring and preventing online threats, as well as detailed data on computer games and the importance of a sustainable approach to gaming. Readers can become acquainted with reflections on "digital natives" and "digital immigrants", which form a basis for inquiring whether today's young people really are indigenous inhabitants of the virtual world and whether they really differ significantly from previous generations.

The authors analyse the Internet's potential as an area of young people's socialisation, learning, privacy management and building digital citizenship. It is assumed that this publication will be of help when solving everyday dilemmas, such as how to protect children and youth from harmful content. The goal is to raise awareness among teachers and parents so that they can effectively protect children from the challenges of the global network and from undertaking risky behaviours.

Agnieszka Wrońska,
Rafał Lew-Starowicz,
Anna Rywczyńska
(editors)

Home

1

Home

The Internet – social and legal contexts

Home

The Internet, socialisation and youth – from the perspective of contemporary social paradigms

Marek Konopczyński, Filip Konopczyński

The article attempts to describe the dominant social science's discourses related to the phenomena of youth socialization into internet-mediated environment. The authors present major paradigms conceptualizing new forms of socialization and examine their validity and usefulness in analyzing processes induced by the ongoing technological revolution. In the second part the article examines the impact of new cultural practices on spheres associated with emotions, aggression and personal identity-creation strategies among the contemporary youth.

Keywords:
internet
youth
socialisation
pedagogics
education
students
social media

Home

Paradigms of social and pedagogical sciences in the face of socialisation on the Internet

The issue of the functioning of young people within the space of the Internet is as multifaceted and complex as the whole process of psychophysical and social human development, and for this reason alone we should beware of simplifications, generalisations and hasty conclusions. Due to the importance of the problem and the scale of interest, many researchers, striving to obtain answers to the questions asked, often formulate them based on partial research, not always supported by the highest methodological diligence. Not wanting to follow this path, the authors of this article attempt to present the latest state of expert discourse in the area related to socialising aspects of today's Internet, focussing on several effects typical for this process. The first part discusses the conclusions of research and analyses on the socialisation functions of the Internet in relation to popular (e.g. in the media) outputs on this topic. The second is a detailed presentation of three theoretical problems related to the socialising functions of the Internet in relation to empathy, aggression and self-presentation mechanisms.

Reflections presented in this article are theoretical and synthetic in nature, and their task is to highlight the changes in socialisation processes caused by the creation and popularisation of the Internet and computer technologies. Until recently, the aforementioned changes took place only in the natural environment or – in a population of more technologically advanced people – with the participation of media much less psychophysically involving children (i.e. print, radio, television). Compared to other media, the Internet is "more powerful", also in the sense that it is getting out of control: it is more difficult to monitor how long it is used for, and for what purpose. From the point of view of a parent or guardian, it is much easier, for example, to check how long someone watches TV than to limit their access to a smartphone or to computer equipment.

Pedagogical thinking, which is shaping the perception of our surrounding social world and the social and educational processes taking place within it (including functioning on the web), is based on specific paradigms. By this we mean a set of general assumptions explaining an area of reality, adopted by representatives of a given scientific discipline as a model of final thinking. The last century was dominated by several socio-educational paradigms, which had an immense impact on our perception of the complexity of the situation of young people in terms of upbringing and socialisation, and thus also on educational practice. The emergence of the Internet has set new challenges for theoreticians and practitioners in the realm of education. In order to be able to embark upon them, it is necessary to analyse the legitimacy of the use of previously dominant models – not to absolutely abandon them, for example in favour of increasingly popular network theories, such as the actor-network theory of Bruno Latour (2005), but to assess their usefulness in the face of the broad conditions of civilisation.

The humanist paradigm is derived from nominalism and voluntarism, i.e. scientific subjectivism, and focuses on the individual meaning of social life. It presents a critical stance towards culture as a set of facts imposed on an individual from above, from the outside, usually without an alternative. According to this trend of thinking, an individual has the right to set rules, to have a real impact on culture and to interpret social conflicts from the point of view of protecting their own interests.

Similar assumptions are adopted by the interpretive paradigm, which also assumes scientific subjectivism, rejecting (like the humanist paradigm) the deterministic order and dealing with the development of consciousness of individuals functioning within social structures. The interpretive paradigm consists is a subjective understanding of social experience, obtained by testing specific groups of individuals.

The structuralist paradigm, in turn, derives from realism and determinism, i.e. scientific objectivism, and assumes the existence of objectively and supra-individually experienced structures according to which social life functions. Each individual is assigned to a specific structure and subjected to forces determining their fate. Structuralism examines assumed social conflicts from the point of view of social organisations (structures).

Derived from realism and determinism, the functionalist paradigm captures the social world in a similar way – as an objective being with ready-made structures regulating the life of the individual. The world is here described as a cultural system which subordinates the personalities of individuals. In a sense, it is a paradigm of social homeostasis, recognising that the occurrence of social inequalities is the price of maintaining the balance of the whole system.

Home

On these foundations two tendencies of building pedagogical theories were created. The first is paedocentrism (child-centredness), the aim of which is the unrestricted development of the child (humanist paradigm). It prefers purposeful, radical actions strengthening the child's development and removing social blockades during this process (anti-pedagogy, pedagogy of postmodernism) as well as purposeful actions regulating and strengthening the registers of subjective meanings given to surrounding reality (interpretative paradigm – personalistic pedagogy, pedagogy of religion).

The second, and opposite, tendency is didascaliocentrism (teacher-centredness), which falls within the structuralist and functionalist paradigm, and consists in conscious and radical actions shaping the child's personality in conditions of structural conflict (Herbartian pedagogy, positivist pedagogy) as well as in accordance with the psychological and social standards prevailing in a given culture.

The result of the clash of the above-mentioned visions are two basic currents of thought about pedagogy – as a theory and as a social practice. The first is neo-positivist pedagogy, the second is pedagogy of culture. Neopositivist pedagogy refers to the achievements of Johann Friedrich Herbart's "educational teaching", based on psychological determinism (behaviourism) and sociological determinism (Auguste Comte), as well as the achievements of Émile Durkheim (defining the theoretical and practical conditions of the relationship between the individual and society). Pedagogy of culture, on the other hand, recognises and prefers the education and upbringing of the individual through their contacts with objective cultural goods. It is focussed on hermeneutics, i.e. on a deepened interpretation and understanding of symbols through the inclusion of various educational and upbringing influences (aesthetic, ethical, artistic education) as a pedagogical stimulation of the influence of cultural values on the formation of human personality. In a sense, it became a defence of pedagogy against strictly scientistic, naturalistic and materialistic orientations.

Contemporary concepts in Polish pedagogy (Śliwerski, 2012) are more and more reaching towards paedocentric visions based on humanist and interpretative paradigms. This fundamental difference in the theoretical approach to the problem, resulting in new methodological solutions, provokes lively polemics and discussions in scientific circles, but, above all, arouses anxiety and numerous doubts in the circles of practicing educators. Therefore, it is worth taking a closer look at this issue.

The object of any educational activity are young people, while its subject matter is their welfare. This notion should be understood without contextual and interpretative shades. The good of every human being is their development, which enables them to overcome adversity in such a fashion that each time they look to the future, they can perceive social prospects opening up to them. These references come together by means of socialisation and educational culture.

Values and norms are the basis of any socialisation culture, especially educational culture. They give people a sense of meaning and form a set of guidelines regarding their conduct. The quality of our existence depends on the level of their assimilation and our ability to use those guidelines properly. The socio-cultural conditions that accompany people from birth influence their behaviour without depriving them of individuality and spontaneity (Giddens, 2006). It is socialisation culture that co-creates the most important parameters of our identity, making it possible for us to achieve self-realisation in our social roles. Individual and social identity determine the essence of our understanding both ourselves and other people. We can understand ourselves better due to the parameters of personal identity, and we are understood by others thanks to the parameters of social identity. Socialisation and educational culture and, primarily, the creative solution to problematic situations resulting from it make it possible to individualise human fate and equip people with creative possibilities. Culture and creativity are key social determinants of human development and, at the same time, define the main parameters of individual and social identity. The content of these concepts shapes people's inner intellectual space and influences their life roles.

Theoretical considerations should be supplemented with new ideas related to the growing popularity of cybernetics-inspired approaches based on network theory (Latour, 2006; Castells, 1996). They do not refer directly to the issues of education, pedagogical aspects of socialisation or changes in social norms, but they provide invaluable references to the manner of distributing information, and thus of cultural models of behaviour. Furthermore, what is particularly important, they convincingly explain problems today faced by social sciences and humanities. The use of analyses based on the study of communication networks in many cases makes it possible to capture, for example, the scale of social change or the real extent of a phenomenon, and even to carry out an analysis of users' sentiments. It also draws attention to the importance of communication infrastructure in which – in line with Marshall McLuhan's prophetic intuition – the relay is (also) the message, the role of non-human communication actors and how people interact with them is likewise important, all of which constitutes a creative contribution to the development of social sciences.

Due to the changes in the way knowledge is reproduced, traditional scientific, educational and media institutions are finding it increasingly difficult to keep up with the scale of civilisation changes occurring in connection with the low-cost, rapid exchange of information. Changes often take place under the surface of official public and private factors, which forces existing institutions to face a difficult dilemma, namely should they defend the *status quo* or should they adapt to the unpredictable directions of social change?

The search for theoretical references, which are the foundation of deliberations on the contemporary (new) socialising "power" of the Internet, defined within the framework of concepts broader than those habitually referred to, takes place in the course of fierce discussions and various interpretations concerning the socialisation and educational possibilities of "augmented reality" offered by today's Internet environment. A legitimate question arises: does the functioning of the mechanisms of Internet socialisation fall within the current, traditional pedagogical paradigmatic thinking? Perhaps we should redefine the existing pedagogical paradigms and work out new definitions.

According to World Bank data, in 2016 over 46% of the Earth's population already used the Internet[1]. Global leaders in this respect are Luxembourg, Kuwait, Denmark, Norway, Sweden, the Netherlands and Japan – in each of these countries the number of web users exceeds 90% of citizens (with a score of 75%, Poland is above average). Among young people, the percentage of web users is greater than average – according to the International Telecommunication

[1] World Bank data for 2018, bit.ly/2BGjdB8 [access: 18.01.2019].

Union by up to 30% compared to the entire population[2]. This means that the information revolution, heralded since the beginning of the 1990s, has already taken place in relation to young people, and adults are lagging behind.

Twenty-eight years after the World Wide Web was made available to the general public, the Internet environment is today a widespread ecosystem in which children around the world function. As quantitative research shows (for example, the “Global Kids Online LSE” project, led by Sonia Livingstone3, or the NASK (Polish Research and Academic Computer Network) report from the “Nastolatki 3.0” [“Teenagers 3.0”] survey[4]), the age of Internet initiation has lowered significantly in the last decade. Nowadays, even very young children use the Internet for several hours a day. From an anthropological point of view, we can speak of the real existence of a global prefigurative culture (Mead, 1978), in which the behaviour and attitudes of younger people set the tone for changes in civilisation. Of course, this does not happen entirely from the bottom up – technological solutions and activity platforms are provided by adults, especially those with adequate capital. However, within the digital market economy model, it is the needs and preferences of young consumers that determine the directions to be followed by both the private and – often with problems and delays – the public sector.

The paradox of this situation consists in the fact that we do not know what the consequences of the digital revolution involving younger generations will be. The “digital natives” generation (Prensky, 2001), which has explored the world in parallel streams through both traditional media and the Internet, only relatively recently entered adulthood. This is one of the reasons why the impact of information technology on the cultural process of growing up (psycho-emotional, social, professional and political) cannot be definitively assessed at this stage. This does not mean, however, that it is not possible to attempt to outline the direction of the changes taking place.

[2] *ICT Facts and Figures 2017* report, bit.ly/2zOy0Xi [access: 18.01.2019].

[3] *Global Kids Online Research Synthesis* report (2017).

[4] *Nastolatki 3.0 Wybrane wyniki ogólnopolskiego badania uczniów w szkołach* [*Teenagers 3.0 Selected results of the nationwide survey of students in lower and upper secondary schools*] report (2018).

There is no doubt that those dubbed the Millennial Generation (despite the lack of a universal consensus, this term generally refers to people born in the years 1980–1995) and Generation Y (people born after 1995) are characterised by a significantly different declared values, attitudes and expectations compared to representatives of earlier generations. This is evidenced by the *Deloitte Millennial Survey* (2018), which polled young citizens of several dozen countries around the world. An interesting statistic concerns social prestige, which is perceived by young people in a different way than in previous generations. Religious and political leaders enjoy much less respect among them than leaders of civil society, or even heads of private companies.

Looking at this phenomenon from the point of view of social sciences, these research results can be interpreted as a vote of no confidence towards traditional authorities and the institutions they lead. Regardless of socioeconomic factors – growing up, especially in Western countries, in times of global financial crisis and of progressing economic inequalities[5] – what clearly differentiates today's younger generations from their parents and grandparents is the media environment in which they are raised. The information revolution and the proliferation of computers mean that today the main mediators of young people's getting to know the world and adapting to it are no longer books, newspapers, radio or television – it is the Internet. That children learn about the world through an interactive, multimedia information environment from an early age is of great importance for the process of socialisation, and thus for creating social identity. This is a challenge that is faced not only by parents, but also, above all, by educational institutions.

In our reflections regarding selected identity-related consequences of socialisation mechanisms occurring in "augmented reality" (virtual reality), the impact of social media (not limited to portals) on the perception of oneself in the dimension of social relations is particularly interesting.

When discussing the socialising functions of the Internet, it should be stressed that they are linked to the communication and technological applications of the World Wide Web, which enables users to interact with

[5] *World Inequality Report 2018*, bit.ly/2N5WNzG [access: 18.01.2019]

one another. Historically, platforms enabling person-to-person contacts (e-mail, chats, discussion forums, applications and programmes for communication like MSN or Gadu-Gadu) were the first mass way in which the Internet was used – initially on a continental scale (North America, Europe), and thereafter globally. For the purposes of this article, issues related to the entire information infrastructure of the web will not be addressed. Such aspects, especially in the framework of the so-called Fourth Industrial Revolution (Schwab, 2016), include The Internet of Things, big data, smart devices, etc., which all constitute an increasing part of the global information transfer. Indirect impact of the web integration of technological solutions surrounding us (for example, household appliances interfacing with one another without the owner's knowledge, autonomous bots) is very interesting. However, it seems that due to the current scale of its occurrence it is too early to speak on this topic authoritatively and draw any general conclusions from the point of view of the socialisation process within the World Wide Web.

The UNICEF *Children in the digital world* (2017) report is an ambitious attempt to describe issues related to the impact of digital technologies on the development of children and youth. According to the authors, access to the Internet is presented as a tool enabling students' individual development and, consequently, that of their countries of origin. The starting point is the recognition of the need to adapt educational and legal systems to the challenges that arise in connection with the ongoing digital revolution. The report focuses on the opportunities created for young people by the Internet and on the dangers of digital inequality and exclusion. These must be prevented so that today's youth can in the future function productively within society and the global economy.

In the aforementioned report, the "dark side of the Internet" is described primarily in light of children-inappropriate content that can be found in this space. The list of threats includes pornographic material, harassment, paedophile and terrorist networks, gambling and digital surveillance that violates the right to privacy.

The issue of what is termed "problematic Internet use" (PIU) is described primarily by means of the fear expressed by parents and the media. The authors claim that there is a lack of empirical research confirming a significant occurrence of Internet addiction (addiction to electronic equipment). Instead, an interpretation is proposed according to which children and young people escape into the virtual world because of the problems they face in the real one.

The UNICEF expert literature review published in the same year (Kardefelt-Winther, 2017) indicates that, in the absence of convincing empirical evidence on the negative impact of digital technologies on the development of young people, one should not give in to fears and limit the role of the Internet in education, and thus in the socialisation of school-age children and youth. Furthermore, the authors of the publication refer to many observations proving the positive effects of bringing up children in the digital environment. Young people's greater multitasking abilities (being able to perform many activities at the same time), faster response to new information or deeper social networking are benefits which, in the authors' opinion, determine the positive assessment of the impact of digital technologies on children's development. It should be noted that the approach presented in the report caused some controversy – contrary to the authors' declarations, scientists have as yet not reached a consensus on the impact of the Internet, and especially of social media, on the psyche of children and young people (Sherman et al., 2011).

The development of the Internet and the broadening of the scope of its use have created the basis for ever-greater personalisation of its functionality by users. In effect, at the beginning of the 21st century a particular type of websites, portals and services began to appear around the world. Today they are known as social media. In the beginning, we had services such as LunarStorm and Myspace. However, it was a service set up in 2004, called Facebook, which gained significant recognition and within a few years became the most popular social networking site in the world (Edosomwan et al., 2011). According to official data, in 2018 2.3 billion people had created a Facebook account. Today, Mark Zuckerberg's company, Instagram and Twitter constitute the "big three" – a group of platforms giving users access to broadly understood communication, information and (recently) the ability to shop online. Due to the rapid increase in popularity among children, the phenomenon of social media quickly caught the attention of parents[6], the media (Pogue, 2008), officials (for example, the Polish

[6] *Parents, Children & Media. Kaiser Family Foundation Survey* (2007).

Supreme Audit Office[7]) and international organisations[8]. Interestingly, while there was real permissivism regarding the use of social media by children, the media often used epidemiological discourse in the spirit of "moral panic". The situation has changed in recent years in light of more and more psychological, sociological and pedagogical publications on this matter.

The authors of the study entitled *Social Media Use and Children's Well-being* (McDool et al., 2016) confirm that frequent use of social media by children leads to deterioration of their well-being, to more frequent occurrence of anxiety and anxiety disorders, and increases their susceptibility to depression. Other researchers (Wood et al., 2016) indicate that although the use of social media can reduce the feeling of loneliness in children and teenagers, regular and frequent use is associated with many negative psychological and socialisation-related effects. In seeking an explanation for these results, three main possible causes are identified:

- the nature of interaction on social media, associated with incessant comparing oneself with others, especially from the perspective of the idealisation of users' self-presentation behaviours;
- "finite resources" theories arguing that the increase in the number of hours spent by young people on social media results in their spending less time on activities which positively affect development and well-being;
- frequent violence on social media, such as cyberbullying, or offensive or illegal content. The more time spent on the Internet, the greater the chance of becoming the target of an attack, which leads to negative effects on the psyche. This approach focusses on the web as a space where aggressive behaviour and harmful content occur more frequently than in the real world.

It should be remembered that these interpretations are not inherently separate and constitute a multidimensional characterisation of the social media environment.

[7] Raport pokontrolny Najwyższej Izby Kontroli *Przeciwdziałanie e-uzależnieniu dzieci i młodzieży* (2016). [*Prevention of e-addiction of children and youth* audit report of the Supreme Chamber of Control].

[8] Report *The Protection of Children Online* (2012), OECD.

Empathy, aggression and self-presentation – emotions in online socialisation interactions

The change in the environment of social interactions brought about by the development of communication technologies within the global network also significantly affects the modification of boundary conditions, which until now were treated as natural elements of socialisation of children and youth. We can identify six key factors implying the socialisation quality of online contacts:

- Anonymity and pseudonymity in some interactions on the web. With the progress of machine learning technology and the development of Artificial Intelligence, the certainty of whether a user is interacting with a human or a machine is on the decline.
- Change of existing rules when it comes to building social hierarchy – currently this is based on popularity and coverage obtained through online channels. Likes, views or subscriptions create a new system of social prestige distribution which often translates not only into acceptance and popularity, but also into tangible financial benefits.
- Sense of closeness with the rest of the world – on social media we interact with strangers as if they were our friends. Information from anywhere in the world reaches us in real time.
- The Internet offers support groups in almost any area: by falling into such an "information bubble", it is easy to believe that there are plenty of "people like us", which can distort the picture of social reality in cases when a given phenomenon is actually rare.
- The frequency of the occurrence of disorders, for example addiction to online multiplayer games, proves that at least some web users show susceptibility to behaviours that are harmful from a developmental point of view.
- The ease of access to illegal and harmful content is higher than before, while there are fewer real possibilities of control.

These factors are ostensibly similar to phenomena occurring in the natural socialising environment. The similarities concern interaction content, while the differences are visible in its form. On the Internet, there is a real possibility of maintaining anonymity during interactions, which is impossible in the natural environment. Similarly, as regards other issues mentioned above – due to the technological possibilities of computers and the Internet – some aspects of natural human tendencies take on a new character in the digital realm. Therefore, we shall delineate a few selected issues concerning emotions in Internet relations and their visualisation effects, i.e. self-presentations. We would like to focus briefly on three issues: empathy, aggression and social self-presentation on the web. In principle, these problems do not feature in pedagogical literature, yet they are an important factor determining the form and essence of the functioning of young people in the augmented reality environment.

A point of interest to those who research the Internet as a socialising environment is its influence on the empathic attitudes of users. In the opinion of critics, children's intensified contacts via the medium of the Internet create conditions in which the youngest users adopt behavioural models that are defective from the social point of view, and the World Wide Web leads to loneliness or causes "virtual autism" (Heffler, Oestreicher, 2016).

The problem of empathy was first addressed within the psychoanalytic concept of personality (Wojciszke, 2004; Aronson, 2000; Reykowski, 1979), where this category was defined as a factor regulating an individual's behaviour towards the object of identification. Another way of understanding empathy is through reflections inspired by the words of Jean Piaget (2012) regarding the degree of maturity and organisation of cognitive structures, considered in terms of the ability to take on the role of another person. Currently, three types of empathy are distinguished – emotional, cognitive and compassionate. The main division criterion is the genesis of the types of empathy, not the quality or order of mental processes or differences in their mechanisms of operation. In the position represented by Janusz Reykowski (1979), emotional empathy is understood as an emotional reaction caused by perceiving someone else's feelings. It enables a person to: experience someone else's emotions as their one's own, to co-feel, i.e. transfer someone else's emotions onto oneself, and to feel compassion, i.e. an emotional reaction to another person's feelings which takes into account their state and is oriented towards them. Cognitive empathy is a process that involves putting oneself in someone else's position, and therefore to correctly perceive someone else's reactions. Cognitive empathy is sometimes identified with the ability to enter the cognitive situation and social role of another person with interpersonal accuracy.

In this approach, the increase in the popularity of the Internet among users whose personality and identity are under development is extremely interesting. Of course, a global web based on information technologies is not the first medium that acts as an intermediary in socialising processes, but because of the interactivity and rapid popularisation of this tool, and thus its supplementing and supplanting previous forms (writing, radio, television), it deserves the greatest attention in contemporary intellectual reflections.

The conclusions contained in the study entitled *Changes in dispositional empathy in American college students over time: a meta--analysis* (Kornath et al., 2010) made it possible to accept the hypothesis that the significant decline in empathic attitudes among American college students was indeed influenced by the development of the Internet. According to this interpretation, online relationships, unlike those formed in the physical world, are superficial and thus prevent the harmonious development of personality towards empathic behaviours.

However, in the following years this hypothesis met with criticism. Particularly noteworthy is the publication entitled *Virtual empathy: positive and negative impacts of going online upon empathy in young adults* (Carrier et al., 2015), whose authors, based on surveys conducted among young adults, prove that alarmist voices about the fall of empathy in digital times are exaggerated. According to them, Internet users do show empathic behaviour – both in the real world and online. However, in the case of contacts mediated via the Internet, "online" empathy in interpersonal relationships is much more diluted than its face-to-face version. Areas in which empathic attitudes are clearly weaker are specific forms of activity (such as computer games). In other words, the impact of modern communication technologies on attitudes is not radically different from the impact of earlier media: television, radio or magazines.

According to the hypothesis explaining the correlation of frequent use of social media with a decrease in "finite resources" (i.e. of time), problems only appear when online interactions replace interpersonal relationships that are not mediated by technology. This is of great importance from the point of view of education and upbringing sciences because, on the one hand, there is a danger of squandering socio-educational achievements implemented in the family and school environment and, on the other, there is a chance to correct some of the processes involved in upbringing in instances where it may not have been properly implemented in the real lives of young people.

Therefore, the following questions arise:

→ Is it possible to be empathic towards the entirety of the online community?

→ Who is truly emotionally close – people one often communicates with but does not know, or one's family and classmates?

→ When one develops relationships mediated through the web, does one behave in the same way as in face-to-face interactions and, if not, which of these versions is realistically probable?

In the face of such dilemmas, appropriate socialisation and educational methods and techniques should be developed which could replace or supplement the functioning of these processes in augmented reality. As can be seen from the above cursory analysis, the problem itself is an interesting one and should be met with further empirical exploration. Questions arising here, regarding the limits of empathy and its psycho-social conditions, still need to be answered.

A separate issue raised by researchers, educators and parents in relation to the increasing availability and popularity of digital technologies among children are problems connected to aggressive behaviour. From the outset, attention was drawn to the impact of violent computer games on gamers, focussing on content which views physical violence as entertainment. Some researchers have also tried to explain this phenomenon as the psycho-physical consequences of staying in front of the screen for a long time and focussing attention in a way which (due to evolutionary conditions) is not natural for humans (Ko et al., 2009). Modern research confirms these assumptions. This is evidenced, among others, by the results of laboratory experiments which confirm an increase in aggressive behaviours recorded immediately after playing video games (Kühn et al., 2018). Longitudinal meta-studies (Anderson et al., 2010) also confirm the link between frequently playing brutal games and antisocial and aggressive behaviours. According to the authors of these analyses, the impact is undeniable and doubts exist only in the area of the interpretation of this phenomenon. In 2015, the American Psychology Association published a research result-based appeal to parents, guardians, educators and institutions, calling for their greater involvement in combating the excessive brutalisation of games and preventing young people from spending excessive amounts of time playing such games[9].

Another, separate issue related to the problem of online aggression is users' easy access to dangerous content, and thus to models of aggressive behaviour. In recent years, along with the development of Artificial Intelligence algorithms, there appeared the increased possibility for web filters to hide dangerous content. Still, these mechanisms are not perfect. Children and young people constantly, usually accidentally, find themselves accessing websites with extremely violent or demoralising content. These are often illegal and harmful materials, for example recordings of executions, child pornography or clips showing animal abuse. The Dyżurnet.pl team, working as part of the NASK in 2017 alone received and analysed nearly 14,000[10] reports regarding such issues.

Recently, the problem of aggression has been widely discussed in connection with the phenomenon of "incels", i.e. a group of (mainly young) men who communicate with each other on the Internet and propagate ideas described as anti-women and anti-feminist (Zambrzycka-Kościelnicka, 2018). This term became famous in 2018, when Alek Minassian, a twenty-five-year-old resident of Toronto, Canada, committed a terrorist attack using a van, killing ten people[11]. While there are not many examples of real physical aggression on the part of people identifying with the "incel" movement, the situation illustrates the ease with which online communities can influence their members. Even in the case of a small number of people with radical views, thanks to networking modern information technologies can make them convinced of the universality of a given worldview or attitude. The Internet is also a tool that can affect the radicalisation of people with disturbed socialisation parameters, ones who are lonely or struggling with life, or facing emotional or psychological problems.

The presented effects of the influence of "web" socialisation, with particular emphasis on the mechanisms of shaping social and personal

[9] *Resolution on Violent Video Games* (2015), American Psychology Association.

[10] bit.ly/2FPIcEb [access: 18.01.2019].

[11] *Alek Minassian Toronto van attack suspect praised "incel" killer* (2018), BBC News, bbc.in/2sEphEC [access: 19.01.2019].

Home

parameters of an individual in the virtual world, are in a continuous dialogue with educational influences in terms of scope and quality. That is why, in the course of qualitative development, people's identities are conditioned by these influences, and their results to a large extent co-determine the functioning of the given person in the individual and social dimensions, both in the real world and online.

From the point of view of psychological and pedagogical theories, socialisation mechanisms measurably impact the formation of aggressive behaviours as well as the type of aggression. The boundary parameters of the social roles played, filled with identity content, determine the defined and socially accepted framework of human behaviour. Interpersonal aggression outside this framework is a significant social problem and the resocialisation process is largely oriented towards its elimination.

The most common and capacious definition of aggression is that it is a behaviour aimed at inflicting suffering on another person who is motivated to avoid this suffering (Barron, 1969). Biological concepts of human behaviour seek sources of aggression in dynamic forces inherent in human nature. These theories treat aggressive behaviour and the associated experience of anger as a symptom of the innate fight instinct. This view was shared, among others, by William McDougall (Aronson et al., 1997), who claimed that human behaviour is guided by many instincts, one of the most important being the fight instinct. It is a source of feelings of anger, which, in turn, are the impulse that causes the appearance of differences in aggressive behaviours.

Anger arising on the basis of this instinct is, according to William McDougall, a positive phenomenon from a biological point of view, as it stimulates the individual to acquire the resources necessary to meet their needs, inclines them to defend themselves against attacks and allows them to maintain their current state of possession. Anger can be triggered by many different stimuli associated with experienced failures, which thus become impulses that cause aggressive behaviour.

Sigmund Freud (1976) based the theory of aggression on psychoanalytical assumptions. He believed that human personality consists of three components: "id", "ego" and "superego". Conflicts arising between these components are the reason behind the frustration that stimulates aggression directed against people or objects. In the final phase of his scientific activity, Freud focussed mainly on the life instinct and the death instinct. He regarded the contradiction between them as a source of aggressive behaviour.

Representatives of the psychoanalytical approach to aggression (among them Alfred Adler) also assumed the existence of an innate, genetically-conditioned aggression instinct, which occurs independently and – apart from the sexual instinct – is the main driving force of human activity. Susceptibility to aggression potentially lies within the body, while frustration can only create conditions conducive to its liberation and manifestation to the outside world. A slightly different opinion regarding aggression is presented by those supporters of psychoanalysis who reject the existence of the innate aggression instinct and claim that in humans innate social instincts are dominant. According to this outlook, aggression is released when social instincts are inhibited or for some reason cannot be satisfied.

The physiological theory of aggression assigns special importance to both the hypothalamus and the cerebral cortex. These two parts of the brain are antagonistic. The stimulating effect of the processes occurring in the hypothalamus plays an important role in the formation of anger and the accompanying aggressive behaviour, while cortical inhibition processes can neutralise the state of arousal thus generated. The stimulation of the sympathetic system and corresponding internal organs is of secondary nature and is the result of the operation of nerve impulses originating in the peripheral nervous system, which do not arise spontaneously, but are a consequence of specific external stimuli on the body.

Behavioural studies of aggression concern behaviours that can be included in the stimulus–reaction framework. Aggressive reactions that are rewarded become reinforced, which results in the creation of appropriate habits concerning this type of behaviour, and if they are punished, they are inhibited and cease. Acquisition of new life experiences leads to a gradual differentiation of stimuli, in effect of which only strictly defined (not similar) kinds of rewards and punishments have a reinforcing or inhibiting influence on aggressive behaviour.

Behaviourists have also proven the relationship between aggressive behaviour and certain environmental conditions. It was found that the aggressive behaviour of group members and the anonymity of certain individuals acting in the group stimulate the occurrence of this type of behaviour. An individual shows aggression when they work together with a group that provides them with models of such behaviour, approves them, and ensures their anonymity. Social factors (for example, positive behaviour models and widespread disapproval of violence in the environment) can both stimulate aggression and counteract it. Behaviourists also confirmed the existence of innate factors that can affect the intensity and frequency of aggressive reactions.

The phenomenon of aggression seemingly has many common features in the real world and in virtual reality. However, the dominant behavioural perspective here is not always suitable for the Internet realm. While aggression and aggressiveness in the understanding of behavioural concepts often have an adaptive and defensive meaning in real everyday life, in augmented reality such meanings cannot be found. Instead, we can speak of instrumental, maladaptive aggression aimed at causing someone harm for harm's sake. However, as in the case of empathy, the problem of aggression in the process of socialisation on the Internet requires more thorough analysis and in-depth empirical research. Traditional definitions of the conditions and symptoms of this phenomenon occurring in the real world cannot be applied to the Internet environment without reflection, which is unfortunately often the case. A significant number of individuals writing about the problem of online aggression use traditional methods of understanding this phenomenon and try to adapt such concepts to augmented reality. This is not a fully justified procedure.

The influence of the Internet on the phenomena of aggression and empathy is inherently connected with the subject of human self-presentation behaviour. Social media, which can be described as virtual platforms based on behavioural reward for successful acts of self-presentation (Davidow, 2013) – the number of friends and likes, the range and reach of published content – exploit the human desire for social acceptance for business purposes, i.e. bringing profit to shareholders. From an economic point of view, it is in the interest of portal owners that users spend as much time as possible creating digital content for the purpose of self-presentation. It is activity, attention and manifestations of users' self-presentation behaviour – in the form of personal data – that the owners of websites, applications and portals sell or make available to advertisers, financial institutions, researchers or government institutions.

On a theoretical level, it should be noted that self-presentation on the Internet may be adequate or inadequate to the situation and may fully or poorly express a user's "self". The basic factor related to self-presentation are the goals set by the directions of emerging needs. On the other hand, the ways of reaching the assumed goals are conditioned by the properties of socialisation experiences. Achievement of goals is carried out thanks to the scripts and plans of individuals mediated by technical capabilities provided by the communication platform (for example, an application or service).

The functioning of scripts can be compared to the operation of a computer programme, which – once turned on – runs independently, attaining the assumed goals without the user's participation. The relation between an assumed goal and a script or plan connected with it is defined as an aspiration (Baumeister, 1986). Interpersonal contacts require the maintenance and presentation of a relatively consistent identity. Social interactions, including those involving young people, require them to behave in accordance with assumed social roles.

Young people create scripts that are closely related to their concept of identity, which is why they are not always capable or indeed able to play the roles required of them in a socially acceptable manner. By presenting themselves to others, both in the real world and on the Internet, people show parameters of their own identity, creating their public image. This image directly affects the quality of interpersonal relations and determines the user's place in social stratification. People who are poorly socialised, possessing limited language code, generally leave a bad impression on others. In some cases this impression increases social distance and the feeling of discomfort and interpersonal isolation. Such persons are generally not aware of the reasons for this state of affairs and justify their inadequate reactions to the situation (aggression, withdrawal) with external causes (the environment's attitude towards them). It is hard for them to understand that this situation is influenced by the manner in which they present themselves.

Situational and planned presentation of one's characteristics to others bears the hallmarks of self-presentation. In principle, self-presentation behaviour reveals true information about a person. Typically, in real-world social situations, examples of creating false public images are encountered relatively rarely. Undoubtedly, however, this phenomenon concerns people for whom the self-presentation effect is to play a specific role – among them professional fraudsters, actors or politicians. If the model of self-presentation is relatively permanent, cyclically repetitive and contextually identifiable, one can talk about the phenomenon of visualisation of identity parameters (Konopczyński, 2007).

Self-presentation is the purposeful action of an individual aimed at creating their desired image in a social environment (Szmajke, 1999). It is, therefore, a specific form of exerting social influence, and even – as some authors emphasise – a way of manipulating other people. A person's motivation to modify their image depends on the importance of the goals they want to achieve, and is driven by the belief that there is a correlation between the impression left on others and the actions taken, as well as a divergence between the presented image and its social perception (Leary, 2004).

Erving Goffman noted that a prerequisite for the existence of social interaction is that people build public dimensions of their identity. Thus, social identity parameters enable interpersonal contacts and form the framework of created life roles. This applies equally to people who are referred to as "normal" and to individuals with far-reaching disorders in social behaviours and attitudes. Only the internal and external factors and mechanisms triggering the structural framework of identity parameters of both categories of people are radically different. It can be hypothetically assumed that young people undertake self-presentation in the Internet space for various reasons, such as:

- protecting themselves (contacts at the level of subcultural environment) or increasing their self-esteem (contacts with people who matter to them and come from outside the subcultural environment);
- forming what are (from their point of view) valuable, interpersonal relationships that meet their psychological needs;
- exerting a manipulative influence on others, confirming their supposed social significance (this is due to a reduced level of self-esteem);
- creating and maintaining their own identity or certain features (Leary, Kowalski 1990; Goffman, 2000; Szmajke, 1999). For the purpose of this article, this category is particularly important. For many people falling into it, it will usually manifest as negative

> traits and socially unacceptable attributes, which is why their identity is a barrier limiting their internal and social development. At the same time, such people are unable to do anything about it, because the self-presentation of their identity occurs automatically, in accordance with learned socialisation models.

It can be assumed that the form and content of the roles played by young people are the result of social situations in which they participate and of the ways and forms of their self-presentation. Through this mechanism the identity parameters (sets of characteristic features of the individual and the social "I") prevent them from functioning properly and in an accepted way in roles and lead to a narrowing of the circle of their contacts and a decrease in the quality of interpersonal relations.

When analysing the phenomenon of creating identity parameters on the web, we should include this issue in the categories of self-presentation norms. They can be prescriptive, i.e. determine what kind of impression should be made on the social environment, or restrictive, limiting the scope and content of self-presentation. Socialisation processes play an important role in shaping both the ability to identify the social circumstances of the functioning of self-presentation norms and the attitude towards them. It can be assumed that people who adhere to self-presentation norms have undergone a proper socialisation process, so ultimately the image they create (and its perception by others) is in line with their intentions. However, if poorly socialised individuals have problems identifying this category of norms, their image is created contrary to their intentions.

Self-presentation norms, i.e. contextual models of how social impressions are made, depend on many factors. The most important of these include the culture dominating in a given type of environment, civilisation and social conditions, binding legal regulations, religious and worldview influences, and current political ideology. These are categories that belong to traditional spheres of pedagogical interest. The shaping and visualisation of identity parameters results to a large extent from these limitations and conditions. Therefore, this process is actualised by means of contextual actions, taking into account cultural and social conditions and consequences resulting from them.

Stigmatisation is one of the main psychosocial factors hindering or even impeding the proper functioning of many people in their social and life roles. It consists in the social environment “fixing” the individual in their roles. The interpersonal distance of a perceptual and emotional nature thus created results in an internal conviction of persons functioning in a deviant manner that the environment in which they function “cuts itself off” and does not want to maintain relations with them. An opportunity to reverse this phenomenon is the initiation of de-stigmatisation processes – possible in the world of the Internet, which enables users to maintain their anonymity.

Socialisation on the web can occur in a similar fashion to socialisation in the natural family environment, yet it can have significantly different effects due to the change in the technological and cultural environment. The main difference here are temporal as well as biological and physical factors – in the Internet space it is impossible to satisfy first-order human needs, which has a huge impact on our emotions and sense of security. Interpersonal contacts within the family are practically not limited by time constrains, while in the Internet space there are objective boundaries independent of us as individuals. It seems to many that socialisation in the family environment cannot be supplanted by socialisation in the “family of the Internet”. This thesis is confirmed by known examples of individuals isolating themselves from interpersonal relations in their natural environment (e.g. family or school) and engaging in Internet relations. Observation of such individuals indicates that the minimisation of real contacts with people closest to them results in emotional and psychophysical problems, yet it does not have a negative impact on intellectual development. Perhaps this is a civilisational model, leading to alienation of the coming generations from real interpersonal contacts in favour of those that are virtualised and stripped of any categories of emotions which have so far been recognisable.

Online socialisation – an opportunity or the curse of our times?

The problem of socialisation and the educational “power” of the Internet, analysed briefly in this article, leads us to conclude that from the point of view of social and pedagogical theories, the scope of our ignorance is territorially and qualitatively greater than that of our acquired knowledge (which in itself is speculative and probabilistic). It can be said that the current pedagogical understanding of social reality, based on paradigmatic thinking adopted and categorised in the 20th century, requires reflection and correction, because it does not fit the complex overlap of two worlds: the real, material world and the highly mediatised virtual world. It is difficult to determine unequivocally whether the humanist and interpretive paradigms used by the pedagogical academic community of the 21st century are adequate for perceiving and interpreting the complex reality of the Internet, which contains a purely technical aspect and should, therefore, be subject to structuralist or functionalist interpretations.

Therefore, we are dealing with a completely new phenomenon of social perception, i.e. observation, analysis and evaluation of surrounding reality. Socialisation is shifting from the sphere of well-worn intellectual and environmental models to an area still not sufficiently described, which is the subject of disputes and discussions.

It is worth remembering that it is only recently that the media, such as magazines, radio, television and the Internet, have become mass media on a global scale. People, as the "product" of biology and culture, have so far treated technology primarily as a way of making their life easier and satisfying lower-order needs. It was only the (still ongoing) information revolution that has made technology take on a different meaning in our life and play a dominant role in it.

The Internet is, therefore, not only a manifestation of a highly personalised technology. Above all, it is a tool used to discover new dimensions of human existence, with all this process entails. Its use as a new technical solution that facilitates our obtaining information and communicating with others is just another step in the civilisational development of humanity. Perhaps, however, it is something more. Maybe, as Ray Kurzweil (2004), a futurologist and chief development expert at Google, claims, it is a way of realising the eternal dream of humankind – securing immortality. From the point of view of social sciences and pedagogy, however, many questions about the web remain unanswered. Only in a dozen or several dozen years, when the generations raised on the web determine our economic, technological, cultural and political processes, will it be possible to make a reliable assessment of the effects of the information revolution begun in the 20th century.

This article contains fragments of texts previously published by the authors.

Home

A child in a web of threats – risky online behaviours of youth as a challenge for education

Maciej Tanaś, Sylwia Galanciak

The aim of the article is to present the complexity of the issues of threats related to the presence of children and young people in cyberspace. The authors attempt to systematize the problem, as well as identify the most dangerous phenomena. They also describe and classify the latest threats, stressing that as a result of the dynamic development of the internet, their catalogue is constantly growing, and thus requires regular updates. An important role in the process of monitoring threats, counteracting them and mitigating the effects should be played by media education, whose importance, although growing in education systems around the world, remains a trivial matter in Polish education.

Keywords:
cyber dangers
child in the internet
cyberbullying
hacking
sexting
patostreaming
media education

Home

The web's dizzying pace and the immense peer pressure to keep up crank up the speed of the treadmill our children are running on – until they have no strength left.
Michael Schulte-Markwort

Introduction

It is hard to believe that the Internet – a medium which has triggered the largest cultural change of a total nature since the invention of printing, encompassing social, economic, political and personal phenomena – has only recently settled into its early adulthood, while its actual revolutionary phase referred to as Web 2.0 is still coming of age. Within the 28 years of Tim Berners-Lee's devising the HTML language and of the creation of the first WWW page, the number of Internet users has exceeded 4 billion. Social media, which have only been around for 13 or 14 years, have more than 3 billion active users. This number keeps growing by about 14% year-on-year (Kemp, 2018). What is more, new technologies are not losing their developmental impetus. According to a law formulated in 1965 by Gordon Moore, device computing power continues to double about every two years (cf. Sienkiewicz, 2015, p. 100). It is imminently approaching the limit of physical possibility as the question arises: how could we build a transistor smaller than an atom?

All this comes with an exponential growth of means of communication and entertainment, as well as tools for learning and working, available on the Internet, which is still such a new, yet extremely variable space of human activity. The web's flickering, protean nature makes it a particularly difficult area of social research so necessary given the medium's unprecedented global significance. The digital world offers its users amazing opportunities for self-development, knowledge-sharing, networking and engaging in all sorts of entertainment, but, at the same time, it is a territory studded with traps and threats of an increasingly complex character.

Cyberthreats. An attempt to map out a new territory

Threats posed by the cyberworld can be twofold: relating to the history of the digital medium and to its specific character. When cyberspace was created as Web 1.0, developed to transmit content created by a limited number of originators to many recipients (within the so-called star structure), the problem of harmful materials posted on websites became immediately evident. It was also obvious from the very beginning that there was the issue of data confidentiality breaches. The second type of threat, which came about when Web 1.0 transformed into Web 2.0, is connected with human behaviour on the Internet and types of activity undertaken by users. Web 2.0 has upturned the entire philosophy of how we think about the shape of the network and the role of its users. The shift from a division into publishers and recipients towards a model in which everyone can create content has resulted in profound changes both in the structure of the Internet and in the attitudes of its users – who are now active creators of digital materials and commentators, or even judges, of virtual life, which is also increasingly intertwined with real life. Those users have different communication, cultural and social competences, different skills, goals and needs, and, finally, they are of different ages. A huge percentage are children – a group which is particularly vulnerable to digital threats.

As "digital natives" – to use the popular term coined by Marc Prensky (2001a; 2001b) – they intuitively navigate the Internet with certain boldness and great ease. Extensive research conducted by the NASK (Polish Research and Academic Computer Network) in 2016 (Kamieniecki et al., 2017, pp. 13–16) showed that the average age of Internet "initiation" was nine years and four months in the case of the studied young people. Today it is probably lower as there is a growing generation of children who have been exposed to touchscreens (i.e. tablets and smartphones) from a very early age. Significantly, most of the surveyed lower and upper secondary school students said that no one had taught them how to use the Internet and that they had acquired digital competences independently (68.6%). This not only exposes them as relatively easy victims to online crime and social threats, but also makes them more likely to become the perpetrators, often unaware of the dramatic and very real consequences of their actions in the virtual world.

The list of dangers to which young Internet users are exposed is extensive and difficult to exhaust because of the extraordinary dynamics of web evolution. Researches dealing with this issue regularly attempt to systematise it, yet usually end up with a list that comes with a reservation that it must continue to be updated because of the emergence of new types of threats. A useful classification has been proposed by Anna Andrzejewska and Józef Bednarek, who, significantly, introduce their list with the phrase "including, but not limited to":

- information addiction (Internet addiction);
- mental and physical health disorders, including vision and hearing disorders, musculoskeletal disorders and self-destructive tendencies;
- risks to cognitive and intellectual development, including, but not limited to, difficulties with active acquisition of knowledge, lack of information verification skills and isolation in an information bubble;
- moral dangers, such as cyberpornography, Internet prostitution, sexting, sugar babying and others;
- socio-educational dangers, especially those related to attitudes, behaviours, relationships and ties, such as cyberbullying and cyberviolence, online gambling, problems with interpersonal relationships or the use of the Internet by sects as a new and under-supervised recruitment space;
- negative effects of using chemical substances found in and inspired by the Internet space (narcotics, legal highs, psychoactive drugs, steroids and other doping substances);
- risky behaviours involving cybercrime, including copyright infringement, hacking, unlawful destruction of information, cybersabotage, dissemination of computer viruses and document fraud (Andrzejewska, Bednarek, 2018, pp. 28–29).

Sylwester Bębas has come up with a slightly more detailed division of cyberthreats, distinguishing seven basic categories:

1. Exposure to inappropriate content:

- cyberpornography;
- Internet prostitution (including sexting which leads to material benefits);
- content that promotes an unhealthy lifestyle.

2. Dangerous activities: cyberbullying, sexting, suicides inspired by and under pressure from the Internet (including suicides broadcast live online, suicides as a result of humiliation or harassment suffered online, suicide manuals and online suicide pacts).

3. Dangerous encounters:

- child grooming;
- online paedophilia;

4. Cyberstalking.

5. Dangers of a sexual nature (sexting, cybersex).
6. Internet addiction disorder (IAD), including information addiction, fear of missing out (FOMO) and online social networking addiction.
7. Cybercrime and Internet fraud:

- threats related to the security of data stored on the Internet;
- fake likes and cookies containing malware;
- fake websites and phishing;
- social media hacker attacks;
- tabnabbing (sites impersonating genuine websites);
- clickjacking (tricking a user into clicking on a link provided by the criminal);
- threats to mobile systems (Bębas, 2018, pp. 36–44).

Many threats cause "[...] blurring of the authenticity of one's identity and its virtual multiplication in cyberspace. In everyday life or in the mass media, originators have a specific identity. We know, or we can learn, much about them, because they are identified by a particular worldview and the socio-professional role they play. This identity is shaped by body language, gestures, timbre and pace of speech, and behaviour in direct, indirect, audiovisual and, to a lesser extent, audio contact. The Internet, on the other hand, by lifting space and time constraints, creates enormous opportunities to hide, manipulate and self-create identities" (Gajda, 2006, p. 16).

It seems that the Internet brings about two possibilities: on the one hand, it allows the user to shape an imaginary or desired identity (for example in social media, on an institution's website, in correspondence or on the user's own website). On the other hand, online presence, and information created on the Internet, make it possible to carry out an analysis which provides much more complete and precise knowledge about the creator, who is also the recipient of information and comments left by others. Undoubtedly, however, this replacement of direct by mediated contact – which is so frequent and common – has its social, personal and educational consequences.

Contemporary generations, unlike their predecessors, grow up surrounded by many media. Such an environment leaves deep and lasting traces in the mind of a child, because media are not only transmitters of information, but they also trigger emotions, shaping the sphere of imagination, and create dreams and desires, muddling up hierarchies of values and making it possible to obtain goals only partially in line with the expectations of parents, educators and teachers. Issues related to manipulation, propaganda, lobbying or lying arise, and new definitions of reality, the process and the result of cognition, truth and wisdom, are created (Postman, 2005, pp. 20–21). These, in turn, require a diagnosis, but also preventive and therapeutic measures. The new layer of culture created with electronic media changes and expands our senses and the reality we perceive. It affects the human mind, psyche and attitude towards the world (Kerckhove, 1997).

Social networking sites have made it possible for anyone with web access to publish materials. These are traces of human thought and creativity, but also evidence of naivety, aggression and criminal behaviour. Universal connectivity has given people's activity – their greatness and goodness, as well as their baseness and evilness – powerful support tools. There is a folk saying that "a word may start off as a sparrow and come back as an ox". The web has increased not only the number of such "oxen", but also their strength and impact.

Although IT networks connect institutions and people, disparities between countries which invest in ICT infrastructure and those which cannot afford it are becoming more apparent. Power over information systems is associated with the monopolisation of culture and political influence. On the one hand, cultural homogenisation processes are in full swing, but on the other, great efforts are undertaken to record the sound of languages and specific features of ethnic cultures. It is difficult to determine at present whether the 21st century will be dominated by the fatalistic paradigm of the annihilation of global cultural and linguistic diversity, its hybridisation and the extinction of languages, linguistic groups and many local cultures, or whether digital tools of information and communication technologies will prove their usefulness in maintaining the authentic pluralism and originality of languages and cultures (Mayor, 2001, pp. 355–373), thus supporting the paradigm of survival and development, or – put simply – saving the treasures of cultural heritage.

The web can also be a weapon of war. It is worth noting that the free global flow of images and words facilitates criminal activity. Criminal groups are supranational and ruthlessly use differences in the laws of various countries to their advantage.

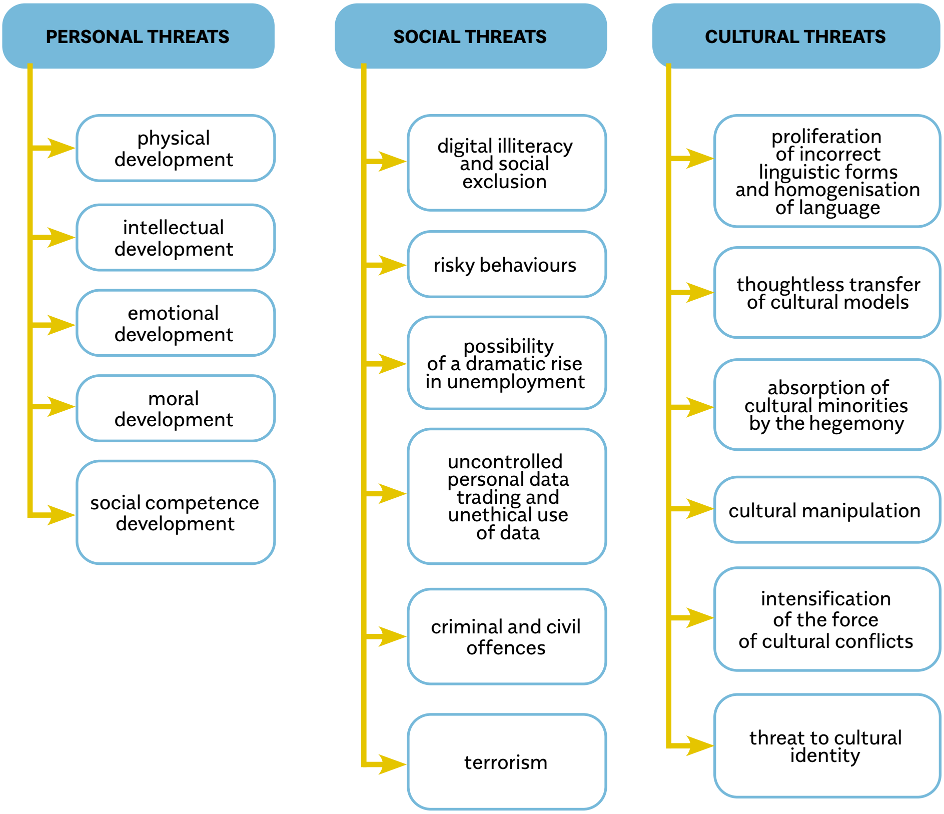
The lack of universal media education has very undesirable effects and this applies to all user spheres: personal, social, cultural, political and economic. For years, academics and educators alike have been unsuccessfully calling for its incorporation into teacher training and school curricula. Just as it is necessary to develop an appropriate legislative framework for safe navigation of the Internet, Polish education at the turn of the 21st century needs universal information and media training. Today – more than ever – this is essential.

Media regulations in Poland encompass a unified system for classifying television programmes and the European system for assessing computer games known as PEGI (Pan European Game Information). The latter is undoubtedly one of the best video game content rating systems, but not the only one. There are other solutions such as the Japanese CERO, the American-Canadian ESRB (Entertainment Software Rating Board), British ELSPA (Entertainment and Leisure Software Publishers Association), as well as USK (Unterhaltungssoftware Selbstkontrolle), created by a German organisation which evaluates computer games and broadly understood entertainment software in terms of safety for children and young people, and OFLC (Office of Film and Literature Classification) of the Australian Classification Board.

Can, however, existing tools for protecting children against the negative consequences of computer games and web access be treated as sufficient and ultimate solutions? It has to be emphasised here that no classification alone is capable of increasing knowledge and awareness. The label on a product is only an indication whose interpretation depends on one's knowledge – and the indication is not the product itself. There are many works available dealing with the dangerous effects of cyberspace and media use. *Digital Dementia* by Manfred Spitzer and *Homo Videns* by Giovanni Sartori are just two examples. The human species may have been described differently over time (*Homo sapiens*, *Homo volens*, *Homo creator*, *Homo faber*, *Homo sedes*), but the stage of "numb man" is certainly not something we should be striving to reach.

Given the level of recorded threats and flagged social needs, coordination of efforts is required to ensure that children are safe in cyberspace. It is necessary to take comprehensive social action in the field of universal media education and preventive education programmes. Legislative action in this respect is also imperative. The need to create a national strategy in this area is becoming increasingly apparent, especially in the context of the bold and impressive initiative of the Polish National Education Network[1], which intends to bring broadband to all schools in Poland.

Figure 1. Personal, social and cultural threats resulting from the development of cyberspace according to Maciej Tanaś


PERSONAL THREATS
physical development
intellectual development
emotional development
moral development
social competence development
SOCIAL THREATS
digital illiteracy and social exclusion
risky behaviours
possibility of a dramatic rise in unemployment
uncontrolled personal data trading and unethical use of data
criminal and civil offences
terrorism
CULTURAL THREATS
proliferation of incorrect linguistic forms and homogenisation of language
thoughtless transfer of cultural models
absorption of cultural minorities by the hegemony
cultural manipulation
intensification of the force of cultural conflicts
threat to cultural identity

Source: Author's own work.

[1] The Polish National Education Network initiative aims to give schools universal and equal access to high-speed (at least 100 Mb/s), safe and free Internet. According to the project's underlying assumptions, all primary and secondary schools are to be connected to the Polish National Educational Network by 2021. Cf. M. Bochenek. *Rok pilotażu OSE* [*One-year pilot programme of the Polish National Educational Network*]. In: *Akademia NASK, O OSE* [*NASK Academy, on the Polish National Educational Network*]; bit.ly/2yBDGbx [access: 17.07.2018]. The Act on the Polish National Education Network was signed by the President of the Republic of Poland and published in the Journal of Laws on 28 November 2017 (Journal of Laws 2017, item 2184, vol. 1).

Anyone building a system would like it to be compact, finite and coherent. Figure 1 does not represent such a full system. It is a systematoid at best, as many phenomena related to the development of information and communication technologies have not yet been studied, described or explained.

Let us begin with pointing out certain **personal threats**. Some of them are associated with the **physical development** of children and adolescents and concern the skeletal, nervous, cardiovascular and metabolic systems. The following seem particularly dangerous:

- underdevelopment of the musculoskeletal system;
- postural defects, including scoliosis and abolition of lordosis in the cervical spine, carpal tunnel syndrome, shoulder and neck disorders, as well as degenerative changes;
- decrease in physical fitness and a general weakness of the body;
- obesity, bowel disease;
- eye defects, conjunctival disorders, keratitis;
- allergies;
- consequences of the harmful effects of the electrostatic and electromagnetic field (especially frequencies from 10 to 300 kHz)[2].

Many of those threats were already warned against during the development of microcomputers and CRT monitors (Tanaś, 1993, pp. 127–132). However, issues of child and youth safety in the space created by web-connected computers – which combined features of several media, were increasingly poly-sensory and interactive, and thus attractive to users – were not identified (or were downplayed) at the time. Neither was it comprehended that the Internet would soon become not just a place of creativity, but also an economic, ideological and political battlefield. A space where dreams could come true and human organs could be trafficked. A global economic market and a place of baseness. While physical space has been legally codified for centuries, cyberspace, under the false pretext of unlimited freedom, has become open to criminal activity and to controlling people and entire communities.

[2] In particular, reports of inhibited bone growth, accelerated spread of leukemia and other forms of cancer, and abnormal prenatal development require further analysis and evidence as lack of awareness and false beliefs can generate undesirable social reactions in this area.

Another group of threats which requires analysis and serious reflection is associated with **human intellectual development**. Research points to many risks in this area, for example:

- cognitive impairment (disturbed perception, decreased fluidity of attention, limited or non-existent ability to think logically, obsessive or intrusive thoughts);
- intellectual passivity;
- memory impairment (resulting from lack of memory training and from the misconception that since all information can be found on the Internet, memorizing has become redundant);
- false or fragmentary picture of the world (perception of the world as a series of video clips, rather than as interrelated and interdependent phenomena), intellectual immaturity (treating the created world as real);
- underdevelopment of systematic learning skills;
- poor verbal and writing skills, thoughtless imitation, dominance of concrete/pictorial thinking over abstract thinking, reduced ability to synthesise and generalise as well as to analyse and perceive relationships, and – as a consequence – reduced ability to reason and understand;
- inability to construct full, logical and coherent statements, inability to use language creatively, reliance on Internet jargon and ignorance of stylistic variations of spoken and written language.

Many personal threats are also related to the **emotional development** of children and young people:

- seeing friendship, love, care or responsibility through the distorting prism of, for example, video games (the same applies to the relationship between good and evil in the simplified world of a player), emotional immaturity;
- development of inappropriate emotions regarding love and sex, treating virtual relationships as real;
- creation of negative ways of expressing emotions, escalation of uncontrolled emotions on the web;
- priming towards content, behaviours and attitudes which are undesirable, as well as cognitive and emotional desensitisation;
- Internet addiction disorder (Internet addiction syndrome), altered states of consciousness, which are reminiscent of alcohol

or pharmacological intoxication, fear of missing out (FOMO) and gaming disorders (gambling behaviour), including addiction to programmes containing elements of psycho-manipulation, persuasion techniques and subliminal stimuli (video clips, advertisements, techno music), and possibly also based on neurolinguistic programming procedures, mind control techniques or biological neural manipulation techniques;

- psychological discomfort associated with the "withdrawal syndrome";
- compulsive behaviour, neuroses.

Furthermore, personal threats can be associated with **moral development** and include, in particular, a disturbed hierarchy of values and their relativisation, as well as disregard for ethical principles (they do not apply in some video games).

When analysing potential dangers associated with the development of information and communication technologies, we cannot ignore threats to the **development of social competences** in children and youth, such as:

- social alienation and weakening of family ties, escape from the real world;
- access to pornographic and racist materials as well as to pathological and "toxic" cult groups;
- treatment of aggression and violence as desirable social behaviour, xenophobia, copying pathological and destructive behaviour (social consequences of cognitive priming towards educationally undesirable content), social desensitisation;
- brutality of behaviour and expression resulting from a sense of "anonymity" and "impunity", unjustified individual or collective aggression and self-aggression;
- relativisation of social relationships, world image disintegration.

Many of the above dangers were observed already at the initial stages of the deployment and spread of the Internet in Poland (Tanaś, 2005, pp. 25–40). The diagnoses made at the time have, unfortunately, been proven to be correct.

The developmental dangers mentioned above are undoubtedly closely associated with a large group of **socially dangerous impacts**, such as:

- digital illiteracy and social exclusion – these issues usually affect poor, disadvantaged or unemployed people, deprived of access to the web, mobile devices or smartphones, as well as numerous groups of people with disabilities and people without IT, technological and media competences. Threats of this kind are faced, in particular, by inhabitants of villages and small towns where schools operate without broadband Internet, proper infrastructure and Wi-Fi access – i.e. localities with no web communication, lack of or difficult access to open educational resources, open science and other online sources of knowledge and culture;
- risky behaviours – these involve undertaking risky actions which are described and/or recorded with sound and/or image and intentionally made available to children and young people. Adolescence is a particularly critical period in this respect. Susceptibility to risky behaviour is caused by psychobiological and evolutionary factors (Romer, 2010; Steingerg, 2007). On the one hand, information and communication technologies fascinate teenagers and satisfy some of their major emotional and communication needs, which are important during adolescence (Dolev-Cohen, Barak, 2013; Valkenburg, Peter, 2011), yet, on the other hand, they provide an outlet for manifestations of many risky behaviours. The Internet facilitates participation in situations which increase the likelihood of such negative consequences as emotional stress, victimisation or deterioration of social, school or academic life (Valcke, De Wever, Van Keer, Schellens, 2011). The most frequently reported problem related to online behaviour has been cyberbullying (Livingstone, Smith 2014; Young, de Abreu, 2011). In recent years, increasingly more attention has been paid to the tendency to use the Internet to contact strangers, social groups or institutions, unions and organisations (Valcke et al., 2011). Research (Gámez-Guadix, Borrajo, Almendros, 2016) has also pointed to the importance of impulsiveness, which is characteristic of adolescence (irresponsibility as a possible mechanism explaining risky behaviour). Loss of control over

Internet consumption, as well as excessive cognitive engagement with using it – even despite negative consequences – are becoming increasingly widespread (Caplan, 2010). This problem is sometimes referred to as "compulsive Internet use" (Meerkerk, van den Eijnden, Franken, Garretsen, 2010) or "Internet addiction" (Smahel, Brown, Blinka, 2012);

- potential rise in unemployment as a result of disappearance, in several years, of many existing professions, practiced by millions of people around the world. Individuals and entire enterprises base their activities on those professions or rely on persons who perform them. The process of many types of jobs being wiped out is real and is already underway ("The Guardian", 2017). Research conducted by the University of Oxford and many other academic centres, as cited by Alux.com (2016/2017), suggests that in the next 20 years there will be a significant reduction in employment in 15 commonly practiced professions, such as farmer, driver, supermarket cashier, travel agent, factory worker, dispatcher, bartender, waiter, bank cashier, military pilot, soldier, fast food chain worker, telemarketer, accountant, stock trader and construction worker. In spite of existing problems, further activities undertaken in the realms of academia and education should be based on appropriate decisions regarding both current fields of education and further training and retraining of persons employed in these professions. There is an urgent need for serious reflection in the field of social sciences and engagement in intentional and wise educational action, otherwise we risk political, economic and social crises and, above all, human tragedies;
- uncontrolled personal data trading and unethical use of data – the advancement of information and communication technologies is ahead of both awareness of the consequences it entails and legislative regulation. The huge amounts of data, obtained as a result of media digitisation, software development and widespread connectivity, have not only a high volume and velocity, but also a high variety and veracity. Data sets whose size or type makes it impossible for them to be captured, managed and processed by traditional algorithms and relational databases are known as "big data". Their analysis makes it possible to carry

out previously unavailable decision-making processes in many areas. This undoubtedly opens up completely new cognitive perspectives, but also raises the possibility of unethical and even criminal use of such information;

- criminal and civil offences – these include, for example, terrorism, mafia activities, dissemination and sharing of manuals regarding, for instance, suicide, murder, rape, weapon or bomb construction, and drug production, dissemination of criminal or socially undesirable phenomena (religious sectarianism or hostility towards ethnic groups or nations, or social groups with a different sports club affinity), threats to the security of institutions, violence with the use of digital tools, harassment, identity theft and impersonation for material benefits, misinformation and media manipulation, dissemination of pathological content, as well as initiation and creation of anti-social groups;
- terrorism – attacks on institutions, direct meddling with the internal affairs of a country, political terrorism, threat to the information security of a state, possibility of training in virtual worlds, and attacks aimed at mastering the skills of reconnaissance, surveillance, group cooperation and analysis of the possible media response.

Another group of dangers are socially perceived and manifested **cultural threats** such as:

- spreading of macaronic language (Volapük) and incorrect linguistic structures;
- disappearance of the territorial diversity of language (homogenisation);
- transferring models of behaviour, rituals and celebrations stripped of their cultural context to another cultural area, uniformisation of culture and clothing;
- absorption of cultural and linguistic minorities by larger cultures;
- intensification of cultural conflicts;
- threat to cultural identity (social stress caused to some groups);
- cultural manipulation – influencing views and attitudes through culture.

The most important law of medical ethics is *primum non nocere* ("first, do no harm"). After centuries, it has also become the guiding principle of ethical research and social activity. This principle is of great importance for those educators and teachers who enter the sphere of computers, mobile telephony and the Internet, trying to understand the fate of children and young people in the electronic cave of the world of digital media.

An aspect of the web which is particularly dangerous to children's safety is its information and propaganda function which – although providing considerable learning possibilities – prevents the recipients from making proper independent judgements and makes it difficult for them to find the right place in reality. Furthermore, because of the speed of communication and the multitude of channels operating in parallel, it deprives the content consumer of the time required for reflection and action. Another significant factor is the jumble of the real and the virtual, which produces an inconsistent, discontinuous vision of the world, resulting in ethical and ideological chaos and personality disorders. Yet another important issue is the pursuit of fun at all costs, focussing on temporary gain and adopting a consumer lifestyle, which generates the risk of information overload and disruption of the sense of identity and understanding of reality. And finally – content published on the Internet contradicts many educational goals, and also causes a multitude of negative consequences, such as replacing natural interpersonal relationships with interactions with computer game or television series characters and media idols.

We should, above all, remember that the Convention on the Rights of the Child was ratified in Poland in 1991 with reservations and interpretative declarations (the United Nations General Assembly adopted the Convention in November 1989). While the provisions of this document should never be disregarded, one must be aware of the necessary and constant legal additions resulting from the development of information and communication technologies, as well as from civil and criminal offences. It is not just new types of risky behaviour or criminal acts that are of significance here. Even traditional crime conquers new territories and gains incomparable impact in cyberspace. Its forms are changing, as is the language in terms of connotations and designations of basic concepts (for example, the traditional "I wasn't there" alibi gains a different meaning).

Excessive consumerism and widely observed social disintegration reduce the quality of life and undermines the material foundations of a country's development. The most difficult and important pedagogical tasks relate to the digital generation's value system, its aspirations, attitudes, behaviours and lifestyles. Many years ago, Bogdan Suchodolski (1937) accurately predicted that the future would take place in the sphere of broadly understood culture. Indeed, the revival of traditional European culture and ideas of tolerance and humanism must go hand in hand with care for the harmonious development of children and youth. The symbolic values of freedom, equality and brotherhood will be a dead letter without a new pedagogical leaning and education focussed, on the one hand, on the sovereignty of an individual and, on the other, on the reconstruction of the human community.

Although virtual reality tries to imitate the real world, it remains different from it. Similarly, education using digital media is also different from previous systems. That is why information and media education pose a challenge for Polish politics and the Polish system of education at the beginning of the 21st century. Therefore, educators, teachers and parents, politicians, lawyers, psychologists and doctors, scholars and practitioners should together make every effort to ensure that this education is not defective and meaningless. The problem of modern training and education systems does not only relate to the sphere of human intellect and ability, but also to that of values. In pursuit of the eternal dream of exceeding our own biological, temporal and territorial limits, we have constructed an electronic cave. It is now time to learn how to live in it to the fullest extent possible and how to provide intellectual sustenance, movement and fresh air to our children.

It is striking that the previously cited classifications, although relatively new, already require an update. Every now and then, the Internet community is shaken by information about new disturbing phenomena, such as streaming of socially pathological content, new forms of ransomware attacks, risky online challenges or symptoms of information and communication overload which can be referred to as "digital burnout" (Galanciak, Siwicki, 2018).

The catalogue of problems, many of which relate to the Internet activity of young users, is expanding at an alarming rate. This is a huge challenge not only for the family as the primary educational environment, but also for the school, which is a key space of young people's socialisation and learning, as well as for the social sciences, primarily pedagogy, which can make use of an extensive range of research methods, means and tools taking into account the specific nature of a child as an active entity in a social environment. However, science is unable to keep up with the pace of changes taking place in the media. Its quern demands precision and deep reflection on the subject under consideration and grinds the researcher's input thoroughly but slowly. This often makes scientists feel helpless in the face of media reality and leaves young network users defenceless against emerging threats. Meanwhile, people increasingly consolidate the real and the virtual and, as a result, need support in the process of shaping their digital competences, both in order to avoid threats and in order to be able to optimally use the opportunities and capabilities – whether cognitive, creative or social – that cyberspace offers. The responsibility faced by social sciences, including pedagogy, is, therefore, enormous and requires perseverance to make unceasing attempts to view this new reality, no matter how short-lived the effect of such an analysis may be and how soon it will need revising. The three basic areas of threats related to online activity – contact with inappropriate content, undertaking dangerous social activities and electronic crime against security systems – require continuous monitoring, diagnosis and provision of solutions to counteract negative phenomena, as well as developing therapeutic strategies for the victims of situations which could not have been prevented.

To fully understand problems related to the safety of children and young people online, it is necessary to adopt a technical perspective and recognise the great importance of protective and pre-emptive actions. To ensure technical security, the following is required at a minimum:

- protection of domains and blocking of offending sites based on a blacklist;
- scanning and checking a website in order to block any harmful content;
- online analysis of uploaded and shared content in terms of user safety.

Constant fight against existing and ever newer types of viruses and attacks continues. Technological development generates further threats. Digital media can be used to benefit the user, but it can also be used against the user. For example, there is a growing number of devices which communicate with one another, commonly referred to as the

"Internet of Things". According to the Computer Emergency Response Team Polska report (2016, pp. 23–29), already in 2016 malware enabled hackers to take over a huge number of webcams and smart TVs via the Mirai botnet and to paralyze Twitter, Spotify, Reddit, as well as "The New York Times" and "Wired" services. Around two and a half million smart refrigerators, industrial machines and car parking systems were infected. This is just one example of the battle for user safety on the technical field. Global threats and incidents are accompanied by attacks on particular countries, institutions or individuals, as well as random malicious attacks.

Technical threats are such a broad issue that they cannot be exhaustively analysed in this article. It should be pointed out, however, that nowadays not only the above-mentioned Internet of Things is being developed, but also the domain of speech and language recognition, augmented reality, and, last but not least, Artificial Intelligence and robotics. Both the number of risks and the range of methods and means for detecting and combating them are growing. A war is waged – often brutal and ruthless – for the security of the web and the safety of its users. To understand this phenomenon, it is necessary to look from both perspectives: the technical and the human/social one.

Complexity of the issue – the example of cyberbullying

One of the key problems related to risky behaviours engaged in by Internet users is cyberbullying. According to the United Nations, it is any "aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" (2014, p. VII). This seemingly concise definition covers a wide range of different manifestations of electronic aggression. Common features of this type of violence include "use of electronic means, intentionality, imbalance of power (it may involve being outnumbered by persecutors, who are additionally joined by bystanders, but also the level of efficiency in using technology, e.g. when hacking an account or swapping files), repeatability (long duration of bullying, which gains additional strength on the web, because content once uploaded on the Internet never disappears and may be subject to duplication and modifications which reinforce its destructive power), and sense of anonymity – physical separation from the victim, which makes the bullying easier as any mental discomfort is alleviated because the persecutor is not directly looking at the effects of their violence" (Pyżalski, 2012a; Tłuściak-Deliowska, 2017).

Jacek Pyżalski (2012a, pp. 126–128) proposed a valuable suggestion for the classification of phenomena related to cyberbullying, subsequently updated by Maciej Tanaś for the purposes of an assessment of the European legal and organizational solutions in the field of cyberbullying prevention prepared for the Supreme Audit Office (Tanaś, 2018, p. 72). According to the researchers' findings, the concept of electronic aggression may encompass the following forms:

- flaming – aggressive exchange of insults, for example in an online chat or a discussion group;
- harassment – regular sending of unpleasant messages to the victim via electronic communication channels, also known as online harassment;
- griefing – harassment within an online game or virtual world;
- trolling – persistent posting of inflammatory comments about someone online;
- cyberpersecution, cyberbullying – constant, repetitive online harassment, use of threats and/or victimisation;
- masquerading – creating a fake online identity in order to harass someone;
- fraping – changing data on someone's Facebook page to humiliate them;
- dissing – posting cruel information, photos and videos about someone on the Internet;
- grooming – befriending a child, and sometimes their family, to lower the child's inhibitions with the objective of sexual abuse;
- cyberbullying sexting – exchanging sexually explicit photos without the victim's knowledge and consent;
- sexcasting – exchanging sexually explicit videos without the victim's knowledge or consent;
- happy slapping – recording aggressive statements or behaviours towards someone and then sending the recordings to friends or publishing them online;
- impersonation – creating an online presence in the victim's name, as well as stealing the victim's online identity (catfishing)

to recreate their Internet social network and obtain information about them or their friends or to engage in masquerading;

- outing – sharing the victim's private materials (e.g. photos, message records);
- trickery – sharing with third parties someone's private materials (e.g. photos, message records) obtained by tricking or extorting the victim;
- cyberstalking – keeping the victim under surveillance and harassing them with unwanted messages;
- denigration – public spreading of degrading and false information or materials about the victim;
- exclusion – deliberately removing the victim from one's list of Internet contacts or preventing the victim from joining a certain network of contacts;
- defamation – verbal communication based on malicious gossip without being in possession of any materials to support it (similar to humiliation);
- slam books – electronic versions of paper notebooks circulating among children and teenagers with questions to be answered. They contain malicious, usually anonymous, comments with the objective of stalking or defamation;
- technical aggression – actions against the victim's computer equipment, not directly against the victim themselves (Pyżalski, 2012a, pp. 126–128; cf. Tanaś, 2018, pp. 72–73).

On the one hand, the long list of different forms of cyberbullying makes us aware of how complex and multidimensional a phenomenon we are dealing with. On the other, it proves that intensive work on education-based prevention of this type of behaviour is indispensable, especially among children and young people, i.e. groups particularly vulnerable to peer cyberviolence (among others), as well as to its personal and social consequences. Research carried out in recent years shows that the scale of the problem is very large. According to the *Nastolatki 3.0* [*Teenagers 3.0*] report prepared by the NASK, more than half of Polish teenagers have witnessed aggression against their friends in the virtual space, 59.7% have seen a friend being insulted, 58.1% have been humiliated or ridiculed, 40.5% have come across their friends' being impersonated, and 34.2% have witnessed them being threatened (Kamieniecki et al., 2017, pp. 86–87). Over 30% of respondents have experienced online verbal aggression: 32.2% were insulted, 19.4% – humiliated, and 13.6% – threatened (ibid., p. 89). Similar findings were presented in the report of the Supreme Audit Office on preventing and counteracting cyberbullying among children and adolescents: 26.7% of the surveyed students admitted that they had been victims of cyberbullying (*Zapobieganie i przeciwdziałanie…*, 2018, pp. 25–27). Disturbingly, both studies reveal that a very high percentage of the respondents have never sought (or will not seek) help when directly affected by aggression on the Internet: 39% according to the NASK study (Kamieniecki et al., 2017, p. 91) and 48.8% according to the Supreme Audit Office study (*Zapobieganie i przeciwdziałanie…*, 2018, pp. 54–55). Lack of support from one's environment may result in serious psychosocial consequences for the persecuted person (such as peer isolation, sense of loneliness, depression, low self-esteem, and – in extreme situations – suicide attempts). Meanwhile, according to the report of the Supreme Audit Office, efforts undertaken against cyberbullying in Poland are not coordinated, which is not conducive to their proper targeting and dimensioning, and so reduces their effectiveness. Schools do not receive sufficient expert and technical support in this regard from state authorities, governing bodies or school boards, so, instead, they focus their actions on responding to reported acts of cyberbullying (ibid., p. 13). This does not contribute to solving the problem and increasing children's online safety.

New types of activity, new problems

In spite of certain deficiencies in the policy on diagnosing and preventing cyberbullying, it is still one of the best-studied threats associated with online activity. Unfortunately, most dangerous phenomena in the digital world remain little explored. They include risky behaviours such as sexting (which has entered the social discourse thanks to the "Myślę, więc nie ślę" ["I think therefore I don't send"] campaign of the Dajmy Dzieciom Siłę [Empowering Children] Foundation), dangerous Internet challenges or streaming of socially pathological content, which is gaining increasingly more popularity among audiences.

Sexting, which involves "sending nude photos or short video clips of an erotic nature to another person […] using a mobile phone

(MMS) and the Internet (e-mail)" (Ronatowicz, 2014, p. 129), is not only a reflection of the emotional – or economic, in the "commercial" version of this phenomenon (for example, sending photos of an erotic nature in exchange for topping up one's phone) – needs of the people who engage in it, but also, above all, is a testimony of shortcomings in their ethical and emotional development. As regards the process of engaging in this activity, Justyna Woźniak (2018, pp. 204–205) has proposed the following model:

- curiosity phase, which involves, among others, a fascination with browsing other people's autopornography;
- initiation phase, when the desire to participate in sexting arises;
- active participation phase, which may take one of two courses: either gain social approval (reward and encouragement to continue) or evoke disapproval, derision, and – in extreme cases – hatred;
- commercialisation phase – which does not apply to all persons who engage in sexting – involving gaining financial benefits from sending autopornography or presenting one's nude body on the web via a webcam.

Young people involved in sexting, in the absence of sufficient sex and media education, often do not realise the scale of the consequences they are risking – and these are not only moral, but also social, which are usually perceived by them as more severe. Once uploaded onto the Internet, materials never completely disappear, especially in times of instant content sharing through social media. People who have been victims of aggression, ridicule, blackmail or embarrassment as a result of leaked intimate content will be forced to deal with the consequences for years to come. Social ostracism, long-lasting feeling of shame, destroyed career opportunities or difficulties with having a settled private life are just a few of the possible effects of this dangerous phenomenon.

Another threat arising from the need for self-presentation and social acceptance, as well as the need to compete and participate in activities undertaken by the group, is the phenomenon of taking on dangerous Internet challenges. It should be emphasised, however, that many of them are intended to send a positive message, are used to promote pro-social attitudes or support charitable goals (for example, the famous Ice Bucket Challenge, which spreads knowledge about amyotrophic lateral sclerosis and raises money for an organisation supporting people affected by this disease). However, there are also those challenges that can pose a real threat to the health and life of those who undertake them. These include the Choking Game (choking to achieve a state of euphoria), Game of 72 (going missing from home for three days, particularly popular with younger teenagers) or the Salt and Ice Challenge (sprinkling salt on one's hand and then placing ice on it, which sometimes results in burns, including second-degree ones). From time to time, the media are swept with sensational reports about suicide challenges, such as the Blue Whale Challenge or the Momo Challenge, and although these are usually classic examples of attempts to cause moral panic, the reports themselves may become an incentive for young Internet users who are searching for their identity or cannot cope with their emotions.

Streaming socially pathological content is also becoming an increasingly dangerous phenomenon. It involves live online presentation of anti-social, shocking behaviours, such as insulting random people, being violent towards others (one of the streamers became famous for beating his mother with a chair), drinking sprees or urging minors to undress in front of a webcam. Comments posted on streaming services (mainly YouTube) reveal the worrying fact that a large group of socially pathological content viewers and active commentators are children. Creators of such streams are guided by the desire to earn money (fans make payments to their favourites), shock or cross socially acceptable limits. Children, who are unable to foresee the consequences of certain actions, cannot properly assess the situation and watch such streams only to learn some of the worst models of social behaviour and, in effect, acquire anti-social attitudes, which they may even perceive as attractive. And even if the actions of the creators of socially pathological content are ridiculed, their channels accustom audiences to improper social behaviour, which results in consent to petty crime, as well as in the perception of aggression as fun and stupidity as an attractive feature that can generate financial gain. This new cultural model is a significant threat to the socially respected set of attitudes and values as well as to the accepted axiomatic system.

Countermeasures

Counteracting threats in cyberspace can follow two main tracks. One, which is extremely difficult to implement due to the cross-border nature of the Internet, involves legal codification of dangerous behaviour and use of punishment. The inability to regulate behaviours which produce consequences in the territory of one country but are initiated in another prevents the effective penalisation of pathological behaviour on the Internet (Kulesza, 2012, p. 11) and makes it extremely difficult to prosecute perpetrators of evident and codified crimes (such as paedophilia or online banking theft). In addition, due to the libertarian ideas that have accompanied the Internet since its inception, all activities related to interfering with content posted online trigger a reaction in the form of social protests against Internet control (ACTA, PIPA or SOPA). "It turns out that young Internet users – who represent a new type of social sensitivity, use new information carriers and new symbolism, and express their commitment in an often unconventional way – can quickly mobilise powerful social resources online when faced with challenges in order to defend their freedoms, rights and democracy" (Galas, 2018, pp. 80–81). It is a force that should not, and must not, be wasted. Education is a much more effective and durable tool for social change than legal sanctions, and this is what the energy and intellectual resources of young people should be funnelled towards.

Smart and mature **media** education, which prepares young people to consume and co-create content, is the only possible path to counteract the threats of the digital world, and, at the same time, to release its creative, self-developmental and social potential. However, for it to be effective, teachers need to be equipped with tools for diagnostic, preventive and even partially therapeutic activities (e.g. aggression replacement training). It is, therefore, important to emphasise proper positioning of media competences in teacher training curricula.

It is also essential to provide children with an alternative to digital reality – offline spheres of activity, such as sports or scouting, as well as involvement in the cultural or social life of their community.

However, those efforts will not produce the desired results without parental involvement. Treating smartphones, tablets or computers as technological successors of the nanny or time-occupiers is not conducive to children learning how to use the media wisely and creatively. The presence and involvement of a parent as the child ventures onto the web seems to be a *sine qua non* condition for successful media education and proper preparation of the child for immersion in cyberspace.

Conclusions

The online world, increasingly amalgamated with the real one, has become the second home of modern humans. It occupies their free time and devours their work time, it is a place and tool for social communication, building relationships and organising one's private life. It is a space of globalisation, but also social atomisation, an area open to political, social and cultural manipulation, as well as a military and economic battlefield. Furthermore, it is a space for searching, performing and evaluating work, and for scientists – a territory of scientific research and a source of research methods, means and tools. Among this multitude of functions and tasks there is also room for important pedagogical ideas, which, in fact, have from the very beginning guided the creation of the Internet, but which are fully feasible only today. The web is, after all, an emanation of utopian philosophical ideas postulating the need to synthesise human knowledge and make it available to all. Concepts of a collective mind in the form of Teilhard de Chardin's "noosphere" or Pierre Lévy's "collective intelligence" have for years inspired academics working on a network connecting scientific institutions, companies and the homes of ordinary people (Galanciak, 2016, p. 248). Today they provide an impulse to develop the noble idea of open science and education. Open educational resources (OER), i.e. educational materials made available free of charge through the use of information and communication technologies, are democratising access to sources of human knowledge on an unprecedented scale. They are further complemented by massive online open courses (MOOCs), which are organised for mass audiences by the world's top universities (Massachusetts Institute of Technology, Stanford University, Princeton, Harvard), as well as, more and more often, non-academic institutions, such as museums and foundations.

This is the first time since the invention of printing that the world has gained a tool with a similarly great potential for equalising educational – and life – opportunities and eliminating social inequalities. In order to take advantage of this potential, while steering clear of the threats it poses, one needs appropriate competences, which cannot be acquired without prior media education.

Home

Home

Virtual world as a place where young people establish and maintain relationships

Anna Andrzejewska

The space of human functioning undergoes constant changes, which are a natural process. Recent years have been the dynamic development of the digital space. The virtual word is not only a place of human activity in many areas, but also a place for establishing and maintaining relationships by young people. It is a meeting place for strangers who interact with each other, from very incidental ones, sometimes to those close and even intimate ones.

The following issues were discussed in the publication:

1. Growing up in the digital era – that is, about the Y and Z generation.
2. Conditions for creating relationships during adolescence.
3. Communication in the virtual world as a factor determining the relationships of young people.
4. The virtual world is the place of initiation of closer relations – friendly, partner and intimate.

Keywords:
youth
generation Y and Z
adolescence
relationships
communication
virtual world

Home

Introduction

Before I begin my analysis of issues relating to young people's establishment and maintenance of relationships in the virtual world, I wish to quote the following words of Józef Bednarek: "On the one hand, the virtual world offers its users a wealth of opportunities – it gives them access to worldwide resources, makes any distance a negligible factor, gives them a kind of freedom they do not enjoy in everyday life. However, on the other hand, it imposes great limitations. Great imagination is needed to be able to live and breathe only words and images [...]. The virtual word is appealing, quite separate from reality, it is fascinating and seducing with its extraordinariness, which is why it attracts many people. Living in a virtual community allows many to combat alienation, loneliness and isolation" (Bednarek, 2014, p. 23). These issues are becoming more and more significant in light of what is so typical for our times: the virtual world's primacy over the real one as a place of young people's activity.

Growing up in the digital era – Generations Y and Z

The Network Generation, also called Generation Y, are people born in the years 1980–2000. Other names include Millennials, Global Generation or Multimedia Generation, Freewheelers, MTV Generation, Free Market Digital Children, and Generation of Flippers and iPads (Kubacka--Jasiecka, Passowicz, 2014, p. 175), as well as the Searching Generation, Net Generation, Generation Why or IKEA Generation. Generation Y comes after Generation X (Bergh, Behrer, 2012, pp. 21–22). The TV set, which for decades dominated many homes, has been replaced by a computer connected to the Internet. As Edwin Bendyk says: "In the modern world, the net, involving both the Internet and mobile phones, is something as obvious as air and water" (Bendyk, 2004, p. 16). Generation Y is the first cohort to have grown up in this cyberspace.

Generation Y is one of the largest demographic groups. As Josh McDowell says, it is "perhaps the richest, most populous, best educated and most physically fit generation in history" (McDowell, 2000, p. 16). "They have a true understanding only with their peers, with whom they share coherent meanings and youth culture values, as well as its symbols (memes) building community identity. They attach great importance to friendship and establishing deep non--institutional relationships – when it comes to social relations, they can be called a ″generation of quality rather than quantity″. They consider themselves individualists and emphasise their distinctness from other people. They like attracting attention and showing off, sometimes in disregard of others' intimacy and privacy, which is seen as something typical of this ″reality-show generation″. In principle, they avoid entering into relationships with their wider surroundings – they do not get involved in active citizenship or community life and shun authorities and politics. At the same time, they say they do not preclude deeper personal involvement in selected social problems" (Kubacka-Jasiecka, Passowicz, 2014, p. 176).

These people already play key roles in culture, business, society, economics and politics, and will continue playing them in the future. This generation is heavily dependent on information and communication technologies. The way in which they make friends, lead their social lives and buy things is conditioned by the time in which they grew up. That is why they are called "children of the technological revolution" (Bergh, Behrer, 2012, p. 20).

Generation Y's growing up in the digital era had an enormous impact on their way of thinking. The prevalence of technology presented them with significant challenges relating to an excess of information bombarding them from all directions. It is difficult to maintain a balance between the two worlds: the real and the virtual. It is a fact that Generation Y members are excellent at coping with those aspects. "It seems that they will never be tired of new technological developments, and their talent for anything digital is amazing" (Tapsott, 2010, p. 51). Today people no longer directly experience reality, everything reaches them through the media. More and more activities are shifting to the virtual world. "What is real is what is happening on the TV or computer screen" (ibid., p. 51). "Virtual life is so attractive to some people that it becomes their primary life. They create their own, closed world in cyberspace, limited to the closest living space containing their kitchen, bed and computer. When they are away from it, they feel uneasy and they regard time spent in a different way as wasted" (Andrzejewska, 2012, p. 171).

The virtual world offers an opportunity to freely create one's image depending on one's needs. It allows users to hide what they do not want to show in social networks (vices, complexes, problems) and makes it easier to present and emphasise virtues and strengths. Those who are timid in the real world may be talkative and sociable in cyberspace and certain users cheat a little due to their wanting to appear blameless and hide their faults (Trejderowski, 2013, pp. 61–62).

As Józef Bednarek says: “For many people cyberspace has become part of everyday life. We are in cyberspace when we read electronic correspondence or when we use the web to book aeroplane tickets. It is in cyberspace that we can talk, exchange opinions and create an imaginary being. We can also build new kinds of communities – virtual ones – to which we belong together with people from all over the world” (Bednarek, 2014, p. 22). It is indisputable that communication requires less and less time, thus the majority of everyday life processes are organised around the web.

Although Generation Y representatives are active and do many things for other people, they can also act for selfish reasons. They function like a computer – immediately. They are accustomed to quick responses: having entered a specific phrase into a web browser they want an immediate result and they expect the same in real life. Each activity requires other people’s immediate response and sometimes waiting too long causes frustration (Bendyk, 2004, p. 30). That is why Generation Y members quickly get bored and expect to be rewarded as soon as they obtain a result. They feel an enormous need for speed, and they want to live their life to the full. They know perfectly well that in today’s world the sky is the limit. However, “unlike previous generations, Generation Y does not consider work or a career as the most important things in life. In turn, their essential values include self-development, social and civic consciousness, as well as good relations with the people around them (parents, friends)” (Bergh, Behrer, 2012, p. 8).

Freedom is a notion Generation Y members consider important and identify with. They understand it as being free to do anything and being free to do nothing. They want to have a choice in every aspect of their functioning. They decide whether they are active during the daytime or at night, they live in a dream world, yet at the same time they want to be effective. “The freedom of the Internet and expressing views online is just as important as the ”Solidarity” movement, symbolising a fight for freedom of speech, was vital for previous generations” (Bergh, Behrer, 2012, p. 8). Modern technology makes it possible to break the mould. Young people strive to be free in their choice of work, way of life, place of residence or self-expression – "they cannot live without a choice just like they cannot live without air" (Tapsott, 2010, p. 85).

Generation Y is marked by an older age of maturity (up to about 30). Representatives of this generation extend their period of study and postpone marriage. They are their parents' dependants for longer periods of time, as they wish to live their life to the full as long as possible and extend their youth.

The way in which they were brought up is one of the reasons for this. The majority of Generation Y representatives grew up enjoying a high standard of living, as their parents were more mature and better educated. Adults would take account of their children's opinions and allow them to make quite a number of decisions. They also devoted much more time and attention to them than previous generations, and by making sure they had future opportunities they made them the most important family members. Mutual acceptance and tolerance replaced strict discipline.

Today, parents are willing to talk and negotiate, trying to avoid conflict, mutiny or resistance. Even two thirds of parents ask their child's opinion as to where the family should spend their holidays (Bergh, Behrer, 2012, pp. 22–27). Such a model of parenting makes Generation Y representatives more cynical and critical. It is also more difficult to surprise them.

Generation Y did not have the kind of childhood previous generations had had. Their leisure time was dominated by activities online, which is why they are often also called the "Uncle Google and Auntie Wiki Generation". Computer games and a choice of a dozen or so TV channels for children prevented them from exercising their brains by being involved in creative play.

At the moment, we are dealing with Generation Z, otherwise known as Tweens or Generation C (also GenC) – "connected to the web" (Zajada, 2014, p. 61). Generation Z are people born after 1990 (although some experts set 1995 as the starting year of birth). They are sometimes referred to as "digital natives", Generation M (for multitasking) or the Net Generation. They are the children of today's 40-year-olds, that is of those who were able to take advantage of the opportunities brought about by the transformation of the political system. Owing to this, Generation Z representatives have been given a good education, they are affluent, open to the world and have the opportunity to have a successful career. However, it is also – to a large extent – a generation of egocentric only children. They are accustomed to a nice and easy life. They find it more difficult to establish durable relationships and they are marked by a growing absence of empathy.

Generation Z members are now experiencing their youth. Their adolescence coincides with the most intensive development of new information and communication technologies. They were born at a time of economic instability full of dangers (such as terrorist attacks, violence in society, addictions, cybercrime). Despite being aware of these threats, Generation Z is marked by optimism, idealism, diversity, ambitions, creativity and innovativeness. They draw views and ideas from many sources. Some characteristics were inherited from the previous generation and some – from earlier sources. They are able to think about global problems as well as global possbilities.

This is a generation of many opportunities and, at the same time, since the end of WW2 there has been no generation so divided from the cultural, economic and mental perspective. Dorota Kubacka-Jasiecka and Piotr Passowicz emphasise that this is “a generation raised by the Internet in a world of illusions, [which] in the real world is forced to be confronted with modern society openly divided in terms of finance, wealth, prestige and politics” (Kubacka-Jasiecka, Passowicz, 2014, p. 175). Their birth coincided with a time when the Internet and new technologies were booming, owing to which they are familiar with them from early childhood. Therefore, they are capable users of digital media. This generation has achieved “a high level of competence relating to making use of technology” (Zajada, 2014, p. 61). Its members believe that they are able to influence the future and change it. Their capable use of information and communication technologies has also affected their real life. They have transferred terms previously used in digital media to the real world. In conversation, they use abbreviations like “CU”, “G2g” or “4U”, and they display a strong need for peer acceptance and unity with a group. It can be said that peers have a strong influence on the shaping of attitudes and behaviours.

New technological developments are an immanent part of these young people’s lives. They move proficiently in the virtual world. Various electronic gadgets are their indispensable attributes. They do not know a world without smartphones, tablets or the Internet. As they were born into a digital world, they cannot remember TV sets without remote control units or phones without touchscreens. Whereas adults' entry into the digital world was gradual, Generation Z was raised submerged in this environment.

In the case of this generation, real life and face-to-face interactions are replaced with virtual contact. Therefore, it can be concluded that for its members it is, above all, that which is online that matters. They live in a virtual community where they meet people with similar passions and interests. They are not afraid to work remotely, operate complicated machinery and IT programmes. In their case, reality does not need to be tangible. They perform several tasks at once – they study while listening to music, sending and receiving text messages and looking at a computer screen. They find it difficult to focus on one task, they become distracted. Their world is a compilation of hundreds of pieces of a puzzle which they are perfectly able to put together. They move in a maze of various applications and are bombarded with messages. They treat the digital world like the air they breathe from the moment they wake up.

Apart from benefits, using the resources of digital reality can bring quite a number of threats, including those which are still unknown and unnamed, especially in the field of making choices. The fading of the boundary between the real and the virtual is a worrying phenomenon. Bronisław Siemienicki emphasises the fact that "the immersion of contemporary civilisation in media favours an increasingly stronger correlation of our behaviour with the virtual world" (Siemieniecki, 2002, p. 43). Therefore, when analysing young people's time spent in cyberspace, we have to agree with Marta Wrońska, who says: "Unfortunately, permanent dwelling in the media space often makes [young people] cross out face-to-face meetings from their daily agenda. They begin to enter various virtual worlds where their relationships become superficial, invisible, non-spatial and non-temporal. The boundary between the real and virtual world is fading and virtual space is becoming their real one. Drifting away from reality, they risk immersion – becoming submerged in a world difficult to escape, all the more so that it is a place where they can construct their life outside the control of adults" (Wrońska, 2015, p. 71). We may add that this can lead to the inability to establish stronger social ties in the real world. Maciej Tanaś emphasised the fact that "the world of media leaves a profound mark on the child's mind. Today's generation is growing in a media environment, unlike previous generations. This mark is indelible as media not only pass information, but also stir up emotions, shape imagination, generate new desires and dreams, mixing the hierarchy of values and fulfilling tasks which are only sometimes consistent with educators' and teachers' expectations" (Tanaś, 2007b, p. 198). That is why nowadays great importance is attached not only to media-based education, but also to media education, which – according to the author – should result in "developing people's adequate approach to the world of media and virtual reality and their understanding of the place of the media and their relation to the real world, shaping people's convictions and attitudes, their system and hierarchy of values, their purpose in life, as well as relationships with other people and a humanistic attitude towards them" (ibid., p. 202).

In light of those thoughts, the following view of Anthony Giddens seems reasonable: "Modernity is inherently globalising, and the unsettling consequences of this phenomenon combine with the circularity of its reflexive character, forming a universe of events in which risk and hazard take on a novel character" (Giddens, 2008, p. 125). In turn, Janusz Morbitzer says that "each technology, as well as each culture, idea and person must find an appropriately prepared environment to reveal their full potential. The problem is that technological development is always ahead of cultural and social development" (Morbitzer, 2013, p. 11). These reflections give rise to a kay question: to what extent have Generation Z members been prepared by previous generations to avail themselves of the benefits of new technologies in a way that is useful for themselves and for those who will come after them?

Generation Z members have only just entered their adulthood and the labour market. That is why research into their expectations towards life and employment is at an initial stage. However, it is already said that this generation will exert a strong influence on the surrounding world, will revolutionise and modernise our existing reality and, perhaps, change it on an unprecedented scale.

Determinants of establishing relationships in adolescence

Relationships with other people, especially peers, are very important in adolescence. Social contact and good relations with their environment enable young people to behave properly and cope with stress, as well as prevent depression and other mental disorders. Having friends makes people happy in the same way as being aware that support will be available in crisis situations. Young people need acceptance and want to be members of their community. Meeting this need strengthens their self-esteem and allows them to acquire and practice various social competences. This is why they are usually happy and willing to meet new people and establish ties. However, interpersonal relationships providing ample opportunities for action require interaction with other people, awareness of current norms and rules and of one's own position in the community.

During the special and complex period of adolescence young people undergo many rapid changes. New relationship models emerge, the number of social and personal experiences rapidly increases and competences are developed. There are also immense changes linked to building a sense of personal and social identity. Adolescence is the last period of intense human development. When it ends, we are adults, mature and independent, and our lives become relatively stable from the biological and mental perspective.

Young people frequently fear external judgement and criticism, they are afraid to speak freely, so they withdraw. Things like complexes, shame, bad experiences or negative attitudes are barriers hindering contacts with other people. Here, the digital world comes to the rescue – it is possible to spend long hours there and overcome those limitations, rendering interpersonal interactions much easier. Using the Internet, young people can "manage impressions" – create their own "selective ego". This is especially applicable to young users of social networks. As Adam Andrzejewski says: "The way in which we present ourselves there, the kinds of content we share and, in particular, how we are judged by other users, who do not necessarily have to be our real-life friends, has a specific impact on the fundamental components of identity" (Andrzejewski, 2018a, p. 22).

The era of global access to information and communication technologies enables people-to-people contacts to spread rapidly. They create a network of various ties. The development of technology, in particular of the Internet, was instrumental in the mediatisation of interpersonal communication, thus influencing the creation of social relations and ties. The web is a form of media where communication is the core and information is the content (Goban-Klas, 2005, p. 2). However, it should be emphasised that the virtual world facilitates not only interpersonal communication, but also the establishment of relationships (acquaintance, companionship, friendship or even love). According to Janusz Morbitzer, the contemporary global world, with its plethora of various interactions and interdependencies, is becoming more and more complex and difficult to understand (Morbitzer, 2014, pp. 193–194). It is in this space of truth and falsehood that people look for closeness and engage both in incidental and very intimate relationships.

According to Maciej Tanaś: "The social and pedagogical dimension of modern information and communication technologies emerges regardless of the directions and ways of exploring them. When reflecting on the consequences of technological development and the media civilisation thus constructed, one must not underestimate its creator and the consumer, who is too often manipulated and almost defenceless. Digital media have become a factor determining not only social, civilisational and cultural transformation, but also (directly or indirectly) almost everyone's fate, including – which is of particular importance to educators – the lifestyle, social relations and types of cognitive, creative and even playful activity of children and young people" (Tanaś, 2015, p. 11). Sylwia Galanciak emphasises that "living in a dynamically transforming world makes it difficult to notice the continuity and logic of its changes which – from the perspective of the user – may seem more like a radical break from the existing order, fully deserving the name of a revolution" (Galanciak, 2015, p. 247). Therefore, educators are faced with Bogusław Śliwerski's fundamental question: "How is the virtual world experienced and which of its aspects affect our children?" (Śliwerski, 2016, p. 30).

Communication in the virtual world as a determinant of young people's relationships

When analysing the issues of virtual communication and its determinants in respect of the establishment of relationships by young people, we should emphasise that "the development of information and communication technologies has expanded possible personal contacts and provided an attractive communication tool enabling the establishment of new contacts and their maintenance without respecting territorial, and even time constraints" (Tanaś, 2016a, p. 6).

Following this thought, Adam Andrzejewski says that: "Along with the development of contemporary information and communication technologies, the web becomes a medium fulfilling the needs of interpersonal communication. E-mails, chats, instant messaging, blogs, discussion forums and social networks are lively virtual platforms where people establish group ties, and where they exchange opinions, thoughts and emotions. Nowadays, the Internet allows users to discuss practically any topic. Users from all over the world participate in various groups and discussion forums, exchange knowledge, information, views and advice concerning the issues they are interested in" (Andrzejewski, 2018b, p. 183).

Interpersonal communication over the Internet is undergoing a major transformation. It can be divided into "indirect and direct, depending on whether it happens face-to-face or involves digital media" (Andrzejewska, 2012, p. 295). "Non-verbal cues, i.e. facial expressions, tone of voice, body orientation, hand movements, way of looking, etc., are the main source of information in direct communication" (Kacprzak, Leppert, 2013, p. 22). It is on their basis that people receive messages sent by their interlocutor and check them against relevant verbal communication. Indirect messages are more difficult to read as there is an additional barrier between two people. "The source of information about a person in not only our conversation with them, but also the way in which they formulate their utterances" (ibid., p. 23).

Nowadays, face-to-face communication is being replaced by interface-to-interface communication (Szpunar, 2007, p. 96). The former involves close contact between the interlocutors, direct interaction composed of words and gestures, as well as body language, facial expressions, tone of voice and focus on the other person. Non-verbal cues often express more than the words being said as they are emotionally charged, which is natural for everyone.

The latter type of communication deprives interlocutors of their naturalness, people as such become unnecessary and interacting with a machine comes to the fore (Wasylewicz, 2012, p. 121). Emoticons, font size and descriptions of users' movements, behaviours and reactions aid virtual interaction. Webcam communication is becoming more and more widespread. Interlocutors can see each other and, although they cannot touch each other, they see the reactions of the other person and talk to them face to face. "The absence of non-verbal communication has its benefits, as it makes somebody's looks, status or gender less important. Participants in online communication are less likely to label people or use attribution to explain the behaviour of others" (Branicki, 2013, p. 168). Therefore, it is the frequency of web presence and communication, ways of formulating messages, views and interests of a recent virtual world acquaintance that are important, and not their looks.

Another advantage of virtual communication is that it offers easy ways of establishing contact. The lifestyle of people today (including young people) is marked by haste, lack of time, insecurity and many inhibitions. It is more and more difficult to establish relationships, let alone maintain them. The virtual world removes those barriers and makes it possible to search for and meet people at any time. It can happen on the way to school, during a break at work or a rest, or even immediately after waking up in the morning.

Let us, then, explain the operation of the mechanisms that enable today's wide social contacts and take a closer look at the characteristics of virtual communication. Bogdan Zeler and Urszula Żydek-Bednarczuk list the following characteristics of online communication:

- → Virtual space has no limits. Interactions on the web know no territorial or time constraints, which makes it possible to communicate and maintain relationships with people all over the world.
- → Synchronous and asynchronous activities. Virtual communication has no time constraints, which enables immediate communication in real time (synchronously). It is also possible to send messages, which will be read by their recipient a bit later – dialogue participants do not have to be simultaneously present when this happens (asynchronously).
- → Virtual communication is bodiless. Text, as well as sound and image, became its main media. The use of webcams is becoming more and more frequent, which allows people to see and hear their interlocutor and enables them to communicate using gestures, facial expressions and body language. However, all these components of virtual communication do not include physical contact, which is only possible when communicating face to face.
- → Virtual communication guarantees anonymity. When online, users very often "create" themselves as they want to be because they

are able to withhold true information about themselves. This may lead to falsifying their identity, but also to passing themselves off as somebody else.

- The web enables people to change their identity. Users creating their profile may easily go beyond the point where personality disorders start. This results from excessive involvement in creating an image of oneself, different from the real one, for the needs of the virtual world, and from excessive involvement in social networks (Zeler, Żydek-Bednarczuk, 2009, pp. 86–87).

Anna Słysz and Beata Arcimowicz emphasise that virtual contact satisfies the need for support (Słysz, Arcimowicz, 2009, p. 30), which is indispensable to people at various points in their life. The Internet provides many opportunities in this respect.

Subject literature lists three basic types of support: emotional, informational and instrumental. (Sęk, 2004, p. 11). Emotional support may be obtained mainly in forums dealing with particular issues (for example diseases). Apart from offering comfort, users establish private relationships and conduct conversations during which they can confide in others. However, this support is not accompanied by non-verbal gestures – such as hugging or holding one's hand – which are very helpful in difficult times. They are sometimes replaced by emoticons or words. People looking for emotional support on the web frequently lack the courage to tell those in the real world that they need help, that they want to talk to someone and be listened to – they find it easier to open up to someone whom they cannot see, but can only imagine. Providing emotional support creates bonds between Internet users. They maintain contact because of the mutual interest in each other's problems and the readiness to provide comfort. With time, some such relationships may turn into friendship.

Informational support means the exchange of information which is useful in a difficult situation and offers ways to solve it. The source of informational support is someone who has already successfully coped with a situation similar to that of the other person. The Internet offers its users many opportunities to provide mutual informational support. Almost all everyday problems have their solutions posted online. The same goes for feedback concerning products and services. The absence of any territorial or time constraints makes it possible to find those who are in a similar situation, establish contact with them and share the ways in which a particular problem may be remedied. However, it is to be borne in mind that information found on the Internet is not always reliable and true, and that feedback may prove crypto advertising or a subjective view expressed on the basis of personal experiences not actually related to the problem.

Instrumental support consists in providing a with a ready-made instruction telling users what to do in a specific situation. Users look for advice and information concerning a given matter and that is why they visit specific forums, ask questions and visit web pages with contents relating to the issue.

Apart from the need for support, virtual friends also satisfy other needs relating to contact with people, acceptance and respect (Słysz, Arcimowicz, 2009, p. 45). Therefore, it can be said that interaction made possible by the web is only second-best to the real thing. Nowadays, when conversation is replaced by keystrokes and emoticons supplant emotions, virtual acquaintances do not necessarily guarantee human contact, although they require time and energy. Acceptance and respect provided by online communities can be a mere illusion, as people present themselves in the way they want others to see them. It is in this context that the view expressed by Adam Andrzejewski is particularly significant. He says that "specific discussion groups active online may have psychological influence on users to shape their models of behaviour in any way they want" (Andrzejewski, 2018b, p. 185). He then goes on to add that: "It is important to have a wide-ranging discussion relating to the matter of online forums of a destructive nature, more and more frequently created and used by very young people" (ibid.).

The virtual world as a place where closer relationships – friendships, as well as partner and intimate relationships – are initiated

Establishment and maintaining of social relations on the Internet is rapidly replacing traditional forms and places associated with meeting new people and socialising – housing estate playgrounds, meetings with friends and face-to-face conversations. It is, however, worth mentioning that some virtual relationships transferred to the real world may be the start of friendships and, as such, continue to develop offline.

Relationships established in cyberspace may later evolve in various ways – they can become permanent or ephemeral and be established slowly or quickly, depending on those involved in them.

Apart from family ties, most people consider friendships and partner relationships the most important interpersonal ties in their life. Everyone needs to be close to someone on whom they can rely regardless of time, place and circumstances. This is particularly important for young people. Establishing relationships over the Internet has become very convenient and easy. Quite a lot of people do not want to waste time and energy looking for those whose perception of the world is similar to theirs. It is in such situations that the Internet proves useful – it is enough to turn on the computer or smartphone and go to a place (chat room, instant messaging system, social network, discussion forum, blog) where we can meet future friends – conversation partners with whom we may openly share our thoughts and talk about our problems.

A friend is defined as someone who is emotionally close and plays an important role in someone's life. A confidant, advisor and companion providing support in many real-life situations. "Friendship is an interaction which is completely voluntary, spontaneous, subjectively experienced and felt, one which escapes any normative definitions and logical laws. That is because each relationship of two people called friends is based on principles and expectations known to them only, as well as on satisfaction derived from this relationship" (Szewczuk, 1998, p. 498).

Friendships made in the real world are often exposed to adversities. Friends want to spend all of their time with each other, which is by no means simple. This kind of relationship depends on external circumstances and often involves the participation of third persons. It is also influenced by the environment in which the friends live and the way in which they were brought up. In turn, "friendships established in cyberspace are compensatory in the case of those who – due to their fears – have problems with establishing friendships in the real world" (Branicki, 2013, p. 168). Cyberspace offers them a sense of anonymity, which boosts self-confidence. It also allows users to conceal what they are ashamed of. "However, in order for [users'] interactions to be fuller, virtual meetings often need continuation in reality, 'a real equivalent', which allows for a physical meeting and direct contact" (Stachura, 2006, p. 68). At this point relationships undergo devirtualisation, that is a conscious substitution of virtual contact for real contact (Barani, 2009, p. 113). Transferring virtual contact to the real world does not mean that the relevant relationship will not be continued online. There is no doubt, however, that a relationship transferred to the real world enters a higher level – people met face to face are more real, authentic and trustworthy.

Contacts most often transferred to the real world result from a certain kind of partner relationships. Inasmuch as remote friendship is accepted, the maintenance of a remote partner relationship is difficult and is usually a short-term solution. This is due to the fact that partner relationships are based on the closeness of two people, so direct physical contact is very important.

Young people wishing to find a partner more and more frequently use dating sites. This is a good solution for shy people who, in the real world, would not have the courage to invite someone met by chance to have a coffee or go for a walk. The computer screen barrier makes them open up to others easier and faster – sometimes they do not even realise they have started confiding in a person they know nothing about. This kind of relationship takes the form of intimate conversation based on liking and trusting the other person, that is on conditions indispensable for lasting relationships (Kacprzak, Leppert, 2013, p. 44). This contact can become closer as we use the Internet practically non-stop – on receiving a message from somebody met online we immediately get a notification so we can reply at once, as if we were talking in real time. Virtual relationships may turn into real or even partner ones which can last for the rest of our lives.

People looking for life partners often want to transfer their relationships to the real world. This makes it possible to get to know the person as they are and not as they want to appear. It is also possible to check whether the partners have bonded and whether they have feelings for each other. "Reasons for this speedy development of events may include the need to see whether the partners will hit it off, the desire to check more profiles as soon as possible if the relationship with that partner was to be unsuccessful, a lack of trust in information included in the user profile or the need to check who the profile really conceals" (Whitty, Carr, 2007, pp. 199–201). Devirtualising such a relationship allows us to see who the person met online really is. It saves us time when the relationship proves meaningless. However, transferring relationships to the real world is often impossible or highly unlikely, for example when those involved live halfway across the world from each other, are not independent or lack confidence and fear that they will no longer be attractive or interesting for the other person in a face-to-face meeting.

Some people in Poland continue to mistrust online relationships, but there is also a growing number of those who use the Internet to find their "other half". Some of them take time to turn their intentions into positive action – they are reluctant to post their photograph on a dating site, fearing that their family or friends would not accept people met in this manner. However, as the Internet is becoming a widespread tool for meeting new people, soon saying in public that someone met their partner online will be nothing extraordinary. With teenagers this may already be the case – they treat cyberspace as their natural environment, in which they meet new people and establish partner relationships with them.

Dating sites are intended to help people find a life partner. "E-dating is just as popular among inhabitants of big cities as among those who live in villages. Thanks to cyberspace, people can meet whoever they want, wherever they want, at any time of day or night. Moreover, the Internet guarantees a sense of anonymity, which removes many inhibitions, making people feel safe and bold. Personal questions are more easily asked in cyberspace, the same applies to imposing requirements or flirting. It is also much easier to say: 'I don't want to see you anymore'" (Witak [online], 8.10.2018). "Online flirting (cyberflirting) is a specific form of interaction, which should be considered separately from flirting in the real world. When exploring the exchange of text messages alone, it is obvious that it does not contain any signals characteristic of flirting in the real world" (Whitty, Carr, 2009, p. 84). Online flirting may be a form of entertainment or satisfy the need to be in a relationship. But above all, it is an opportunity to find true love.

"Online affairs provide an opportunity for low-risk relationships and excitement. The lesser degree of risk and moral criticism associated with such contacts also enables the participants to avoid sadness in the short term and having their heart broken in the long. The presence of many attractive online partners increases the discomfort of doing nothing about an unsatisfactory offline relationship" (Ben-Ze'ev, 2005, pp. 111–112). Just how intense online affairs can be is reflected in the attitudes of young users of dating sites who have been in such relationships. “We hear people say more and more often, especially young people, that they met a wonderful person on the Internet, in a discussion forum, during a chat or within something called free online dating. Some of them are inclined to say – as early as after the first conversation – that this is love and they want to be in a relationship with that person” (Bartoszewska [online], access: 12.10.2018).

“Love at first chat is consistent with the 'attractiveness halo', i.e. attributing additional positive characteristics to somebody possessing a particular good quality. It is like falling in love with a perfect stranger – we do not have all the required information, but we fill the gaps by means of idealisation” (Ben-Ze’ev, 2005, pp. 205–206). Aiz Ansari says that “online dating is like another job requiring the knowledge and skills that few possess” (Ansari, 2016, p. 108).

The reasons why people log into dating sites deserve consideration. Poland lacks such analyses (especially in relation to adolescents), yet we can use American research on this issue, conducted by Monica T. Whitty. According to her, people create profiles on dating sites because:

- they count on establishing a long-term relationship – 91% of respondents admitted to this;
- dating sites are an alternative way to meet a partner – this was said by over 50% of respondents;
- dating sites allow people to look for a partner when they are reluctant to use other (more traditional) methods;
- no preparation or leaving home is necessary;
- people feel more secure meeting someone from the comfort of their own home, although they are generally reluctant to let strangers into their home;
- casual relationships and affairs are possible (Whitty, Carr, 2009, p. 196).

There are lots of sites of this nature in cyberspace. It would seem that the users are adults. However, there are many sites intended for teenagers, for example poszkole.pl, mates.pl, milosnykontakt.pl.

The creators of teenage dating sites warn users that the minimum age for being able to add a profile is 13. However, in practice this requirement is disregarded. It happens that not only much younger people use those services, but also those who are very mature.

Going through the content, we can find many photographs of very young persons, scantily dressed and puckering up. Users award such photographs the highest number of stars. There are certain doubts and questions arising in relation to such young users looking for friends on the Internet.

When analysing the issue of dating sites, it is impossible not to mention Tinder, a location-based dating application very popular among Internet users. It was created at the end of 2012 by Sean Rad, Justin Mateen and Jonathan Badeen, who were studying at the University of South Carolina. This application is available in 24 language versions and enables people to look for an ideal sexual partner in their immediate vicinity. It can be called “virtual speed dating”. The application is very easy to use. When building a user profile, people upload their photographs, select the area in which they want to look for a partner, and indicate the gender and age of someone they are looking for. Photographs ranging from subtle to bold appear at once. Viewing someone’s profile provides detailed information about that person (for example their height or bra size). That is how partners meeting our requirements can be selected (also those for sex). When a user “likes” a specific profile, they wait for the other person’s response. If that person is also interested, a chat opens where they can start a conversation. Those who are less patient can immediately agree to meet in the real world.

The popularity of Tinder is due to the culture of convenience consumption where young people in particular have a strong urge to fulfil their needs as soon as possible, without unnecessary postponing and unpleasant tension. The way in which virtual relationships are transferred to the real world depends solely on users’ will, preference and attitude. The Internet may break barriers and push towards previously unacceptable behaviour.

It has to be emphasised that young people are often unaware of the dangers linked to their dating site activity and fall victim to erotic messages. They are often sexually harassed. In light of this, Sylwia Galanciak’s reflection is very much to the point: “Can social ties formed in the real world, developed over dozens or even hundreds of years, be transferred to cyberspace? Enthusiasts will nod, and critics will shake their heads. Regardless of scientific findings and visions presented by prophets of digital progress, the process of transferring attitudes and values continues. Internet users are colonising a new space of activity, heedless of the verdict and diagnoses. Rather than enter into an axiological dispute, let us think how we can turn Internet users into competent people who are aware of the consequences of their actions. How to use the need for social integration to create a better and wiser society is a major challenge faced by the pedagogy of tomorrow" (Galanciak, 2017, p. 29).

Conclusion

The virtual world is an important place of human functioning in numerous areas. It has changed interpersonal contact on an unprecedented scale. It has become part of young people's lives. There, they look not only for information and fun, but also for contact with other people. They establish and maintain closer and more distant relationships. Sometimes they are lucky enough to find someone who will be a permanent and positive element of their life. However, contact with people met in the digital world often proves a negative experience. Young people's attitude to human relationships in cyberspace does not involve deep reflection, which frees them from social supervision and poses various threats.

This is a major challenge faced by educators, who should prepare the youngest generation for the establishment of proper relationships on the Internet. It is also necessary for parents to become involved in this process as it is they who are the most important educators.

Selected aspects of the e-Safety in the Pan-European legislation and in the Polish education system

Rafał Lew-Starowicz

Preventive measures in the e-safety area, including education, have a long history and have been addressed at the Pan European as well as at national level in Poland. Active attitude of public institutions that should support and coordinate, monitorize, and present openness in relation to all stakeholders of the process of ensuring the e-safety of students, is one of the most important determinants of the effectiveness of such policies. It can be assumed that the existing regulations in this area give an opportunity to develop policies for the e-safety of students in the school environment, what is more, they demanding its implementation. The Digital Education Action Plan adopted by the European Commission assumes the prevention of threats on the Internet and in relation to that, one of the basic goal of the education system in Poland is to prepare students for safe and responsible activity online.

Keywords:
educational law
core curriculum
EU directives
conventions of the Council of Europe

Home

The Council of the European Union took action against illegal content on the Internet for the first time in July 1996, as part of a plan to combat racism and xenophobia. In 1997, the Telecommunications Council adopted a resolution on illegal and harmful Internet content. Finally, in January 1999, the European Parliament and the European Council adopted an action plan to promote safer use of the Internet by combating illegal or harmful content on global networks. Pursuant to this document, the Safer Internet Action Plan (SIAP) was launched, which promotes safe use of the Internet and new technologies, including new generations of mobile phones, online games, chatrooms and instant messengers. The programme focuses on:

- improving the security of online resources (through self-regulation of content providers);
- developing filtering and rating systems;
- promoting awareness-raising;
- setting up a network of hotlines for combating illegal content;
- supporting activities (project evaluation, research and publications, conferences, seminars and final evaluation of the programme).

SIAP was initially to run between 1999 and 2002. Ultimately, it was extended to four editions, the final one lasting from 2009 to 2013. One of the main goals of this initiative was to make all users aware of how to avail themselves of the Internet safely and effectively. The programme has resulted in the setting up of national Awareness Points across Europe. These focus on creating an understanding of the threats which users can face online. Presently, the Awareness network spans 19 countries. Their cooperation at a European level is coordinated by INSAFE[1].

SIAP was evaluated in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Interim evaluation of the multi-annual Union programme on protecting children using the Internet and other communication technologies. In 2014, the

[1] bit.ly/31V4tcv [access: 12.04.2018].

Polish government adopted its position towards the communication, wherein it evaluated the national component of the programme.

In the European Commission document it can be read, among others, that: “The programme was run efficiently […]. The programme is also effective according to the evaluation”[2]. The evaluation highlights the programme’s achievements, such as the launch of intervention hotlines, helplines and information centres in most Member States.

A major document at the European Commission level designed to strengthen the protection of minors on the Internet was the European Strategy for a Better Internet for Children. It supports:

→ identification and exchange of best practices between Member States in the areas of formal and informal education on online safety, creation of relevant educational content, and public-private partnerships aimed at reaching out to children, parents, teachers and carers;

→ development of a special module within Europass for digital competence, and improving indicators of the use and impact of ICT in education;

→ benchmarking and testing of parental control tools and relevant services to empower parents and children;

→ research and development to look into how age-rating and content classifications systems could be made interpretable by means of effective parental controls that can deal with a wider range of languages;

→ legislative measures if industry self-regulation fails to deliver[3].

Furthermore, the strategy sets out the responsibilities of the Member States and of the industry regarding the improvement of child safety on the Internet. The European Commission provides financial support both to organisations that associate members of the online industry, for instance the Internet Content Rating Association (ICRA), and to organisations that are active on the

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Interim evaluation of the multi-annual Union programme on protecting children using the Internet and other communication technologies, p. 5, bit.ly/2X9AgI0 [access: 17.07.2018].

[3] Ibid., p. 10, 14.

computer and video games market, for example the Interactive Software Federation of Europe (ISFE).

ICRA has established the RSAC iRating System, designed to filter online content for themes that are potentially harmful to children. In addition, ISFE has developed the Pan European Game Information (PEGI) classification of computer and video games, which is co-funded by the European Commission.

The development of digital media has brought to attention the need for legislation to address specific situations involved in this process. A good example in this respect is Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities. Article 44 therein reads: “The availability of harmful content in audiovisual media services continues to be a concern for legislators, the media industry and parents. There will also be new challenges, especially in connection with new platforms and new products. It is therefore necessary to introduce rules to protect the physical, mental and moral development of minors as well as human dignity in all audiovisual media services, including audiovisual commercial communications”[4].

Further, Article 45 of the Directive emphasises: “Measures taken to protect the physical, mental and moral development of minors and human dignity should be carefully balanced with the fundamental right to freedom of expression as laid down in the Charter on Fundamental Rights of the European Union. The aim of those measures, such as the use of personal identification numbers (PIN codes), filtering systems or labelling, should thus be to ensure an adequate level of protection of the physical, mental and moral development of minors and human dignity, especially with regard to on-demand audiovisual media services”[5]. These provisions encourage Member States to take specific measures to safeguard children against harmful media influence.

Article 25 of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse

[4] http://prawo.vagla.pl/node/7730 [access: 16.01.2019].

[5] Ibid.

and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA[6], specifies the following:

“1. Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.

2. Member States may take measures to block access to web pages containing or disseminating child pornography towards Internet users within their territory. These measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress”[7].

Furthermore, Judgment of the Court of Justice of the European Union of 2 December 1986. – Commission of the European Communities v Kingdom of Belgium – Failure by a Member State to fulfil its obligations – Directive not fully implemented – Case 239/85 ruled: “Each Member State must implement directives in a manner that fully meets the requirement of legal certainty and must consequently transpose their terms into national law as binding provisions”[8]. This is a clear instruction as to how Member States should implement EU directives into their own legislation.

Since 2016, the European Observatory on Infringements of Intellectual Property Rights managed by the European Union Intellectual Property Office (EUIPO) has been operating the IP in Education network. It brings together representatives of Member States who meet regularly to discuss intellectual property rights in education. This includes the existence of issues pertaining to copyright, patents and trademarks in core curricula,

[6] bit.ly/2Rus94X [access: 19.07.2018].

[7] Ibid.

[8] Judgment of the Court of 2 December 1986. – Commission of the European Communities v Kingdom of Belgium – Failure by a Member State to fulfil its obligations – Directive not fully implemented – Case 239/85, no. 7, ECR 1986, p. 1661 (as cited in: *Zapewnienie skuteczności prawu Unii Europejskiej w prawie polskim. Wytyczne polityki legislacyjnej i techniki prawodawczej, Urząd Komitetu Integracji Europejskiej* [*Ensuring the effectiveness of European Union law in Polish law. Guidelines of the Office for Official Publications of the European Communities regarding legislative policy and technique*], Warsaw 2003).

as well as promoting these topics in schools in the field of student entrepreneurship, creativity and innovation skills, in addition to creating educational materials for students and teachers.

As regards European Community legislation in the field of computer and video games, which are becoming an increasingly popular form of entertainment, one should mention two communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The first concerns a European approach to media literacy in the digital environment (COM/2007/0833), wherein media literacy online is, among others, described as "empowering users with tools to critically assess online content"[9]. The second communication of 2008 on the protection of consumers, in particular minors, in respect of the use of video games "calls upon Member States and stakeholders to evaluate the possible negative and positive effects of video games, notably on health"[10].

An important guideline to encourage the industry to adopt agreements on children's and young people's safety (to "self-regulate") is the Directive of 8 June 2000 on electronic commerce, whose Article 16 mentions the need to encourage by Member States and the European Commission "the drawing up of codes of conduct at a Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15", as well as "the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce", and "the drawing up of codes of conduct regarding the protection of minors and human dignity"[11].

As a result of the Social Summit in Göteborg in November 2017, and based on the Council conclusions of December of that year, on 17 January 2018 the European Commission launched new initiatives designed to improve key digital competences and skills

[9] bit.ly/2RzSmPC [access: 26.08.2014].

[10] bit.ly/2QmSrBv [access: 26.08.2014].

[11] bit.ly/2R9k1rv [access: 26.08.2014].

among European citizens, to promote shared values and to raise students' awareness of the functioning of the European Union. One of the initiatives is the Digital Education Action Plan, which lists a series of actions which will be implemented by the European Commission in cooperation with Member States and relevant stakeholders until the end of 2020. The plan focuses on the development of digital competences (skills, knowledge and attitudes) that will be useful for work, will support wider involvement in public life and will encourage effective use of technology in education, as well as use of data and foresight to improve education systems.

The plan has three priorities:

- to make better use of digital technology for teaching and learning;
- to develop digital competences and skills needed in life and work in a time of rapid digital change;
- to improve education through better data analysis and foresight.

The following priority actions were proposed in the action plan:

- Increasing female students' interest in ICT (information and communication technology) and STEM (science, technology, engineering and maths). The European Commission undertakes to work with members of the industry, nongovernmental organisations and education systems to provide girls in primary and secondary education with opportunities to develop digital skills, and to provide role models and authority figures to involve them in studies and professions in these fields on equal terms as boys/men. The Commission will encourage the EU Code Week initiative to organise more coding classes for girls. The Commission will also work with the Digital Skills and Jobs Coalition and other organisations across Europe to promote actions that encourage girls and women to develop their digital skills.
- Supporting the modernisation of fast broadband connections in schools. Responding to the evident digital divide between Member States, the European Commission will work to change this *status quo*, including through the recently launched EU network of Broadband Competence Offices. The Commission will also consider supporting school access to fast Internet connections, in particular through a voucher scheme, with a particular focus on disadvantaged areas.

- Providing a framework for digitally confirmed qualifications and skills. Digital technologies make it possible to increase the credibility and transparency of qualifications and to prevent document fraud. Digitally-signed qualifications are more transferable than paper certificates – they can be stored on several servers or in several institutions. Moreover, they can contain extensive metadata. Such documents make it easier to present qualifications in CVs, on social media and personal websites. The framework for digitally-signed qualifications will ensure greater data consistency and will support quality assurance. It will also foster mobility, cooperation and staff exchange.
- Promoting coding skills. By 2020, the European Commission aims to involve at least 50% of schools in Europe in the EU Code Week. The EU Code Week is a dynamic grassroots initiative seeking to spread coding and other digital skills among Europeans to give them the opportunity to learn basic programming and to understand topics from the fields of hardware, 3D printing, robots, etc. A rudimentary understanding of programming as part of various school subjects will allow students and teachers to develop their competences in using coding to teach and learn digital skills. In order to promote coding skills, the European Commission will work with the Ambassadors of the European Code Week, Member States, the eTwinning network, the Digital Skills and Jobs Coalition and digitalisation leaders, as well as other institutions and organisations.
- Preventing cyberthreats. With an increasingly complex network of online connections, the level of cybersecurity decreases, and there is a greater threat regarding personal data and negative incidents, including financial malpractice, dissemination of fake information, cyberbullying and online radicalisation. Subsequently, everyone must know how to manage their online presence and to protect their accounts, information and devices. It is, therefore, important to teach children critical thinking and media literacy. Regardless of age, all citizens must be digitally aware, in other words, they must know how to avail themselves of the possibilities offered by information technologies whilst understanding cyberthreats and knowing how to deal with them. The European Union will promote education and

awareness-raising activities designed to develop the potential of all citizens in the Community, to help them become active, responsible, critical and safe users of technology.

→ Launching an EU campaign on cyberhygiene and media literacy, including social media, as well as effective ways of preventing threats like cyberbullying, fake information or disturbing content. The campaign will involve all stakeholders and reach out to children, young people, parents and educators[12].

The Council of Europe

The provisions of the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, open for signing on 25 October 2007 in Lanzarote, also highlight the need to design a cooperation framework for protecting children and young people on an international level in light of the development of electronic media. Article 23 of the Convention forbids the solicitation (grooming) of children for sexual purposes through information and communication technologies. At present, this is a serious challenge due to paedophile activity in chatrooms and online forums used by children.

Likewise, the Convention on Cybercrime of the Council of Europe of 23 November 2001, also known as the Budapest Convention, defines new categories of crime involving illegal access to and infringement of IT systems and data, computer fraud and illegal interception of data, as well as producing, making available, distributing, transmitting and procuring child pornography through IT systems. Moreover, in July 2018, the Committee of Ministers to Member States adopted specific guidelines for Member States to respect, protect and fulfil the rights of the child in the digital environment[13]. Of particular significance is the fact that the Convention mentions providing children with access to the digital environment in order to enable them to fully exercise their rights and develop their skills of critical content analysis, as well as protecting them from dangerous content, and protecting their privacy and personal data.

[12] https://bit.ly/2KbHB0e [access: 30.01.2018].

[13] https://bit.ly/2CGPGcc [access: 18.01.2018].

Student safety on the Internet in the Polish education system

The most important documents in the Polish education system which affect the safety of students on the Internet are:

- Act of 14 December 2016, Education Law;
- Act of 7 September 1991 on the system of education;
- Regulation of the Minister of National Education of 14 February 2017 on the core curriculum for preschool education and on the core curriculum for general education in primary school;
- Regulation of the Minister of National Education of 30 January 2018 on the new core curriculum for general education in four-year secondary schools, five-year technical schools and two-year upper secondary vocational schools.

Pursuant to the Education Law, in force as of 2017, a fundamental responsibility of the education system is to teach children and young people about safety on the Internet, and to develop proper attitudes towards threats, including those resulting from the use of information and computer technologies and from extraordinary situations (Article 1 (20)). Another responsibility is the development of students' skills in the efficient use of information and communication technologies (Article 1 (21)). In the past, potential threats to students' safety were natural disasters and extraordinary situations. The Education Law, however, stipulates that "schools and educational institutions which give students access to the Internet are required to undertake measures to protect students from content that may pose a threat to their proper development. In particular, they are required to install and update security software" (Article 27). The provision most often has been interpreted as a requirement to provide in-school measures for using the Internet in class, but the focus is currently shifting to equipping students with knowledge and encouraging appropriate attitudes towards cyberthreats. This means the problem is now dealt with on a much wider scale.

Another very important factor concerning students' safety is training teachers to respond to their concerns. As shown by research, students turn to teachers for help, especially when they experience online problems caused by other people (Kwiatkowska, Dąbrowski, 2012).

Setting the standards of teacher training is the responsibility of the Ministry of Science and Higher Education. These are specified in the Regulation of the Minister of Science and Higher Education of 17 January 2012 on the standards for initial teacher training (Journal of Laws 2012, item 131). The regulation was drafted in consultation with the Minister of National Education, since in-service teacher training lies within this ministry's domain. According to the general learning outcomes listed in the annex to the regulation, "on completing initial teacher training the graduate shall:

- have psychological and pedagogical knowledge that provides them with an understanding of the processes of development, socialisation, education and teaching/learning;
- have detailed knowledge of didactics and methods for teaching activities supported by relevant practice;
- have skills and competences required to fully deliver the school's teaching, educational and care responsibilities, including independent preparation of curricula and their adaptation to students' needs and capabilities;
- demonstrate the ability to learn and improve their own pedagogical skills using modern methods of sourcing, organising and processing information and materials;
- skilfully communicate using various techniques, both with people who are the subjects of their pedagogical activity and with others who contribute to and support the educational process;
- demonstrate ethical sensitivity, empathy, openness and reflectiveness, in addition to prosocial attitudes and a sense of responsibility;
- be practically prepared to carry out professional duties (teaching, education and care) that constitute the role of a teacher"[14].

Article 6 of the Act of 26 January 1982, Teachers' Charter, requires teachers to "educate young people in an atmosphere of love of their homeland, respect for the Constitution of the Republic of Poland, freedom of conscience and respect for all people, and to foster the

[14] Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 17 stycznia 2012 r. w sprawie standardów kształcenia przygotowującego do wykonywania zawodu nauczyciela (Dz.U. 2012, poz. 131) [Regulation of the Minister of Science and Higher Education of 17 January 2012 on the standards for initial teacher training (Journal of Laws 2012, item 131)].

development of their moral and civic attitudes."[15] Ensuring students' safety during their time at school is the responsibility of the school head (Article 39 (1) (3) and 39 (1) (5a) of the Act on the system of education and Article 68 (1) (5) of the Education Law). The principles of safety in school are defined by the Ministry of National Education in consultation with the Ministry of Family, Employment and Social Policy in specific regulations, namely Article 95a of the Act on the education system and Article 125 of the Education Law.[16] The principles of safety and promotion of health in individual schools and educational institutions are defined in their statutes. This is required by the Regulation of the Minister of National Education of 21 May 2001 on general statutes of public preschools and public schools (Journal of Laws 2001, no. 61, item 624). Since 1 September 2017, this has also been directly required by the Education Law (Article 98 (1) (4)).

The competences of parents' councils are stipulated in Article 54 of the Act on the system of education (Articles 83–84 of the Education Law). A council may submit proposals and opinions on all matters regarding the school to the school head and other school bodies, the supervisory authority for pedagogy or the authority running the school. This gives the council the right to express their position on disturbing events involving students and to initiate preventive measures. The competences of parents' councils also include the adoption of measures, in consultation with teachers' councils, such as "school educational and preventive programmes covering all content and activities of an educational nature addressed to students" (Pilich, 2009, p. 548). The Act clearly requires that this is done in partnership with the above-mentioned bodies.

School boards, which take part in "solving school problems", have different powers. They may "request the supervisory authority […] to evaluate a school's operations", for instance regarding its performance on student care and education (Pilich 2009, pp. 530–531). Parents' councils also take part in teacher evaluation and promotion (Articles 6a and 9c of the Teachers' Charter). Furthermore, school superintendents

[15] Ustawa z dnia 26 stycznia 1982 r. – Karta Nauczyciela (Dz.U. 1982, nr 3, poz. 19) [Act of 26 January 1982, Teachers' Charter (Journal of Laws 1982, no. 3, item 19)].

[16] Binding regulation – pursuant to Article 365 of the Act of 15 of December 2016 on regulations introducing the Act, Education Law (Journal of Laws 2017, item 60). The regulation is effective until a new regulation is adopted pursuant to Article 125 of the Education Law.

work with relevant bodies and organisations to prevent social pathology and to support schools in their educational mission (Article 51 (1) (14) of the Education Law).

Regulation of the Minister of National Education of 10 May 2013 amending the regulation on pedagogical supervision[17] lists the requirements to be fulfilled by lower secondary schools with regard to external evaluation. Pursuant to this, a school has to organise learning processes which are conducive to respecting social norms. The processes entail creating an environment in the school that ensures students' physical and mental safety, wherein "relations between all members of the school community shall be based on mutual respect and trust. Students shall work together on projects resulting from the activities of the students' council. Principles of conduct and coexistence in a school or institution shall be accepted and observed by students, school staff and parents"[18]. The regulation also states: "students and parents shall analyse the educational activities of the school or institution, including those designed to eliminate threats and reinforce proper conduct. The effectiveness of the activities shall be evaluated and, if necessary, modified"[19].

Other legislation includes Regulation of the Minister of National Education of 27 August 2015 on pedagogic supervision (Journal of Laws 2015, item 1270) and Regulation of 6 August 2015 on requirements for schools and institutions (Journal of Laws 2015, item 1214). The regulations apply to all stages of education and all types of schools. Cyberthreats are also addressed in the revision of health and safety regulations in public and non-public schools and institutions. New laws are being adapted to the current situation and expectations of the school environment. The existing legislation of 2002[20] does not take into account current needs in the field of students' digital safety in school.

[17] bit.ly/2YkABbh [access: 6.10.2014].

[18] Ibid.

[19] Ibid.

[20] Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz.U.2003, nr 6, poz. 69, ze zm.) [Regulation of the Minister of National Education and Sport of 31 December 2002 on safety and hygiene in public and non-public schools and institutions (Journal of Laws 2003, no. 6, item 69, as amended)] shall be effective until a new regulation is adopted pursuant to Article 125 of the Education Law.

Core curriculum

Pursuant to the provisions of Regulation of the Minister of National Education of 14 February 2017 on the core curriculum for preschool education and the core curriculum for general education in primary school, the latter is to:

- → introduce students to a world of values, including the development of attitudes based on generosity, cooperation, solidarity, altruism, patriotism and respect for tradition; to provide standards of conduct and to build social relationships that foster the students' safe development;
- → to develop critical and logical thinking, reasoning, arguing and deducing skills.

The most important skills developed as part of general education in primary schools include:

- → seeking, organising, critically analysing and using information from various sources;
- → creative problem solving in various fields using ICT methods and tools (including coding) in an informed way.

School should also prepare students for making informed and responsible choices when using online resources, for critical information analysis and for safe interaction in the digital space, including establishing contacts and maintaining relationships with other network users based on mutual respect. To this end, school should make every effort to educate children and young people in a spirit of acceptance of other people.

A school's educational activity is one of the core objectives of the national education policy. Education of the younger generation is a shared responsibility of schools and parents. In their work, educational institutions must take into account the will of parents, as well as that of the state, which is responsible for creating proper conditions for education. A schools' duty is to focus the education process on values that determine the objectives of education and its evaluation criteria. Primarily, value-oriented education involves a subjective approach to students, who, based on the instilled values, are prepared to make good choices and decisions.

The new core curriculum for Computer Science, effective as of 1 September 2017, sets the same general objectives for all education levels. These include the development of social competences, for instance group communication and cooperation (also in virtual environments), participation in and managing group projects, observing the law and safety regulations, respecting privacy of information and data, respecting intellectual property rights, observing communication etiquette and social coexistence standards, as well as assessing technology-related risks and taking these into consideration in order to maintain one's own and other people's safety.

The achievement of the general objectives of the new core curriculum regarding the development of social competences is aided by the widespread use of virtual social environments by students. The responsibility of a Computer Science teacher is to use this fact to develop proper attitudes to communication and groupwork, to demonstrate how to interact safely in these environments and to prepare students to work on team projects.

A new element in the general objectives of the core curriculum is the broadening of the previously functioning safety provision to include observance of the law. This highlights issues such as information confidentiality, data protection, intellectual property, and safe interactions in cyberspace as extremely important in the proper social functioning and development of students.

The interpretation of the general objectives at the subsequent stages of education is broken down into specific requirements. Their description is of a spiral (incremental) character, which means that at each stage students are expected to have the skills they have acquired at previous stages, which are then expanded to include further qualifications.

According to specific requirements for safe interaction in cyberspace for Computer Science taught in grades 1 to 3, students should:

"1) use the technology they have been given access to in compliance with relevant rules;

2) distinguish between desirable and undesirable conduct of other technology users (including students), especially on the Internet;

3) observe the rules of using other people's work and of safety on the Internet"[21].

[21] Regulation of the Minister of National Education of 14 February 2017 on the core curriculum for preschool education and the core curriculum for general education in primary school, including for students with moderate or severe mental disability, for general education in lower secondary vocational school, for general education in special school preparing for employment and for general education in postsecondary school (Journal of Laws 2017, item 356).

Specific requirements for safe interaction in cyberspace for Computer Science taught in grades 4 to 8 stipulate:

“Developing social competence. Students should:

1) take part in problem solving in a team using technology, such as electronic mail, forums, virtual education environments and dedicated education portals;
2) identify and appreciate the advantages of cooperation and problem solving in a team;
3) respect the principle of equality of access to technology and information, including access to computers within the school community;
4) identify occupations and give examples from everyday life where ICT competences are used.

Observing the law and safety rules. Students should:

1) use technology in compliance with the law and relevant principles; observe the principles of work safety and hygiene;
2) acknowledge and respect the right to data and information confidentiality and intellectual property rights;
3) identify risks associated with public access to technology and to information, and describe methods of avoiding them;
4) use antivirus software and be able to protect computers and information against risks”[22].

The implementation of the core curriculum is obligatory for all schools and institutions of the system of education.[23] This process is the responsibility of the school or institution head, who also exercises pedagogical supervision over the teaching staff. The core curriculum in schools and institutions of the system of education is delivered on a continuous basis throughout the school year.

Every year, the Minister of National Education sets out the priorities of the national education policy, including guidelines as to what activities the national authorities expect from schools. An analysis of the successful implementation of the priority “Student safety

[22] Ibid.

[23] The core curriculum content for each learning activity must be included in the curricula taught by teachers.

Home

on the Internet. Responsible use of social media" by in-service teacher training institutions in the school year 2017/2018 shows its impact on the overall training offer for teachers. Between 1 September 2017 and 22 June 2018, more than one thousand training courses focussed on this priority were conducted in all provinces.

In the Mazowieckie Province, 127 courses on cybersafety were run between 1 September 2017 and 31 January 2018. These were attended by 2530 teachers from all types of schools. Courses on "Education problems connected with using new media with a particular focus on cyberbullying" comprised various topics related to students' online activity, including "What do young people really do on the Internet – opportunities and risks", "Individual factors and social involvement in cyberbullying" and "How to make students familiar with new media at school – examples of specific solutions".

During the same period, 31 courses attended by 538 teachers from all types of schools were organised in the Podkarpackie Province. For example, training on "Cyberthreats and safety of children and young people on the Internet" covered the following areas: online tools, classification and effects of cyberthreats and prevention measures, protection of ICT devices, available help, legal protection, and addiction to online pornography.

By the end of January 2018, eight training programmes on cybersafety were conducted in the Zachodniopomorskie voivodeship. Those relating to "How to counteract cyberbullying among students" focussed on the following issues: cybercrime and cyberbullying, how to identify and prevent cyberbullying, how to quickly identify and respond to hate and making friends online, as well as preventive measures and data protection.

In addition, in all provinces trainings were provided on personal data protection and legal aspects of online activity, including copyright and use of free software.

Excerpts from the core curriculum concerning safe and responsible use of computers and the Internet in schools

Early School Education, grades 1–3

In early school education, schools are required to provide access to information sources and modern technology that benefit student development.

Teaching content – specific requirements:

III. Social Education

Students should:

- present themselves and the group they belong to, write down their personal and school address, and their parents' occupation and workplace;
- use personal data only in situations that are safe for them and the people they represent;
- be cautious about using this data in new situations and online.

IV. Natural Science

Knowledge of human life functions, healthcare, safety and rest.

Students should:

- be aware of fake news, for instance in the virtual or public space, and check information, for instance by directing questions at teachers, parents or police officers;
- observe safety rules, and understand and respect time limits when using digital devices, as well as follow the rules of netiquette;
- be aware of how irresponsible use of technology can lead to health problems;
- be aware of the positive impact of technology on everyday life.

VII. Computer Science

Observing legal and safety principles.

Students should:

- use technology they have been given access to in compliance with relevant rules;
- distinguish between desirable and undesirable conduct of other technology users (including students), especially on the Internet;
- observe the rules of using other people's work and of safety on the Internet.

Grades 7–8

Polish

III. Building statements

Elements of rhetoric

Students should:

- identify means of persuasion and manipulation in advertising, and describe their function;
- identify the language manipulation and counter it with rules of language etiquette.

IV. Self-education

Students should:

- use information accurately and with respect of copyright.

Teaching conditions and methods

At the second stage of education, teachers of Polish should above all:

- develop students' ability to independently seek, organise and critically assess information, and to use it for their self-development;
- teach students to adopt active attitudes to life and to take responsibility for their actions.

Citizenship Education

Learning objectives – general requirements:

I. Knowledge and understanding

Students should:

- have a basic understanding of human rights, mass media and selected international affairs.

III. Self-knowledge and identifying and solving problems

Students should:

- identify rights violations in their environment;
- provide arguments for civic attitudes, including responsibility, concern for the common good, and tolerance.

V. Minors and the law

Students should:

- identify behaviours related to physical and emotional abuse, including verbal abuse, self-abuse and abuse towards others; identify people and institutions who they can inform about such situations;
- describe the risks and advantages of using Internet resources;
- identify cyberbullying and explain how to respond to it.

Computer Science

Grades 4–6

V. Observing the law and safety regulations

Students should:

- use technology in compliance with the law and relevant rules;
- observe the principles of work safety and hygiene;
- acknowledge and respect the right to data and information confidentiality and intellectual property rights;
- identify risks associated with public access to technology and information, and describe methods of avoiding them;
- use antivirus software and be able to protect computers and information against risk.

Grades 7–8

V. Respecting the law and safety principles

Students should:

- describe ethical issues associated with using computers and computer networks, for instance safety, digital identity, privacy, intellectual property, and equal access to and sharing of information;
- behave ethically when working with information;
- distinguish between different types of licenses for software and online resources.

Technology Education

IV. Identification of advantages and risks related to technology in the context of integral human development and respect for human dignity

- Identification of technological accomplishments that have contributed to technological advancement, and thus to people's well-being (e.g. easier work, higher living standards, etc.);
- Description of threats existing in modern civilisation and caused by technological progress (e.g. war, terrorism, pollution, threats to physical and mental health, etc.);
- Foreseeing threats caused by various products of technology and technological devices.

Family Education

Learning objectives – general requirements:

VII. Using media, including the Internet, in a selective way ensuring protection against their destructive impact

Teaching contents – specific requirements:

II. Adolescence

Students should:

→ know the potential dangers of adolescence, for example chemical and behavioural addiction, sexual pressure, pornography, cybersex and underage prostitution;

→ identify preventive measures and counteractions.

IV. People and the world of human products

Students should:

→ reflect on intellectual property rights; define plagiarism and formulate a moral evaluation of plagiarism;

→ give examples of right and wrong use of modern information technologies.

Core curriculum for general education in four-year secondary school and five-year secondary technical school

Major skills acquired by students during general education in four-year secondary school and five-year technical secondary school include:

→ efficiency in using modern information and communication technology, including observance of copyright and safe interactions in cyberspace.

Computer Science

V. Observing legal and safety regulations

Students should:

→ explain the role of authentication methods, cryptography and the electronic signature in protecting and accessing information; use good practices in protecting sensitive information (e.g. passwords, PIN codes) and securing operating systems;

→ describe potential harm caused by online piracy to individual persons, specific institutions and society as a whole.

From Internet safety to digital citizenship – practices and perspectives

Janice Richardson

Internet has transformed the face of society, and how people learn and interact within it. During the transition period from the early days of internet to today's almost seamless online-offline society, internet safety has played a crucial role for citizens of all ages. But today the face of society has changed, democracies are challenged, yet education systems tend to churn out more of the same, with internet safety at best no more than an add-on to the curriculum. The chapter highlights some of the key turning points in child online safety and compares internet safety approaches to digital citizenship, and the role of the family, NGOs and industry to that of schools. It examines the competences young people need to successfully cope with digital-related challenges, and some of the models proposed by international organisations to address emerging needs.

Keywords:
digital technology
citizenship
competences
education
internet safety

Introduction

Today young people live in a realm of big data, information overload and the selfie culture. Much of the time, their social life plays out in a vast virtual world where, to be noticed, they have to show themselves as the most extraordinary, the smartest and the best... or the worst. The world has become a global village to the detriment of local communities, with a good many of us placing more focus on our mobile phone than on family members and friends who are sitting right beside us. The art of journalism has been outpaced by a world of "would be" reporters and free-lancers who focus only on the most spectacular topics as, otherwise, their articles will not be published and they will not get paid. The main "information" sources for many young people nowadays are YouTube videos created by other youngsters and dealing, in particular, with delicate topics such as dating, sexuality or make up. Yet how many of these YouTube "gurus" are really driven by sharing reliable information, and how many mould their advice to the interests of advertisers eager to use this powerful channel to reach a generation that shuns traditional media?

In short, the Internet is constantly pushing educators and safety experts – who have spent the last two decades struggling to keep apace but never quite managing it – into unexpected and challenging realms. At last we are beginning to accept that responding to specific Internet challenges is a Sisyphean task, and human rights organisations such as the Council of Europe and UNESCO have gone back to the drawing board to completely revise their approach.

A short history of Internet safety

In the Internet's history, already spanning several dozen years, it is possible to distinguish some interesting stages, important not only from the perspective of users, but also from that of parents, educators and safety specialists. Until the late 1990s, only a privileged few had been able to replace the slow dial-up via modem with broadband access at home. Nevertheless, visionary educators were already looking for ways these powerful information and communication tools could be adopted into the classroom to open up new learning opportunities for all. Children and young people, too, were quick to see the opportunities Internet could offer. Despite the inconvenience of dial-up access, it was not long before browsers such as Mosaic (1993), Netscape Navigator

(1994), and Microsoft Explorer (1995) had turned web surfing into adventurous leisure-time activity.

Although by the year 2000 no more than 5% of the world population had taken their first steps on the Internet[1], things were moving at a much more rapid pace in certain European countries. In the United Kingdom, for example, a survey carried out at the turn of the millennium showed that 75% of children aged 7–16 used the Internet, compared to just 38% of the adult population, and that 36% of homes with children had Internet access (Wigley, Clarke, 2000).

The increasing number of children and young people gaining access to the Internet heralded growing public fear. In effect, the European Commission introduced its first Internet Action Plan, which ran from 1999 to 2002. This has been followed by 2- or 3-year programmes from the European Commission ever since, with the initial Internet Action Plan morphing into Safer Internet and then Safer Internet Plus programmes, until the launch of the European Strategy for a Better Internet for Kids in 2012. The European Union has grown and so has the reach of its Internet safety programme – from 15 countries in 2004, when the Commission set up the European Safer Internet Network (Insafe), to a total of 28 EU countries plus Iceland, Norway and Russia. In this way, the European Union was able to support national Safer Internet Centres through funding and training, as well as promoting the sharing of tools and good practice.

Over this period, the global web has brought an exponential growth of challenges. At first, the main online safety focus was on protecting children from harmful and illegal content, as the number of publicly accessible websites rapidly increased. In 2001, the number of registered Internet domain names – giving an approximate idea of the number of websites in existence – stood at 10 million, by early 2002 it had already reached 20 million. The milestone of 1 billion websites was reached in September 2014, and today there are c. 1.7 billion, though not all of them are active[2]. Despite the fact that building a website was beyond the tech skills of most children and young people, blogs offered an exciting new way for them to extend their social circle and express

[1] These are other recent Internet-related statistics are available at bit.ly/3boOWVT [access: 25.03.2019].

[2] These statistics are available on the website: bit.ly/2LlpWUZ [access: 25.03.2019].

their opinions publicly. Today, they can be seen as a forerunner to social networks. The term “Web 2.0” was coined to describe this more open, social Internet.

From social media to selfies, fake news and more…

With the launch of My Space in 2003, and national social media platforms such as Bebo in the UK and Hyves in the Netherlands shortly after, Internet safety awareness raisers rapidly turned their sights to unwanted and harmful online interactions, adding the issue of “contact” to that of “content”. Both Facebook (created in 2004) and Twitter (launched in 2006), added fuel to the fire for anxious parents and rapidly became the object of interest of organisations dealing with Internet safety. Around the same time, YouTube (2005) offered young people an entirely new way to communicate and share content on a global scale as the graphic nature of the material bridged linguistic differences. Flickr, Tumblr and multiple similar tools sprang up to fill specific social media niches and increased the challenge for educators and families. Copyright became a growing issue on the safer Internet agenda, along with the unintentional sharing of personal data.

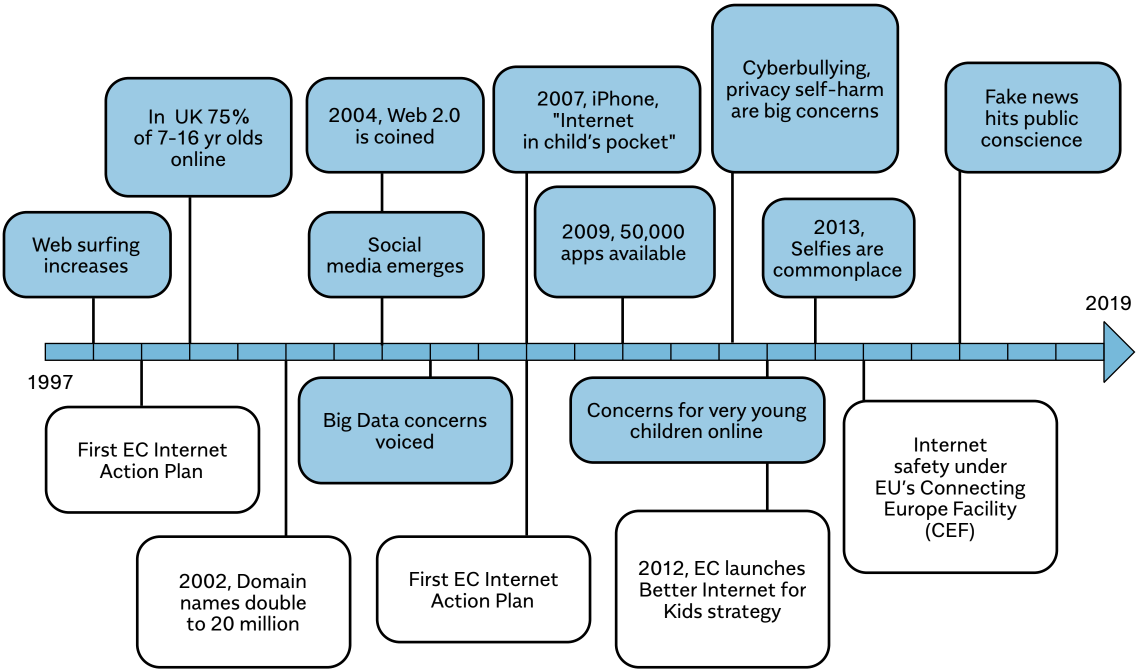
The launch of the iPhone in 2007, which gave children a large extent of freedom, caused the appearance of a great gap in the most carefully devised family and school safety policies. Parental controls and filters were already under-used, especially in non-English speaking countries where the offer was limited and poorly adapted. Overnight, safety tools became of no use as children could freely use the Internet all day, wherever they were. By 2008, 1.4 million iPhones had been sold and a wide range of powerful lower-budget smartphones was already on the market. Just one year later, in 2009, already more than 50,000 apps had been launched, raising new concerns relating to, among others, the submission of personal data and obtaining parental consent. Easy to use and available on most devices, smartphone cameras brought about new challenges in terms of privacy and safety. In 2013, the word “selfie” became the much-coveted *Oxford English Dictionary’s* “Word of the year” (Backer, 2017).

From 2008 or 2009 onwards, as mobile phones and tablets became commonplace in many families, new societal concerns were raised when it was realised that children were taking their first steps on the Internet even before they could walk or talk. At an age where they should be integrating values and attitudes observed in the family home, they were being flung headfirst into a global world where parents and educators had difficulty controlling their every encounter with people and content. Pervasive access to technology in a child's early years is, moreover, associated with delays in the development of their attention, fine motor skills and dexterity, speaking, socialisation, as well as with an increase in the occurrence of aggressive and anti-social behaviour, obesity and tiredness (Aiken, 2016).

One secondary effect of the take up of technology by very young children was that it put paid to the decade-long debate regarding where responsibility of teaching Internet safety should lie – with families or with schools. It also brought about a growing social divide. It affects children in families across all socio-professional categories and, as always, some parents are better able to cope with the challenge than others. A recent study in the United States on 350 children aged 6 months to 4 years living in low-income, minority communities showed that 97% of them had already come into contact with the Internet. The study also showed that 20% of 1-year-olds had their own tablet, 28% of 2-year-olds could navigate a mobile device without help, and by age 4 about three-quarters of the children had their own mobile device (Kabali et al., 2015).

In 2016, sights turned to fake news, profiling, media manipulation and excessive violence. The list is long and growing longer each year. Such serious social challenges go beyond the remit of Internet safety, since they tear at the very fabric of society itself.

Figure 1. Two decades of Internet safety challenges and European responses


Web surfing increases
In UK 75% of 7-16 yr olds online
2004, Web 2.0 is coined
Social media emerges
2007, iPhone, "Internet in child's pocket"
2009, 50,000 apps available
Cyberbullying, privacy self-harm are big concerns
2013, Selfies are commonplace
Fake news hits public conscience
2019
1997
First EC Internet Action Plan
2002, Domain names double to 20 million
Big Data concerns voiced
First EC Internet Action Plan
Concerns for very young children online
2012, EC launches Better Internet for Kids strategy
Internet safety under EU's Connecting Europe Facility (CEF)

Safer Internet Day – a constant in the fast-changing Internet safety arena

Created in Luxembourg in 2003, the Safer Internet Day (SID) concept was first launched by a 14-country EU project called "Safeborders", coordinated from Spain. The idea was to have one day in the year when the public and the media were pushed to reflect on the development of the Internet and its impact on the lives of Europeans. The first Safer Internet Day was held on 6 February 2004 and was celebrated by children and families in 12 European countries (Denmark, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Spain, Sweden, United Kingdom), as well as in Australia[3].

[3] *EU celebrates Safer Internet Day 6 February* (2004). More information: bit.ly/2TZsJsT [access: 20.03.2019].

Now SID is organised annually in more than 140 countries worldwide and is celebrated by more than 50 million people. It is, also, widely propagated on social media – in 2016, more than a billion tweets appeared in relation to it. It has grown from a day to a week in some countries, and even to a month in others (for instance in Russia). It has become an occasion for companies to launch new products, and European[4] and international[5] institutions to inform the public of new initiatives to protect children and their rights online.

Why is Safer Internet Day important? Why is it celebrated so widely? Public interest usually rapidly wanes in awareness campaigns, but this has not been the case with SID. Every year brings a new focus, a sort of turning point in public awareness. A slogan to be used worldwide is annually developed by the European Commission's Insafe network to mark the most important aspects of Internet use by children and adults. Another reason for its continued success is that it has been designed in such a way that the medium is the message. In 2005, for example, an SID blogathon brought together subsequent countries which joined it in accordance with their time zones. From 2008 onwards, key messages have been communicated via video clips, and nowadays social media, among them Facebook and Twitter, are included in the campaign platforms. There has always been a third element, too, which has kept interest in SID alive – its focus on children's rights rather than restrictions and limits, on opportunities rather than on dangers, and on users rather than on tools. In an environment evolving as rapidly as the Internet, such constants are important, and Safer Internet Day has acquired recognition and renown.

The Internet – the tip of the iceberg

The Internet today is a place where about half of the world's population spend, on average, almost two hours each day[6]. With 1.47 billion active

[4] *Project activities: 7th Safer Internet Day* (2010). More information: bit.ly/2UMuB5g [access: 20.03.2019].

[5] *Celebrating 10 years of child online protection* (2018), More information: bit.ly/2VAz4fS [access: 20.03.2019].

[6] Statistics available on the website: bit.ly/2GZCVb7 [access: 20.03.2019].

users per day in 2018[7], Facebook has become an environment with far more "inhabitants" than any single country on Earth.

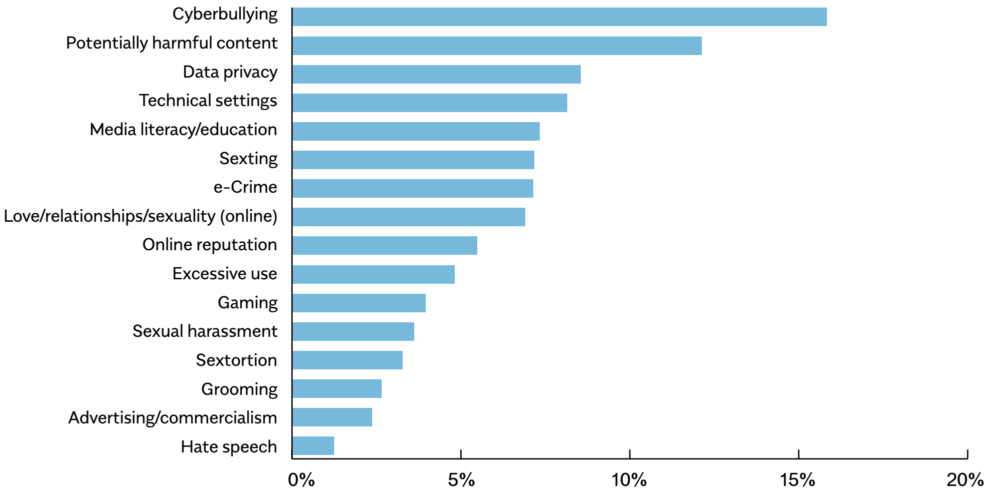
Today the word "Internet" itself has a very different connotation than it did when the term "Internet safety" was first coined. Without realising it, many of us are filling our homes with devices that relay our data in the form of images, text and speech through the Internet to be stored on servers located we simply don't know where. From talking–listening teddy bears to digital baby monitors we place in our children's rooms and web-connected black boxes we have in our cars, we are giving various data to organisations that try to shape our viewing and shopping habits or quantify our insurance risk coverage. If we accept the assumption that Artificial Intelligence defines computer systems that can perform tasks normally requiring people (for example, visual perception, speech recognition, decision-making, and translation between languages), then society is inundated with Artificial Intelligence and the Internet is no more than the tip of an enormous iceberg. To tackle these more complex issues we should be educating children and ourselves in a more holistic, comprehensive way.

When the term "Internet safety" was coined more than two decades ago, main challenges revolved, as stated earlier, around protecting children from harmful and illegal content. Another important issue was to prevent the Internet from becoming a facilitator to the dissemination of child sexual abuse content, and to this end the INHOPE network was set up at the end of the 1990s. The number of challenges has grown exponentially with the advent of social networks, increasingly smaller and more powerful mobile devices, and constantly broadening bandwidth, which resulted in focus being placed on behaviour and opportunities. The European Commission's Safer Internet Network, Insafe, was created with these perspectives in mind. It provided a very necessary means of reducing a costly duplication of actions in various countries by improving the propagation of knowledge and the sharing of experience across European Member States. Until 2012, it also served as a sort of warning system for countries where implementation of new technologies was slower than in others.

[7] Statistics available on the website: bit.ly/2VDI9Qo [access: 20.03.2019].

Helplines have, over the past decade, played an important role in the sphere of safety, providing specialised psychological advice to young people, as well as to their parents and teachers. They were also useful in spotting emerging trends and rising social concerns. Whereas once helplines were called in order to solve more technical issues or to remove content, today they are confronted with problems such as lack of well-being and behavioural issues. Progressively more calls are being received from disoriented youth (nearly 70% according to Insafe statistics from the second quarter of 2018), as compared to a greater percentage of calls from parents, teachers and carers a few years ago. Figure 2 here-below categorises the cases recorded by the Insafe helplines over the quarter mentioned.

Figure 2. Breakdown of Insafe helpline call categories (2nd quarter of 2018)[8]



Based on the fact that over one fourth of all calls related to cyberbullying and potentially harmful content, it seems reasonable to infer that young people are seeking help when there appear symptoms that hide a deeper malaise typical of the deregulation connected with digital technology. Young people's personal data and privacy concerns

[8] Insafe Helpline statistics: helplines.betterInternetforkids.eu [access: 20.03.2019].

have diminished over the past couple of years, indicating that they have probably become more aware of the value of their data and the importance of their digital identity and footprint, and able to handle these issues themselves.

One facet of the work of helpline employees is to confer with their counterparts in other countries and exchange data on the problems they handle, to build a more useful shared knowledge base. This makes it possible to better train national teams, and to prepare them for challenges looming in line with the "fore-warned is fore-armed" approach. Helpline workers are also able to use the information and knowledge they draw from their direct contact with users to negotiate corrective actions with social media platforms and tool providers. The industry has been quick to recognise this as an opportunity to learn more about user needs and to accordingly shape their tools, as well as to protect children and respect their rights. Most of the big social media providers have set up advisory boards and created meeting opportunities not only with helplines, but also with child well-being experts and educators.

A further trend that seems to indicate that the Internet is but the tip of a much larger iceberg is the seemingly greater responsibility that young people themselves are showing in the ways they are supporting each other not just on Internet-related issues, but also in other areas of their lives. For many of them, the Internet has become a platform where they can meet and have their voice heard on all sorts of issues ranging from culture, diversity and environment to banning guns and overturning political parties, as we saw with the Arab Spring. They are also using these new opportunities to become entrepreneurs or creators of applications and tools (e.g. YouTube videos) that are shaping both the digital and the broader world.

Since 2009, within the European Commission's Safer (today known as Better) Internet network, national youth panels have become a sort of advisory board, with several young people from each participating country meeting for a few days every year to give their viewpoint on how to make the Internet, and sometimes more generally Europe and the world, a better place. On Safer Internet Day 2018, a permanent youth Council for Digital Good (CDG) was set up comprising 15 young people aged between 13 and 20 from seven European countries. Its aim is to work with educators, politicians and international bodies in order to integrate the perspective of young people in political debate. Similar councils exist in the United States, the Middle East and Africa. Through these and comparable structures worldwide, policy-makers are beginning to notice and take into account the wishes and needs of young people, though unfortunately it is often only youth from more affluent, multi-lingual backgrounds who get to have their voice heard in this way. Though the Internet is the starting point and communication platform, the impact goes far beyond its realm.

These various trends underscore the constant change and growth of the digital dimension. It also shows the urgent need for schools, families and communities to integrate better adapted concepts of gaining competence and knowledge, as well as of citizenship into their children's education.

Digital citizenship in a borderless world

As the Internet has made its way into every corner of our lives and the borders between online and offline, local and global, continually fade, the unseen facets of this "iceberg" are impacting society in unanticipated ways. A decreasing belief in democracy and the rise of nationalistic attitudes is one example, highlighted in a recent international citizenship survey[9] and visible, among others, in poor participation in national elections. Back in 1996, Jacques Delors, former president of the European Commission, already hinted at some of the deep societal scissions he anticipated, when he wrote: "[...] how can we learn to live together in the 'global village' if we cannot manage to live together in the communities to which we naturally belong – the nation, the region, the city, the village, the neighbourhood?" (Delors et al., 1996).

According to Delors, society can only win out if every one of its members is willing, able and feels sufficiently responsible to participate in and contribute to public life. This also requires a sense of accountability, an element which is fundamental in a society rapidly moving towards blockchain-type technology as an antidote to lack of transparency and trust in the rights held. With such technology, generally described as being decentralised, distributed and open, every individual becomes directly or indirectly responsible for the validity and transparency

[9] International Civic and Citizenship Study (ICCS), implemented in 2016 and subsequent years. More information on the website: iccs.iea.nl/home.html [access: 20.03.2019].

of actions. We have been observing this type of structure for many years now in social media, where the providers create a platform, but it is the users who fill it with content, interact within it and validate it. Cryptocurrencies are a more elaborate, refined example.

Today the blockchain model is making its way into the public sphere, for instance healthcare. It is, thus, worth asking: What about those citizens who lack the basic competences which make it possible to respond to and participate in such processes in an informed way? Are they still masters of their own lives?

Internet safety or digital citizenship, what is the difference?

Although Internet safety once consisted mainly in offering rules and regulations to keep children safe, fortunately it quite rapidly broadened. Today, it also encompasses educational activities aimed at children and young people and dealing with using technology safely and responsibly, and avoiding its pitfalls. The concept is now dealt with by many partners and includes, but is not limited to:

- → tools: filters, timers, firewalls, security software;
- → people: from parents, carers and educators to the users themselves;
- → resources to be used by the people involved;
- → guidance for the industry about the tools and services used on platforms, often referred to as "safety by design";
- → services: helplines to support and advise users in the case of problems, and take into account lessons learned regarding safety by drawing awareness raisers' and educators' attention to them.

There is obviously much overlap between Internet safety and digital citizenship. Whereas safety focuses on protecting children and predicted user practices, approaches and tools, digital citizenship is a bottom-up process that encompasses a wide range of "life-competences" and begins the moment a child is born. Digital citizenship is about the values, attitudes, skills, knowledge and critical analysis, i.e. elements that individuals bring to every aspect of their life, whether on- or offline. It shapes who we are, the way we learn, act and communicate with our immediate circle or community as well as the broader world. It can be interpreted as a framework or a filter which amplifies or enhances the input we receive though all five of our senses. It shapes the way people behave everywhere, and under any circumstances. Competent digital citizens are people who:

→ engage with society and the digital technology that society uses;
→ are active participants in the community in which they live, and have a positive and constructive input in its functioning;
→ continue learning throughout their life, to keep up with the changes taking place around them.

At the heart of digital citizenship is education: at home, in the community, at school and wherever we encounter information and other people.

The role of the family, the role of the school

Despite the efforts of the European Commission (within its Safer Internet and Better Internet programmes), the ministries of education in some countries and many organisations including public institutions and NGOs, Internet safety has never been fully integrated into school curricula. Indeed, since the Internet became part of children's lives we have witnessed an ongoing battle between school and family as to who should be responsible for children's safety online. Whilst the battle continues, NGOs and the industry appear to have stepped into the divide. Yet the question arises: why do educational institutions and trained educators relinquish their responsibility on an issue on which the future of society may depend?

There is a number of reasons schools are being so slow in taking up the gauntlet. The first is related to infrastructure. There is big disparity in access to digital technology in schools across Europe. This is more especially the case in primary schools, where teachers should be helping children develop skills and practices they will carry forward as they get to use the Internet more independently. Nowadays, most children, at least in Europe, have computers or smartphones of their own, and certain countries such as Austria have implemented a Bring Your Own Device policy to fill the gap. However, cybersecurity challenges, visible social inequalities related to the quality of devices children may bring to schools, and teachers' fears about disruption of lessons have proven very difficult to overcome. In certain regions, the industry or government provide schools with equipment, but this is a costly, usually one-off activity and too unsustainable in the long term to be seen as a permanent solution, at least for public educational establishments for younger children.

The second factor is the curriculum. Learning about and with digital technology has, until now, not generally been considered a compulsory subject in elementary education. When it becomes part of the curriculum in secondary school, the focus is usually placed on STEM areas (science, technology, engineering and maths) rather than on preventive and/or citizenship facets. Until digital technology is integrated fully across the curriculum, and ministries of education determine clear definitions as well as requirements, achievement and evaluation guidelines, it seems that only the most enterprising of teachers are ready to tackle the topic of Internet safety. There are many very interesting programmes open to teachers, eTwinning being a good example, but the number of participating schools and teachers remains low.

The third factor contributing to issues of Internet safety not being properly taken up in schools is related to government-approved training as well as teaching resources. Not surprisingly, teachers themselves are often avid consumers of digital products and services, using them for travel, banking, shopping, etc. Usually, however, they are quite wary of applying unproven pedagogical strategies in an area that can have far-reaching effects (and influencing a child's behaviour online is just such an area). This is why schools in many countries have preferred to opt for a policy that limits computer and Internet use outside of specific classroom activities closely approved by the curriculum, and ban mobile phones at school, rather than to undertake lessons on Internet safety. MOOCs, online training webinars and training sessions are available, but until Internet-related topics become an integral part of initial teacher training or compulsory professional development, Internet safety will be off the teaching agenda of most educators. School staff tend to define the school walls as the boundary of their responsibility. What happens in the home is the responsibility of the parents, and what happens between the school and home seems to remain in limbo until the situation becomes so critical either side needs to take action.

Somewhere between the home and the school there are the services of helplines which, as mentioned earlier, are often co-funded in Member

States by the European Commission. Here young people can call, e-mail or open a chat session to obtain advice from psychologists and specialists on the Internet-related issues that trouble them. However, the role of helplines is to provide support and guidance, not to educate, and statistics indicate that teachers and parents use these services as much as, if not more than, children and young people. Helplines could, nevertheless, be a valuable resource for educators since they have information on emerging trends and can help spot vulnerabilities that may otherwise go undetected. Yet in order to be able to undertake this role they would require more funding and appropriate cooperation mechanisms would need to be set up between them and the schools they advise. What is more, Internet safety would have to be included as part of their mandate.

Digital citizenship combines the role of the family and the school, as it is built on broader, more clearly defined competences. The development of many of them has to begin much earlier, before children even begin their school education. Infrastructure becomes superfluous because citizenship competences are the same both on- and offline. Curricula in schools across the European Union should already encompass civic and moral education, though generally no more than 6–8% of the overall curriculum at either primary or secondary school level is devoted to these subjects[10]. Digital citizenship integrates and therefore could replace both these subjects. It is, then, quite conceivable that it could be taken up by schools, providing that the necessary training and resources are made available to teachers.

Digital technology, social-emotional development and behaviour

Some interesting research has been conducted in recent years on how digital technology may be impacting the way we live, learn and interact. In his book *The Shallows* Nicholas Carr (2010) contends that our thoughts, mental processes, and even physical brains are being restructured by technology. He provides empirical findings which show the potential impact of frequent use of digital devices on young brains whose lateral lobe activity becomes over-developed

[10] *Key Data on Education in Europe* (2012), Eurydice/Eurostat, bit.ly/2NdPXJp [access: 25.03.2019].

due to the fast-moving images and sounds that children are exposed to. This appears to be to the detriment of other areas of the brain related to reasoning, metacognition, and the capacity for analysis and critical thinking.

Another researcher, Roman Krznaric (2014), focuses on the importance of empathy as the basis for respecting human rights and social justice. The author presents factors which can explain both what influences young people and their interactions in the virtual and real world.

Preschool and primary school teachers are also voicing concerns about children's frequent use of technology at too early an age (Aiken, 2016). They believe it can be causing them to skip certain important developmental phases and weaken language formation. Attention spans shorten and creativity decreases when children and young people consume far more content than they create. Results of a 2016 study, carried out among children aged 11–14 within the framework of the ENABLE anti-bullying project[11], showed that, possibly due to reduced time of face-to-face social interaction, 40–57% of the representatives of the studied group had difficulty defining negative emotions. Around 25% of the teenagers admitted that they did not know how nor want to help others. The percentage ranges varied considerably between the five European Union countries involved in the project, which requires further analysis to understand the factors behind the figures.

Major social media providers are aware of the social and behavioural changes connected with the platforms they offer. Whilst obviously striving to keep their business models alive, they regularly work alongside safety experts, institutions and governments in self- and co-regulation programmes, trying to ensure that social media have a positive effect on young people. Through such initiatives they have, among others, set up mechanisms to rapidly delete extremism and child sexual abuse content from websites, improved reporting procedures, tightened privacy settings and provided tools to help users control their image online. Facebook and Google, for example, have worked with leading scientists and experts to produce digital libraries containing lesson plans and resources. Twitter has recently developed "safety indicators"

[11] A summary of ENABLE activities and outcomes is available in the document library at bit.ly/2fYQbQG [access: 20.03.2019].

that are meant to serve as a barometer to gauge the properness of interactions taking place on the platform. The indicators include the level of diversity that people feel able to express on the platform, and the level of receptivity they show when they are confronted with values that are different than their own. Twitter has also put out a call to researchers to take the analysis further.

In light of initiatives such as these, it seems that the industry and researchers alike are aware of, and are reacting to, the deep changes that are taking place in society. They are aware that more than rules and advice are needed if users are to be appropriately protected and if digital technology is to provide safe, open spaces where they can exercise their rights. We have already seen to what extent social media can empower young people and enable them to freely express their opinions, meet and work with their peers and have a say in matters affecting their lives. These are unalienable rights of children enshrined in the United Nations Convention on the Rights of the Child (UNCRC)[12], and today's young generation have unprecedented possibilities to exercise them with digital means that overcome the challenge of time, distance and physical limitations. The recent General Data Protection Regulation (GDPR)[13], implemented in May 2018, contributes to the framework developed by the European Union to reinforce these rights for people of all ages.

Digital technology has disrupted former social orders to such an extent that only an in-depth change to education can bring about desired effects. Internet safety has proven a reasonably effective stop-gap solution during the transitional period we have just undergone. Yet in today's age of Artificial Intelligence and machine learning we need to look for new methods to prepare citizens for a future based on digital technologies. Digital citizenship can contribute to solving this problem.

The roots of digital citizenship education

In his above-mentioned publication, Jacques Delors underlines the great importance of education in enabling children to realise their full

[12] *United Nations Convention on the Rights of the Child* (1989). The document is available at website: bit.ly/2JJh9O1 [access: 20.03.2019].

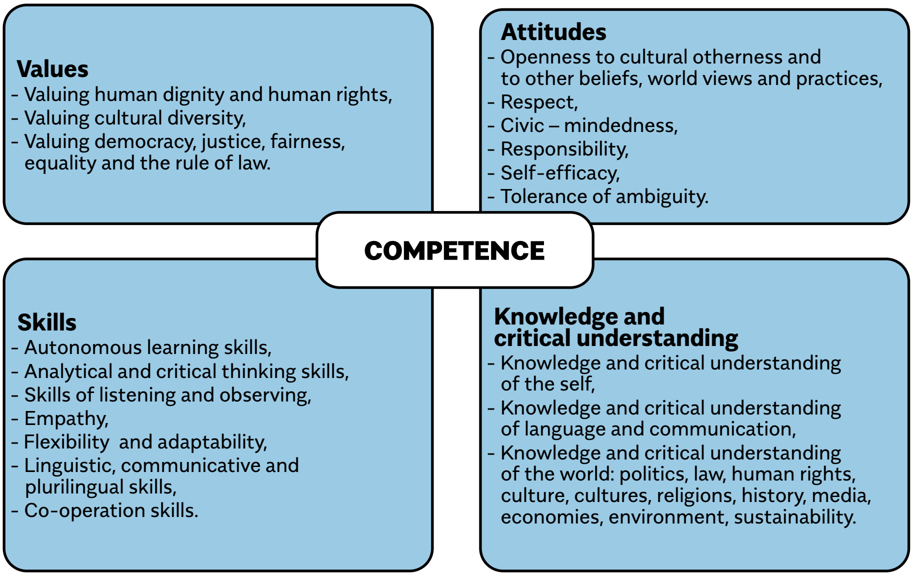
[13] *General Data Protection Regulation* (2018). Text in all European Union languages is available on the website: bit.ly/2vHVeNC [accessed 20.03.2019].

potential as citizens, and hence contribute to their own well-being and to the sustainability of the environment in which they live. He contends that education is the only solution, and that it needs to be built on four pillars: learning to know, to do, to be, and to live together. Education institutions and policy-makers in Europe, but also across the world, struggle to bring about changes in education that can meet these goals. In the last few decades this has been visible in the orientation of institutions such as the OECD (Organisation for Economic Co-operation and Development) in its PISA studies (Programme for International Student Assessment)[14]. Findings from the International Civic and Citizenship Education Study (ICCS) conducted by the IEA (International Association for the Evaluation of Educational Achievement) in 2016 also seem to reinforce the necessity to bring a changed approach to education.

Given its mandate to promote democracy and protect human rights and the rule of law, the Council of Europe has, since its creation in 1949, been very much focussed on guiding its 47 member countries to adapt their education systems in a way that would empower children to become active, responsible citizens. In 2013, the Council set up an international and interdisciplinary expert group with a mandate to develop non-prescriptive guidelines and descriptors of competence for democratic culture and intercultural dialogue that national authorities and education institutions could use and adapt as they saw fit. The model draws on findings and proposals of many organisations specialising in education. It is built around four areas of competence: values, attitudes, skills, and knowledge and critical understanding.

[14] A detailed description of the triennial Programme for International Student Assessment (PISA): www.oecd.org/pisa/aboutpisa [access: 20.03.2019].

Figure 3. Competences for a democratic culture, Council of Europe



Values
- Valuing human dignity and human rights,
- Valuing cultural diversity,
- Valuing democracy, justice, fairness, equality and the rule of law.

Attitudes
- Openness to cultural otherness and to other beliefs, world views and practices,
- Respect,
- Civic – mindedness,
- Responsibility,
- Self-efficacy,
- Tolerance of ambiguity.

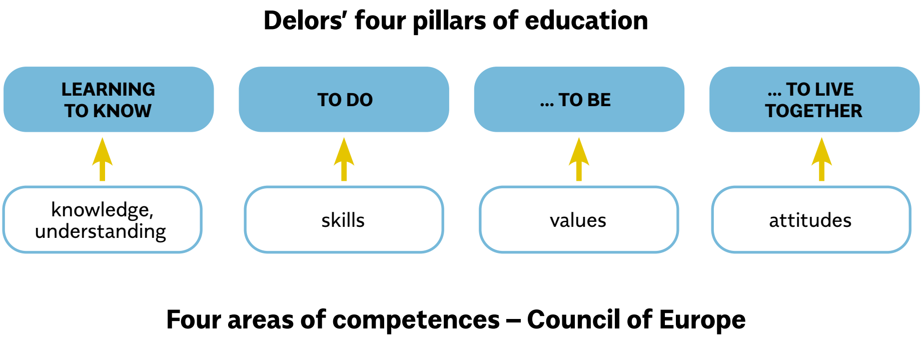
COMPETENCE

Skills
- Autonomous learning skills,
- Analytical and critical thinking skills,
- Skills of listening and observing,
- Empathy,
- Flexibility and adaptability,
- Linguistic, communicative and plurilingual skills,
- Co-operation skills.

Knowledge and critical understanding
- Knowledge and critical understanding of the self,
- Knowledge and critical understanding of language and communication,
- Knowledge and critical understanding of the world: politics, law, human rights, culture, cultures, religions, history, media, economies, environment, sustainability.

The four areas of this competence model correspond closely to the four pillars Jacques Delors defined two decades ago as being the foundation for 21st century education.

Figure 4. Competences for democratic citizenship, correlation between the models of Jacques Delors and of the Council of Europe



Values correspond to what Delors described as "learning to be". "Learning to live together" can be defined as attitude, and competences in this domain include respect, openness, civic-mindedness and responsibility. The third pillar, "learning to do", translates into skills, including listening and observing, cooperation, empathy, critical thinking and conflict resolution. "Learning to know", or knowledge and critical understanding in the competences for citizens in a democratic culture, begins with understanding oneself and the power of language and communication, both necessary if one is to grasp the full meaning of concepts such as sustainability, the environment, culture, economy, history and media. These are all essential components in today's landscape.

Over the past years, the Council of Europe has appointed a digital citizenship working group to adapt the competences for a democratic culture into an educational framework. This work has culminated in a Recommendation adopted by Ministries of Education in Member States to promote and integrate digital citizenship in education. This can, through an interdisciplinary approach in national school curricula, help educate young people to become competent, responsible citizens both on- and offline. It is of fundamental importance for society, but also for children themselves, that they are guided by values such as justice, honesty, equality, human rights and dignity as they learn to navigate the labyrinths of life and the Internet.

Mastery of all four areas of competences should make a far greater contribution to children's well-being than simply ensuring their safety online. It will enable them to benefit more fully and in a meaningful way from the opportunities that digital technology brings as well as help them resist being overly influenced by it. They will become capable of shaping the digital environment rather than being shaped by technology. They will have the capacity to apprehend the impact that technological innovations can have on society or certain sections of it and gain a raised awareness of the risks, thereby contributing to sustainability.

In almost every sphere of their lives young people today face challenges very different to what past generations were confronted with. As a valuable commodity to industry as well as to government and other service providers, they do not even need to go online to have their data gathered and stored as loyalty cards and similar mechanisms are making it an everyday practice in stores, restaurants, public spaces, etc. As quickly as regulations are being developed and implemented, innovative means are being found to extract and use even more data. And today – as young people have become the gatekeepers of the data of everyone they interact with, at least online – they need to think not only about their own personal information and privacy.

Looking up information for homework used to be a straightforward task. Nowadays young people cannot trust the sources they find online. They have to check and compare information. They also have to learn to resist the temptingly easy solution of cutting and pasting chunks of texts and using exciting tweets and information snippets, despite the seemingly constant quest to be interesting and the will to publish only perfect content. They are endlessly manoeuvring around and through the false information that abounds online in an ever-increasing supply.

European and international institutions and organisations have been struggling for several decades now to devise educational solutions that will harness the power of digital technology and promote effective lifelong learning skills among children and young people. They have been seeking ways to empower young people confronted with these and many other challenges, build their resilience, and equip them with the tools, values, attitudes, knowledge and skills they need to actively and positively contribute to society. Above all, however, they want to make possible the creation of an ethical society where human rights are respected and societal well-being is not supplanted by technological innovation. Many of the proposed models encompass Internet safety, but through strategies that are sufficiently generic to adapt to emerging tools and contexts.

A glimpse at some competence-based educational models

In 2012, UNESCO first published its Global Education Initiative, within the framework of its strategy for *Preparing learners for the challenges of the 21st century.* This was followed in 2015 with the organisation's publication of a detailed compendium of topics and learning outcomes for *Global Citizenship Education* (UNESCO, 2015). The publication and the framework provide clear guidelines that are implemented by teachers across the world. Digital technology is seamlessly integrated across the core conceptual dimensions, much in the way many of us are now switching between the real and virtual worlds depending on the topic or the task at hand. The 3 core dimensions of global citizenship education are:

→ **cognitive**, which refers to the acquisition of knowledge, the understanding and critical thinking about global, regional, national and local issues, and the interconnectedness and interdependency of different countries and populations;

→ **socioemotional**, which refers to the sense of belonging to humanity, sharing values and responsibilities, empathy, solidarity and respect for differences and diversity; and

→ **behavioural**, i.e. providing education that will help learners act effectively and responsibly at local, national and global levels for a more peaceful and sustainable world.

At much the same time, the Joint Research Centre (JRC) of the European Commission published the DigComp model[15]. Its objectives were similar to those put forward by UNESCO in *Global Citizenship Education*, with an equally strong emphasis on clearly defined and teachable competences and an extensive teacher training programme. While appreciating the necessity of children learning how to protect themselves online and use digital technology responsibly, both models adopt a broader cross-curricular approach aimed at empowering young people to become lifelong learners and critical thinkers, whether on- or offline. DigComp and its follow-up version DigComp 2.0 identify 5 key components around which school curricula can be built:

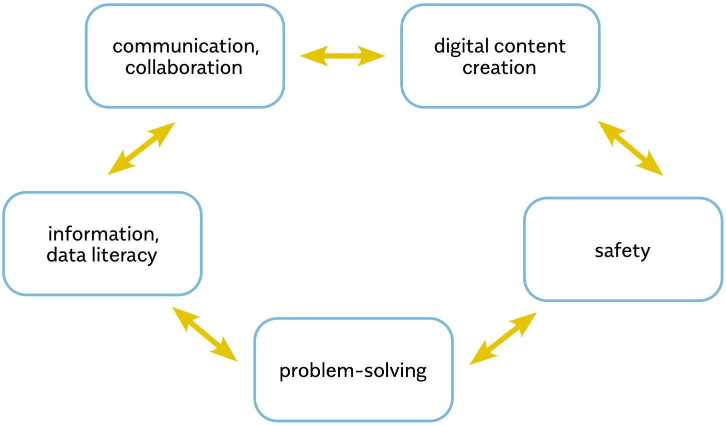
1. **Information and data literacy**: to articulate information needs, to upload and retrieve digital data, information and content; to judge the credibility of sources and contents; to store, manage and organise digital data, information and content.
2. **Communication and collaboration**: to interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity; to participate in society through public and private digital services and participatory citizenship; to manage one's digital identity and reputation.
3. **Digital content creation**: to create and edit digital content; to improve and integrate information and content into the

[15] More information on the website: bit.ly/2vxeWKn [access: 20.03.2019].

existing body of knowledge while understanding how copyright and licences are to be applied; to know how to give instructions understandable to a computer system.

4. **Safety**: to protect devices, content, personal data and privacy in digital environments; to protect physical and psychological health, and to be aware of the impact of digital technologies on social well-being and social inclusion; to be aware of the impact of digital technologies and their use on the natural environment.
5. **Problem-solving**: to identify needs and problems, and to resolve conceptual problems and problem situations in digital environments; to use digital tools to innovate processes and products; to keep up to date with the digital evolution.

Figure 5. DigComp 2.0 education model of the European Commission



The Council of Europe – a competence-centric, domain-oriented approach

Given its mandate to uphold human rights, democracy *and the* rule of law, education and empowerment of citizens is central to the actions of the Council of Europe. Since education is the means by which citizens acquire the knowledge, skills, convictions and habits, as well as learn the values needed to be able to fully participate in society, it is essential that education is continually adapted to reflect the transformations and realities of society.

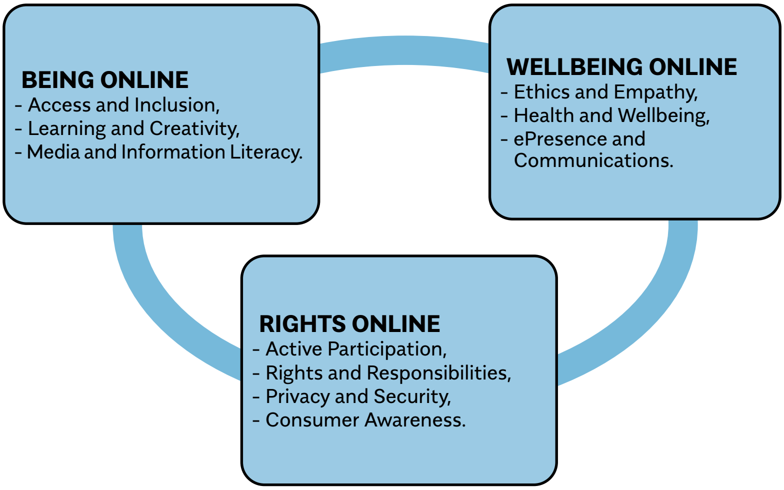
The Council of Europe has for a long time been developing educational tools and strategies for digital citizenship. One example is the first version of its *Internet Literacy Handbook*, published in 2003. This was a series of factsheets, each dedicated to a different Internet tool or platform. They meant to provide background and concrete examples of how these solutions worked. The publication was intended for teachers, parents and policy-makers, and provided educational activities, resources and examples of good practice that could be used at home or at school.

The *Handbook* highlighted, in particular, the educational added value of using various types of digital technology, as well as potential ethical issues raised by each. Already back in 2003, the contents of the *Internet Literacy Handbook* were at the crossroads of citizenship education and Internet safety, an approach that the Council of Europe has maintained ever since. The recently published fourth version of the *Handbook* (Richardson et al., 2017)[16] tackles issues as widely diverse as access and social inclusion, online shopping, Artificial Intelligence and data mining. Over the years, all four versions have been created according to a similar format. They provide information and highlight good practices, but ultimately leave it to (well-informed) citizens to decide for themselves when and how digital technology can be appropriately and responsibly used.

The digital citizenship working group that the Council of Europe set up in 2016 went several steps further and created a comprehensive breakdown of digital citizenship into 10 different domains. These are underpinned by the development of 20 competences, with clear examples of requirements for specific domains. These are categorised into three main areas, as follows:

[16] *Internet Literacy Handbook* – online version: bit.ly/2nRDjU3 [access: 20.03.2019].

Figure 6. Ten domains of digital citizenship (Council of Europe)



BEING ONLINE
- Access and Inclusion,
- Learning and Creativity,
- Media and Information Literacy.

WELLBEING ONLINE
- Ethics and Empathy,
- Health and Wellbeing,
- ePresence and Communications.

RIGHTS ONLINE
- Active Participation,
- Rights and Responsibilities,
- Privacy and Security,
- Consumer Awareness.

The *Digital Citizenship Handbook* (Richardson et al., 2019)[17], defines and describes in a practical way the ten domains, and the multiple dimensions involved in each one. Ways of using digital technology and opinions of educators, parents and policy-makers are described for each domain, which makes it possible to learn of anticipated developments in a given area and their potential impacts on society.

Using a format similar to that of the *Internet Literacy Handbook*, educational added value in each domain is outlined, and potential ethical issues are investigated. The publication provides lists of resources, ideas for classroom work, good practices and suggested reference materials. The Council of Europe will progressively add resources, teacher training initiatives and other support and evaluation tools over the coming years to facilitate implementation for interested schools and public authorities.

Together, the 20 competences for a democratic culture and their analysis across the 10 domains provides a comprehensive transversal framework that is teachable and measurable. This is intended as a means of ensuring that digital citizenship issues can be easily embedded in curricula, school and community, regardless of the country

[17] *Digital Citizenship Education Handbook* – online version: bit.ly/2Z20z2i [access: 20.03.2019].

or education system, rather than simply being an add-on, as used to be the case of Internet safety. In this way, learning about and with digital technology can become a practical, open process, adaptable to the needs of formal, informal and non-formal learning contexts. Open educational processes correlate more closely to the "anywhere, anytime" learning preferences of young people nowadays, and leave ample opportunity for families and communities to get involved.

The road ahead

Digital technology has transformed the way people act, interact, obtain information and make decisions. It is, therefore, increasingly important that each and every one of us knows how to use the Internet safely, constructively and competently, and that we are accountable for our actions and the information we post. However, social media have changed the very way people communicate. They have increased people's desire to connect, and to play a greater role in shaping the world around them through their network of social relationships.

Education is a vector and in some ways a gatekeeper of societal transformation, especially with the progressive breakdown of family and community values which can be observed in Western societies. At the same time, digital technology has opened us more than ever before to cultural diversity. If we are all to benefit from the changes brought about by digital technology, our education systems have to step up and begin shaping certain new competences, as well as take over those whose development was once the responsibility of family and community. The school curriculum is not freely modifiable, and every subject and every anticipated educational outcome must be carefully defined and monitored to ensure that they reach the goals intended. Although Internet safety affects the well-being of citizens of all ages, we must acknowledge that it is one of the necessary obligations to be carried out by the education system.

Digital citizenship education aims to ensure that people know how to use today's communication modes positively and master those competences that will enhance democracy rather than undermine it. The more people are engaged in finding solutions to the challenges emerging from the development of digital technology, the greater the possibility that societal transformation will benefit a higher percentage of our populations.

Are young people digital natives? Analysis of selected research findings

Jacek Pyżalski

The text raises the issue of the legitimacy of using the term "digital natives" for young internet users. Critically analyzed are the potential criteria for such distinction and research results referring to such adopted criteria, including more recent quantitative research on Internet use by children and youth in Poland (*EU Kids Online 2018*). The text closes the discussion on the legitimacy of the so-called digital generation theories *per se*.

Keywords:
digital natives
digital generations
the internet
children and adolescents

Home

Introduction

There is a widespread belief that information and communication technology (ICT) plays an important part in the lives of young people and, in particular, in their development. The immersion of young people in this technology, which pervades every aspect of their lives, is what apparently distinguishes them from previous generations.

This type of thinking can be observed in the concept of the "digital generation". Concepts like this involve attaching a name or label to a specific generation and describing it in terms of the technology used by its members or the way such technology use affects their functioning in society. Descriptions usually suggest that young people have a better know-how of a specific technology and a significant advantage over the adult generation (especially in a student/teacher context).

Perhaps the best-known concept in popular and scientific discourse (e.g. Krauze-Sikorska, Klichowski, 2013) is Marc Prensky's theory (2001a; 2001b; 2009) describing young people born in the Internet era as digital natives. The theory has been outlined in widely cited texts which contain the terms "digital natives" and "digital immigrants" in their titles (over 22.000 hits on Google Scholar). In general, its main premise was to characterise the generation which was "born in the era of the Internet" and the generation born before the Internet, which had to "learn it" at some point in life. Prensky proposes that the generational shift brought about by new media is so profound that there is "no turning back" (Prensky, 2001, p. 1), thus questioning the possibility of communication between such fundamentally different generations. He believes that new technology has made the generation gap much deeper and more radical than ever before, when technological shifts were not as substantial.

Prensky selectively cites neurobiological findings and claims that using the new media from a very young age permanently modifies cerebral anatomy and the way in which people perceive and process information (2001a; 2001b). According to Prensky, digital natives prefer image-based (as opposed to textual) communication and can easily read text and view photographs or films in very small windows on screens. Subsequently, they are not capable of learning linearly and have considerable difficulties with remembering longer content. They prefer hypermedia materials that allow them to move (using hyperlinks) from an initial document to many other sources of information (Prensky, 2001a; 2001b; 2009).

It is this above-described concept that has made its way into this article's title, which should, nonetheless, be understood more broadly. namely as a representation of all similar reflections. After all. there are other analyses based on comparable premises, for instance the concept of the "digitally born" (Palfrey, Gasser, 2008) or the "Net Generation" (Tapscott 1998, 2009), which point out that young people think, work, play or shop in a very different way than their parents. Don Tapscott believes that the Net Generation or (N-Gen) will "force" schools to change the existing learning model from a teacher-centred to a net-centred one based on cooperation. In Tapscott's opinion, such a change would be due to the fact that for members of this generation the basic medium is the Internet, whereas other media, for instance television, are an obsolete source of information. Ultimately, even the name of this generation emphasises its media-centricity. The same is true for the term "Millennials", which, despite being broader, sees the extensive use of ICT as a characteristic feature of this generation (Woodman, 2015).

Finally, it is worth noting that in all the digital generation concepts, ICT is not regarded simply as a part of young people's life (which is obvious), but as its central element and the main socialisation factor. Interestingly, though not empirically proven, these theories are widely and uncritically cited in research papers.

Digital natives. What does this mean in an empirical context?

If we want to confirm or deny the existence of digital generations, we should empirically identify various aspects of how young people function online and list the associated phenomena and dimensions. This paper discusses several key issues suggesting the extent to which these factors are relevant in distinguishing a digital generation. The discussion is illustrated with the findings of recent analyses, in particular the representative findings of the *EU Kids Online* survey conducted in 2018 on a sample of Polish children and young people aged 9–17 (Pyżalski, Zdrodowska, Tomczyk, Abramczuk, 2019). The discussion focuses on using the Internet, which is connected with using most information and communication technologies. This includes the following factors:

- the prevalence and frequency of using ICT;

- → the subjective significance attached by young people to using ICT and being online;
- → the qualitative aspect and wide range of the young generation's ICT use.

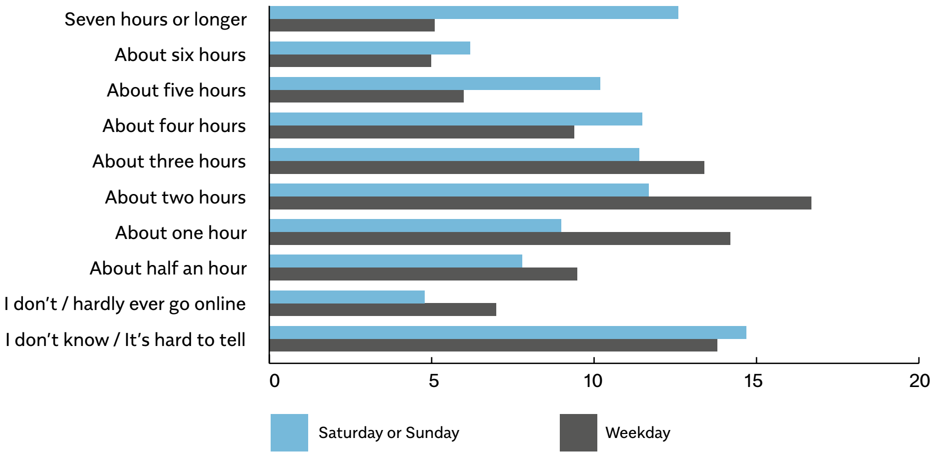
Prevalence and frequency of using ICT

It is a common perception that all young people use the Internet often and for a long time. In part, this perception is true, but to a certain extent it simplifies or even distorts the *status quo*.

Indeed, simple indicators of using the Internet, even of using it every day show that nearly all young people use this medium – not only in Poland but also in other developed countries (Pew Research Center, 2018; Pyżalski, 2012a; Tanaś et al, 2016). The recent *EU Kids Online* survey also confirms this trend and additionally demonstrates that mobile Internet is becoming increasingly prevalent: up to 82.5% of the respondents went online several times a day using a smartphone or mobile phone. At the same time, there is a decline in the frequency of using fixed Internet access: already more than 18% of students never or almost never use a laptop or personal computer to communicate online (Pyżalski, Zdrodowska, Tomczyk, Abramczuk 2019).

However, looking at the distribution of the time spent online, it becomes apparent that the population of young people in Poland is quite diverse. On weekdays, nearly one third of the respondents use the Internet for up to one hour, and only one in ten students use it for six hours or longer. A similar diversification can be observed in using the Internet during weekends (Figure 1).

Figure 1. Time spent on the Internet on weekdays and during weekends (N = 1249 persons aged 9–17)



Source: own work based on J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, A. Abramczuk (2019).

In analysing the above data, it is worth noting that despite young people being the most frequent users of the Internet in comparison to other age groups, indicators in other age groups are also rising, as shown by longitudinal analyses (Batorski, 2015). This is caused, among other factors, by the ever higher age of people who have used the Internet since birth. Consequently, the age of the generation who grew up without the Internet, which could serve as a comparison to the digital generation, is also increasing.

Furthermore, there are major differences in the time spent online. Contrary to common perception, the population of young people is not homogenous. In fact, there are relatively few people who use the Internet for a very short or a very long time: the distribution is close to normal. Moreover, the population diversity of Internet users depends on many other more general factors, for example the socioeconomic status of the young person's family (Pyżalski, 2012a; 2012b; 2016; 2017).

Finally, and most importantly, it is disputable to look at the usage frequency or even high usage frequency indicator alone. The indicator does not have to (and often does not) point to any deeper changes in the young people's mental or social functioning. What is more, it is insufficient if we acknowledge the already stated fact that the gap between the older and the younger population groups is narrowing.

Subjective significance attached by young people to using ICT and being online, and their self-evaluation of their digital skills

The importance attached to being and communicating online can be used as a determinant of belonging or not belonging to the digital generation. In the "EU Kids Online" survey, the respondents were asked if they found it easier to be themselves on- or offline; if they talked about personal matters online that they would not reveal offline; and if what they talked about online was different to that which they talked about offline.

Table 1. Distribution of young people's views on the importance of the Internet in their lives and communication (N = 1249 persons aged 9–17)

	Never	Sometimes	Often	Always	I don't know/ It's hard to tell
It is easier for me to be myself on the Internet than when I talk to people face to face.	42.3%	27.8%	8.8%	7%	14.2%
On the Internet I talk about personal matters which I would not reveal when I talking to people face to face.	65.3%	13.9%	4.7%	2.3%	13.8%
On the Internet I talk about different things than when I meet with people face to face.	39.1%	29.1%	11.7%	5%	15.1%

Source: own work based on J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, A. Abramczuk (2019).

An analysis of the respondents' views does not make it possible to determine whether young people attach particular importance to the Internet or if they perceive it as a qualitatively different environment for communicating with other people. Only 7 out of 100 respondents declared that it was always easier for them to be themselves on the Internet than when talking to people face to face, and only 8.8% declared that this happened often. This corresponds to the findings of a large survey conducted in Poland eight years ago on a group of 15-year-olds, where only one in ten respondents declared that the Internet was their top interest (Pyżalski, 2012a).

Equally rarely does the choice of indirect communication (via the Internet) correspond to the respondents' preference for talking about more personal issues online (about 7% of "often" and "always" responses) or to whether they talk about different subjects online than they do offline ("often" and "always" jointly accounted for less than 17% of responses).

This distribution of responses means that the Internet is of great significance to a smaller part of the population of young people (when the indicators are used in this way). Additionally, it is worth noting the high percentage of users whom the Internet does not help in being themselves and who never communicate online differently than offline (this also includes personal matters).

It is therefore difficult to ascertain that young people in general perceive the Internet as a special communication or social environment; rather, it is an area of functioning where its various aspects exist and are determined by other non-Internet-related factors.

Another important consideration is the young people's self-evaluation of their digital skills. Contrary to the common view that young people are very capable, the survey respondents (aged 11–17) were very critical of their own skills (Pyżalski, Zdrodowska, Tomczyk, Abramczuk, 2019).

Table 2. Young people's self-evaluation of their online skills – percentage of respondents who declared the highest indicators (N = 985, young people aged 11–17)

SELF-EVALUATION OF ONLINE SKILLS	WHOLE SAMPLE OF YOUNG PEOPLE AGED 11–17
I know how to install applications on a mobile device (e.g. on a telephone or tablet).	74.8%
I know how to remove someone from my contact list.	74.6%
I know what information should and shouldn't be made available on the Internet.	66.2%
I know how to save a photo found on the Internet.	62.9%
I know how to change my privacy settings (e.g. on a social media portal).	59.9%
I know how to shop using mobile applications.	50.7%
I know how to check the cost of using mobile applications.	49.2%
I know how to make and publish music or videos on the Internet.	39.0%
It is easy for me to choose the best keywords to find something on the Internet.	37.6%
It is easy for me to check if the information I found on the Internet is true.	31.9%
I know how to edit and change the content that other people created and published on the Internet.	24.0%

Source: own work based on J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, A. Abramczuk (2019).

Data concerning the respondents' self-assessment of their online skills (Table 2) show that even the simplest skills (which are, in fact, often practiced as part of the school curriculum) are not, in the opinion of the young people, well mastered. This low assessment concerns mainly security measures (6 out of 10 respondents think that they have mastered them well), and looking for information and checking its correctness (only one third of the respondents think highly of their skills in this respect). It is, however, necessary to note that in surveys where the actual level of skills cannot be objectively verified, the values of the indicators are overestimated in relation to the actual level.

The recent study confirms earlier observations (see Pyżalski, 2012a; 2012b) that young people have a relatively low opinion of their digital skills and that they display considerable differences in mastering skills that are often mistakenly attributed to the whole population. Hence it is difficult to treat this as a positive verification of the characteristics specified in most digital generation concepts, which speak of a high level of ICT proficiency. Nonetheless, from the point of view of an empirical verification of these concepts, this indicator should also be considered significant and worth applying.

Qualitative aspect and wide range of the young generation's ICT use

The last, albeit very important, indicator showing whether or not young people belong to the digital generation is their actual activity online. Therefore, it represents not so much simply using the Internet or the amount of time spent online, but rather the quality and range of undertaken activities (Table 3).

Table 3. Activity of young people on the Internet in the month preceding the survey (N = 1249 people aged 9–17, data in %)

	NEVER	ALMOST NEVER	AT LEAST ONCE A WEEK	EVERY DAY OR ALMOST EVERY DAY	SEVERAL TIMES A WEEK	ALMOST ALL THE TIME	I DON'T KNOW OR PREFER NOT TO ANSWER
I join an online campaign (protest) or sign an online petition.	79.5	9.8	3.0	0.9	0.5	0.3	5.9
I discuss social or political issues with other people online.	72.4	11.4	6.5	2.5	1.5	0.5	5.3
I make my own video or music and publish it on the Internet.	68.3	16.3	6.2	2.2	1.1	0.6	5.3
I use the Internet to talk with people from other countries.	52.9	19.2	10.8	6.8	3.0	2.1	5.1
I take part in an interest/ hobby group on the Internet.	48.7	16.3	12.2	9.8	4.5	3.2	5.4
I look for health information for myself or for someone I know.	45.3	26.5	13.1	4.6	1.9	1.1	7.4
I visit a social media portal.	25.3	7.8	12.2	21.6	17.5	10.2	5.4
I use the Internet for learning school subjects.	25.2	20.9	30.4	11.1	3.6	2.0	6.7
I use the Internet to find information about national and international issues.	24.7	26.3	27.1	9.4	3.4	1.7	7.4
I play games on the Internet (alone).	18.2	18.7	24.7	18.3	9.6	5.1	5.4
I look for something to buy or for information about how much something costs.	15.3	21.9	33.4	13.5	5.2	4.0	6.8
I look for information about employment/learning opportunities.	11.9	22.2	35.1	13.6	4.0	3.5	9.7
I communicate with friends or family.	8.3	8.7	16.9	28.9	18.5	13.0	5.7
I listen to music online.	8.1	8.8	15.9	27.9	19.1	14.5	5.8
I watch videos online.	4.0	6.3	18.6	33.9	21.6	9.9	5.7

Source: own work based on J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, A. Abramczuk (2019).

As it turns out, the most frequent activities are watching videos, listening to music and daily communication with friends or family. These are activities (especially the first two mentioned) where the user is passive, and which could easily be replaced by watching television or listening to the radio. It would be difficult to be critical of these findings if other, more social activities online were equally frequent.

It is worth noting that the survey revealed many differences within the studied population concerning activities depending on gender and age. As shown by other studies, the type of activity undertaken online is also connected to socioeconomic status, which in turn is connected to digital inequality. This means that the present inequalities are connected not with access to hardware or Internet connection, but to who is capable of using the Internet and for what purpose (van Dijk, 2012).

Taking into account the analysis so far, it is difficult to say that ICT permeates all areas of young people's lives, since many of them never or hardly ever undertake any valuable or creative activities online. Obviously, the cause of this situation can include other, more general factors. For example, if someone is not involved in any social campaigns, then usually they are likewise not involved in any on digital media. And if they are not interested in the news, they will not look for such information online. This interpretation further highlights the fact that traditional socialisation factors, not related to digital media, continue to play an important role, also in respect to using the Internet. Hence attaching key importance to the Internet in the socialisation of young people without a holistic, multifactor approach is unfounded.

Digital generation concepts: a critical approach

The author would like to use the findings presented above to critically analyse the assumptions of the digital generation concepts. This is not the first negative research-based assessment of this phenomenon. Such concepts (especially those created by Marc Prensky) have already been examined (Bennett, Maton, Kervin, 2008; Boyd, 2010; Helsper, Eynon, 2010; Pyżalski, 2012b). On the whole, researchers raised the following arguments:

- The digital generation concepts are often based on anecdotal evidence of how young people function, and usually concern individual examples. Population-based research does not confirm most of the characteristics described in these concepts (at least for the whole or the majority of the population). The research presented herein confirms these observations. At present, there is no sufficient empirical evidence to confirm the concepts' assumptions (cf. Pyżalski, 2012b).

- The authors of such concepts attach too much significance to how the Internet affects the lives of young people. They mistakenly place it at the centre of their lives, ignoring other factors that impact on their personal and social development. As Neil Selwyn points out, "such deterministic discourse obscures the key values and relations behind the growing use of technology in society" (Selwyn, 2003, p. 368).
- As shown by the previously described presentism error, the authors of these theories ignore information that some of the features attributed to the present generation have already been highlighted (before the Internet era), for example, multitasking, which to some extent also refers to earlier generations.
- These theories do not take into account the evolution of the Internet and the fact that in most countries both adults and young people are active Internet users.
- They ignore the diversification of young Internet users and attribute high digital competences to their whole population, whereas in reality only a smaller group demonstrates these competences.

Accepting the digital generation concepts indiscriminately is a dead end for educators: both researchers and teachers (Boyd, 2014). The subsequent false diagnoses may lead to ill-considered and worthless didactics designed for a population whose image is simplified, stereotyped and falsely homogenous (despite the fact that in reality it is very diverse).

Observing the current discourse on young people, one may repeat the appeal of Susan Herring (2008), which I have already referred to (Pyżalski, 2012b). She challenges the radical concepts of an intergenerational digital gap and points to the necessity to shift the paradigm from technology to the needs of young people. These needs should be treated as a point of departure for analyses aiming to fulfil them in the age of digital media. Such a proposal is valuable also from the axiological perspective and stands a better chance of building a foundation for educational theories which, in turn, will provide a basis for educational practice. As Neil Selwyn points out (2009, p. 366): "there is a pressing need to develop and promote a realistic understanding of the relationship between young people and technology [...] if we are to play useful and meaningful roles in supporting current generations of young people".

2

Home

The Internet – selected aspects of child and youth protection

Home

Praxeological dimension of the prevention of threats related to the activity of children and young people in cyberspace

Józef Bednarek, Adam Andrzejewski

This publication concerns a pragmatic orientation of prevention activities, against threats related to the activity of children and youth in cyberspace. The current classification of threats in virtual space is presented. The theoretical assumptions of problem behaviors in relation to cyberspace was analyzed. The indicators of the preventive process in the educational environment of children and adolescents are discussed. The authors presented a proposal of family and school interactions in the aspect of prevention of cyberspace threats.

Keywords:
children and youth
cyberspace
prevention
threats

Home

Introduction

It is not only the circumstances of the activity of children and young people both in the real world and in virtual space that are changing, but also – more importantly – its pattern, especially in light of a number of new determinants and multiple consequences. The subject of the above analyses has been relatively well explored in scientific literature. The same refers to its causes, pattern and consequences in the real world, and to the objectives and principles of prevention in this respect. It is noteworthy that the existing extensive literature on the subject of preventing the dangerous activities of the youngest generation in the real world helped to prepare and apply validated procedures aimed at individual risks and social pathologies. In turn, dangers in cyberspace have not been reflected on to a sufficient degree from the research perspective and, above all, from that of prevention and therapy.

New dangers in cyberspace have caused a discrepancy between the scale and scope of the pathological behaviour of children and young people and the current condition of not only prevention, but also education focussing on the safe and responsible use of the new opportunities that are offered by the media and digital technologies. It is due to this dangerous and dynamic global phenomenon (no longer only a process), whose consequences are often disastrous, that a new kind of prevention – other than conventional strategies at global and local levels – is becoming more and more important. The necessity to explore and apply praxeological prevention arises from new and particularly significant risks faced by children and young people in cyberspace. Praxeology is the study of the pragmatic nature of human actions engaging people in purposeful behaviour. When explaining the scientific definition of praxeology, Tadeusz Kotarbiński's words should be quoted: "What we do can be judged from different perspectives, for example from the viewpoint of morality or the satisfaction we derive from doing something. However, such a judgement can be not only emotional, but also utilitarian. This is when an action is judged from the perspective of so-called technical merit: usefulness, general purposefulness, and from the perspective of efficiency which boils down to two main advantages: effectiveness and thrift" (Kotarbiński, 1975, p. 13). As the author then says: "Educators find this topic very attractive for at least two reasons. After all, their task consists in instilling various skills in their students and being an educator is in itself a practical skill" (ibid., p. 22).

This particularly important dimension is not yet fully explored and verified as the period of various uses of the Internet is relatively short – only 30 years. It is also worth emphasising that parents, teachers and prevention practitioners are not competent enough when confronted with the dynamics of cyberspace development and the threats it generates.

Therefore, these analyses do not seek to present the wide and not yet fully verified praxeological dimension of prevention aimed at children and young people and seen from the perspective of a number of new and dynamically emerging dangers in cyberspace. Instead, they look at the following issues:

- theoretical and empirical circumstances of cyberspace dangers;
- classification of cyberspace dangers;
- theoretical fundamentals of preventing problem behaviours;
- classification of prevention levels;
- school climate as an indicator of the prevention process;
- parenting style supporting prevention;
- parental control tools applicable to children’s online activity;
- scenario of a prevention lesson at school.

Theoretical and empirical circumstances of cyberspace dangers

When analysing the development of the Internet as a global network, we can identify at least two factors owing to which this medium enjoys such widespread acceptance. One of them consists in putting into practice the idea of an information society and a borderless world devoid of communication barriers, the other – in the willingness to create a communication network which was supposed to serve military purposes and which would survive even if traditional means of communication were to be destroyed. Nobody knew that this global network would offer so many opportunities. Practically all (there are only a few exceptions) countries on the map of the world have access to the Internet. However, it is to be borne in mind that the deeper we delve into the world of cyberspace, the more we are exposed to various negative phenomena.

“Being in cyberspace is determined by two basic factors: 1) interactivity embedded in the process of sending and receiving signals; and 2) telepresence – an illusion that we are 'right there'. To achieve this, we need so-called full sensory immersion involving at least two most important senses – usually sight and touch" (Bednarek, 2009, p. 31). That is how the effect of virtual reality is achieved. This rapidly developing process involves above all children and young people, but also, to an ever-increasing extent, adults. People's education, social status and the families they function in are not important. We are all under the far-reaching influence of the latest information technologies and virtual realities dominated by means rather than objectives and values.

Young people immersed in cyberspace can become involved in many activities, they can simultaneously design and create their own identity without exposing themselves to direct criticism. The interactivity of cyberspace often replaces socialising with peers, thus creating the category of people known as "cyberhermits". These are young people who interact perfectly in cyberspace, but not in the real world. This phenomenon is caused by hyperactivity, intense sensitivity, low self-esteem, living in a dysfunctional family or difficulties in coping with everyday life problems. According to Katarzyna Krzystanek, such behavioural issues can be remedied by appropriate parental attitudes and good family relationships creating an atmosphere diminishing young people's vulnerability to media aggression (Krzystanek, 2007, pp. 59–68).

It is worth quoting selected aspects of the latest surveys conducted by the Empowering Children Foundation, which show the ways and forms in which children and young people use cyberspace, as well as the content they are exposed to. Analysis of those surveys allows us to conclude that children and young people have lots of freedom in using cyberspace resources in terms of the time they spend there and the content they may come across.

Teenagers spend more time on the Internet during days on which they do not have to go to school. 43% of respondents spend at least three hours on the Internet on school days and when there is no school the percentage grows to 61%. Every third (33%) respondent uses the Internet for at least five hours on days with no school. Every fourth (26%) respondent aged from 11 to 18 said that (very often or quite often) they had caught themselves browsing web pages, even if they were not particularly interesting. Slightly less, that is 23% of respondents, unsuccessfully tried to limit the time spent online, 17% of young people felt uneasy when they could not be online, and 16% of them neglected their family, friends, school or hobbies because of spending time on the Internet. Every twelfth person (8%) said they did not eat or sleep because of their Internet use. Around one half (51%) of respondents using the web said that during the twelve months preceding the study their parents or guardians had not asked them what they were doing on the Internet or which sites they visited (Makaruk, Włodarczyk, Michalski, 2017).

Therefore, educating people in the proper and rational use of cyberspace becomes significant as the youngest users may be exposed to harmful content. Unfortunately, only slightly over half (58%) of students said that during the school year preceding the study they had had classes making them aware of harmful content on the Internet. These were mostly the youngest respondents, aged between 11 and 12 – 65% of them claimed they had participated in educational activities on the subject (Makaruk, Włodarczyk, Michalski, 2017).

Young people often encounter pornographic or sexualising materials. In light of these surveys, as much as 43% of children and teenagers aged between 11 and 18 have been exposed to them. 55% of those aged 15 or 16 and 63% of students aged 17 and 18 said they had encountered content of this nature. Every third teenager (34%) aged between 15 and 18 encountering pornographic content was worried about it, and 28% of them said they had spoken to someone about it. 17- and 18-year-olds spoke about it with other people much more rarely – only 9% of respondents spoke about it with their mothers and 3% with their fathers. Almost two thirds (61%) of respondents aged 11 and 12 and 43% of those aged 13 and 14 were worried about coming across pornographic content (Makaruk, Włodarczyk, Michalski, 2017).

Every fifth respondent (19%) exposed to pornographic content said that they encountered such materials every day, and every fourth (24%) – once or twice a week. Every fifth (20%) teenager aged between 13 and 14 came across pornographic materials where sex was accompanied by violence. Over half of the children (58%) exposed to pornographic or sexualising materials say that they came across them by chance. Every tenth respondent, however, deliberately uses the Internet to look for information about sex (Makaruk, Włodarczyk, Michalski, 2017).

It is, therefore, clear that cyberspace is a world where children and young people spend long hours, are exposed to various content, and meet people who frequently pose a threat to their psychological, moral and social development. It is in this aspect that the words of Maciej Tanaś are all the more important: "Human imagination continues to open the door to that world. Inasmuch as in the world of mass media passive reception of information was enough, Internet users surf the web by themselves, they get the sense of agency by drawing information from databases and talking to other Internet community members. Unfortunately, this surfing is too often like erring, and creative activity in that world is replaced by reception of information, cultural garbage or cheap entertainment. It sometimes happens that content reaching [users] is in line with their needs and preferences revealed during Internet searches. However, sometimes information gets to them in line with the sender's more or less hidden intention, which often hurts the mind and heart of children unaware of dangers or only seemingly resistant to media manipulation performed by adults" (Tanaś, 2007a, p. 9).

Classification of cyberspace dangers

New groups of specific dangers have come to light thanks to the current analysis of subject literature and scientific research into the harmful and dangerous role that computers, the Internet and its resources, mobile phones and other information and communication technologies play in the life of children, young people, adults and the elderly. As Maciej Tanaś says: "The social and pedagogical dimension of modern information and communication technologies emerges regardless of the objectives and ways of analysing them. […] Digital media have become a factor determining not only social, human and cultural transformation, but also (directly or indirectly) almost everyone's fate, including aspects of particular importance to educators – lifestyle, social relations, and types of cognitive, creative and even playful activity of children and young people. In a similar way, information and communication technologies change adults' scientific, professional, cultural or social activity – although it must be said that adults do not always notices them as readily, and more rarely see them in a good light" (Tanaś, 2015, p. 11). Sylwia Galanciak emphasises: "Living in a dynamically transforming world makes it difficult to notice the continuity and logic of its changes which – from the perspective of the user – may seem more like a radical break from the existing order, fully deserving the name of a revolution"

(Galanciak, 2015, p. 247). It is advisable now to ponder Bogusław Śliwerski's thoughts on the virtual world – that new space in human life. "The virtual, online world frequently functions as a synonym of the real world, perhaps – to a certain extent – experienced just as intensely, truly and meaningfully thanks to the stimuli received from it and transmitted to it. However, it is not real, because that is not its ontological status" (Śliwerski, 2016, p. 29).

Therefore, the existing categories of dangers need ongoing reclassification. This is the key paradigm for prevention strategies. It is worth presenting the classification of cyberspace dangers which is now being developed and regularly updated in numerous publications. It is authored by Józef Bednarek and Anna Andrzejewska – research staff members at the Maria Grzegorzewska University:

- Threats to mental and physical health: problems with sight, hearing and the musculoskeletal system, carpal tunnel syndrome, thumb problems, conditions involving other organs, self-destruction, self-inflicted injuries, suicide in cyberspace, impaired mental and physical development.
- Social and educational threats: cyberbullying, online violence and aggression, online gambling, second life, virtual world sects, human and organ trafficking, difficulties with interpersonal contact, human functioning in the world of humanoid robots and in a surveillance society.
- Cognitive and intellectual threats: using electronic and other gadgets, threats resulting from non-exposure to problems and the absence of the need to solve them, and from no activities in the scope of cognition and knowledge acquisition.
- Chemical substance threats: bigorexia, addiction to, among others, drugs, medication, energising drinks, legal highs and food supplements.
- Moral threats: cyberpornography, online prostitution, online paedophilia, cybersex, sexting, erotic gadgets, tattoos, implants, human surveillance and control, youth subcultures.
- Infoholism and threats linked to computer games (this category encompasses their reasons, course and consequences of risks and dependencies).
- Cybercrime threats: offences against information protection, computer hacking, computer bugging, illegal destruction

> of information, computer sabotage, copyright infringement, offences against document credibility, cracking, computer viruses, storage and seizure of computer data, and virtual financial offences (see Bednarek, Andrzejewska, 2018, p. 28; Andrzejewska, 2018, pp. 389–390).

It is clear that the scope of such dangers is very broad and that in the future it will encompass new areas still unknown today. The above factors are complementary, and they create the effect of synergy in terms of harmfulness, which stems from the interdependence of devices and information and communication technologies present in the life of children and young people. This problem needs effective and appropriate counteracting. The document also discusses praxeological activities aimed at prevention and education, undertaken by families and schools as a response to current threats and in respect of the online safety of children and young people.

Theoretical fundamentals of preventing problem behaviours

In the era of the fourth industrial revolution, problem behaviour of young people functioning in the real world is echoed in cyberspace. That is due to the omnipresence of the Internet and devices using information and communication technologies. Interactivity and dynamic development have become a characteristic of virtual reality. Dangers present in the real world are transferred to the virtual one and vice versa. Activity in cyberspace, initiation and long-time exposure to dangerous content pose threats to children's personal psychological and axiological space, cause antisocial behaviour and implicate not only personal problems, but also those relating to childcare and education in the real world.

The concept of resilience – the significance of risk factors and protective factors

There exist certain processes that contribute to people's good adaptation to the environment in which they function, despite the occurrence of various harmful, destructive, degrading, threatening and bad stimuli called risk factors. Such processes are not directly noticeable, and their existence can be inferred by the objective observation of people functioning in difficult living conditions. These observations allow us to hypothesise that, despite the risk factors those people are exposed to, quite a number of them cope much better than expected. In fact, many get on quite well in spite of highly stressful experiences in their life. Risk factors are deemed to be those which increase the probability of unwanted behaviour. However, it turns out that there are also positive stimuli in human life which protect people from problem behaviour and prevent it. We call such stimuli protective factors.

The construction of numerous prevention programmes is based on activities limiting risk factors, thus increasing the impact of protective factors (Gaś, 1998, p. 9). The concept of resilience (meaning resistance, flexibility, adaptability and elasticity) is the starting point for the above activities. It originated as a result of observing children on the brink of psychopathology. Some children were observed not to be influenced by their environment and, in turn, to achieve good results in terms of development, education, society and life in general, despite being exposed to risk factors. Such children, though brought up in unfavourable conditions, develop properly and adapt well. This encouraging finding led to gaining more knowledge about such cases and to the discovery of mechanisms regulating the effects of protective factors. Searching for specific differences in children coping well despite adversities contributed to the initiation of analyses of problem behaviour prevention.

Research into resilience was pioneered by Emmy E. Werner. In 1955, she initiated a thirty-year longitudinal study of the development of 698 children born in the same year on the Hawaiian island of Kauai. The study involved a team composed of paediatricians, psychologists, psychiatrist and social workers and led to a number of valuable conclusions concerning positive adaptation. Almost one third of the Kauai children grew up in very difficult living conditions (poverty, alcoholism, parents with mental problems, no access to education). When analysing their development and individual life, researchers noticed that despite unfavourable circumstances at early stages of development and the presence of potentially destructive risk factors in their environment, this cohort developed properly, and in adulthood they achieved better welfare standards than others. The most resilient part of the cohort had the benefit of favourable circumstances – elements acting as protective buffers in the environment in which they grew up, i.e. protective factors.

Experience gained by Emmy E. Werner's team over several decades encourages reflection on the fact that although innate resilience to difficult conditions undoubtedly gives an advantage and helps, it is never too late to develop protective factors to fight adversities (Werner, Smith, 2001).

Literature on the subject in question offers a definition of resilience as a process and mechanisms conducive to positive adaptation in the presence of two components: a heightened level of risk in an individual's life and positive adaptation resulting from overcoming threats to proper development (Borucka, 2011). The concept of resilience being a precondition for an individual's good functioning despite unfavourable living conditions forms the basis for the preparation and development of prevention programmes concerning children's and young people's health and problem behaviour.

Apart from Emmy E. Werner, other pioneers of research into resilience include Michael Rutter, Norman Garmezy, Suniya Luthar, Ann Masten and Michael Ungar. Norman Garmezy's theory states that all children experience stress at some points during their development, and to maintain resilience they have to display "functional adequacy", which is understood as the maintenance of competent functioning despite an interfering emotionality, and which is a benchmark of resilient behaviour under stress (Garmezy, 2011a, pp. 459–466; 2011b, p. 416). Michael Rutter offers one of the latest redefinitions of resilience – in his opinion it is an interactive concept which is related to a combination of serious risk experiences and their relatively positive psychological results (Rutter, 2006, pp. 1–12).

J. David Hawkins, Richard F. Catalano and Janet Y. Miller, whose research concentrated on the prevention of children's and young people's health and behavioural problems, prepared a list of risk factors underlying problem behaviour in adolescents, including substance abuse, delinquency, early pregnancy, dropping out of school and violence. They created factor categories from the perspective of relevance to individuals, families and local communities and included such aspects as access to drugs, rebelliousness, violence in the media, extreme economic deprivation, conflict in the family, school failure, early and persistent antisocial behaviours, peer groups involving the individual in problem behaviour and dysfunctional families (Hawkins, Catalano, Miller, 1992, pp. 64–105). They also indicated personal characteristics, life situations and environmental conditions preventing problem behaviour. These are understood as protective factors and include: a strong bond with parents, regular religious practices, respect for authority, positive school climate, involvement in social activities and good school achievements (ibid., pp. 64–105).

Ego-resiliency **as a personality component**

Resilience is associated with a type of personality (ego-resiliency) able to function in various life situations while exerting control over behaviour adequate to a specific situation. This personality possesses characteristics making it particularly resilient to stress and allowing it to maintain welfare despite adversities (Luthar, Cicchetti, Becker, 2000, pp. 543–562). This results in optimum social adaptation, resistance to addictions, keeping away from crime, and obtaining good school achievements. Literature focussing on psychology offers many profiles of ego-resilient personalities.

Particia J. Mrazek and David Mrazek presented interesting conclusions following their study involving people subjected to severe physical and mental abuse in childhood. They pinpointed certain personality characteristics allowing those persons to function well in adult life despite the trauma they had experienced. This can be achieved thanks to such things as: rapid responsivity to danger, immediate adaptation of behaviour to a situation to avoid risks, dissociation of affect, ability to seek and avail oneself of help, sense of self-responsibility, positive projective anticipation and an optimistic view of reality, ability to see constructive experiences in difficult events and undertaking altruistic actions for others (Mrazek, Mrazek, 1987, pp. 357–365).

When constructing their resilience scale, Cynthia L. Jew, Kathy E. Green and Jane Kroger conducted an analysis of variance and defined three dominant personality characteristics necessary for resilience: an optimistic view of the future, self-confidence and confidence in other people, as well as higher self-perceived competence (Jew, Green, Kroger, 1999, pp. 75–89).

Kathryn M. Connor and Jonathan R. T. Davidson, in turn, developed a tool measuring resilience involving five characteristic variables:

- personal competence, high standards, and tenacity;
- trust in one's instincts, tolerance of negative affect;

- positive acceptance of change and relationships giving a sense of security;
- sense of control;
- spiritual support (Connor, Davidson, 2003, pp. 76–82).

At the same time as the concept of resilience, another theory was developed whereby specialists explain processes of positive adaptation and resilience in stressful environments. Let us mention Aaron Antonovsky's model of *salutogenesis*. He analysed the life of concentration camp survivors. Most of those people were diagnosed with mental disorders and social adaptation problems. However, there was a group which was in good mental health despite the enormous trauma. Having performed numerous case studies involving those people, Aaron Antonovsky developed the concept of "sense of coherence". It denotes people's life orientation which can explain the functioning of individuals' general resistance resources. The "sense of coherence" is developed as a result of acquiring individual and social competences and the ability to use them in coping with problems and difficult and extremely stressful situations in life. It encompasses three elements:

- comprehensibility – awareness of predictable and explicable stimuli generated in internal and external environments;
- resourcefulness – ability to use available resources to effectively cope with challenges posed by environmental stimuli;
- meaningfulness – conviction that the challenge is worthy of involvement, is valuable and meaningful, and positively motivates an individual to act (Antonovsky, 2005).

International organisations use Aaron Antonovsky's work to develop and evaluate programmes improving people's physical and mental health.

Having reflected on the omnipresence of various risks posed by cyberspace (such as access to harmful content, dangerous activities and aggressive influence of other users), it is only logical and reasonable from the perspective of improving preventive activities to consider an adaptation of models based on the concept of resilience to problems generated by that environment.

Classification of prevention levels

It is assumed that preventive interventions appropriately adapted to their target groups and to the scale of risk are the optimum method to stop or limit phenomena considered socially harmful. In exploring modern prevention challenges relating to threats in cyberspace, brought about by Web 2.0 and modern IT devices, selected action strategies were adapted to the current classification of prevention levels.

Table 1. Intervention plan for cyberspace dangers

LEVEL	VARIABLE	INTERVENTION STRATEGY
Primary prevention	It is of a universal nature. It targets children and young people not involved in problems arising from their online activity. Its main tasks involve providing information, promoting safe use of the Internet and ICT, instilling media competences, and delaying the moment of exposure to harmful content in cyberspace thus minimising risk behaviour.	Activities are inspired by involving schools and families in the process of raising awareness of cyberspace risks posing a threat to the safe and proper development of children. Parents who talk, educate, exert elements of control and limit the effect of risk factors are the first implementers. It is them who strengthen and provide protective stimuli. In this scope, school prevention programmes are implemented by external specialists, school counsellors, psychologists and teachers competent in cyberspace matters. Activities are aimed at information, prevention, development of children's various life and social skills helping to cope with difficulties and requirements associated with developmental periods and to minimise risk factors in children's environment. Information should be reliable and adapted to the specificity of recipients.
Secondary prevention	This is the stage of early identification and diagnosis of improper use of Internet resources. Activities focus on telling users about the symptoms of disorders linked to harmful activities in cyberspace, raising awareness of the problem and providing support in the process of withdrawal from dysfunctional Internet use as well as on minimising the personal and educational consequences suffered by children and young people as a result of their activity in virtual space.	Intervention covers informational, preventive, therapeutic and compensation activities targeting specific identified problems resulting from online activity. When designing activities, the specificity of target groups reflecting existing disorders should be taken into account. Such interventions are usually long and require recipients' active participation and involvement. They focus on the elimination or reduction of risk factors and on the introduction of new protective factors while strengthening existing ones. Preventive activities should be provided by specialists qualified in young people's problems linked to cyberspace.

Tertiary prevention	It is aimed at high risk groups – people displaying symptoms of dysfunctional Internet use and behavioural disorders. It is meant to prevent further aggravation and the recurrence of disorders. It also enables people with such disorders to go back to normal functioning and a satisfying as well as socially acceptable lifestyle.	The objective of tertiary prevention is to cause durable changes to an individual's behaviour and make them last as long as possible. When designing a therapeutic intervention strategy, the circumstances of an individual's social dysfunction must be taken into consideration together with their activity online and the specificity of the relevant behavioural disorders. Therapeutic activities are frequent and last long. The intensive nature of such interventions requires recipients' deep involvement. Interventions are entrusted to specialists possessing therapeutic and clinical qualifications. In some cases, hospitalisation and cooperation with healthcare units is necessary.

Source: Authors' own work based on Z.B. Gaś (2006).

When analysing Table 1, let us point out the key and pragmatic role of primary prevention. Many pathologies can be warded off by preventive interventions, optimally adapted and professionally administered to children and young people, combined with education based on the development of media competences, selective and critical reception of online resources, and knowledge of how to apply them in a creative way. The praxeological aspect of school prevention at a universal level can be summed up in the following principles and strategic objectives:

- → maximum raising of the age of initiation of risk behaviours caused by online activity;
- → implementation of prevention programmes at school – encouraging reflection on the causes and consequences of decisions made in the virtual world, indicating ways and methods of conflict solving, emotional education and encouraging reflection on declared and internalised values, as well as the integration of school groups and classes;
- → promotion of positive attitudes and instilling normative convictions in children and young people on the topic of online activity and online safety;
- → support in problem situations – intervention activities in classrooms, counselling for teachers, consultations for parents, integration of cooperation with school counsellors and teachers;
- → improvement of cooperation channels between institutions, services and aid organisations in order to enhance the

teaching staff's application of prevention practice concerning cyberspace dangers.

Therefore, guaranteed safe use of online resources increases children's and young people's chances of healthy and good physical, mental, psychosexual and social development. Should primary prevention be neglected, the consequences will include not only the cost of indispensable interventions involving therapy, resocialisation and rehabilitation, but also, above all, the harmful consequences of young people's disorders in a number of fields and – in extreme cases – the loss of health or even death.

School climate as an indicator of the prevention process

Functioning in a school community shapes experiences important for children's emotional and social development. This is undoubtedly one of the key places where they gain such experiences. It is on their basis that young people acquire new skills, learn different behaviours, and shape their attitudes, identities and character.

Rudolf H. Moos defined the "school climate" as the social atmosphere of an educational environment and divided it into three dimensions:

- relationships – an individual's involvement in their creation, sense of belonging and collective provision of support;
- personal development – self-enhancement in various personal and educational aspects by all school environment participants;
- system maintenance and optimisation – bringing order to an educational environment, introducing a code of principles and duties, as well as rights of all its members, and joint involvement in the observation of those rules (Moos, 1997).

A positive, friendly and safe school climate enables children and young people to develop in a healthy way and allows them to establish and maintain relationships, determines their cooperation aimed at the achievement of specific goals and shapes their sense of responsibility for the observance of principles and norms.

During the last few decades, numerous studies have been conducted on links between the school climate and risky behaviour, impact on mental health, behavioural and chemical addictions, prevalence of aggression and other social pathologies. The same kinds of problem behaviour are evident in cyberspace and their etiology is similar and involves interaction between causes in the real and virtual worlds. Physical aggression transforms into online abuse and hate speech. Traditional bullying takes the form of cyberbullying. Premature sexual behaviour starts with cybersex stimulated by online pornography. Experimenting with psychoactive substances involves social media where participants can freely exchange information about dangerous drugs.

As the phenomena are similar, it would be worthwhile to analyse the correlations that exist between the school climate and problem behaviour, and then to consider these issues in relation to the existing and emerging dangers and individual behavioural disorders caused by the virtual world.

The role of the school in the creation and maintenance of a good climate is significant from the perspective of preventing children's and young people's dangerous activity in cyberspace. Not only the teaching staff, but also students and their parents should be involved in this task. Sharing information about the processes of interaction and communication in the family and school environment and about child–child as well as child–teacher relationships increases participation in the life of a school and strengthens factors protecting against dangers in cyberspace at all prevention levels.

In 2004, Mona Khoury-Kassabri, Rami Benbenishty, Ron Avi Astor and Anat Zeira conducted research in over 160 Israeli schools. The results showed that bad climate in particular schools significantly raised the index of relevant forms of violence, including serious physical aggression, threats coupled with using dangerous tools as well as physical and mental harassment (Khoury-Kassabri, Benbenishty, Astor, Zeira, 2005, pp. 187–204).

Dexter R. Voisin, Laura F. Salazar, Richard Crosby, Ralph J. Diclemente, Wiliam L. Yarber and Michelle Staples-Horne conducted a study in the United States involving a sample of 550 young people aged between fourteen and eighteen and proved that those respondents who gave their teachers low scores for supportive attitudes and behaviours and did not feel attached to them were twice as likely to use psychoactive substances, display dangerous sexual behaviours and become involved in criminal groups (Voisin, Salazar, Crosby, Diclemente, Yarber, Staples-Horne, 2005).

In 2011, Laura M. Hopson and Eunju Lee conducted an online cross-sectional study involving 485 students and showed that good climate (education quality, support provided by the school and the quality of relationships with teaching staff and other school workers) in the New York schools in which the study was administered had influence on the reduction of problem behaviours involving truancy, missing homework, arguments with teachers, fights with other students and suspensions. The school climate was a stronger protective factor than parental support (Hopson, Lee, 2011, pp. 2221–2229). It is worrying that disturbed school climate is (in accordance with the concept of resilience) a risk factor in light of the above empirical studies and multilevel analyses.

By considering that "school children's (but also adult school staff's and parents') dysfunctional behaviour prevalent in schools is the best indication that changes must be made to the school environment", Zbigniew B. Gaś (2006, p. 106) recognises that the growing incidence of behavioural problems and disturbed healthy lifestyles may be counteracted by building a strong, efficient and emotionally integrated school community. There is a cause and effect relationship between the school climate and unwanted behaviours, which also result from children's online presence.

Parenting style supporting prevention

No social institution will be able to fulfil its preventive mission if its activity is not correlated with that of the family – the fundamental social unit. In Polish psychological literature, the system-based approach to the family was also undertaken by Jan Cz. Czabała, Mieczysław Radochoński and Maria Ryś (Czabała, 1988; Radochoński, 1986; Ryś, 2007).

As the child's primary and formal nurturing environment, the family can become a source of preventive measures provided that it fulfils certain conditions. According to Zbigniew Gaś, this is possible if, firstly, the quality of family life is constructive, meaning that the family fulfils its most important tasks, and, secondly, there are no problems linked to the child's development and behaviour necessitating specialist interventions (Gaś, 2006, p. 151). According to David H. Ohlson and his team, a constructive family is a system based on three pillars: cohesion (defined as emotional bods between family members), flexibility (understood as the family's ability to respond to problem situations) and communication (communication within the family to ensure cohesion and flexibility) (Olson, 1991, pp. 74–79; Olson, 1983, pp. 69–83).

When a family fails to fulfil its functions, it becomes dysfunctional. Maria Ziemska claims that this negative pattern may cover the following aspects: procreation, care, socialisation, mental hygiene as well as failure to meet family members' basic, care and emotional needs (Ziemska, 1975, pp. 35–40).

A stable and emotionally bonded family where children are safe and feel parental love is a source of factors protecting against dangers and pathologies existing in the real and virtual worlds. Table 2 contains suggestions of recommended parenting attitudes which prevent children from cyberspace dangers.

Table 2. Parenting attitudes shaping protective factors

ATTITUDE	CHARACTERISTICS	PROTECTIVE FUNCTION
Sensitivity and empathy	The role of parents/guardians is to empathise with children's emotions. Discerning and correctly interpreting the child's mood, with particular emphasis on negative emotions: anxiety, anger, sadness or withdrawal.	Strengthening bonds with parents in an atmosphere of understanding, sympathy and love. The child learns to develop interpersonal relationships based on empathy and trust. They develop the skills of telling parents about their problems and needs, and the skill of empathy.
Support and devoting attention	Devoting attention and showing interest in the child's activity. Readiness to help with the child's personal objectives linked to the consequences of their own choices.	Developing the child's own will as well as responsibility for the consequences of their decisions.
Transparency	Communication with the child is intelligible and clear. Parental behaviour stems from moral values. No labile and ambivalent attitudes.	Shaping of the rules and principles of entering into, developing and maintaining interpersonal relationships.
Observation	Parental readiness to respond to warning signs relating to the child's problems.	Establishing in the child a feeling of safety and of not being left alone in the face of difficulties and dangers.
Dialogue initiation	Frequent discussions with the child. Readiness to talk about difficult subjects. Active listening and respecting the child's arguments presented to support their reasoning.	Acquisition of constructive dialogue skills by the child and development of assertiveness.

Fairness	Adequate adaptation of parental requirements to the child's development stage, competences, skills and abilities.	The child develops their identity by integrating their experiences resulting from parental attitudes.
Consistent parenting	Establishing clear boundaries for the child. Defining principles and rules, and strictly enforcing them. Establishing the consequences of non-observance.	The child learns respect for norms, rules and principles existing in society. Being aware of the negative consequences of breaking the rules, the child avoids risky behaviour leading to this outcome.
Full commitment	Constant presence in the child's life. Accompanying the child in their tasks. Playing the role of guide and friend. Offering various paths of development, support and acceptance during the process.	Active participating observation of the child's functioning combined with controlling potential risk factors is a chance to delay or prevent risk initiation.

Source: Authors' own work.

Parental control tools applicable to children's online activity

There are many parenting styles. Those close to permissive parenting are based on trust as the main argument for the development of self-control mechanisms and self-confidence. On the other hand, autocratic parenting means increased control and supervision in respect of the child's activity, choices and decisions. Today, as soon as they are born, children become users of digital devices, such as computers, smartphones, tablets and the media that accompany them. In 2014, Americans studied parents of children aged from 6 months to 4 years. A disturbing picture was revealed: 73% of parents busy with household chores allow their children to play with mobile devices, 65% calm their children by using digital technologies and 29% try to put children to sleep in this way (Kabali, 2015).

Things are no different in Poland. The Nobody's Children Foundation (currently operating as the Empowering Children Foundation) conducted a survey which revealed that over 64% of children aged between 6 months and 6 and a half years had already had their first encounter with mobile devices (including 25% using them every day), 26% had their own mobile device, 79% watched films and 62% played games on a smartphone or tablet, 69% of parents busy doing something else let their children play with a mobile device and 49% of parents treated this as a way of rewarding their children (Bąk, 2015, p. 7). The 2017 survey administered by the Empowering Children Foundation to a group of 3943 respondents aged between 11 and 18 showed that almost one half (46%) of those using the Internet on a daily basis said that there were no online safety rules in their families. This indicator goes up to 76% in the group of 17- and 18-year-olds. Only one person in nine (11%) said that their phone was equipped with parental control applications. The parents of every fourth child aged between 11 and 14 (24%) had not introduced any rules of Internet use and every third child (34%) had a ban on visiting adult websites (Makaruk, Włodarczyk, Michalski, 2017).

The youngest users have no skills or are incapable of an informed, critical and selective choice and reception of online content, for example relating to violence or pornography. Because of their naivety and credulity, children left to themselves on social media are particularly vulnerable to intentional abuse. Therefore, it is advisable to consider the application of solutions enabling parental control of the youngest users' online activity during the complex process of familiarisation with the Internet. The market of computer software and mobile applications offers lots of practical and effective tools facilitating parental control in the field of their child's online activity.

Due to the limited length of this article, the presentation below contains only those which – in the authors' opinion – deserve particular attention:

- BeSt browser – a free web browser for users aged between 3 and 10. The project is implemented by the Empowering Children Foundation and the Orange Foundation as part of the European Commission's Safer Internet programme. This software offers effective protection for youngsters using the Internet via access to eight service catalogues and websites safe for children and by the possibility of blocking access to websites not listed in the BeSt catalogue. The "Guardian" function also makes it possible to monitor websites visited by children and those which have been blocked, and offers the option to block other programmes when using the BeSt browser.
- Beniamin – a computer programme tracking the child's activity relating to access to various services linked to the Internet. It makes it possible to block websites by a choice of settings preferred by the person controlling the child's access to the

computer. Moreover, it offers the possibility to limit access to selected services and functions (such as instant messengers, electronic mailing lists, downloading files, e-mail, video content and social networking services). The configuration is intuitive. The programme is free for fourteen days – after this period a licence has to be bought to continue using it.

- Kurupira WebFilter – a free and user-friendly computer programme offering a wide range of parental controls. Among other things, it makes it possible to monitor visited websites, launched applications and time spent using the computer. After opening, the programme runs in hidden mode and access to the panel is secured with a password. Moreover, it blocks selected instant messaging software and social networking services. Parents can also receive reports documenting the browsing history.
- Anti-Porn Parental Controls – a functionality enhancement applicable to the most popular browsers, such as Firefox, Internet Explorer, Chrome, Opera or Netscape. This application filters pornographic web pages, which are blocked on the basis of their description and multimedia content. It is also possible to set a time limit for how long the child uses the computer. The application is free and simple to install.
- Spyrix Free Keylogger – a free programme monitoring and registering operations on the computer. It can be used to track the child's activity for example on social media websites and Internet forums from the perspective of posted content, chats with other users and types of information searched. The programme runs in hidden mode and registers all keystrokes, recording information on a system clipboard. It can also periodically capture screenshots and register video images using a webcam.
- Kids Place – a free mobile application for Android smartphones and tablets. It offers parental control using the parent's/guardian's mobile phone. It makes it possible to configure a "playground" for the child. The parent/guardian chooses applications which the child may use and blocks access to prohibited programmes, applications and functions. The tool allows parents/guardians to prevent children from installing games and applications, supervise and limit time spent using

the mobile phone, as well as monitor text messages and incoming and outgoing calls. There is a PIN securing the configuration panel which makes it impossible for the child to switch the application off.

- Norton Family – an application for Android and iOS mobile phones and tablets. It makes it possible to set up two separate profiles: for parents and for children. The level of monitoring can be set from the parents' profile, and can encompass, for example, the choice of websites the child may visit or the list of applications the child may use or install. "Alerts" and "Activities" make it possible to monitor the child's activities on the mobile device and which supervision rules they tried to break, and to inform parents/guardians thereof.
- Family Time – a parental control application for iOS mobile devices. The programme offers a wide range of parental control options to monitor the use of mobile devices and the Internet by children. The application makes it possible to supervise the length of time spent on the device by the child, deny access to the Internet at night and block pornographic websites, and offers a catalogue of dangerous websites, a GPS service as well as supervision of telephone calls and text messages.

Scenario of a prevention lesson at school

Legislative solutions make schools responsible for conducting comprehensive preventive activities. Unfortunately, not every prevention programme covers issues related to dangers linked to cyberspace and social media. Children as young as 13 may register on Facebook, yet in reality much younger ones have active profiles there. Anonymity allows child groomers, paedophiles and other perpetrators meaning to hurt children to pass themselves off as anybody. In 2016, the NASK [Research and Academic Computer Network] conducted a survey involving 1294 respondents. Nearly one fourth (23.1%) of teenagers (12.5% more than in 2014) said they had met face to face with an adult met over the Internet, 29% of them said they had not informed anybody about this meeting and only 39% claimed they had informed their parents[1]. The issue of grooming should be one of the priorities of prevention in schools as in reality it is this phenomenon that causes most harm.

The scenario below presents an indicative workshop on grooming and is intended for primary school children.

Topic: Grooming – a new danger in social networks.
Duration: 90 minutes.
Target group: primary school children in grades 4–6.
Instructor: school counsellor, psychologist or the class teacher.
Goals:

- sensitising children to grooming in social networks;
- providing basic information on how to recognise a child groomer in social networks;
- making children aware of protective factors and risk factors, providing information about where to look for help in case of contact with online child groomers.

Working methods:

- short lecture;
- discussion.

Teaching aids:

- paper and pens;
- Annex No. 1 – Ania's story;
- Annex No. 2 – a list of factors protecting against grooming and guidance where to look for help.

Plan of the meeting
Introduction:
Participants greeted by the instructor, introduced to the topic and told about working methods (5 min.).
Main part:

[1] Survey report: *Nastolatki 3.0 Wybrane wyniki ogólnopolskiego badania uczniów w szkołach 2016* [*Teenagers 3.0. Selected results of the 2016 national survey of schoolchildren*]. The survey was administered by the research team of NASK, supervised by prof. Maciej Tanaś, which included: Wojciech Kamieniecki, Marcin Bochenek, Agnieszka Wrońska, Rafał Lange, Mariusz Fila and Bartosz Loba. The survey was conducted by the Pedagogium Foundation in cooperation with Ośrodek Sondaży Społecznych Opinia [Public Opinion Poll Centre] in June 2016 and was supervised by prof. Marek Konopczyński.

Exercise 1 How to recognise danger and protect oneself from it? (40 min.).

The instructor distributes among the students the story of 13-year-old Ania (Annex No. 1). The class is then divided into three groups. The groups choose leaders who will present the results of their work before the class. Each group gets a flip chart sheet and pens. The groups read the story and each works on one issue. The first group answers the question: "What can save Ania from contact with a dangerous child groomer?", the second group: "How can Ania recognise a child groomer in social networks?", and the third: "Where should Ania look for help if she encounters a child groomer on the Internet?". Representatives of the groups record ideas on the sheets provided (10 min.) and them present the results of the groups' work. The groups working on the same issues complement one another's answers (15 min.). After the presentation the instructor demonstrates a display board (Annex No. 2) containing protective factors and marks those appearing in the answers given by the groups. The instructor then shows which other resources may help them with solving this kind of difficult situation (15 min.).

Exercise 2 Offer of help in situations involving exposure to danger (20 min.). By making a reference to the story the instructor asks the children to whom Ania can turn for help. Their answers are recorded on the board or flip chart (the help in question may be divided into institutional and friendly/personal). If necessary, the instructor provides more information. To sum up the workshop, the instructor gives the children handouts listing protective factors and helpline numbers (Annex No. 2). Summing up: children's reflections (25 min.).

Annex No. 1 – Ania's story

Ania is 13 years old and is in the 6th grade of primary school. She is active on Facebook. Some time ago she was invited to join the friend list of a boy she did not know personally. He said his name was Paweł, that he was 14 and that he went to her school. For some time, Ania communicated with him using the Messenger application. Paweł was very nice, he said nice things about the way she looked, commented on her photos and liked her posts. One day he asked her to send him her nude picture of herself. At the beginning, she was frustrated and refused to do so. Paweł did not give up and suggested they should meet at a shopping centre. Embarrassed after his earlier request, Ania refused. Then Paweł threatened her and said that if she did not meet him, one day on her way to school something bad could happen to her. Ania became very frightened and has been afraid of leaving her home since then. She is wondering whether or not she should take a naked selfie and send it to Paweł or meet him in person.

Annex No. 2 Factors protecting against grooming in social networks

1. Have limited trust in user profiles.
2. Avoid talking to adults.
3. Do not share your real personal details with unknown users.
4. Do not send your intimate photos to strangers.
5. Disable GPS in social networks to mask your real location.
6. Refuse job offers, participation in competitions, promotions and suspected events offered by strangers.
7. Tell your parents whom you have met in social networks.
8. Space for your resources:

....

Where to look for help?
School counsellor / psychologist: Full name (..........................)
Room number, duty hours and days (..................................)
Counselling and guidance support centre (address, phone number, working hours)

....

Dyżurnet helpline: 801 615 005
Helpline for children and young people: 116 111
Helpline of the Ombudsman for Children: 800 121 212
Emergency number: 112

Conclusion

The above analyses and interpretations point towards the fact that children's and young people's activity in cyberspace is extremely dynamic, and has its specificity, pattern and consequences. This article presents a brief description of the praxeological dimension of prevention which has not yet been fully verified. Prevention is becoming increasingly important for the family and teaching staff in schools and institutions.

When the youngest users are exposed to new and exceptionally dangerous risks in cyberspace, the praxeological dimension of prevention must be explored, applied and scientifically validated, and appropriate models or procedures of action must be adopted. It is worth emphasising that there is a wealth of literature on prevention of children's and young people's risky behaviours in the real world, including sets of relevant procedures. However, there are no solutions applicable to threats and social pathologies in cyberspace and the virtual world.

The theoretical and empirical dimension of cyberspace dangers draws from numerous theories and concepts involving children's and young people's activity in the real world, as well as interdisciplinary knowledge applicable to the area of Social Sciences, especially pedagogy and IT. We have to be aware that the competences of parents, teachers and prevention practitioners are insufficient when confronted with the dynamics of the development of cyberspace and the risks it generates.

The attempt to classify cyberspace dangers presented above points to a synergy between traditional threats existing in the real world and new ones linked to digital media and technologies. Seen from this perspective, preventive efforts aimed at minimising the negative consequences of children's and young people's online presence take on a whole new meaning.

How to develop safer online behaviours

Karl Hopwood

Keeping children and young people safe online is a priority for teachers and parents alike. Although there is now a proliferation of tools and technology that will help with this there can be no substitute for education, dialogue and discussion. This chapter will seek to establish the key areas that need to be addressed and suggest some ways to establish a meaningful channel of communication with young people.

Keywords:
parents
communication
gaming
cyberbullying
sexting
dialogue
screentime
online reputation
Insafe

Home

In order to properly support children and young people when they are online, we need to consider three key issues.

- → What do children and young people really do on the Internet? What do they do in the online spaces that they inhabit? In order to fully understand this we need to look at the latest research (of which there is a great deal), but we also need to speak to children and, perhaps more importantly, listen to what they tell us, even if we do not like what they say.
- → What are the real risks they face when they go online? Most adults are very aware of what can go wrong online – the media constantly bombard us with sometimes quite horrific stories of things that have happened to children and young people on the web. The problem is that this has already happened, children have been harmed. Yet most of the time this is not reason enough for parents to stop them from using the Internet. We have to think about probability vs. possibility. There is always a chance that something dreadful could happen, but the likelihood is quite slim.
- → What is the best support parents, teachers and other adults could provide children and young people with? Yes, there are technical solutions – more on that later – but we should never underestimate the power of dialogue and discussion.

It is important to acknowledge that the world has changed, it is a common sight to see both adults and young people walking along the street unaware of what is happening around them because they are so focussed on the device that they are holding in their hand. Indeed, in several cities now we can find white lines on the footpath showing where it is possible to walk and text at the same time – designed to minimise the likelihood of bumping into someone or being knocked down by a car. We also know that children and young people begin going online at an ever earlier age. Recent research from Internet Matters[1] found that 87% of children up to 4 had access to portable devices. Similarly, 62% of 4-year-olds uploaded content onto the Internet. Clearly, technology is here and it is here to stay.

[1] www.Internetmatters.org

Unfortunately, we are now seeing a wide range of devices aimed at very young children. For example, a potty with an iPad docking station. It allows a child to learn how to use a potty (for toilet training) whilst using a tablet. No doubt it makes it easier to keep the child in the right place while they are learning this important life lesson, but perhaps this is not the best way to go about it. Technology plays an important role and can transform our life, but if we use it as a substitute for human interaction and engagement from a very early age, we are sure to face certain problems in the future. Many teachers will talk about how proficient 4-year-olds are when using devices, in particular tablets. These same teachers will also say that these 4-year-olds do not have the same verbal and communication skills they would have had 3 or 4 years ago. Of course not everything is the fault of technology, yet it must to an extent contribute to this state of affairs. Most of us will have been in a restaurant or café and seen a family or a group sitting together but, rather than talking, every one of them was looking down at a device and there was no verbal communication taking place at all. This is not just an issue concerning children and young people but rather society in general.

Interestingly, some research is beginning to emerge which suggests that parents are not necessarily setting the right example for their children when it comes to technology and tech habits in general. 36% of children said that they had asked their parents to stop continuously checking their mobile devices. And almost half (46%) said that this made no difference at all. Interestingly, 82% of children said that they thought mealtimes should be device free. A 9-year-old girl shared her thoughts on this: "We have a rule about no devices at the dinner table, but my mum always breaks it. She's addicted to Instagram. She uses her phone in secret, she has it on her lap under the table. You'll be talking to her but she's only half listening, she's more interested in what her friends are saying on Instagram or whether they've liked the photo that she's just posted". When asked how she felt about this, she replied: "I don't think it's fair. I spend all day at school, I work hard and I want my mum and dad to be proud of me. I think that when we're eating dinner they should ask me what I did at school, if I had a good time, how my day was – that sort of thing. My dad always does that, but mum is more interested in her phone".

Some very honest words from a 9-year-old. Difficult to hear, perhaps, but maybe they will make some of us reconsider our behaviour. Is there really anything more important that talking to our children and making time for them? We all know that there will come a point when they no longer want to talk to us about many things so, when they do, we should encourage it. Dialogue, discussion, debate, even disagreement is important and needed. Of course there is also room for technology. Being able to FaceTime a friend or relative who is not there in person is amazing, but it should not replace those all-important face-to-face interactions. As with all, balance is key.

The issues

It is important to consider the challenges that children and young people face when they go online. There are many, but we should recognise that in most cases they relate to behaviour rather than technology. Technology is a facilitator, it makes it easier for people to come across unpleasant content and helps them to overcome their inhibitions, but ultimately the issue is behavioural.

The table below was produced by the "EU Kids Online" project back in 2010 and shows the types of risks (and opportunities) that children and young people are likely to encounter on the Internet.

Table 1. A classification of online opportunities and risks for children

		***CONTENT*:**	***CONTACT*:**	***CONDUCT*:**
		CHILD AS RECIPIENT	**CHILD AS PARTICIPANT**	**CHILD AS ACTOR**
OPPORTUNITIES	Education learning and digital literacy	Educational resources	Contact with others who share one's interests	Self-initiated or collaborative learning
	Participation and civic engagement	Global information	Exchange among interest group	Concrete form of civic engagement
	Creativity and self-expression	Diversity of resources	Being invited/inspired to create or participate	User-generated content creation
	Identity and social connection	Advice (personal/health/ sexual etc.)	Social networking, shared experiences with others	Expression of identity
RISKS	Commercial	Advertising, spam, sponsoring	Tracking/harvesting personal info	Gambling, illegal download, hacking
	Aggressive	Violent/gruesome/hateful content	Being bullied, harassed or stalked	Bullying or harassing another
	Sexual	Pornographic/harmful sexual content	Meeting strangers, being groomed	Creating/uploading pornographic material
	Values	Racist, biased info/advice (e.g. drugs)	Self-harm, unwelcome persuasion	Providing advice e.g. suicide/pro-anorexia

Source: Results of „EU Kids Online" report, 2010.

One key issue is inappropriate content. Research by the UK Safer Internet Centre found that 70% of 8- to 17-year-olds had seen images and videos that were not suitable for people of their age in the 12 months preceding the survey. Many will be surprised at how high that percentage is but surely it should actually be 100%? How many adults have, when online, seen content that has disturbed or upset them? Anyone can publish content on the Internet, and although users can install filters, these are not and can never be perfect. This is why dialogue and discussion are so significant.

Looking at that statistic it is also important to recognise that these were users aged 8–17 themselves determining what – in their opinion – was suitable for someone of their age. This may be considerably different from what an adult might think. A 10-year-old boy explained that he regularly played both *Call of Duty* and *Grand Theft Auto V*. He acknowledged that these were games for persons 18 or older and that he was not old enough to play them, but justified doing so by saying: “I don’t mind shooters”. Clearly, his view of what is and is not appropriate is likely to be quite different from that of many adults.

Very often when a parent discovers that their child is looking at or has seen something “inappropriate” online they assume that this is because they purposefully searched for it. Sometimes this is true, yet not always. How many of us were innocently searching for something online but were met with content we were not expecting? This can be due to mistyping or misspelling, or it can be the result of an algorithm working incorrectly. The industry is increasingly (and probably rightly) relying on technological solutions and machine learning to help monitor and filter content on platforms, but this can go wrong. There has been a number of recent examples: “In March 2018 Facebook users discovered that when they typed ‘videos of’ into the search tool, some of the suggestions were highly inappropriate – in some cases suggestions of videos of children performing sexual acts.”[2] Facebook were quick to apologise and explain that there was a problem with the algorithm, but what had happened could not be undone. Similarly, Google have had issues with their autocomplete tool. Back in December 2016 if a user typed in the phrase “are Jews”, Google suggested the question “are Jews evil?” Google VP and Head of Google News, Richard Gingras, when speaking in the British parliament said that their algorithms will never be perfect. All this means that the dialogue and discussion mentioned earlier is of paramount importance.

If we take a very specific example of harmful content which affected some of the youngest users, we can see how important it is for parents/carers/trusted adults to react in the right way. In March 2017 the BBC reported[3] that there were a number of parody Peppa Pig videos on YouTube and other social media sites. Very well made, the videos looked genuine but contained unpleasant and disturbing content. One showed Peppa visiting the dentist, where she was tortured – there was blood, screaming, etc. For a 4-year-old to see something like this would be traumatic, but presumably not their fault.

[2] A. Hern, *Facebook apologises for search suggestions of child abuse videos*, “The Guardian”, bit.ly/2DTgwfT [access: 7.05.2019].

[3] *The disturbing YouTube videos that are tricking children*, BBC, bbc.in/2NjW8Xi [access: 05.07.2019].

Google (who own YouTube) have taken on more moderators and are constantly trying to improve their machine learning to better spot this type of content, but in 2017 they admitted that every minute over 400 hours of video are uploaded to the site. It is not pre-moderated. And so, while many tech companies pride themselves on using AI to remove much harmful and inappropriate content before it is even reported, much can still slip through the net. Therefore, the challenge for tech companies is scale.

It would be unreasonable to suggest that a parent should always be sitting with their children when they are doing anything online – this is simply not possible. We must, however, hope that when (not if) our children stumble upon some difficult, challenging or inappropriate content, they will come to us in order to talk to someone who can offer them the right support. A parent who sees their child looking at shocking content will often blame the child, thinking that they were consciously looking for it. Sometimes this is the case, and we can consider this later. Often, however, the situation is different – the content simply appeared as an accidental search result or, as can be the case with teenagers, maybe a friend sent over a link knowing or hoping that it would be shocking, embarrassing or upsetting. What young people need in such situations is for adults to react in the right way. Nobody likes to be chastised for something they did not do or that was not their fault. It is important to think about the impact that this can have on children and young people, as well as the likelihood of them coming back to talk to their parents the next time something like this happens.

Another key area is cyberbullying. It is bullying – something that we have dealt with as a society for a long time – but the "cyber" component brings with it new challenges. Before the Internet came along if a child was being bullied, they were able to get some respite (at least until the next day) when they closed their front door after coming home from school – the bullies were not able to get to them there. Nowadays many children are constantly online. They keep devices with them in their bedrooms, which means that a bully can get to them at any time. Taking away the child's device and forbidding them from checking their messages seems an easy solution. But the device, via which they receive hurtful, unpleasant and offensive comments, is also their means of receiving messages of support from a friend or someone else they care about. It is valuable for them to know that someone (be it only one person) is actually looking out for them and is on their side. Cyberbullying manifests itself in a variety of ways. Quite often messages can be misconstrued or misinterpreted by the recipient. A comment posted online can have serious consequences, while the same message said in a face-to-face conversation, with the benefit of facial expressions, body language, tone of voice and context, could provoke a very different outcome. Being able to speak to someone and tell them what has happened is important. There are a number of very useful resources available for parents, carers and teachers to use in talking with young people about cyberbullying.

Another area which is, at the moment, constantly in the public eye is sexting. Often defined as consensual or non-consensual sending or receiving of sexual images (including appearing in such images) and/or texts via mobile and other devices amongst peers, it causes great concern for parents and teachers, yet is seen as mundane by many young people. It is a complex issue and in recent years there has been a great deal of research carried out looking into why young people engage in this type of activity and what we as concerned adults can and should do about it.

The first thing to say about sexting is that it is not the epidemic that some of the popular press would have us believe. Yes, it is happening, and most young people will probably know someone who has done it. But in many cases it is not a problem – images are shared with consent and nothing goes wrong. In the research[4] carried out among young people aged between 13 and 17 in Denmark, Hungary and the UK found that only 6% of respondents said that their nude or nearly nude image was shared with other people without their permission, 8% said that they had shared a nude or nearly nude image of someone else without that person's permission and 41% said that they had seen other people sharing nude or nearly nude images of someone they knew. As adults we can probably agree that most of the 41% had perhaps seen the same image which happened to be circulating around a particular school at a given time, but for the individuals involved, this can be devastating. If a person shares an image because they trust someone and never think anyone else will see it, only to find that their

[4] bit.ly/2YkHf1d [access: 7.05.2019].

trust was betrayed or something occurred which was not intended by them, it can be traumatic.

As mentioned earlier, it is particularly hard for children and young people to talk about this type of thing: it is embarrassing, awkward, simply difficult. Research carried out in Poland[5] found that young people who had watched pornography were 5 times more likely to engage in sexting. Unfortunately, the widespread availability of pornographic content makes this a real challenge.

Researchers agree that we (as adults) should understand that sexting is quite normal for today's teenagers and suggest that for many young adults sharing intimate images is increasingly seen as a normative part of courtship and dating. The key problem is that sexting is against the law if the image is of someone under the age of 18. In many countries this results in an indirect conflict with existing legislation – for example in the UK young people can legally have sex once they reach the age of 16, but it is illegal for them to share such images when under 18. This poses a great challenge for the legal system, which is struggling to manage the large numbers of young people who are (according to the research) engaging in this type of activity.

Many of the national Safer Internet Centres, which are part of the Insafe network, have developed guidance and resources to educate young people and adults alike about the potential dangers of sexting and how it should be approached. The *So you got naked online* publication (available in English and Danish) comprises materials helpful for young people who have come engaged in sexting. Rather than telling them that it is too late, the damage is done and cannot be repaired (which is precisely not what someone wants to hear when something like this has gone wrong), the guide provides sensible solutions and examples of actions which can help a young person to regain control and show them that all is not lost.

Similarly, the Belgian Safer Internet Centre has produced a guide for schools to help them to develop an approach to sexting[6]. If young

[5] Research, carried out by the Polish Safer Internet Centre, entitled "*Exposure to pornographic and sexual materials among children and youth – problem and solutions*". Presentation given by Szymon Wójcik, Dajmy Dzieciom Siłę [Empowering Children] Foundation at the Insafe Training Meeting, Manchester 18 December 2018.

[6] bit.ly/2HN7PF0 [access: 7.05.2019].

people, despite warnings, are nonetheless going to take part in such practices, perhaps a sensible solution is to talk to them about how to do it (more) safely? For some, such an approach may be too radical, but for a long time schools, parents and various organisations have been telling children and young people not to engage in sexting. As research suggests, to no avail – they are still doing it. When asked about this, a 16-year-old student explained that they knew lots of people who had shared images with a relationship partner and nothing had gone wrong, and added that they were willing to take the risk. Given that this is how many young people feel, perhaps a new approach is needed. In fairness, we talk to children and young people (from a fairly early age in some countries) about how to have safe sex and we do this long before we expect them to be having it. Maybe, then, we are sending mixed messages? As with all aspects of online safety, dialogue and discussion are paramount. Whilst very uncomfortable for many parents, sexting is not so unusual. Most young people carry a camera around in their pocket and taking a picture is extremely easy. This is very different from the reality of most parents. Stories of how this used to be done, of having to remove the film from the back of the camera and send it off to be developed, could be met with a lack of understanding on the part of today's children. For them this process is infinitely simpler, so we must accept that every once in a while they will make mistakes. Sharing some of the research and statistics with parents can be helpful in trying to ensure they do not overreact. They may not think it good that their children share images of this sort, but recognising that it is not so unusual might help them to react in a more measured way.

We know from scientific research that the pre-frontal cortex of a teenager has not developed to the point where they can think about, deal with, manage or understand risk or think about its consequences until it is too late. Teenagers will act first and think about the consequences later. In girls this part of the brain is fully developed by the early 20s, whereas in boys this process takes longer and lasts until their mid-20s. In effect, young people will take risks without a thought for what they will do if something goes wrong. Discussions with youth have found that constant reinforcement of the messages is useful. We should not, however, be telling them what not to do, rather we should present them with facts and information so that they are able to make more informed choices. A good example of this are online challenges. These are very popular and are often promoted by YouTubers who, of course, have a huge following with teenagers. "Pain challenges", consisting in enduring intense pain, are common but can have serious and, in some cases, fatal consequences. When young people are spoken with about risks, it turns out they do understand them, but they think that nothing will ever go wrong for them, that they will be careful or that the threats are exaggerated by adults or the media – the bottom line being it is not something for them to be worrying about. It is quite challenging for parents and teachers to address this. In some cases, raising awareness of a particular issue can cause more problems and can sometimes point young people towards something that they had previously been unaware of, i.e. it can give them ideas. Yet awareness among children and youth does need to be raised as, from time to time, this will be enough to put some young people off from undertaking such experiments. Although such conversations may encourage some, which may lead to problems, awareness and education (as always) are key.

Rules, policies and boundaries

Although young people are unlikely to admit this to their parents and teachers, they do appreciate some boundaries and guidance around their use of online devices. A common concern amongst adults at the moment is the amount of time children and young people spend online. Headlines warn us of a generation of young people addicted to devices, which results in mental health issues, depression, loneliness and many other concerns besides. Researchers are feverishly trying to assess the impact that technology has on our everyday lives. In early 2018 Apple's shareholders wrote an open letter to the company[7] demanding that they do more to address the concern that children are becoming addicted to their devices. Arguably, this is not just an issue for children but perhaps for society in general. It is very easy for teachers or parents to tell young people to stop spending so much time on their devices. But, of course, these very devices were designed to be used as much as possible. One can say that if it were easy to stop playing a particular game or spending so much time on a social networking site, the

[7] S. Gibbs, *Apple investors call for action over iPhone "addiction" among children*, "The Guardian", 8.01.2018, bit.ly/2qHxVUT [access: 7.05.2019].

developers would not have done their job properly. It is clear that tech companies have invested millions in designing products, platforms and devices that will keep us hooked. This is often referred to as persuasive design. In June 2018, the 5Rights Foundation published a research paper entitled *Disrupted Childhood – the cost of persuasive design*[8]. It looked at ways of designing the most popular platforms connected with user addiction. This can be seen for instance on YouTube where, when we finish watching one video, another one starts playing automatically.

Neither did Snapchat streaks, of great significance to young people, appear by accident – someone was paid to come up with the idea. This is a simple enough concept whereby one user sends an image/message to another. Each consecutive day that a message is sent both ways contributes to building up what is known as a streak, and these are very important to some young people. A survey carried out by the UK Safer Internet Centre[9] among young people aged 8–17 found that you needed 73 days in a Snapchat streak to show that you are a good friend. It is for this reason that some young people would be genuinely upset if a streak was broken. It is not unusual to hear stories about teens who have given their phone – or at least their Snapchat username and password – to a friend so they can streaksit for them. This is particularly common if they are going away with family and are unsure whether where they are going they will have a good Internet connection. It's better to get someone else to exchange messages on their behalf than to break the streak. A 15-year-old girl explained that she had a streak of 936 days. When asked how she would feel if the streak was broken, she faltered, but then said that she could not really imagine what that would be like. This would be the worst thing that could happen to her. Although not everyone in her peer group agreed – for some streaks were not so important – there was a considerable number of young people who nodded in agreement and admitted to being afraid of losing something they had spent years building up.

It is widely known that many social media sites have used some of the same strategies that the gambling industry employs in order

[8] bit.ly/2xcETBx [access: 7.05.2019].

[9] bit.ly/2sjp10s [access: 8.05.2019].

to keep people coming back for more. This is perhaps understandable, but not ideal when parents and teachers are worried about the pull technology already has on children and young people.

In fairness to tech companies, they have made some efforts to address this. During the summer of 2018, tools were built into the Android and iOS systems enabling users to manage their screen time and be more aware of what they are doing and for how long.

The tools work in much the same way on both platforms and are also built into some of the more popular apps and social media sites. Users are informed of how much time they are spending on their device per day and per week. This can be broken down into individual apps, e-mails, games, etc. It is also possible to set daily limits – so, for instance, if a user does not want to spend more than 45 minutes per day watching YouTube videos, they can set a timer and the device will notify them when the time is up. Of course, users can ignore the notification, but feedback from young people who have used the tools shows that even the raised awareness of how much time is spent and a reminder when a time limit is reached can be enough to moderate usage.

Another useful feature is the ability to turn off push notifications. Again, initial feedback suggests that this is helpful. Such notifications can be a distraction and abandoning whatever we are working on in order to quickly answer an e-mail or a Skype message can result in lack of concentration. Switching off such “noise” can be a helpful strategy to keep us focussed. Social networking sites have added some features, particular to the given service. For example YouTube have an option where users can be reminded to take a break, and Instagram offer a feature which tells users that they are “all caught up” and that nothing new has been posted, so scrolling through the feed becomes pointless as there is nothing there the user has not already seen. Of course, some will criticise these measures and say that it would be much better if these products were not purposefully designed to keep us hooked in the first place, and that tech companies have only introduced these tools because they were put under pressure to do so. Whatever the reason for their introduction, however, they are useful and raised awareness of the number of hours we are spending on our devices can be helpful and constitute the first step to changing our habits. Given that in 2018 the World Health Organisation designated Internet gaming addiction as a disorder[10] it would seem a step in the right direction to have access to tools which help us control such behaviours and raise user awareness.

A simple solution is for parents to take their child's device away overnight or insist that it is kept outside the child's bedroom. There is some conflicting research about the impact that using devices just before sleep has on its quality. Most scientists agree that the blue light emitted by the screen can supress the melatonin levels in the brain (melatonin is important in regulating sleep cycles) but there is disagreement as to how significant a role it plays. Yet it seems something else is the source of the problem. Many adults reading this will be able to think back to when they were children, and many will have read books with a torch under their bed clothes or duvet. Most likely they were not supposed to be doing it, but they disregarded the prohibition. Had they had a phone or tablet in their bedrooms at night, they would have watched television, played games, talked with friends or listened to music – simply because all this is really very entertaining. Ultimately, young people will need to learn to manage their time and entertainment on their own. Their parents will not be there once they begin working or head off to university. But to think that they can manage it at 11 or 13, or sometimes even at an older age, is a little naive. The issue in question concerns sleep, but also the way in which parents present their arguments. If they tell children that they cannot have a device in their bedroom because they have no confidence in them and do not know what they are going to be looking at, this is no good starting point for a conversation. Immediately, a conflict will arise. If, however, they suggest that devices be kept in the kitchen to be charged overnight and assure the child that this will be done by everyone in the family – as clearly devices can be as much of a distraction for adults as for young people – then this is an easier discussion to have. It is not about taking devices away permanently, only overnight, so they do not stop us from having a good night's rest.

Part of the challenge that parents and teachers face is that young people often believe that adults have a very negative view of technology. It is frequently demonised in the popular press and its benefits are

[10] bit.ly/2GzsL5n [access: 8.05.2019].

overlooked. We should reflect on whether, as a society, we do not have double standards here. For example, streaming sites offer shows and films actively encouraging viewers to binge watch them. This is frowned upon by adults who think that in this way young people are wasting time. But they are consuming content. A child who spends all weekend devouring a series of books, taking breaks only to eat and sleep, is also consuming content. Yet this child is often praised, possibly referred to as a bookworm, and ultimately seen to be spending time in a productive way.

The challenges that we face online are nothing new. If we refer back to the *EU Kids Online* project table, we can immediately see that the Internet did not create new risks – they have been around since the dawn of time. Parents and teachers constantly protect children from them in the real world. This comes naturally, adults do not think about it, it simply happens. To a certain extent, society is here also helpful. To use pornography as an example – it has been around "forever", but before the Internet came along it would have been much more difficult for a young child to get their hands on it. Not impossible, but pornographic magazines were placed on the highest shelves in shops and in many countries were not sold to anyone under 18. Pornographic films (once they became available) were purchased in adult sex shops, which only adults could enter. Presumably, many young people would have found it quite difficult to walk into one of those establishments, and in effect many simply would not have attempted it. No matter how offensive and distasteful the content of a pornographic magazine may have been, it was nothing like as offensive and distasteful as some of the content that can be found as a result of a fairly simple online search today. What is more, such a search can be carried out from the privacy of our children's bedrooms or from a device that they can conceal in their pocket when they hear someone approach. Anonymity and privacy mean that a lot of the risk and awkwardness has gone. Technology is a facilitator. The issues remain the same, it is young people's access to content that has become much easier.

Practical advice

Some of the advice we give children and young people regarding online safety is no longer fit for purpose. For example: "Don't talk to strangers online" is a message which has been shared with very young children for years now. The original reasoning for giving this advice made sense. As a society we were rightly concerned about the risk to children and young people from predators, individuals who would seek to do them harm, sexually exploit or abduct them. Children were often told stories about individuals who had suffered a terrible fate as a result of meeting up strangers encountered on the Internet. Unfortunately, although these stories undoubtedly shocked and caused young people to be horrified in some cases, they also provoked a reaction whereby they felt that this could never happen to them or to anyone they knew – they would not be that stupid, they would not make mistakes. From working with students we know that they do talk to strangers when they go online, many of them do this through online games such as *Fortnite*. It is important to recognise that this does not necessarily pose a problem. We do, however, need to be confident that if something goes wrong or if there is a cause for concern, young people will seek help, advice or support. So, for example, if while playing an online game a child hears something that makes them feel uncomfortable, worried or uneasy, they should inform an adult. The same applies if they are sent content (images or messages) which they feel are inappropriate or which make them feel concerned. Of course, children have to know that they should not go to meet someone they have only been talking to online. The good news is that most young people do understand this, even from an early age. The real concern is whether or not they are likely to speak to anyone about such problematic situations. If the response from an adult is to ban them from a particular game or service, they may be unlikely to seek advice, guidance or support. As mentioned earlier, very often whatever is happening is not the fault of the child but is the result of someone else's actions. Therefore, responding with a consequence that they feel is negative is not always the right solution.

Another example of such rather authoritative advice is: "Do not give out any personal information online". Again, the motive behind this makes sense, we do want children and young people to be more careful about the personal information they share – we should all be aware of what can happen to our data and how it can be used. Yet, today, it is not possible to do anything online without giving out at least some personal information, be it an e-mail address, a username or a mobile phone number. It is necessary to exercise care regarding what we do share, but saying that we should not give out *any* personal details is not fit for purpose as it is not realistic. A discussion around what we could share and an establishment of safeguards would be more helpful.

Students need to be able to relate to the advice they are being given. Feedback suggests that case studies are helpful as they enable children to see what has happened to people like them in similar situations. Providing young people with possible consequences of what they may be doing online can be a useful strategy as they are then able to make more informed decisions.

Technology as a facilitator

It is easy to underestimate the power of the devices we carry around with us. A mobile phone or tablet is actually a mighty computing device – most smartphones today have more processing power than the rocket that took the first man to the moon in 1969. We take it for granted, but it can backfire very quickly.

Young people are able to publish content to wide audiences at the click of a button, they can record videos on the go and instantly share them. They have seen YouTubers and other influencers making significant amounts of money from the comfort of their own home and it is understandable that for many this will seem an attractive way of making a living. Parents who tell their children that this will never happen and that they should be realistic about what they want to do in life are misinformed. Many young people who are still in school are being actively pursued by companies keen to strike a deal with them so that they can promote their content or products. We talk a great deal about children and young people chasing likes and followers but there can also be a tangible, monetary reward for having lots of these.

The Socialbakers[11] portal shared an article on different types of social media influencers. Whilst "macroinfluencers" need to have more than 100,000 followers, a "microinfluencer" only needs over 1000 – a number more than achievable for a teenager today.

Another example of where technology acts as a facilitator is with the purchase of drugs. This is a well-known problem, but before the era of the Internet it carried some risk for a young person as they needed to approach a dealer and pay for the drugs, and there was a chance that

[11] bit.ly/2Ljj3Bb [access: 8.05.2019].

they could be seen, reported or caught. Now, young people feel that the risk has diminished significantly as they can go to marketplaces on the dark web where they are able to purchase drugs at competitive prices and have them shipped in plain packaging to an address of their choice. The anonymity provided by the dark web affords them protection and so it is much easier (and less risky according to some) to engage in this type of activity than in pre-Internet days.

Digital footprint and online reputation

Everyone has a digital footprint or an online reputation, many of us will have Googled ourselves or, even more likely, will have Googled someone else – a future colleague, a friend or a possible partner. The Internet can provide a rich source of additional information which can help us to make more informed decisions about people. Many companies now admit that they carry out background checks on prospective employees using social media. This is a commonplace practice seen as part of the recruitment process. Indeed, some organisations now clearly state that an online check will be carried out before any appointment is made, so everyone is aware that it will happen.

The problem with our online reputation is that we are not in complete control of it. Other people can tag us in content, they can post images of us, tag us in posts or make comments about us. Research suggests that this can sometimes have a negative impact on our employment prospects. What do employers look for? The obvious: racist or homophobic content, references to drugs, images of people who are drunk, anything that could be deemed offensive, as well as behaviour which could be interpreted as bullying. The challenge is that a photograph on social media is a representation of only a split second in time and usually there is no context around it. It may give the impression that one thing is happening when actually it is something quite different. We know that employers, schools and universities carry out such checks, so it is important to talk to young people about how they can effectively manage their online reputation. Googling oneself and considering the impression that one is giving to others is a good idea and can be helpful in determining whether any changes need to be made to what is visible online. In the past, students applying to university or college often acknowledged that they had posted some content which could have given people the wrong impression or been misinterpreted. Their solution was to deactivate their account, secure the job or place at university and then re-activate it. Presumably, this used to be an effective strategy, but recent research from Career Builder[12] found that 47% of employers are less likely to call someone in for an interview if they could not find that person online. Therefore, not having an online presence is not necessarily the best approach.

There are countless stories about individuals who have lost their jobs as a result of an inappropriate comment or image shared online. Discussing these stories with students can be a useful reminder of what can go wrong.

Conclusion

Ultimately children and young people today are facing the same risks and challenges they have always done. Drugs, sex, bullying, violence all existed long before the Internet came along but the web facilitates access and exposure to all of these issues. Parents, carers and teachers need to focus on behaviours – what children and young people do when they go online – rather than worry too much about a particular app and how it might work. Providing support for young people and offering them a space where they can ask questions, share concerns and seek advice is vital. It is understandable that children will make mistakes, we all did, but those which can be made online are often more difficult to fix. Rather than responding with horror and shock, adults need to be sympathetic, understanding and supportive. Dialogue, discussion and education are the cornerstones of helping to keep children and young people safe online. We should talk and listen to them and work out solutions together.

There are many useful resources that can be found in multiple languages on the Better Internet for Kids portal (www.betterInternetforkids.eu). These come from the Insafe network of Safer Internet Centres (SICs). Co-funded by the European Commission, there are 30 SICs around Europe. They raise awareness, operate a helpline for children (as well as parents and teachers), a hotline and a contact point. The SICs work to promote safer online behaviours and have a wealth of resources that can be used by parents, teachers and young people alike.

[12] bit.ly/2wxacY7 [access: 8.05.2019].

Useful resources

Parents

- → Digital Parenting website from Vodafone: bit.ly/2Xklqi5.
- → www.internetmatters.org – excellent information for both parents and teachers.
- → NSPCC website: bit.ly/1KDWgdW.
- → www.commonsensemedia.org
- → bit.ly/2Mrfeg4 – guide for parents on screen time (advice).

Resources for using with children and young people

- → www.betterInternetforkids.eu – resources from the Insafe network of Safer Internet Centres around Europe
- → www.webwewant.eu – peer education resources (new online lesson plans to download)
- → www.childnet.com
- → www.thinkuknow.co.uk
- → www.digital-literacy.org.uk – digital literacy curriculum for all ages.
- → bit.ly/2XBG3Fw – contains lessons and information on criminal consequences.
- → bit.ly/31Ttvc5 – manual for combating hate speech online.
- → www.enable.eun.org – resources and lessons on cyberbullying.
- → www.allaboutexplorers.com

Sexting

- Sexting in schools – advice and support around self-generated images bit.ly/2FQgDdt.
- British police action in response to youth-produced sexual imagery (sexting): bit.ly/2fDQHSi.
- British Home Office and Govt. Equalities Office guidance: bit.ly/2ywiTSM.

Guidance on policy

- British Internet Safety Strategy (DCMS Green Paper) and Govt. response to it (May 2018): bit.ly/2FDNCRT.
- Cyberbullying – advice for headteachers and school staff: bit.ly/2WSvrQt.
- Advice for parents and carers on cyberbullying: bit.ly/2Ws8IM6.
- www.360safe.org.uk – free audit tool from SWGfL.
- Filtering and monitoring guidance for schools: bit.ly/280dHC8.

Research

- www.saferInternet.org.uk/research – over 100 research summaries from the UKCCIS evidence group
- Ofcom media literacy report (November 2017): bit.ly/2Yl0szZ.
- Digital friendship report from UK SIC (February 2018): bit.ly/2RPtwJz.
- deShame (young people's experience of sexual harassment online): bit.ly/2KaLpjq.
- *Disrupted childhood report* – bit.ly/2GG40BT.

Home

Faces of privacy – challenges and opportunities related to informed participation in the virtual world

Agnieszka Wrońska, Anna Rywczyńska

The article attempts to analyze the term privacy, both in terms of meaning and definition, as well as the social phenomenon in the context of the digital technology. The presented research overview indicates a revolutionary increase in the use of the network in the recent years, especially in the context of the youngest internet users. Their ever-longer presence in the network, often exceeding five hours a day, the increasingly young age of independent use of the web as well as the openness and intense presence in the social networks create more and more challenges in the field of media education. The ability to consciously participate in a virtual world can counteract potential threats, protect against risky behaviors, and help in shaping the digital identity safely. In the context of challenges related to privacy, the authors also present new phenomena such as deepfakes technologies or the "Internet of toys".

Keywords:
cyber dangers
child in the internet
internet
social media
media education
online privacy

Home

Introduction

Privacy is an important and ever more widely discussed topic in contemporary social and legal sciences. From the point of view of dangers related to the development of the Internet, protecting the privacy of young people surfing the net seems particularly important. The Internet is very popular – its rapid growth in popularity is due to a number of infrastructural, economic and social factors, related both to easier access to the web and to benefits resulting from its use. The development of technology has made it possible to connect to the web from anywhere, via any adequately equipped device (tablet, smartphone, laptop, notebook). The attractiveness of the Internet results from the possibility of gaining quick access to up-to-date information, to communication with others, as well as to various types of content. This tool allows people not only to use the available information, but also to create their own content and publish it. The social dimension of Internet use seems particularly interesting. With the dissemination of this tool, borders between countries and languages have disappeared – users from all over the world can easily communicate with one another anytime and anywhere, and distance has ceased to form a barrier to interaction. The influence of the Internet on behavioural models in societies and individual social groups is also noticeable (Wrońska, Lange, 2016, p. 15). The scale of changes is determined by customs, habits and ways of using the Internet by both the general public and young people. And it is the latter group that is perceived as the most active online.

Before the Internet era, the protection of privacy concerned specific areas of human life: health care, schooling, work, as well as diaries or information provided orally. Coming into possession of someone's data or information about them could only be done by breaking into an archive or obtaining materials from a third party. However, the scope of both access to data and their potential distribution was very limited. The development of digital technology has resulted in most formal information about virtually any person being available on the Internet, and the success of social media – in mass publishing of images, videos and records of our everyday life, which from private archives are instantly sent to hundreds or thousands of recipients. The net allows users to present their achievements, promote their work and skills, and establish relationships and friendships, regardless of distance.

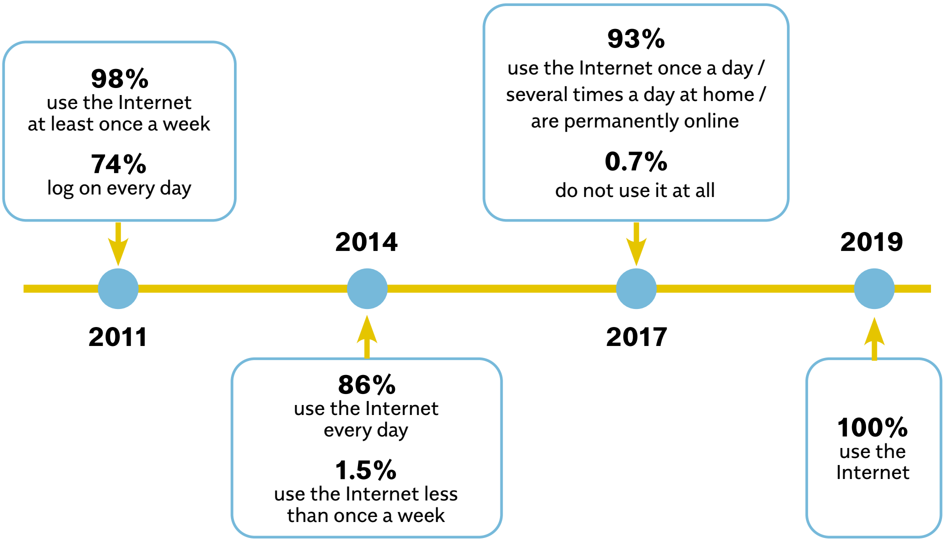
Having as many online "friends" as possible on social networking sites gives especially young people a sense of satisfaction and happiness. It also raises their self-esteem. On the other hand, when publishing information about themselves, often without using privacy settings to manage their profile in a safer manner, they let into their world people whose intentions or actions towards them may pose a real threat.

Web services, websites and portals, which require a lot of data when logging in, do not always guarantee effective protection. Almost every day the media inform us about another serious "information leak" (for example, hacking into nearly fifty million Facebook accounts or taking over large collections of personal data from online dating systems, which served as storage tanks for big data). User data on the Internet also include digital footprints that we or our friends and acquaintances leave behind. These are trails of data the existence of which we may not be aware of or which we do not necessarily want to identify with after a few years' time. For this reason, minimising the amount of personal data posted online, as well as systematic verification of our online identity are key elements of controlling our digital image. From the point of view of dangers related to the development of the Internet, protecting the privacy of young users seems particularly important. Research shows that almost every member of the young generation uses the Internet, but youngsters are not always able to protect themselves from prospective dangers of the virtual world.

Young people online

The scale of young people's Internet use is changing at a very fast rate. In 2014, 74% of teenagers declared they used it daily. In 2016, this percentage already exceeded 93% (*Nastolatki wobec Internetu...*, 2014; Kamieniecki et al., 2017, p. 9).

Figure 1. Internet use



Source: Own work based on L. Kirwil (2011), *Nastolatki wobec Internetu*... (2014), *Nastolatki 3.0* (2017, 2019).

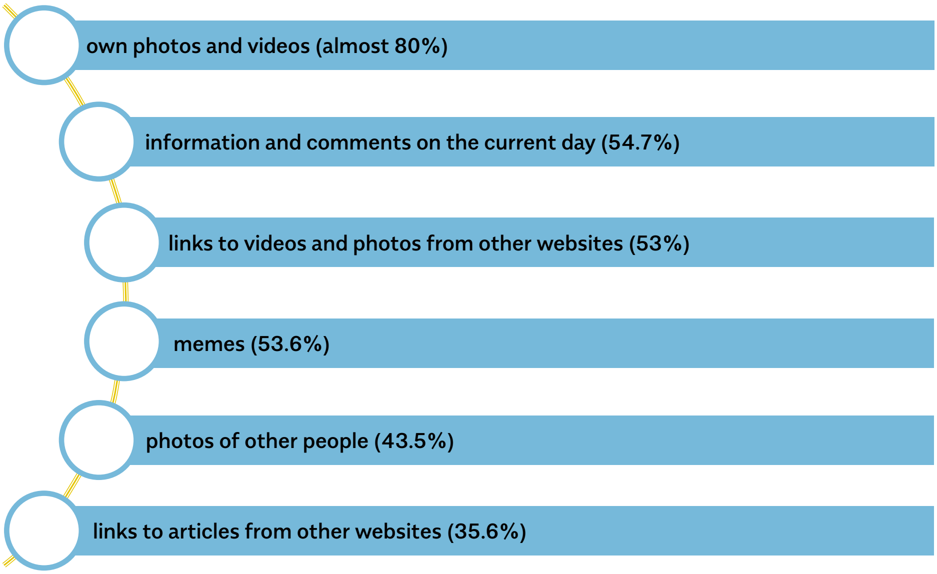
Thanks to the development of mobile technology, the Internet has become a teenager's companion at school, in public places, and on public transport. The vast majority of young people declare that they use the Internet many times a day or all the time: at home (80%), at school (39.2%), at their friends' (32.4%), in public places with Wi-Fi access (29.7%) (Kamieniecki et al., 2017, p. 9). They undertake many different activities on the Internet, where they have "always" been. To them, the web an inherent part of life, and virtual space accompanies them in their cognitive, recreational and interactive activities (Wrońska, Lange, 2016, p. 15). We can also observe a systematic lowering of the age at which children start using the Internet on their own. Only a few years ago, children started their online activity at the age of 9 or 10 (Kirwil, 2011; *Nastolatki wobec Internetu*..., 2014; Tanaś [ed.], 2016). At present, they start using the Internet at the age of 7 or even earlier (UKE 2017; Wrońska, Lange et al., 2018, p. 13). The Internet attracts young people because of its ease of use, interactivity, as well as its use of hypertext and multimedia. It supports school education, serves as a source of information and knowledge, helps in the development of passions and interests, and more and more often becomes the arena for creative activity, shaping one's image, expressing oneself and establishing and building social relationships. To children and young people, the Internet is first and foremost a sphere of learning about the world. They attach importance to access to web browsers (86.7%), to the latest information (80%), to entertainment (57.4%), and to videos and music (86.4%), and 71.2% treat the Internet as a communication tool (Kamieniecki et al., 2017, p. 46). Slightly less frequently, young people view the Internet as a medium for self-presentation, and use it to maintain current contacts and establish new ones (43.5% use it to meet new friends, 42.6% – to access information about other people). Almost all young Internet users are active on social media websites – 95% of teenagers declare that they have profiles on social networking platforms, and their activity on these forums correlates with everyday life offline (Kamieniecki et al., 2017, pp. 52–54). The vast majority of teenagers indicate that they use the Internet every day, and thanks to mobile devices (especially smartphones) almost half stay online all day long.

"The Internet has enabled the emergence of cyberspace and numerous virtual worlds. A teenager entering these worlds has a real influence on them. They can become who they want, not what others want them to be. They are free. They decide on the types of activities they undertake online, create and learn, listen and watch. They can be passive or active users. They have a sense of subjectivity [...]. They create their own lives in cyberspace. They do not need to adhere to any orders or bans. In their opinion, they are anonymous and are not (and will not be) accountable for their actions. They band together with friends to take social action, establish individual contacts, look for their sweetheart and friends who will understand them, post comments, use instant messaging applications and social networks, share photographs, videos and experiences, play games and to an ever greater extent shut themselves away in their very own interactive and multidimensional electronic space" (Tanaś, 2016a, p. 8).

Apart from its undeniable advantages, using the Internet also carries several genuine risks. These include malicious software and contact with harmful contents published online. However, these dangers also result from risky behaviours displayed by teenagers and dangerous relationships they establish, which have consequences in various spheres of life, be it financial, psychological or social. Privacy is also extremely important, as young Internet users who are often unaware of the consequences of not protecting their privacy or who neglect the ramifications of their actions are particularly vulnerable to repercussions unforeseen by them.

Social networking sites are used by teenagers above all to present themselves, communicate and meet other people, but also to share materials, both their own (private photos and videos) and those published by others. The study entitled "Nastolatki 3.0" ["Teenagers 3.0"] indicates that young social media users are making more and more information available in their profiles. In addition to basic data, such as name and surname, teenagers disclose information which makes it possible to identify them. In their profiles young people usually post photos presenting or documenting their various activities, as well as personal information and opinions (Figure 2).

Figure 2. Materials published by teenagers on social networking sites



own photos and videos (almost 80%)

information and comments on the current day (54.7%)

links to videos and photos from other websites (53%)

memes (53.6%)

photos of other people (43.5%)

links to articles from other websites (35.6%)

Source: W. Kamieniecki et al. (2017).

One of the most important dimensions of online activity is the approach to privacy in cyberspace. Although an increasing proportion of young people are aware of the consequences of making private information and content available online, there is still a large group of them who do not protect their data. The youngest Internet users form the largest group here. The vast majority of teenagers apply various procedures to control their digital identity (sharing information only with friends or modifying the possibility of access depending on the type of information presented), but despite the declared knowledge of protective mechanisms, young people online disclose a lot of information about themselves. Online information management changes with the age of teenagers, which results from the growing needs and concerns of the young generation. The majority of respondents declare that they are aware of the possible consequences of lack of control over content posted on the Internet and take various actions to protect their data and content in the virtual space (57.6% say they limit access and protect their privacy, 8.2% use appropriate privacy settings because they are afraid of misuse of their data or photos). However, every fifth respondent (21.9%) claims that they do not see any particular risks connected with this, and therefore they do not feel the need to limit access to their materials, and 5.2% of respondents do not filter information about themselves on purpose, because they want it to reach as many Internet users as possible. In general, the surveyed population is familiar with procedures for restricting online data accessibility. Only a small percentage (1.8%) of respondents indicated that they did not know how to apply such procedures (Kamieniecki et al., 2017).

Table 1. Distribution of answers to the question:
"Why have you chosen the profile settings you are using?"

ANSWER	PERCENTAGE
I restrict access, because I want to protect my privacy	57.6%
I do not use privacy settings, because I want to be visible to as many users as possible	5.2%
I do not see the need to restrict access	21.9%
I do not use privacy settings, because I do not know how	1.8%
I use privacy settings, because I'm afraid of misuse of my data and my photos	8.2%
I do it for other reasons	1.9%
I do not use social networking sites	3.4%
Total	100%

Source: Kamieniecki et al. (2017).

Online image

The modern world offers many ways to create our own image and identity – it is entirely up to us to decide who we are and where we are going (Giddens, 2004, p. 53). There are many opportunities to become popular on social media and actively contribute to shaping the virtual world by posting our own text and multimedia content (e.g. blogs, forums, comments and tweets), which is very tempting for many people. The Internet makes it easier to present our achievements and experiences, as well as to promote our work. It also makes it possible to establish new relationships, as the content can be viewed and commented on by users from all over the world. At the same time, low user awareness of data protection issues and lack of awareness of the consequences of sharing one's daily activities with others increasingly blurs the boundary between private and public life and between openness and provision of too much information. It often happens that Internet users lose control over how much and what information about them is communicated to others. Having in mind the amount of data about us that are available online, and of which we are not even aware, it seems crucial to systematically check both the history of our online activities and data that may have appeared on the web without our being aware. The popularity of websites where it is possible to carry out an online identity audit is growing rapidly. By entering our email address or name in the portal's search engine, we can track what information about us appears on the web. The global reach of the net and diverse privacy laws in different countries often result in our data being transferred between different systems and portals. The biggest change in the scope of systemic personal data protection was introduced by the General Data Protection Regulation (GDPR)[1] of 25 May 2018, which obliges Internet providers and web portals to strengthen personal data protection and imposes an obligation to immediately delete personal data and any account data at the request of an Internet user submitted to the administrator of a given service.

Personal data protection on the web is something we have only partial influence over. Even caring about our image on the Internet and a proper selection of information that is published may not protect us from having our photos or videos presented in circumstances we have not agreed to or transformed using the latest technology to modify content, which results in so-called deepfakes. This technology allows for image synthesis using Artificial Intelligence and machine learning to combine existing images and videos with other source images. This solution is used, among others, in the film industry, as it allows great savings to be made in the production of films, in recording scenes without the participation of actors or in the upgrading of older films. Unfortunately, this solution is mainly associated with the pornographic industry, where it is used to produce fake films involving, for example, public figures. Deepfakes are also used to create false information and can be a tool in an unethical political struggle (for example to manipulate statements of political figures).

Privacy – definitions

The term "privacy" repeatedly appears in publications, but despite several attempts to fully describe the notion, it is difficult to establish a universal definition, mainly because of the extent of the phenomenon and the constant changes in elements comprising the privacy of an individual. The majority of definitions only highlight certain aspects of privacy. Of course, the boundaries between the private and public domain differ depending on the era and society, hence the constant changes in what people consider to be private information.

[1] General Data Protection Regulation (GDPR), Article 17 (1).

Privacy is also linked to specific conditions, meaning that the same information can be considered private when it is shared in certain situations and not in others.

What is more, individual Internet users' understanding of privacy and the public sphere seem to change and blur due to the interpenetration of and interaction between the online and offline worlds. Research into online privacy management is conducted simultaneously in several disciplines, e.g. IT and technical sciences (in which the term is considered, *inter alia*, from the perspective of ICT security in its broadest sense, data protection in the digital space and protecting ICT systems against hacker attacks or unauthorised use of data) (Klimek, 2015, p. 96), as well as legal sciences (*inter alia*, from the point of view of data protection and accessibility of online information as well as legal implications of the right to privacy) and social sciences (the focus here is on e-skills and attitudes, as well as the causes, consequences and interdependencies of changes in the privacy domain and of the Internet's impact on its users).

Privacy is often seen as a right guaranteed to every individual. Louis D. Brandeis and Samuel D. Warren were the first to write about it at the end of the 19th century. They termed it "the right to be alone" – the right to privacy, exclusivity and separateness of what is secret (Pryciak, 2010) and "the right to be left alone" (Gajda, 2008; Siuda, 2015, p. 39), i.e. the right to have a sphere free from the interference of other people, especially the authorities (Breardsley, 1971 [after: Braciak, 2004, p. 38]), understood as the opportunity to decide how much information about ourselves we want to disclose. With their article, these researchers opened a discourse that has led to the right to privacy being universally known, evolving and becoming a fundamental human right. Joseph Kohler described privacy as the freedom to dispose of information about ourselves (Kohler, 1907 [after: Braciak, 2002]). Nowadays, this concept has taken on a broader meaning. According to Beate Roessler, privacy means "the right to be the author of one's own biography" (Roessler, 2010 [after: Młynarska-Sobaczewska, 2013, p. 35]), and is therefore understood as the right not only to seclusion or to keep a secret, but also to decide about our own fate, corporality, and personal and family life, as well as to shape our relations with those around us and our history in our own, freely chosen way (ibid.). This allows us to distinguish three important dimensions: the right to decide about one's corporality (privacy of the body, physical privacy); information privacy, which consists in deciding what information we disclose about ourselves; and personal (local) privacy connected with determining our behaviour and family relations as well as relations with the community. Thus, the need to ensure privacy from the point of view of new technologies can be identified to a large extent with information privacy, and not only with other types of privacy, such as economic privacy guaranteed to businesses (Siuda, 2015, p. 39).

Definitions of privacy (in Latin *privatus* – separated)[2], which can be found in encyclopaedias and dictionaries, describe it as the ability of an individual or a group to control their data and personal habits and behaviours that are not known to the public. In the broadest sense, privacy is identified with an individual's autonomy and independence – it is the possibility to independently decide about one's own life, i.e. it is the freedom to choose one's own way of living without any external interference. It can also be considered from the point of view of the ability of an individual or group to disseminate information about themselves only to selected individuals. Diverse approaches make it difficult to determine a single, full and unambiguous definition of privacy.

We can distinguish three basic methods of approaching privacy: the relational (iterative) one, concerning the control of social contacts; the informational one, relating to resources and nature of information provided; and the spatial (physical) one, relating to the physical accessibility of a person (Dopierała, 2013).

From the point of view of the law, privacy was presented by Andrzej Kopff (1972), among others, as a personal good: "private life includes all elements that, because of the individual's justified isolation from the general public, serve to develop their physical or mental personality and to preserve their social standing".

[2] According to the definition in the PWN *Dictionary of the Polish Language*, the term "private" means: "belonging to or for the use of one particular person", "not subject to the state or to any public authority", "concerning personal and family affairs of a person". The definition in the Small Dictionary of the Polish Language reads as follows: "concerning someone personally, forming someone's personal property, not connected with any institution, office", "non-state, non-official, informal". Encyclopaedias, lexicons and dictionaries provide different definitions of the term "privacy" which, for example, relate to the private or personal nature of something or something that is not intended to be made public, or define it in terms of ownership (as a good not available to everyone or available to a limited extent).

Various conceptual approaches and ways of describing the notion of privacy can be found in the literature on the subject. Daniel J. Solove has developed six categories for these definitions, according to which privacy is the right to freedom, restricted access, secrecy, control of personal data, personality, and intimacy (Solove, 2002). Similarly to legal sciences, there have also been attempts to define the phenomenon of privacy in the field of social sciences. Stephen T. Margulis organises these proposals by distinguishing three groups of meanings: common, empirical and legal (Margulis, 1977 [after: Jędruszczak, 2005]). The definitions collected and quoted by Margulis, which have been developed by various authors, clearly point to the multifaceted nature of privacy in behavioural and social sciences. This concept was referred to, among others, as "selective control of access to an individual or a group to which an individual belongs" (Altman, 1977). It was shown that "privacy refers to the denial of potential power relationships between an individual or a group and other individuals" (Kelvin, 1993). It was also said that "in the psychological sense, it maximizes the freedom of choice, allows an individual to feel free, to behave in a certain way or to broaden the range of options in relation to such behaviours by reducing certain types of social constraints" (Proshansky, Ittelson, Rivlin).

Convenience and data security

The results of the global *EMC Privacy Index* survey held in 2014, which show how consumers around the world view online privacy rights and opportunities, as well as their willingness to trade some of their privacy for benefits or convenience offered by online services, are very interesting. The survey involved 15,000 respondents from fifteen countries. The results identified three paradoxes related to privacy and confidentiality: "We want it all without compromise", "No action" and "Social sharing". Users claim that they want to benefit from technology, but at the same time they do not want to give up their privacy for this. Almost all respondents (91%) appreciate the advantages of digital technologies because of easier access to information and knowledge, but only 27% of them are willing to give up some of their privacy for greater convenience of using online services. Although many consumers are directly affected by privacy risks, the majority of respondents admit that they do not take any action to protect their data – 62%

do not regularly change passwords, four in ten do not customise privacy settings on social networks, and 39% admit that they do not use password protection on their mobile devices. Consumers tend to believe that this is rather the responsibility of those who process their data, governments and businesses for example. On the one hand, the majority of users of social networking sites (84%) do not want anyone to know anything about them or their habits until they want to disclose this information themselves, but, on the other, they acknowledge that they freely share large amounts of personal data – despite the lack of trust in those who are supposed to protect this information.

The "EMC Privacy Index" survey report confirms that the behaviour of Internet users differs depending on the activities they undertake online. Their attitude towards privacy issues varies depending on their role (e.g. citizen, patient, employee or consumer). For instance, there is a greater willingness to give up civic privacy, but in social networks users were least likely to give up privacy in exchange for a better service. The conclusions of the report concern three groups: consumers, businesses and technology providers. According to the authors, there is a need to raise awareness of privacy issues and take individual actions to protect consumer privacy. Businesses should be able to demonstrate that they apply the most effective and practical methods to protect their customers' privacy. The task of technology providers is to increase the level of privacy protection in their solutions, but without compromising user comfort, performance or range of possibilities.

Studies on the privacy of Polish Internet users were conducted in 2013 and 2016–2017 by the Interactive Advertising Bureau IAB Polska[3]. The results indicate, among others, that Poles are doing increasingly better in terms of privacy and more and more often use various types of security measures that protect them. The Internet is perceived by its users as a public space (apart from private websites, other Internet services are considered as public or partially public). The level of awareness and knowledge about privacy is increasing. Only 4% of the surveyed network users declared that they do not use any form of privacy protection. The most commonly used security

[3] *IAB* (2013; 2017), *Raport: Prywatność w sieci 2013* [*Privacy on the web 2013 report*]; *Raport: Prywatność w sieci 2016/2017* [*Privacy on the web 2016/2017 report*]; bit.ly/2SYoTMM [access: 23.10.2017].

measures concern protection against viruses, but in comparison with the previous study, we can also talk about the growing popularity of security mechanisms and methods to protect privacy. The results of the 2016 report show that, compared to the previous survey held in 2013, the percentage of people who care about their online image has also increased. For example, the respondents do not upload private photos and use aliases (49% in 2013 and 62% in 2016). Internet users are more aware of and are interested in privacy, but at the same time they declare that they are not sufficiently informed about it. Their declaration on personal data sharing is very interesting. On the one hand, they underline their unwillingness to disclose their data online, and, on the other, the vast majority confirm that they knowingly place such information on the Internet.

Many Internet users are aware of the principles of operating in the digital environment and see the benefits of content personalisation. The results of the "Prywatność w sieci" [Safety on the web] survey, similarly to the "EMC Privacy Index" quoted above, show dilemmas related to privacy. In this case, they relate to the difference between the declared desire for maintaining privacy and the willingness to use automatic matching of content to the needs of recipients. On the one hand, the vast majority of respondents (79%) claim that they are bothered by behavioural profiling performed by websites, yet on the other hand, they accept the content of websites and advertisements tailored to their preferences based on such a behavioural profile of themselves (IAB, 2017, p. 14).

Children online – adults' responsibility

According to the latest research on the online activity of the youngest Internet users in Poland (*Korzystanie z urządzeń mobilnych...*, 2015), 64% of children aged from 6 months to 6 and a half years use mobile devices (25% of them do it every day). In the group of 1- and 2-year-olds, as many as 43% use this type of devices, and in the group of 6-year-olds – 84%. Youngsters' online presence often begins before they are even born, with the publication of their ultrasound images by their parents. It is the parents who decide to publish images of their children from the moment of their birth, often unknowingly exposing them to future consequences (for example, subjecting them to mockery by their schoolmates). The phenomenon of parents ridiculing children with pictures taken, for example, during their first meals or intentionally ridiculing children as a punishment or joke has even been given a separate name – troll parenting. For this reason, public discourse starts to involve talking about the need to educate adults on how to protect the privacy of their children. Parents' and teachers' awareness of online privacy is also crucial in order for them to be able to support young people when they start to enter the world of social media on their own. Children often ask parents for help or permission to set up their first online profiles. This is why adults need to know the age at which such activity is allowed. According to the GDPR, 13 is the minimum age in Member States of the European Union. Depending on national regulations, in some countries it is 16. It may also be helpful to know the most popular social networking sites and the privacy settings they offer.

Internet of Toys

The Internet of Things (IoT) is an evolving phenomenon, which is also related to child privacy. Devices based on Internet infrastructure and mobile technologies pose risks related to cybercrime, i.e. to possible intrusions to retrieve user data stored on such devices and to create false identities on its basis. They also involve challenges related to recording a child's interaction with a device. What we mean here is the Internet of Toys, i.e. interactive toys with Internet access that record "conversations" with children and make them available to parents via dedicated applications. Research carried out as part of the project entitled "Internet zabawek – wsparcie dla rozwoju dziecka czy zagrożenie" [Internet of Toys – support for a child's development or a risk?] (Rywczyńska, Jaroszewski, 2018), shows that the majority of children do not realise that they are being recorded, and that communication with the toy can be very easily made available on social networking sites, for example.

From the point of view of young people, the Internet of Things also stands for wearable technology. Such devices are often used to increase security, but can also make children accustomed to constant monitoring and control, which may not be without an impact on their development processes. In 2016, Family Online Safety Institute[4]

[4] bit.ly/2h4a9tm [access: 20.03.2017].

published a document entitled: *Kids and the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots*, in which the world of smart toys is analysed from the point of view of safety and the principles of application of the rights enshrined in COPPA (Children's Online Privacy Protection Act of 1998)[5] in relation to toy manufacturers and to suppliers of the implemented technology.

According to "Forbes" magazine[6], experts estimate that by 2025 more than 70% of households across the globe will be equipped with smart devices. The aim of the above-mentioned project focussing on the Internet of Toys (Rywczyńska, Jaroszewski, 2018) was to identify the extent to which the Internet of Things is widespread in Poland, i.e. to test the presence of smart toys and knowledge regarding them. In 2017, quantitative and qualitative research was carried out to this end. The quantitative survey was conducted on the Ariadna panel on a nationwide sample of Polish Internet users (1051 people) aged 18 and over, while the qualitative survey was conducted using in-depth interviews. The interviews were carried out in the places of permanent or temporary residence of the respondents. Twenty-four interviews were conducted with families differentiated according to their place of residence, level of education, number of children and number of carers in the family (both parents or a single parent). Quantitative surveys had to be carried out twice, as the first survey revealed a major problem with the definition of devices belonging to the Internet of Things. Often smart devices were confused with "intelligent" washing machines or dishwashers, which simply have more functions than standard appliances. The most popular smart device in Poland was the smart TV set, the use of which was declared by almost 50% of respondents. Next, in a descending order, cameras, alarm systems and home cinema systems were reported. Currently, around 4% of respondents own interactive toys for children. Interviews with families have confirmed that people using smart devices are very often not aware of what "smart" means.

The aim of the study was also to examine how the development of the smart toys market is perceived. The residents of large cities

[5] bit.ly/1IJZNI0 [access: 20.11.2018].

[6] bit.ly/2G8C5d0 [access: 10.11.2017].

have the most positive attitudes towards these technologies – 10% of them answered "Yes" to the question: "Do you think that the fact that more and more toys are connected to the Internet is a positive thing?" A neutral and positive approach was predominant, although almost 30% of the respondents expressed great concerns. Most often, parents paid attention to the issue of protecting their child's privacy. They were afraid that the toy could instil in the child false emotions and that the child could be exposed to dangerous contacts. People with a positive attitude towards smart toys hope that they will have a positive impact on the child's development, especially on their education. When buying a toy for their child, over 60% of people are guided by the safety of the toy. It is not known, however, if this translates into issues related to Internet safety, because the topic of online threats is still rarely present in Polish homes. More than 15% of parents do not discuss the issue and 38.5% discuss it rarely.

Therefore, online privacy seems to be an extremely complex and ambiguous topic. When deciding on the presence of digital technology in our lives and on the opportunities it offers, we must make daily choices between convenience and anonymity, between the safety of our children and the right of young people to individual, private spaces in which adults should not interfere. Therefore what is of paramount importance is the development of media education, interdisciplinary work on building digital citizenship – raising awareness of how to use the Internet effectively and ensuring that at the beginning of their digital lives children can count on informed adult support, a responsible approach on the part of businesses and support provided by the school at every stage of education.

Home

Business models in online gaming and their implications for the protection of minors

Anne Mette Thorhauge

In this chapter I will describe how the business models in online gaming have evolved throughout the previous decade and discuss the implications this has for the protection of minors in online environments.

Keywords:
online games
business models
hazard
youth

Home

Introduction

The protection of minors in online environments has traditionally focussed on the risks of exposure to inappropriate content such as sex or violence or on the "stranger danger", that is the risk of encountering people with bad intentions. The former perspective has been inherited from earlier media such as film and television and is often met with countermeasures grounded in similar lines of thinking, such as content classification and parental controls. The latter has grown as Internet-based services have become key arenas for social contact, and has been countered by attempts to create "safe spaces" for children or by ensuring that they possess sufficient critical knowledge to navigate the Internet in a safe and sound manner. In addition to these more traditional concerns, a more recent one relates to the alleged addictiveness of mobile technologies, games and online services. This concern is based on the assumption that the use of specific digital technologies can lead to addiction, i.e. excessive and uncontrollable engagement with the digital world with detrimental effects for the well-being of the child.

In this article an alternative approach, focussing on the evolving business models of video games and the way they are embedded into the games' design, is suggested and substantiated. As these business models often result in players spending ever more time and money, it is no wonder that the games are sometimes likened with addictive substances and practices. Yet, shifting the focus from a "pathology of the individual" to a critical review of the way such games are constructed opens up alternative perspectives on the protection of minors, including different strategies for parental mediation and, potentially, legal regulation. This stance will be substantiated in subsequent sections, which describe the ways in which gambling can appear in games as this is an important backdrop for the development of business models in this field. Afterwards, it is explained how the evolution of business models in online gaming follows a general development of web-based services and microtransactions on the Internet. This is supplemented by a description of how this new business approach is implemented in the game design in the form of specific "mechanics". In the following section, there is a discussion of dynamic economic phenomena at the level of gaming platforms and the broader platform ecosystem, and of what brings about economic phenomena and business models worth looking at when it comes to the protection of minors. In the final section, the question why this development should make us readdress our notion of "risk" in online environments is answered, and strategies for protecting minors there are presented.

Gaming and gambling on the Internet

Gaming and gambling can be linked in a range of ways, which has direct implications for the protection of minors. Traditionally, the question has been approached from the field of psychology using the diagnosis of pathological gambling (or comparable lists of potential symptoms) to explain excessive gaming. More recently, a range of alternative perspectives has emerged due to the development of business models in online gaming. They refer to the partial convergence of gambling and gaming industries on social media, which took off in the beginning of the 2010s and has influenced design principles and business thinking in other gaming domains, as well as the emergence of actual gambling in the peripheries of player-driven economies. This does not mean that gaming and gambling are two sides of the same coin or that all online gaming should be treated as gambling. Rather, it means that strategies of customer acquisition, retention and monetisation, which are employed across a broad variety of business domains, are appearing in new ways in online gaming, and some share the characteristics of traditional gambling. Moreover, it should be pointed out that the traditional approach to gaming and gambling involving diagnosing excessive gamers with "video game addiction" is insufficient if we are to understand the potentially problematic features of online business models. In the remainder of this section it is explained in detail (on the basis of research results) how gambling and gaming can be linked. This includes:

- the application of pathological gambling diagnosis to excessive gamers;
- the simulation of traditional gambling games, primarily in social media;
- the integration of retention and monetisation strategies in game mechanics;
- the integration of retention and monetisation strategies above the level of individual games; and
- actual gambling in the context of player-driven economies.

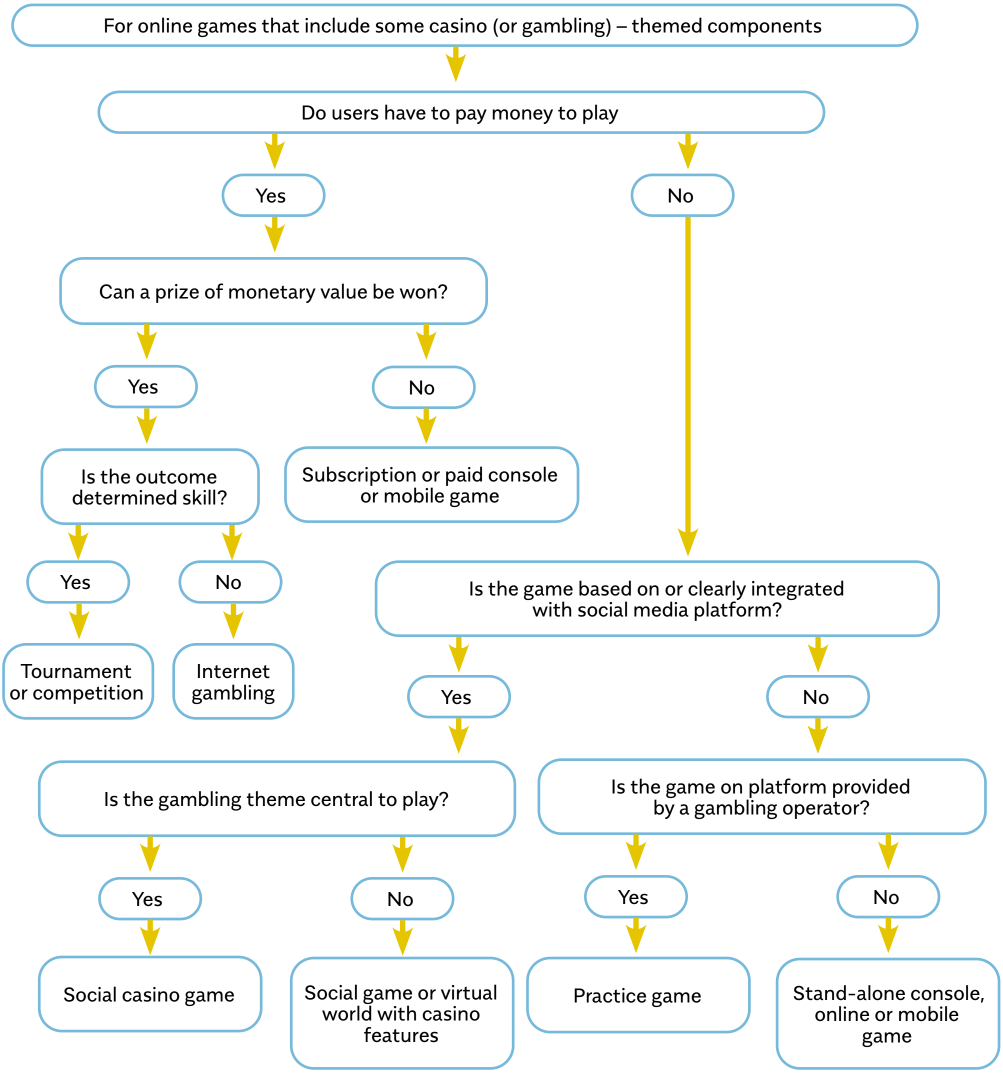
The application of pathological gambling diagnosis to excessive gamers

In psychology we can find a fair amount of research dealing with the notion of "video game addiction". Though the specific symptoms applied do vary, the basic rationale remains the same. By way of surveys a set of symptoms assumed to define a pathology is mapped onto a sample of gamers in order to determine whether they may be defined as "addicts". Though this model of explaining this phenomenon has been the object of extensive empirical research, it is also highly contested. Moreover, seen in a broader theoretical context, this approach tends to ascribe problematic use to a "moral failing" of the individual and to treat all games alike irrespective of their individual differences. Such an approach is insufficient to carry out a detailed analysis of the way business models in online gaming are currently developing.

The simulation of traditional gambling games, primarily in social media

Another way of linking gaming and gambling concerns the partial convergence of businesses active in both fields, which took off in the beginning of the 2010s, when such entities became aware of social media as a relevant context for the distribution of game titles. On the one hand, traditional gambling businesses saw social media platforms as a lucrative new market, on the other, designers of "casual games" distributed on social media platforms sought inspiration from traditional gambling in order to create commercially sustainable games in a context where users were notoriously unwilling to pay up front. This convergence of industry goals was only partial as gaming and gambling companies held very different beliefs about the nature of their businesses. Nonetheless, this led to the creation of a variety of casual games with gambling themes – from regular Internet gambling as part of various social casino games through casino simulations to friendly games. Figure 1 below gives a very good overview of the variety of strategies. As is obvious from the figure, not all games with casino features can be classified as actual gambling.

Figure 1: Gaming and gambling in social media (Gainsbury et al., 2014)


For online games that include some casino (or gambling) – themed components
Do users have to pay money to play
Yes
No
Can a prize of monetary value be won?
Yes
No
Is the outcome determined skill?
Subscription or paid console or mobile game
Yes
No
Tournament or competition
Internet gambling
Is the game based on or clearly integrated with social media platform?
Yes
No
Is the gambling theme central to play?
Is the game on platform provided by a gambling operator?
Yes
No
Yes
No
Social casino game
Social game or virtual world with casino features
Practice game
Stand-alone console, online or mobile game

The integration of retention and monetisation strategies in game mechanics

This convergence of gaming and gambling in applications available via social media has inspired online game designers. While games like *CS:GO*, *PUBG*, *Fortnite* and *Rainbow Six* have traditionally been based on retail or subscription, principles from "play for free" games in social media have increasingly gained ground in mainstream games. This includes a heavy reliance on microtransactions in the business models leading to a greater emphasis on retention and monetisation strategies which can be detected in game design.

The integration of retention and monetisation strategies above the level of individual games

Apart from their integration in specific game mechanics, retention and monetisation strategies have become part of the more general data analyses informing game design and business strategies in online gaming. This includes the segmentation of players based on their willingness to pay and the according adjustment of game design. Such continuous analysis and adjustment of design to documented use patterns are today part of any professional software service, which is not problematic in itself. Yet, it may in some cases be part of "predatory strategies" such as the deliberate identification and manipulation of "whales" or "high rollers" or the deliberate creation of "near miss" situations in games involving chance. Both strategies are known from traditional gambling. Indeed, with the extensive collection and exchange of user data in online settings such strategies can be employed with even greater precision and efficiency. For obvious reasons such strategies are covered by regulation in most European countries and – as will be discussed further –it is worth considering whether the regulatory frameworks can be applied with more weight in online settings as well.

Traditional gambling in the context of player-driven economies

Finally, in the wake of highly dynamic player-driven economies in the context of online gaming, more problematic economic practices, such as scamming and betting, have emerged. Skin-betting is betting with virtual items that hold a certain exchange value in wider gaming communities. It is currently a huge phenomenon and involves the exchange of billions of dollars. Though skin-betting does not involve any conventional currencies, game items are in practice "commodity money" in the sense that they hold a certain exchange value in the community. Thus, skin-betting is and should be treated as actual gambling with the regulatory action this involves.

These links between gaming and gambling are an important backdrop if we are to understand the evolution of business models in online gaming since the microtransaction-based business models that are currently gaining ground in mainstream online gaming have emerged out of casual gaming in social media and the partial convergence between gaming and gambling industries. This development involves the shift of emphasis in business models from boxed content, fixed prices and costumer acquisition toward content-as-service, microtransactions and customer retention and monetisation.

Development of business models in online gaming

Business models in online gaming have changed greatly in recent decades moving from "boxed content" through various types of subscriptions to the complex microtransaction models of today. This development is not unique to video games, it represents a general trend caused by the way Internet technologies have disrupted the creative industries. "Boxed content" is here understood as games (and other cultural products) which are stored on paper, DVDs or in digital files and sold in traditional retail. This is the business model of traditional mass media such as books, films and music albums, which has been challenged considerably in recent years. Thus, changing patterns of distribution and consumption on the Internet have paved the way for alternative business models capitalising on content in different ways. One of these, the subscription model, transforms content into a service that users can access over the Internet for a monthly fee. In the first decade of the 21st century some of the most trendsetting video game titles, such as *World of Warcraft*, were based on this model. Players would pay a relatively low price for an initial download and then continue to pay a monthly fee for playing. Though the initial payment was somewhat lower as compared to the "boxed content games", the total cost quickly exceeded the amount you would usually pay for an individual game title as play went on for months or years. This model has increasingly gained ground in more traditional cultural industries such as film and music, where services like HBO, Netflix, Tidal and Spotify introduce "content as service" and monthly subscriptions as an alternative to the traditional boxed distribution model. However, more recent developments in the field of video games (chiefly inspired by the development of casual gaming in social media) have brought up another range of business strategies, often summed up under the title "microtransaction models" or "play for free". Obviously, the word "free" should not be taken literally, as these business models most certainly manage to capitalise on content (otherwise they would not be business models). Most of these "free" games can be played at no cost in a somewhat down-scaled version. The revenue is created (apart from via advertising) via add-ons in the form of currency, items, services, etc. the players may choose to buy within the game. In this way, the game provider can attract a broad variety of players irrespectively of their willingness to pay at the same time gaining full advantage from those groups that are willing to pay somewhat more than the average player. Again, this development is by no means unique to the field of video games, it represents the norm in extended marketplaces such as App Store and Google Play, where users have become accustomed to accessing applications without any payment "up-front" (and, presumably, are still unaware of the many other ways in which they are being capitalised upon).

Accordingly, the evolution of business models within the field of video and online games has moved from boxed content through subscriptions to various types of microtransaction models reflecting a more general trend on the Internet. Hamari and Järvinen (2011) describe how this development put much greater emphasis on the retention and monetisation of players. Retention is about making them play longer, and monetisation is making them pay as they do. To keep the record straight it should be noted that customer retention and monetisation is a key consideration in any type of business model, both on- and offline. Any supermarket, restaurant or theatre will have strategies whose goal is, above all, to bring customers in, and, once this has been achieved, to get them to stay longer in order to sell them even more. The same applies to online gaming and application providers. As the key economic transaction of the boxed-content model takes place "up front", i.e. when players buy the game, emphasis in this model is on customer acquisition via marketing activities. In comparison, the key consideration in subscription-based business models is ensuring that players keep paying every month by way of different types of retention strategies. What is more, as "play for free" games do not involve any initial or monthly transactions, emphasis here is on alternative ways of monetisation – either by selling things to players or by selling their attention to advertisers. While online games, as mentioned, share these considerations with a broad range of business fields, they also represent a unique case in point as their business rationales are built into their very design. Thus, it is worth taking a look at the way online games are built for retention and monetisation.

How games are built for retention and monetisation

As mentioned in the previous section, irrespectively of its context any business model involves strategies for acquiring, retaining and monetising customers. Yet, an interesting aspect of online gaming is the way these business rationales are built directly into the design of each individual game. For instance, a "boxed content" game will have focus on attracting gamers up front with breath-taking game trailers and eye-catching billboard advertisements, while a subscription-based game will put more emphasis on those aspects that cause users to continue playing for weeks and months. Finally, games based on microtransaction business models will concentrate on aspects that motivate the acquisition of items, resources or services for real money. Juho Hamari and Aki Järvinen (2011) identify some of the game mechanics in question. The term "game mechanics" is here understood as design models which are utilised in various game titles and shape the patterns of interaction within them. Key examples are the design and balancing of resources in strategy games, the design and balancing of races and classes in role-playing games, and the design of weapons and maps in online shooters. While such game mechanics are primarily built for making gameplay meaningful and appealing, according to Hamari and Järvinen, their design is increasingly becoming a business issue as well. In online games they distinguish between mechanics that serve to acquire, retain and monetise players. Their work focuses on casual games in social media, yet, with the proliferation of microtransaction business models into more conventional online gaming, it is definitely relevant in this domain as well.

Game mechanics built for customer acquisition

As examples of game mechanics that serve the business purpose of customer acquisition, Hamari and Järvinen mention gifts, friends as neighbours and friends as hires among others. Gifts are items players acquire during the game which they can pass on to a friend outside the game, in this way inviting them to join. Similarly, a player may gain advantage by collaborating with friends as neighbours or by hiring friends as helpers and inviting them to join the gameplay in this way. Such mechanics are particularly widespread in casual games embedded in social networks such as Facebook as they allow the game provider to use a player's social network to gain advantage of the network effect and turn the player into a voluntary, unpaid marketing employee.

Game mechanics built for customer retention

As regards game mechanics built for retention, Hamari and Järvinen mention profile completions, tutorials, rewards for continuous play, punishments for logging off, daily bonuses and encouragement of networking among others. Profile completions and tutorials are typical "onboarding techniques" which serve to engage a player in the initial phases of gameplay. With profile completions the game, by way of progress bars and similar interface features, signals to what extent the player has completed their profile, and with tutorials the player is provided with a "soft" entrance and manageable learning curve when initiating gameplay.

As concerns rewards for continuous play, punishments for logging out or daily bonuses, these have to do with the design of reward systems within the game and their more general design to keep the user playing. This includes different types of rewards, distribution of rewards across the gameplay cycle and coupling of rewards with specific types of gameplay activities. Encouragement of networking has to do with the formation and maintaining of groups and communities inside the game as this is another key reason that players keep coming back to particular games: to spend time with their friends. As will be discussed further, the design of reward systems, including specific strategies of "reward scheduling", has received considerable attention in academia since this is where new business models of online gaming seem to share some business traits with gambling.

Game mechanics built for customer monetisation

Finally, Hamari and Järvinen identify a set of game mechanics related to the monetisation of players. These include double currencies, pricing in several currencies, needs built into the game design, artificial inconveniences, decay, scarcity, virtual currency, collectibles and showing off. As regards double currencies as well as pricing in several currencies this refers to, among others, pricing items in ways that blur their actual price to entice players to spend more money than they might otherwise do. Needs built into game design as well as artificial inconveniences concern the creation of gameplay situations whereby the player is obstructed or forced to proceed very slowly unless they invest some money in the game. Decay, scarcity and virtual currency are connected with the design of currencies and other resources in the game (the line between these is blurred) according to principles of scarcity and decay to ensure demand. Collectibles are items that players may choose to collect and as a means of showing off. An obvious example of this is the purchase, collection and exchange of skins in games such as *PUBG*, *CS:GO*, *Fortnite* and *Rainbow Six*. Skins are so-called cosmetics such as costumes or decorations for weapons which do not represent any advantage in relation to gameplay but which may obtain a high value as collectibles as well as acclaim within the broader context of player communities. For some player groups, the acquisition and exchange of skins has become a key aspect of gameplay, establishing a sort of player-driven economy beyond the level of the individual game.

Hamari and Järvinen wrote their article in 2011 and in the meantime another essential monetisation technique has entered the scene, i.e. loot boxes. These are containers in the form of boxes, chests, etc. which players either collect or win in the game. To gain access to the content of such a container the player will have to pay for a key or a similar game item that can open it. Accordingly, it is only after this purchase that the player will know the content of the container and whether it was worth the money. This introduction of pure chance into the economical transactions of the game has, along with the reward scheduling mentioned in the former section, resulted in some worry regarding business models in online gaming and their increasing similarities to those known from gambling. To get a full grip of this discussion, however, it is necessary to look beyond the design mechanics of individual games and focus on some of the economic dynamics that thrive in the broader contexts of player-communities and game distribution platforms.

Player-driven economies and derivative economic practices

In the former section, some examples of the way games mechanics can be built for customer acquisition, retention and monetisation were presented. The list is by no means complete and the field is in constant development as the loot box example illustrates. However, to acquire a full understanding of business models in online gaming it is necessary to take a look at the way they are connected to the player-driven economies that arise in the broader context of the games. Thus, as mentioned in relation to skins as collectibles and showing off, some player groups may turn the collection and exchange of skins into a game in its own right, in this way creating another variety of economic phenomena including player trading, scamming and betting. This is enabled and propagated by specific design strategies on behalf of the game provider, but it also thrives on the players' participation as economic actors and "entrepreneurs", as well as on the intersection between games and other economic platforms and markets.

The way game providers enable and support the emergence of player-driven economies has to do with the design of currencies and other resources that may be used as currencies. A classic example is the way gold in *World of Warcraft* works as a currency that can be exchanged within as well as outside the game. Gold is earned by completing quests, defeating monsters or collecting items which can be sold in auction houses in the game. In this way it works as an in-game currency. However, since it takes time to collect it, some players may be willing to buy it for real money. In the case of *World of Warcraft*, for instance, the demand for gold has given rise to the phenomenon of "Chinese gold farmers", i.e. players who collect it in the game and sell it for dollars as a regular day job. It is not only in-game currency that may become an object of exchange within and outside the game in this way. Due to their attractiveness, scarcity or relative stability in value other resources may gain the status of currencies in the broader contexts of gamer groups and communities (e.g. skins and keys for loot boxes). The relative feasibility and lawfulness of this practice obviously depend on specific design choices made by the game provider. For instance, enabling or disabling player trading is essential to the dynamics of player-driven economies. Users may still choose to trade items in games that do not enable player trading, but this is somewhat harder and riskier. Moreover, game providers and platform owners may make it more or less difficult to turn in-game currencies into outside-the-game currencies such as dollars or euro. For instance, Blizzard, the company behind *World of Warcraft*, for a long time worked against the "Chinese gold farmers" as this practice was considered to be against the game's policy. On the other hand, Valve, the company behind Steam, to a much higher degree enable player trading within and beyond the platform by making their API available to 3rd party skin-trading.

In any case, the design of virtual items and currencies as well as the relative feasibility of player trading may lead to various sorts of player-driven economies that can be described in terms borrowed from traditional economic theory such as supply and demand, scarcity and inflation. As player communities collectively endow specific game items with a certain value, these become items of economical exchange and may be turned into a currency in their own right. For instance, the aforementioned keys that have to be purchased in order to open loot boxes have become an important currency in the exchange of skins, most likely due to their relatively stable value. Thus, the (designed) scarcity of an object as well as fluctuations in demand may cause its value to rise and fall. This is not a new phenomenon. Stamps, old coins and *Magic: The Gathering* cards are earlier examples of collectibles with a value by far exceeding their material value due to their status as desirable objects within specific communities. However, the dynamic, connected and global nature of online gaming means that such games represent broader economic phenomena. Moreover, the relatively unregulated nature of these economies has led to the emergence of spurious economic practices.

The sheer scope of exchange leads some players to employ radical measures in order to acquire other players' property, for example scamming, stealing and deceiving. This may take place between friends in shared physical spaces or between strangers in online marketplaces. For instance, a player may take advantage of a friend being away from their keyboard to enter their profile and transfer a desired item to their own account. Similarly, players may scam others in online marketplaces by claiming to put a desired object on sale but refusing to give it to the buyer once the money has been transferred.

Moreover, the connected nature of online gaming economies means that they intersect with other more suspicious types of economic phenomena on the Internet such as gambling and betting. As described in the introductory section, skin-betting is gambling with skins, often in simulations of traditional casino games such as roulette and blackjack. Player-driven economies make this phenomenon possible because they endow in-game items such as skins and keys with a collectively recognised monetary value. Current legislative systems struggle to recognise this phenomenon as gambling due to the relatively new and dynamic nature of online games: specific items may gain or lose monetary value in accordance with particular game titles gaining or losing popularity and market penetration, meaning that new "currencies" may emerge and disappear at a quicker pace than most legislative systems can handle.

Finally, these economic exchanges and practices take place in the context of a broader system of platforms and for this reason they intersect with a number of related business domains. YouTube represent one case in point. The overlap between online gaming and this platform is obvious as gaming videos are one of the most important genres on the streaming platform. Accordingly, some of the most trendsetting YouTube celebrities, such as PewDiePie, JackSepticEye, Johnontheradio and Cryoz, present gaming as the primary content of their videos. Their earnings are mostly based on number of views, a business model that is built on the specific business rationale of YouTube. In addition, they in various ways engage in business partnerships with those active within the domain of online gaming. For instance, they receive "sponsorships" in the form of skins or sets of skins, in this way rising the demand for these skins within the online game economy. Moreover, they host competitions with "giveaways" in the form of skins and items from specific games, thus advertising the games and their economies. While these examples fall neatly within the category of traditional marketing, some YouTubers also partner up with more dodgy economic actors, such as skin-betting sites, and advertise promotion codes for them. They earn a little each time a user enters such a code, thus leading their (predominantly young) audience directly onto these sites. This is why a full understanding of the characteristics and impact of business models in online gaming will have to take into account its intersection with "celebrity economies" on YouTube.

In summary, online games can, on the one hand, be seen as cultural artefacts designed for the retention and monetisation of gamers in the context of individual game titles, and, on the other, they can be perceived as platforms for larger, player-driven economies with various types of derivative economic practices such as scamming and betting. Moreover, due to their connected nature, they intersect with other business domains on the Internet such as streaming platforms. In effect, business models and the way they are imbedded into game design and the broader ecosystem of platforms become the key concern in relation to the protection of minors on the Internet.

Implications for the protection of minors in the Internet age

Business models in online gaming are a complex phenomenon that calls for a broad and diversified approach in relation to the protection of minors on the Internet. First of all, it compels us to look beyond traditional concerns, such as inappropriate content or addiction, and toward the fact that children's and young people's play and social interaction today unfold in a commercially invested environment. Moreover, countermeasures to the more problematic aspects of this development should involve action in relation to the education of children and young people, as well as a stronger enforcement of regulatory frameworks regarding misleading and manipulative business strategies.

What we should worry about: problematic business models in online gaming

In the introduction, it was noted that "video game addiction" is a growing concern with regard to children and young people's use of digital media. This concern is based on the assumption that use of specific digital technologies can lead to excessive and uncontrollable engagement similar to pathological gambling or substance abuse. Yet, as was discussed in the clarification of the possible links between gaming and gambling, this "pathologising" of children and young people tends to turn problematic use into a "moral failing of the individual" – whether of the child or of the parent – and to treat all games alike. Thus, a more constructive approach would be to submit the games and media in question to more critical scrutiny with regard to the business, retention and monetisation strategies they involve. This, firstly, involves a more critical assessment of "play for free" business models within and beyond online gaming and, secondly, an increased focus on the grey zones between gaming and regular gambling in the peripheries of online gaming economies.

A "critical assessment" of the free-to-play games is here understood as he necessity to recognise that these games (and applications) are not free at all. Whether we pay with our time, attention, data or in the form of micropayments made along the way, they most definitely cost something. In this way the "free" prefix can be said to be directly misleading to consumers. This is a problem as many parents and carers tend to greenlight applications on children's devices if they do not contain any violence and do not cost any money. Yet, it is precisely these types of games that may contain the most aggressive retention and monetisation strategies and if our aim is to protect the rights and well-being of children and young people, we should rather look for games with fixed prices and transparent business models. Needless to say, this is not the case only in free-to-play games. As users have become used to being able to access any kind of application for free, these types of business principles permeate online marketplaces such as App Store and Google Play. One example is the application of the one of fast food company, where users can "win" free meals by tapping a button once a day. Accordingly, the proliferation of these business models into the wider context of online marketplaces makes countermeasures even more pertinent.

Apart from the integration of retention and monetisation strategies into the game mechanics of free-to-play games and the design of free apps in general, player-driven economies of online gaming imply a number of derivative economic practices we should be aware of, such as scamming and gambling. It is important to emphasise that this does not imply a general convergence between gaming and gambling. Those are still relatively distinct types of phenomena and gaming excessively is not the same as being a pathological gambler. However, when children and young people go online to engage in competitive teamplay, they increasingly do so in contexts where such economic practices abound. For this reason, it is important that children, young people and their adult carers are given the necessary knowledge to critically reflect on these issues and keep away from more problematic contexts and transactions. At the same time, it is necessary to ensure that directly misleading and manipulative business strategies are regulated in the same manner online as they are offline.

How we should deal with this: media education and regulation

Accordingly, countermeasures to the current development of business models in online gaming will have to cover several approaches. On the one hand, we need to update the critical media literacy of children, young people and their carers with knowledge about the way business models work in online contexts. On the other hand, we need to locate and review regulatory frameworks dealing with misleading and manipulative business strategies offline and consider how they can be applied online.

As regards the former, one obvious way to proceed is to equip children, young people and carers with the relevant knowledge to safely navigate these contexts. This involves an expansion of our current understanding of digital literacy to include the critical understanding of business models in the online environment. Media and digital literacy have received considerable attention in recent decades as digital media have pervaded every aspect of our lives. In the wake of this development several scholars have emphasised the importance of moving beyond a pure skill- or competence-based perspective in media literacy toward a critical approach to literacy as the ability to understand and reflect on the social and ideological investments embedded in any kind of (digital) media representation. As mentioned earlier, this should also include a critical understanding of the business models and rationales underlying such representations and how they are embedded in the very design of applications and platforms.

However, the issue of problematic business models in online contexts should not just be left for individual citizens to solve. The authorities also have a responsibility with regard to the regulation of decidedly "predatory" strategies in online environments. As stated previously, the intersection between gaming and gambling in online contexts on some occasions leads to the employment of directly manipulative strategies such as misleading reward scheduling and the deliberate identification of fragile individuals in order to target them specifically. There is good reason that such strategies are covered by regulation in many European countries and there are no arguments in favour of them not being covered by regulatory frameworks online. One obvious area to begin are offers or advertisements of regular gambling directed at minors, which are illegal in most of Europe. This is against the law both on- and offline and should also cover YouTube advertisements of promotion codes to skin-betting sites and transfer of minors' profile data by gaming platforms to just such sites. It is also worth considering how regulations, in place in some European countries, concerning misleading reward scheduling and the deliberate targeting of fragile individuals could be applied on the Internet. Thus, the challenges abound, but so do the possible countermeasures.

Safe gaming

Jeffrey Goldstein

Video games are used for relaxation, entertainment, and distraction, but also for education, health, and science. Playing video games has potential benefits in four areas: cognitive/perceptual, motivational, emotional, and social. The main concerns about children's video gaming are the content of games, the potential influence of games on behavior, about access to games that may be inappropriate for children. The influence that games have on children, especially younger children, largely depends on the parents own behavior. Parents who are concerned about risks most often try to protect their children by monitoring, applying restrictions on media use, and by supervising the child, whereas parents who feel that the media offer educational or entertainment opportunities more often co-use the media with their children or actively discuss the content. Parents should be good ”role models” for their children, using media in a manner that they want their children to follow.

Keywords:
video games
PEGI and IARC rating systems
parental guidance
parental mediation
technical controls

Home

Video games are enjoyed by a very diverse group of players all over the world. Children and adults, men and women, play regularly on a dedicated console, a personal computer or a mobile device, such as a smartphone or a tablet.

The reasons for playing video games vary with age, abilities and interests. For adolescents, they serve the same basic purposes as other media in enabling them to manage their mood, find excitement, and enhance their social relationships. Games are also challenging and require skill. They can be deeply involving, yet they offer opportunities for social contact both during and after play, online and face to face. In video games, adolescent boys and girls find inspiration, joy and relief.

Uses and gratifications theory proposes that individuals have particular needs that drive their media use. Research suggests that people choose both traditional media and new technologies to gratify at least five general needs:

- entertainment;
- information seeking;
- social interaction;
- emotional satisfaction;
- passing time.

Yet not every game is suitable for every purpose or player. A good game is one that matches the player's abilities, maturity, interests and needs.

The case for games: positive effects of playing video games

The uses of video games are many and varied. Games are used for relaxation, entertainment and distraction, but also for education, health and research. In the 21st century, video games have evolved into effective learning tools. Some types of commercial games have been shown to enhance basic visual and mental abilities. These effects are significant enough for educators to use video games for such practical, real-world purposes as training surgeons and rehabilitating individuals with perceptual or cognitive deficits. Although many people may still consider video games nothing more than mindless fun, they also serve as serious tools for good. They use a number of techniques known to promote efficient and transferable learning. Although some researchers express concern about the potential negative effects of gaming, others see that video game training creates a great number of positive outcomes. "Today's video games are much more than entertainment. They are also weapons in the fight against declining mental capacities in old age. They promote job-related skills. And they are a model of how to teach children complex and difficult tasks and abilities. As with any technology, video games are neither intrinsically good nor intrinsically bad. Instead, the nature of their impact depends upon what users make of them" (Eichenbaum, Bavelier, Green, 2015, p. 67).

Cognition and perception

Playing video games has potential benefits in four areas: cognitive, motivational, emotional and social. Video games can be powerful brain-training tools that can improve visual attention, concentration, memory, navigation and multitasking, simultaneously increasing speed and accuracy.

Some game genres are better suited to particular kinds of learning. For example, playing action video games, like *Grand Theft Auto*, *Call of Duty* or *Battlefield*, requires and improves a range of visual skills. "Action video games have been shown to enhance behavioural performance on a wide variety of perceptual tasks, from those that require effective allocation of attentional resources across the visual scene to those that demand the successful identification of fleetingly presented stimuli. Non-players trained on an action video game show marked improvement from their pre-training abilities, particularly in attention skills" (Bediou et al., 2018). Both brief and extensive exposure to video game play can result in a broad range of enhancements to various cognitive and perceptual faculties that generalise beyond the game to other settings (Mayer, 2014). Furthermore, one study found that 12-year-old children who played video games the most were more creative than those who played less (Jackson, 2012).

Games have been used to teach reading, vocabulary and maths to elementary school students and health care to adolescents (Kato, 2010). One study found that playing video games was just as successful as academic courses in improving a player's capacity to think about objects in three dimensions. This has implications for education and career development, given the importance of spatial skills for achievement in science, technology, engineering and mathematics. The more adolescents reported playing strategic video games, such as role-playing games, the more they improved in problem-solving and school grades the following year (Granic, Lobel, Engels, 2014). Games are most effective when they are designed with learning principles in mind.

Video games incorporate many learning principles by putting learners in the role of decision-maker, confronting them with progressively greater challenges, and engaging them in experimenting with different ways of thinking. Playing video games is a "multi-literate" activity: it often involves interpreting complex three-dimensional visual environments, reading both on- and off-screen texts, and processing auditory information. In computer games, success derives from the acquisition of skills and knowledge. Young people have to learn to "read" subtle nuances, often on the basis of minimal cues. They have to learn the rules and etiquette of online communication and to shift quickly between genres or language registers (Goldstein, Buckingham, Brougère, 2004). Games are most likely to result in learning when they require players to select relevant information from the game, organise this information into a meaningful structure, and integrate it into a useful strategy (Armstrong, 2018).

"Research suggests that on average, boys have an edge over girls in several types of cognitive skills, such as imagining how three-dimensional objects would look from various perspectives and calculating the trajectory of an object (such as a bullet or a football) toward a moving target. This makes it easier for boys to immerse themselves in the shooting, fighting and sports games that require these skills – and may be another reason [in addition to peer pressure] that boys are more likely than girls to prefer these genres." (Kutner, Olson, 2008, p. 218). But note, too, that video games have been among the most successful means for reducing the typically reported sex differences in spatial abilities (Dye, Green, Bavelier, 2009).

Parents and older siblings provide a bridge to children's further mental development when they engage with them and challenge them to more complex play and language. To describe this phenomenon, Lev S. Vygotsky (1986) used the term "scaffolding".

Brain development and functioning

Video gaming can be beneficial for the brain. It brings about increases in those brain regions responsible for spatial orientation, memory formation, strategic planning and fine motor skills.

Brain regions can be specifically trained. NASA, the space agency, have developed video games that use biofeedback to train pilots to stay alert during long flights and calm during emergencies. Signals from sensors attached to the player's head and body are fed through a signal-processing unit to a video game joystick. As the player's brainwaves come closer to an optimal, stress-free pattern, the joystick becomes easier to control (Mason et al., 2004). The technology is commercially available for Sony PlayStation and Microsoft Xbox to target symptoms arising from brain injuries, attention deficit disorder and learning disabilities. The system allows off-the-shelf video games (racing games are best) to be controlled through brain wave activity. The more focussed the player and the faster their brain is working, the quicker the car accelerates and the easier it is to play the game. Children with ADD have been found to increase their attention span through this device (Pope, Bogart 1996). Video games can be controlled using many forms of biofeedback, including galvanic skin response (GSR), heart rate and body temperature (Parente, Parente, 2006).

Playing *Super Mario* has a positive effect on nerve cells in regions of the brain involved in spatial navigation, memory formation, strategic planning and fine motor skills of the hands (namely, the right hippocampus, right prefrontal cortex and the cerebellum). Researchers at the Max Planck Institute in Berlin asked men and women (average age 24) to play *Super Mario 64* for 30 minutes a day over a period of 2 months. The control group did not play video games. Brain volume was quantified using magnetic resonance imaging (MRI). In comparison to the control group, the gaming group showed increases of grey matter, in which the cell bodies of the brain's nerve cells are situated. "While previous studies have shown differences in brain structure of video gamers, the present study can demonstrate the direct causal link between video gaming and a volumetric brain increase. This proves that specific brain regions can be trained by means of video games", state Kühn and Gallinat (2014). Video games could, then, be therapeutically useful for patients with mental disorders in which brain regions are altered or reduced in size, for example schizophrenia and post-traumatic stress disorder, or neurodegenerative diseases, such as Alzheimer's dementia.

Does playing video games affect school performance and learning? The evidence here is mixed. It appears to depend, in part, on *when* adolescents play video games and, in part, on *which* games they play.

In a long-term study of more than 3500 German students, prolonged gaming on school nights was associated with poorer grades overall, though there was no link between gaming and actual competencies, as measured by mathematical and language ability tests (Gnambs et al., 2018). Heavy gamers go to bed later than non-gamers and the physical and emotional arousal produced by intense gaming sessions can reduce the amount of REM sleep they get and make them generally less alert and more prone to cognitive errors (Vitelli, 2018). Gnambs et al. (2018) also write that "much of the hysteria over the academic impact of video gaming on school success is likely misplaced. While gaming does appear to have a negative impact on grades, the effect size, while significant, is still very small".

Playing video games that require strategy is associated with higher academic achievement. A study of 1492 adolescents in the United States found that "more strategic video game play predicted higher self-reported problem-solving skills over time and, in turn, higher self-reported problem-solving skills predicted higher academic grades. The novel findings that strategic video games promote self-reported problem-solving skills and indirectly predict academic grades are important considering that millions of adolescents play video games every day. [...] Strategy games may teach the player to first gather information and think of a strategy before attempting to solve a problem. For example, in *Splinter Cell* (Ubisoft) the main character is a black-ops agent and the goal is to use stealth and remain undetected by enemies when completing missions. Unlike most action and shooter games in which the player rushes toward enemies with guns blazing, in *Splinter Cell* the player often must remain hidden by moving slowly and carefully in the shadows and creating diversions to distract enemies. For example, when approaching enemies, the player must study the scene, gather information about how the enemies move, and formulate a plan regarding when and how to attack without being detected. Such a strategy often involves waiting to attack once the enemy has moved to a remote location, and then hiding the enemy's body in the shadows. Considering that this form of problem-solving (i.e. gain information, weigh different options and formulate a strategy before acting) is repeated at every level of the game, sustained playing over time may increase the player's problem-solving skills" (Adachi, Willoughby, 2013). In the classroom, simulation games make it possible to implement activities which would otherwise be too costly, dangerous, difficult or impractical. Designing games and writing applications fall within digital literacy and are increasingly part of the school curriculum.

Games and health

Entertainment is a public health issue. Enjoying music, a film, a video game or a YouTube video can improve our mood, strengthen our friendships and increase our competence. Simple casual games that are easy to access and can be played quickly, such as *Angry Birds* or *Candy Crush*, can improve players' moods, promote relaxation and ward off anxiety. Even if video games only make people happier, this is itself a healthy benefit (Goldstein, 2015).

Video games are increasingly used both with children and adults in a growing variety of health-care settings to impart information and to promote adherence to exercise and medical regimens. Games have aided in the management of weight loss and dieting, as well as of chronic diseases such as diabetes and asthma (Kato, 2010; Lieberman, 2009). Games designed for mobile phones and tablets have been used to increase physical exercise, improve diet adherence, and increase awareness about health and diet (e.g. Byrne et al., 2012).

Video games may be effective tools to learn resilience in the face of failure. By learning to cope with ongoing failures in games, young people build emotional resilience they can rely upon in their everyday lives (Granic, Lobel, Engels, 2014).

Online gaming spaces can be accommodating environments for socially inhibited individuals who are anxious or shy. Two of the key tasks of adolescence are improving social skills and improving interpersonal communication. Digital devices like telephones and computers offer a combination of intimacy and anonymity that helps them become comfortable with these complex social and communication skills more quickly. The structure of online games allows adolescents to test social boundaries and relationships in ways that they might not recover from as easily in face-to-face settings (Jansz, 2005). Online games have the potential of being socially advantageous for shy individuals by allowing them to overcome their traditional social difficulties as well as generate new friendships and strengthen old ones (Kowert et al., 2014; Trepte et al., 2012). *World of Warcraft* is one of the most popular Massively Multiplayer Online Role-Playing Games (MMORPG). It is a highly social environment that encourages cooperation, communication and friendship. Players experience a significantly lower degree of loneliness and social anxiety online than in the real world (Martončik, Lokša, 2016).

Children with attention deficit disorder are particularly attracted to media, including television, video games and computers. “Boys who show ADD symptoms were more likely than others to use games to cope with angry feelings. Among girls with ADD symptoms, twice as many played games to make new friends compared to other girls. In moderation, these are probably healthy uses of video games” (Kutner, Olson, 2008, p. 134).

Depression is estimated to affect more than 300 million people worldwide. Although there has been some success in treatment of this illness with pharmaceuticals and cognitive behaviour therapy, these are often costly or unavailable. Research supports the effectiveness of digital game-based interventions for depression (Li et al., 2014; Russoniello, Fish, O’Brien, 2013).

Exergames are video applications that require gross motor activity, combining gaming with physical exertion. Digital devices with motion detection sensors (such as Nintendo’s Wii) enable the games to track players’ movements and adapt to them. This can involve dance or simulated sports such as football and tennis. Exergames are a substitute for physical exercise when outdoor play is not feasible, as in inclement weather or in various institutional settings (Peng et al., 2011). One study found that playing active computer games uses significantly more energy than playing sedentary computer games, yet not as much as playing the sport itself (Graves et al., 2010).

If exergames are enjoyable to players, they are likely to stay on task longer, and this may ultimately provide a modicum of exercise. Beyond energy expenditure, exergames can have effects on the perception of confidence, control and engagement. A study of young adults aged 18–35 found that exergames that are more enjoyable produce more energy expenditure (Lyons et al., 2014). Sports video games such as *FIFA* (by Electronic Arts) and Nintendo Wii are not a replacement for real-world sports, but they are a nice complement to them.

Even more activity is required for some augmented reality games that are played in the real world using a phone’s GPS system. Such games bring people outdoors and can be designed to draw them to museums, libraries, festivals and parks. Because many people play the augmented reality game *Pokémon GO* simultaneously, face-to-face communication and relationships develop (Stokes, Dols, Hill, 2018).

Virtual and augmented reality games are increasingly used in teaching. According to one review of the research, "the use of augmented reality games in these environments enhances active and authentic learning. All the studies that have used augmented reality games showed a positive effect both on the participation and involvement of students in learning and on learning outcomes" (Koutromanos, Sofos, Avraamidou, 2015).

Risks and concerns: content, access, influence

Parents' main concerns about their children's video game play centre on the games' content, on their potential influence on their children's behaviour, on access to games that may be inappropriate, and on the risks posed by online multiplayer games. Parents of gamers have expressed concern about violent images and themes in games, bad language, gender and racist stereotypes, sexual images, depictions of alcohol, drugs, and tobacco use, gambling, and in-game purchases. In general, they are concerned that their children spend too much time gaming and engaging in other screen-based activities.

Since 2003, video games available in Europe have been rated with the use of the PEGI system (pegi.info) to indicate potentially undesirable content and to suggest age guidelines for play. Since 2013, the IARC classification (www.globalratings.com) has been used to generate ratings for applications downloaded directly or from an app storefront. In addition, manufacturers of game devices and interactive media have included controls that enable parents to limit the time the devices can be used and to filter unwanted content. Parents are central to their children's play and to the influence that games have on them. In section *Managing games through parental mediation*, there are tips for parents to guide their children's play.

Violent video games

The most controversial aspect of video games is their often-violent content. War, first-person shooters and martial arts are themes in many games, especially those rated PEGI 16 and PEGI 18, but even games rated PEGI 7 and PEGI 12 may contain some violence. Violent video games are teched-up renditions of violent comic books, gothic horror novels and other forms of preposterous violence as entertainment. We should not forget that games with fantasy violence themes have always been part of youthful play, especially among males.

Many boys play violent games to cope with feelings of anger, frustration or stress. Adolescents use them to manage their emotions, particularly boys, who reported playing to relax, forget about their problems and manage anger. Games can also help young people understand their emotions and cope with them (Jansz, 2005; Villani et al., 2018).

"The strong link between video game violence and real world violence, and the conclusion that video games lead to social isolation and poor interpersonal skills, are drawn from bad or irrelevant research, muddleheaded thinking and unfounded, simplistic news reports", write Kutner and Olson in their book *Grand Theft Childhood* (2008, p. 8).

Recent large-scale studies do not find evidence that violent video games play a role in real-life violence. A 2018 study investigated the effects of long-term violent video gameplay using a large battery of tests including questionnaires, behavioural measures of aggression, sexist attitudes, empathy and interpersonal competence, sensation-seeking, boredom, risk-taking and mental health (depression, anxiety), as well as cognitive functions, before and after 2 months of daily gameplay. Participants played the violent video game *Grand Theft Auto V*, the non-violent video game *The Sims 3* or no game at all. No significant changes were observed when comparing the group playing a violent video game either to the one playing a non-violent game, or to the passive control group. "These results provide strong evidence against the frequently debated negative effects of playing violent video games in adults and will therefore help to communicate a more realistic scientific perspective on the effects of violent video gaming" (Kühn et al., 2018).

Patrick M. Markey, Charlotte N. Markey and Juliana E. French (2014) investigated the associations among violent crime (homicides and aggravated assaults), video game sales, Internet searches for violent video game guides and the release dates of popular violent video games. Contrary to popular claims, no evidence was found to suggest that this medium was positively related to real-world violence in the United States. Unexpectedly, many of the results were suggestive of a decrease in violent crime in response to violent video games.

After studying the effects of video games on American youth, Harvard psychologists Lawrence Kutner and Cheryl Olson concluded that "perhaps the biggest lesson learned from our research is that most parents should not worry about violent or other M-rated video games having a profound effect on their children's behaviour or values. Throughout our interviews with young teens who played such games, we were repeatedly impressed by how they had incorporated their parents' fundamental values into their lives. They realised that the video games were play and that, like the crime and horror comic books, gangster films and penny blood novels sold to earlier generations, these games were entertaining but outrageous fantasies" (Kutner, Olson, 2008, p. 210).

Screen time: excessive gaming

A frequent complaint from parents and teachers is that children spend too much time looking at screens. Certainly, among adolescents excessive gaming can be a sign of problems outside the game, such as a deterioration or breakdown of family relationships or friendships, poor school achievement and negative emotions. Gaming can be considered excessive when it interferes with school or work performance, disturbs sleep or displaces other desirable activities, like face-to-face friendships, family relationships or sports.

The notion of video gaming addiction or "Internet gaming disorder" is controversial. There is little clarity regarding diagnostic criteria, appropriate symptoms and measurement. It is unclear if problematic video gaming should be considered a separate disorder or whether it is the expression of other underlying conditions (Aarseth et al., 2017). The current approaches to understanding "gaming addiction" are rooted in substance abuse research and, consequently, do not necessarily translate to video gaming (Bean et al., 2017).

A 2018 review of problem gaming concludes "regardless of how researchers and medical professionals assess the nature of gaming disorder, few who play video games experience negative consequences from doing so and, at most, only a small subset of players might be considered to suffer from an addiction to it" (Gorman, Gentile, Green, 2018).

There are two major early warnings that signal a child's unhealthy relationship with technology. One is behavioural and the other emotional. On the behavioural front, it is important to recognise when screens are taking up so much time that there's none left for playing offline, doing physical exercise and spending time face-to-face with other people. Emotionally, it is important to recognise when children experience negative emotions after screen time because they are feeling bullied or ostracised or are more generally unhappy as a result of their online interactions. This may happen after they spend time on social networks, communicating by text or playing multiplayer role-playing games. If gaming becomes problematic, parents should talk with their children about setting limits on it.

Risks of online games

Playing online can involve a huge number of players simultaneously participating in a single game. Many Massively Multiplayer Online Games (MMOs) support virtual communities, and this can expose players to the risks associated with real-time interaction with unknown fellow players. Young Internet users are not always concerned about the potential risks of online activities. Such risks include:

- user-generated content created within the game which could be unsuitable for young people and a mismatch with the age rating given for the game;
- cyberbullying – some players may engage in behaviour that might not be suitable for young people, such as inappropriate or offensive language; bullying in games that allow text, voice or video communication; unsporting conduct like cheating or aggressiveness towards others;
- breaches of privacy – online gameplay can encourage people, including children, to form relationships, which carries with it the risk of sharing personal details or meeting unknown fellow players outside the game;
- links to websites with content unsuitable for young people.

Children need to learn to protect themselves from online risks such as cyberbullying, unwanted online sexual solicitation and risky online sexual behaviour (Baumgartner, Valkenburg, Peter, 2010). In order to minimize these risks, players and their parents should discuss them, and jointly decide what protection measures to use. This involves a three-pronged approach involving evaluating the content of games, controlling access to games and learning responsible gaming.

Safe gaming

The concerns of parents and teachers about video games focus on content, access and influence. The themes, images and sounds of video games may be unsuitable for younger players. Many parents worry about violence, gender and other stereotypes that may be portrayed, bad language that is sometimes heard or presence of drugs, alcohol and tobacco in games. These and other potentially troubling contents of video games are described by national and international media rating systems. For video games, PEGI and IARC are pertinent to content, describing game themes and elements, and recommending the minimum age for play. At the same time, technical modifications are introduced to limit access to games and other media. Every games device contains parental controls that can be set to limit access to certain games based on their PEGI age classification and to limit the amount of playing time. The influence that games may have on children, especially younger ones, largely depends on the parents' own behaviour. Parents should be good role models for their children, using media in a manner that they would want their children to follow. They are their first and primary teachers of media education. Below are some tips for parents to optimise their children's game play.

Content rating systems: age classification and content descriptors – PEGI and IARC

Adults as well as children play games regularly on dedicated game consoles, smartphones, tablets or computers. Most games are suitable for players of all ages, but a subset is intended for older players. For this reason, games and applications in Europe receive an age rating and content descriptors in order to inform consumers and prevent children from exposure to material that may not be suitable for them. Age ratings provide guidance to consumers, parents in particular, to help them decide whether or not to buy a particular product for a child.

PEGI

PEGI, Pan European Game Information, is the age rating system for video games. The aim of PEGI is to "educate consumers and in particular to protect minors from exposure to potentially unsuitable game content. PEGI does this by providing parents and caregivers with detailed information allowing them to make informed choices when buying games for children". The rating notes the minimum age for each game along with pictograms representing the content (cf. figures below). PEGI classifications are used in 38 countries. Since 2013, IARC, International Age Rating Coalition, has issued ratings for applications and downloads.

In Poland, video games are represented by SPIDOR (The Association of Producers and Distributors of Entertainment Software), which was established in 2008. It conducts educational activities, publishes games information on its website and supports the video games industry in Poland (www.spidor.pl).

An overview of PEGI age classification

3
TM
www.pegi.info

→ Suitable for all ages;
→ Some violance in a comical child like setting;
→ Fantasy characters;
→ No unsuitable content.

7
TM
www.pegi.info

→ Non-realistic;
→ Implied violance;
→ Cartoonish, humorous;
→ Frightening scenes for young children.

12
TM
www.pegi.info

→ Realistic violence towards fantasy characters or non realistic violence towards human like characters;
→ Mild bad language, nudity, horror.

16
TM
www.pegi.info

→ Realistic violence towards human like characters;
→ Sport violence with blood presence;
→ Bad language, drugs use;
→ Depictions of criminal activities.

18
TM
www.pegi.info

→ Gross violence;
→ Violence towards vulnerble or defencless human like characters;
→ Drugs Glamorisation;
→ Depictions of sexual activities.

The PEGI rating considers the age suitability of a game, not the level of difficulty. A PEGI 3 game will not contain any inappropriate content but can sometimes be too difficult to master for younger children. And there are PEGI 18 games that are very easy to play, yet they contain elements that make them inappropriate for a younger audience.

PEGI content descriptors

There are currently eight content descriptors used by PEGI:

TM
VIOLENCE

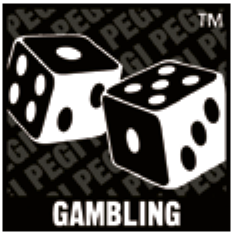
The game contains depictions of violence. In games rated PEGI 7 this can only be non-realistic or non-detailed violence. Games rated PEGI 12 can include violence in a fantasy environment or non-realistic violence towards human-like characters, whereas games rated PEGI 16 or 18 have increasingly more realistic-looking violence.

TM
@*!
BAD LANGUAGE

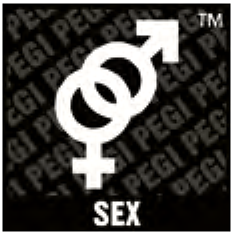
The game contains bad language. This descriptor can be found on games with a PEGI 12 (mild swearing), PEGI 16 (e.g. sexual expletives or blasphemy) or PEGI 18 rating (e.g. sexual expletives or blasphemy).

This descriptor may appear on games with a PEGI 7 rating if they contain pictures or sounds that may be frightening or scary to young children, or on PEGI 12 games with horrific sounds or horror effects (but without any violent content).

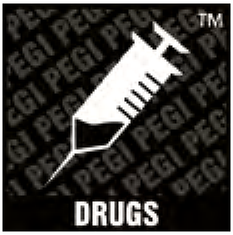
Home



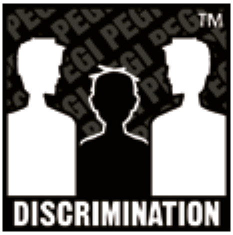
The game contains elements that encourage or teach gambling. These simulations of gambling refer to games of chance that are normally carried out in casinos or gambling halls. Games with this sort of content are rated PEGI 12, PEGI 16 or PEGI 18.



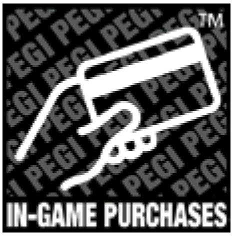
This content descriptor can accompany a PEGI 12 rating if the game includes sexual posturing or innuendo, a PEGI 16 rating if there is erotic nudity or sexual intercourse without visible genitals or a PEGI 18 rating if there is explicit sexual activity in the game. Depictions of nudity in a non-sexual context do not require a specific age rating, and this descriptor would not be necessary.



The game refers to or depicts the use of illegal drugs, alcohol or tobacco. Games with this content descriptor are always labelled PEGI 16 or PEGI 18.



The game contains depictions of ethnic, religious, gender, nationalistic or other stereotypes likely to encourage hatred. This content is always restricted to a PEGI 18 rating (and likely to infringe national criminal laws).



In 2018, PEGI added a new content descriptor for physical games, In-Game Purchases, to inform parents beforehand about the possibility of spending money within a video game. New content, game features and upgrades for a particular game or application are offered regularly to users. If such purchases are made during play, they are called in-game purchases (or in-app purchases on mobile devices), although they can also be made available as separate items in online shops outside of a game. In some cases, a player can make a purchase (a new item or an upgrade) directly with real money, in other cases, they can, with real money, purchase in-game virtual currency that can in turn be redeemed for content during gameplay.

Examples of in-game purchases include:

- coins, points, diamonds, etc.: these are examples of in-game currency which can be redeemed for content, features or upgrades;
- levels/maps: certain extra levels or areas inside a game's universe may be unlocked via a digital purchase;
- characters: new characters with varying skill sets can be acquired to play the same game again, each time with a different approach;
- weapons/tools: a game will give a player a standard set of equipment, tools or weapons to progress in the game, it may also offer other tools with increased functionality, making it easier to complete certain parts of the game;
- appearance upgrades (skins): these are items that can be worn by an avatar or be added to virtual belongings like cars, bikes or houses; examples include all kinds of clothing, tattoos, jewellery, decals, number plates, etc.

Many games are enjoyed without making in-game purchases. As with any online purchase, it is important for parents to understand how to control in-game purchases via the platforms and devices their children may be using. Platforms and online shops include various tools enabling consumers to make informed decisions, also on behalf of their children, and to control the settings relating to digital purchases, Internet access, online interaction and other functionality.

According to an international survey of parents whose children play video games carried out in May 2018, most have an agreement of some kind with their child about spending money. Simon Little, Managing Director of PEGI, stresses the importance of parental involvement in their children's gaming: "Entering into a dialogue with the child about the games they enjoy is certainly a must for all parents. It will provide them with the necessary context to create a gaming environment both the children and the parents are comfortable with".

How games obtain ratings

PEGI

Many PC and console games (for instance Microsoft Xbox, Sony PlayStation and Nintendo) are released as a physical product and sold via retailers. In order to ensure that these games display the correct age classification information on the box, a rigorous procedure is followed:

1. Prior to release, publishers fill in a content assessment form for every version of their product. This questionnaire concerns the content of the product, taking into account the possible presence of violence, sex, bad language and other audiovisual content that may be considered inappropriate for younger players.

2. Based on the responses from the publisher, the online system automatically determines a provisional age rating along with content descriptors.

3. The PEGI administrator receives the product from the publisher and thoroughly reviews the provisional age rating.

4. If the content in the game matches the provisional rating, PEGI delivers a license to the publisher for the use of the age rating icon and the relevant content descriptor(s).

5. The publisher is now authorised to reproduce the age rating logo and content descriptor(s) on the packaging or at the point of sale in accordance with the PEGI Code of Conduct.

IARC

Hundreds of new games and applications are released every day on digital storefronts for smartphones, tablets, PCs or consoles. IARC, a coalition of rating authorities from Europe (PEGI and USK), North America (ESRB, www.esrb.org), Brazil (ClassInd) and Australia (ACB, bit.ly/2LmbUCj), aims to provide age ratings and content descriptions for the globalised market of digital games, downloads and applications. Instead of having to administer their own rating systems, storefronts and platforms use established ones to comply with content classification requirements for each country. Consumers are presented with a consistently applied set of familiar ratings that reflect their local sensibilities about content and age appropriateness.

How IARC works

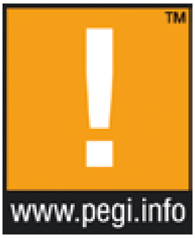
1. A publisher submits a game or application. Part of the submission procedure requires the publisher to fill in the IARC questionnaire, which is a set of questions about a product's content and interactive elements. The questionnaire combines the classification criteria of the participating rating boards (including PEGI, USK and ESRB).

2. Upon completion of the questionnaire, the publisher immediately receives a license with age ratings of the participating rating boards. The classification process is cost-free. As soon as the game or application is released, the appropriate age rating is displayed.

3. Administrators from IARC rating boards check a cross-section of all classifications to ensure that age ratings are correctly applied. In case of an error, the incorrect age rating can be changed.

Applications are often portals for user-generated content. Digital storefronts (such as Amazon), commercial streaming services (for example Netflix), social networking applications (like Facebook) and user-generated content portals (for instance YouTube) contain a broad, variable range of content. There is no way for IARC to determine before release of the application what sort of inappropriate content it may contain. For non-game applications, parents are especially advised to supervise their children. A new label warns parents that specific guidance is recommended when downloading a given application for use by children:

PARENTAL GUIDANCE SUGGESTED



Limiting access with technical controls: parental controls for game consoles and devices

All gaming consoles, mobile devices and PC and Mac operating systems are equipped with parental controls, allowing parents to protect their children's privacy and online safety according to various parameters. With these control tools, parents can:

- → select which games children are allowed to play (based on the PEGI age ratings);
- → control and monitor digital purchases;
- → limit access to Internet browsing by applying a filter;
- → control the amount of time children can spend playing games;
- → control the level of online interaction (chat) and exchange of data (text messages, user-generated content).

Amazon

After activating the parental controls for in-app purchases, it is necessary to enter an account password or a specific PIN code to complete any in-app purchase in the Amazon Appstore on the device: amzn.to/2Ey05Fw.

Apple iTunes Store

Upon enabling restrictions on a device, it is possible to require a password for purchases, prevent certain types of purchases or disable purchasing entirely: apple.co/2GYwIjj.

Google Play

Setting up password protection for Google Play Store will help prevent accidental or unwanted purchases on a mobile device or an Android TV: bit.ly/2zvSKHC.

Microsoft

By creating separate accounts for multiple users, parents can prevent unauthorised purchases on the Xbox One console. By creating a passkey, they can make sure other people cannot sign into their account, make purchases or change settings: bit.ly/1CaEKgL.

Nintendo

On Nintendo Switch, Wii U, Nintendo 3DS or Nintendo 2DS parents can restrict the use of credit cards and online purchasing through Nintendo's Shopping Services. This requires the entry of a PIN code to add funds using a credit card or to complete purchases.

Sony

To ensure that a child does not make unauthorised purchases on devices which are connected to the Playstation Network, parents should:

- password protect their own master account to prevent unauthorised access by their child, and ensure the "required password for checkout" setting is in place to prevent purchasing even if the account is left logged in; and
- create a sub-account for each child and set the parental controls to limit or prevent any spending on the parent's account: bit.ly/2SZV4NP.

Managing games through parental mediation

Technology can be empowering for children of all ages, with tools that help them learn in fun and engaging ways, express their creativity and stay connected to others. Being tech-savvy, young people will also be better prepared for a workforce that will be increasingly digital. At the same time, parents naturally worry about their children accessing inappropriate content online, their healthy development being impacted by too much screen time and their becoming tethered to technology.

Media literacy is the ability to select, evaluate and use media content in a way beneficial to the user. As with most situations, a balanced approach works best. Setting limits on screen time will help to achieve a balance between on- and off-screen activities.

All users of media, including children and adolescents, are selective in how they spend their leisure time. There are so many games and other forms of digital entertainment available that everyone must be selective in the music they listen to, the TV and films they watch, and the games they play. These choices are influenced to a large extent by one's friends and peers (so-called peer pressure). In addition, we choose the music, games and videos that we think will provide us with the most satisfaction. Uses and gratifications theory proposes that individuals use media in an attempt to satisfy their particular needs and interests. Research suggests that people choose both traditional and new media to gratify at least five general needs: entertainment, information seeking, social interaction, emotional satisfaction and a pleasing level of excitement ("sensation seeking"), as well as passing time (Broekman et al., 2016). For example, some video games are extremely fast-paced, with lots of action and high-decibel music, which results in a feeling of excitement for those who are seeking it. But not everyone will want to experience this level of arousal and certain users will avoid this sort of game.

"Parental mediation" is any strategy parents use to control, supervise or interpret media content for children. Parental involvement is of vital importance in developing children's ability to use and interpret the media, as well as foster positive outcomes and prevent negative effects of the media on children. Parents are role models for their children, and their own behaviour regarding technology will affect how their children use such tools.

Parents employ one or more of the five styles of mediation available for games and other media:

1. **restrictive mediation**, posing restrictions on time and content;
2. **active mediation**, discussing content and giving explanations or instructions to the child to enhance safety, raise critical awareness or stimulate learning outcomes;
3. **co-use** of the media with the child, mostly for entertainment or educational purposes;
4. **supervision as a form of mediation**, staying nearby to keep an eye on the child when they are using an electronic device, or **monitoring** the child's online activities afterwards, e.g. checking the browser history or logs from social media;
5. contemporary electronic devices enable parents to use **technical restrictions**, i.e. "parental controls", to regulate or block inappropriate content (Nikken, Schols, 2015).

Parents vary their mediation strategies in accordance with their views on various effects of media content on children. Those who are concerned about risks and harm more often try to protect their children by monitoring, applying restrictions on use and supervising, whereas parents who feel that the media offer educational or entertainment opportunities more often co-use them with their children or actively discuss content. In one study, parents more often co-played video games with their children (aged 8 to 18) when they expected gaming to bring about positive social and emotional effects (Nikken, Jansz, 2006). Restricting children's access can backfire – the "forbidden fruit" can become more attractive.

Parents should enter into a dialogue with their children about what, when and where to play. "The first step is to reframe the often-asked question from 'How do I protect my child from violent games?' to 'How do I help my child make the most of the time spent playing video games?' [...] You want to work with and redirect your child's skills and interests. [...] Parents' awkwardness and hesitancy with video game controls and their lack of familiarity with the games can be used to their advantage when it comes to strengthening relationships with their children... It changes the dynamic of the parent constantly teaching the child to the child teaching the parent" (Kutner, Olson, 2008, pp. 220–221).

It is worthwhile to allow the child to describe their games and discuss with them any concerns about content or time limits, such as whether they can have a computer or game console in their bedroom. (In one study, children who had computers or game consoles in their bedrooms were more than twice as likely as other children to spend over 15 hours per week playing video games [Kutner, Olson, 2008]). In order to set boundaries, parental control tools can be mentioned in that conversation.

Adolescents are less likely to complain about limits if they have a say in setting them. One study found that how rules are made is more important than simply limiting screen time (Przybylski, Weinstein, 2017). The most effective mediation style is one that supports the child's autonomy, with rules and limits communicated in a way that respects their active role in the decision-making (Fikkers, Piotrowski, Taylor, Valkenburg, 2017).

Some tips for parents

1. Always look for the age classification on the game package or in the digital store.
2. Try to look for an online summary or review of the game.
3. Monitor the child's activity on gameplay websites. Even better, play with them. Talk to them about the games they play. Explain

why certain games may not be suitable. This is also the time to discuss how marketing messages try to influence people, and to encourage the child to fact-check rumours and be sceptical of anything they come across online.

4. Agree on the amount of time that can be spent playing games per week, on school nights and weekends. Encourage them to take regular breaks from screen-based media. Establish tech-free times, such as during dinner or in the car.
5. Be aware that games can enable the purchase of additional downloadable content.
6. Online games are played in virtual communities allowing users to interact with unknown fellow players. Tell your child not to give out personal details and to report inappropriate behaviour, such as bullying, threatening or bad language, display of unwanted content or invitations to meet outside the game. Report inappropriate behaviour, using the feedback page or specific complaint mechanisms on consoles or the games' websites.
7. Set limits (age, time, spending, online access) by using parental control tools.
8. Just as sports video games are not the same as participating in sports, online friendships are not a sufficient substitute for face-to-face ones. Young people should seek a balance between on- and offline activities to gain the unique benefits both types have to offer. Video games should be part of a varied "diet" of physical and social activity. For most people, most of the time, they are a healthy and satisfying hobby.

If they are carefully chosen, games have many potential benefits (even action video games can have numerous positive effects). Games that are not suitable are those rated older than the child's age, those that are too difficult regardless of their age rating, and those whose content may be unsuitable to a particular child. With a few precautions – common sense rules, attention to the ratings, involvement with the child's gaming and installing desired filters and limits in gaming devices – there is no reason the whole family cannot enjoy safe gaming.

Regardless of where or how users are active within them, it is important to remember that video games are a form of play with all the enjoyment and benefits that this affords. Like other forms of play, video games allow people to take "time out" from their everyday lives and become immersed in a fantasy world. And while they are having fun, users are also honing a wide variety of social, communication, cognitive, emotional and physical skills.

***For more information:**

*Eichenbaum, A., Bavelier, D., Green, C. S. (2015). Video games. Play that can do serious good. *American Journal of Play*, *7*(1), 50 -74.

The authors review recent research that reveals how today's video games employ many principles psychologists, neuroscientists and educators believe are critical for learning. Some types of commercial games have been proven to enhance basic perceptual and cognitive skills. Also, real-world uses of video games in a variety of areas are described.

*Granic, I., Lobel, A., Engels, R. C. M. E. (2014). The benefits of playing video games. *American Psychologist*, 69, 66 -78.

The vast majority of research by psychologists on the effects of gaming has been on its negative impact: potential harm related to violence, addiction and depression. The authors argue that a more balanced perspective is needed, one that considers not only the possible negative effects, but also the benefits of playing these games. Looking into such potential benefits is important, because the nature of these games has become increasingly complex, diverse, realistic and social. In this article, the authors summarise the research on the positive effects of playing video games.

*Kutner, L., Olson, C. K. (2008). *Grand Theft Childhood: The Surprising Truth about Violent Video Games and What Parents Can Do*. New York: Simon & Schuster.

A thoughtful and well-written discussion of two controversial issues surrounding video games: video-game addiction, and violent video games and aggression. The book also includes Kutner and Olson's research with troubled youth, gamers and their parents.

*Kato, P. M. (2010). Videogames in health care: closing the gap. *Review of General Psychology*, *14*(2), 113 -121.

There are ample examples of innovative ways to use existing commercial games for health improvement or surgical training. Tailor-made games help patients be more adherent to treatment regimens and train doctors in how to manage patients in various clinical situations. This review summarises examples present in the scientific literature of commercially available and tailor-made games used for education and training with patients, medical students and doctors.

Practical tips on how to use interactive technologies in a correct, safe and healthy manner

Veronica Samara

It is widely known that interactive technologies, such as the Internet and the mobile phone, are amazing tools for communication, learning, creation, fun and work. However, as for every tool, we need to know how to properly use these technologies, in order to enjoy their full potential while avoiding the pitfalls. As adults, we are able to judge and avoid the dangers we may encounter, but children need our guidance, in order to create the necessary skills and behariours, which will allow them to enjoy the online worlds and benefit from their abundance of opportunities. The next pages intend to provide you with practical tips, which will help you in empowering children to use the Internet, and the interactive technologies in general, in a responsible, safe and healthy manner.

Keywords:
privacy
online information
communication
cyberbullying
online ethics/reputation
excessive use
phishing
parental control
electronic games

Home

Preface

It is commonly known that interactive technologies, such as the Internet and the mobile phone, are great tools for communicating, learning, creating, having fun and working. With a few clicks children and adults can enter an amazing, miracle space. Yet this vast virtual world, like the real world in which we live, also has its dark sides. An adult is able to judge and avoid the dangers they may encounter there, but for a child the situation is very different.

The responsibility for protecting the child online lies, as in the real world, in the hands of parents and carers. However, the protection of minors is not a simple task. The desired result is neither a total ban on access to the interactive world, which would deprive the child of invaluable tools, nor a complete lack of supervision, relying on the hope that nothing bad will happen.

It is, therefore, time for action. It would be wonderful if we did not need to know what the terms “spam”, “phishing” or “Instagram” mean. We do, however, have to know this for the sake of our children, whom we often leave to navigate the Internet alone – an act comparable to allowing them to wonder alone on the streets in the middle of the night!

Just as we do not need to have a driving license for teaching our children to safely cross the street, we do not need to be a technological “guru” to protect them from pitfalls in the digital world.

We should abide by the same rules that guide us in the real world, i.e.:

→ teach children to be responsible;

→ equip them with proper information and education;

→ help them whenever they ask for it and always be on their side – not only in spirit, but also by means of physical presence;

→ inspire confidence;

→ be informed and make an effort to learn with them.

The following pages intend to provide practical tips, which will help adults in empowering children to use the Internet, and interactive technologies in general, in a responsible, safe and healthy manner.

Knowledge is power

As a parent, think about the following questions:

→ Would you leave your child alone in the park without supervision?

- Would you let your children go into the sea if they did not know how to swim?
- Would you let your children cross a motorway alone?
- If your children did not have a driving licence, would you give them your car keys?
- Would you trust your children to a stranger?
- Would you let your children watch a TV programme not suitable for their age?
- Would you let your children spend their pocket money in a casino?
- Would you give your children your credit card to go and shop alone?
- Would you give your personal information to a stranger on the street?

On the Internet, the above questions translate into:

- Surfing without supervision adequate to the children's age.
- Surfing without rules and limits.
- Surfing without awareness of possible risks.
- Surfing without proper education.
- Communicating with strangers in chat rooms and social networking sites without risk awareness.
- Publishing personal data without thinking.
- Playing age-inappropriate games.
- Intentional or unintentional contact with (illegal) gambling, adult pornography and, in general, with content which is inappropriate or harmful for children.
- Easy prey for online scams.

It is, therefore, vital that we, as parents and educators, become acquainted with the Internet and (why not?) learn to "surf". Let us ask children to show us this amazing world.

Only then we will be able to:

- **Understand the potential dangers**, in order to explain them to children and teach them how to avoid them.
- **Discuss with children** what they can and cannot do online, and **set rules and limits**, explaining the reasons behind all our "No" and "You must" statements.

- **Encourage children to use the Internet** to adequately communicate, study, have fun and find information in a correct way, being **responsible, properly informed and aware**.
- **Inspire confidence**: even if children are far better than we are at technical issues related to computers, the Internet or the mobile phone, **we** are the ones who **possess life experience and the necessary critical thinking** to support them in the process of identifying and differentiating between the opportunities and risks of the digital world.
- **Make the Internet a family affair**. Whenever we can, we should be with children when they use the Internet. It is a great way to immediately discuss any issue that may arise, and to build trust. Learning together is a pleasant challenge.

Online information

The Internet is a vast source of all kinds of information – true and reliable as well as false and even fake – available from anywhere at any time. It is, therefore, of great importance that children learn from a very young age to navigate this “sea” of information with a critical mind. To this end, we should:

- Use the Internet together with children, treating it as a **valuable tool of knowledge** and exploration.
- **Find suitable websites** for children with entertaining, informative or educational content, and surf these websites together with them.
- Teach children to **use their critical thinking** – anybody can publish content on the Internet, not only experts or scientists, so information should be cross-checked with other reliable sources (such as encyclopaedias or scientific journals) to verify its accuracy, as it can be misleading or incorrect.
- Teach children how they can conduct a **targeted online search**: show them that placing a search phrase in quotation marks “ ” is the most effective way to receive matching results; as an example, if they type in the words *the tallest building in the world* without quotation marks, the search engine will show results where the above words appear in any order, whereas if they type the words in quotation marks: “the tallest building in the world”, the search engine will bring up only

those results where all the above words appear in exactly the order they were typed in.

- Teach children to **immediately notify us** of online content or behaviours which make them feel scared or uncomfortable (such as bullying or content which is racist, extremist or harmful to them).
- Teach children to **distinguish information from advertising**. With the help of practical examples, we can explain that many websites offering access to information and services for free – even game websites or those with fun online activities – belong to commercial companies which make profit via (hidden) advertising, encouraging children to buy goods or to indirectly influence their family's consumer habits (e.g. by buying products of a particular brand).

Communication and privacy on the Internet

It is common knowledge that the Internet has evolved from a simple tool for publishing and finding information into a powerful instrument for social interactivity and participation. Nevertheless, it is important to understand that it is like a public square in the real world: if we are careless, anyone can hear what we say. Thus, we should always be careful when engaging in online communication, and we should always protect our online spaces and privacy. There are several rules worth adhering to:

- **Think before posting**. As soon as we publish anything on the Internet, it stops being private and becomes publicly accessible anywhere in the world. We need to explain this to children and discuss with them the implications. In the case of older children, we can ask them to look themselves up on the web (to "Google themselves"); then, together, we can discuss the results and whether they are happy with all the information they found about themselves online.
- Through discussion, we should teach children to **protect their personal data**: to never reveal their home address, phone number, the name of their school or where they spend their free time. The same applies to the data of their family, friends or third parties.
- We should explain to children that our Internet passwords are like our house keys: if somebody gets ahold of them, he or she

can enter our online space. So, we need to teach children to use **strong passwords** for accessing Internet services, i.e. ones that consist of at least 8 characters: letters, numbers and symbols. These passwords must be changed regularly and **should not be disclosed to anyone** except parents, not even best friends. Otherwise, with the use of a password, someone might impersonate the children on the Internet, read their emails, post incorrect or bad information, harass people or spread lies to third parties. A trick to create a strong password, which is not easy for others to guess, is the following: we should think about something we like, e.g. "I like to eat spaghetti with red sauce". Take the first letters of each word: "Ilteswrs". Make the last letter a capital, change the letter "t" to "2", put an "!_" and add a few digits, for example "12", at the end: "Il2eswrS!_12". According to websites where it is possible to check the strength of a password is (we can search for them online by typing in the phrase "how strong is the password"), it would take several thousand years to crack this one.

- When going online on someone else's computer, children should **not visit websites that require their passwords**, especially if the internet connection on this particular device is not protected. Otherwise, there is a risk some of their personal details might get stolen.
- It is essential to emphasise the importance of **avoiding the publication of personal photos online**, particularly those that reflect personal moments. We can never know who will gain access to them. Under no circumstances should children publish photos which make it possible to identify where they are in the real world, because this may allow strangers to locate and find them. We can look for such a revealing photo on the Internet and discuss with children which of its elements are personal and which make it possible to pinpoint someone in the real world.
- It is also important for children to understand how easy it is for someone to **alter an original photo** using appropriate image editing tools, freely available online. Sometimes this is done officially, for example in the context of a cartoon or an advertising campaign. Often, however, such actions are undertaken without the consent of the people who appear in the photo, violating

their personal data to an extent that can **irreparably damage their dignity**. The altered and false photo can be sent by e-mail, published on a website or disseminated via mobile phones all over the world, and we can never know where it might end up.

- It is also very important to explain to children that **they cannot publish photos or videos of others**, or their own photos or videos where other people are shown, if those people have not given their consent.
- We should discuss with children the paradox of their **posting personal data on the Internet without thought**, and with the assumption that these posts will be only visible to friends, while at the same time conceal their online activity from us as a way of exercising their right to privacy. We need to explain to them that **nothing on the Internet remains private**.

Strangers and the Internet

In electronic communication we can never be sure of the identity of the person we are talking with – even if they send us a photograph or use a web camera – if we do not know this person in the real world. Many perpetrators exploit online anonymity to reach minors, giving false information about their identity and age in order to become friends with children and establish a trusting relationship with them, with the purpose of e.g. involving them in sexual acts (so-called “grooming”). For this reason we need to:

- **Talk to children about strangers on the Internet**. Children need to realise that people on the Internet, even those with whom they have been communicating for a long time but whom they do not know in the real world, are not necessarily who they say they are. As people do not always tell the truth online, they must always be treated as strangers.
- Ask children if, **in the real world, they actually know all of their friends’ friends** or even the friends of their siblings. They should think about the answer to this when we ask them about their online contacts. They should always consider people they only know in the virtual world as strangers.
- Discuss with children situations regarding secrecy. **If an online “friend” asks a child to keep their friendship secret, then something is wrong**. What true friend would ask something like

this? We should talk to children about such situations so that if they do occur, they will inform us immediately.

- → Explain to children that they need to **be extra careful when communicating online**. Even in a children's chat room it is not possible – at least today – to check if all the participants are indeed minors. There may be an adult there, claiming to be a child and trying to mislead young people.
- → Make sure children **never talk about personal matters** or give personal details online, even if they know the person in the real world, as strangers could be following the conversation as well.
- → Make sure that children **would never arrange a meeting with someone they knew only through the Internet**. Even if they insist that they have seen a photo of this person, we must explain that this photo may be fake and used with the aim to mislead them. Moreover, even if children see someone through a webcam, they are facing the same potential risk from paedophiles or other groups which may have recruited minors (to put them in front of the camera) to attract children.

Creating positive digital footprints – managing one's online reputation

Our digital footprint is the trace we leave every time we use the Internet, for example every time we "like" something on a social networking site, visit a website or carry out an online search. These footprints can reveal a great deal about us. They may be positive or negative, and can influence the way others perceive us, not only today, but also in the future. In other words, **our digital footprints can shape our online identity and reputation**. Below are some simple tips which will help children – and adults – to manage their digital identity and maintain a good online reputation.

- → **Look for information about yourself online**. Do you really know what there is on the Internet about you? Make a simple search using your name to see what you find. If you come across content that you do not like, take the necessary actions to remove it. If your profiles on social networking sites are displayed – which means that everybody online can view them – it is advisable to change this through the respective "privacy settings".

- **Check your privacy settings**. Make sure you know what information you make public on websites and social networking sites. Most of these have privacy settings that help you manage both the content you are sharing and the users who can access it. For example, you can decide to post information only to your friends. Do not forget that your friends' content and settings can also affect your digital footprint.
- **Think before you click**. Before you upload that funny photo of your friend online or write a silly tweet to someone, ask yourself if it would be OK for anyone to see this photo or read this tweet: friends, acquaintances, family, future employers. Would you like it if others published such content regarding you? Only share content you will not be ashamed of later. Remember, everything that is published on the Internet can stay there forever.
- **Disable and delete**. When you stop using a social networking site or another web service, it is a good idea to disable or delete your account. This means that your content will no longer be active and will not be searchable online. It will also protect you from the risk of your account being violated.
- **Create a positive digital footprint**. The best way to maintain your digital reputation is to use your time on the Internet productively, in order to create a positive digital footprint. For example, why not write a blog about all the important things that interest you, create a social networking page to promote your family's business or make a video which can teach others something new?

Cyberbullying and harassment

Communication with the help of the Internet and mobile phones has many great advantages. However, it can also lead to unpleasant experiences. Children can receive or send messages with content that may hurt their feelings or the feelings of others.

Cyberbullying and online harassment involve the misuse of information and communication technologies to intimidate or harass a person or group through e-mail, chat, mobile phones, etc. Among children and adolescents, this is an evolving fashion with a constant increase in incidents of pupils harassing pupils, or even pupils harassing their teachers. Behaviours that may occur include:

- sending texts, e-mails or instant messages with mean content;
- publishing personal information, unpleasant photos or mean messages about others in blogs, on social networking or other sites;
- identity theft: spreading rumours and lies about others under someone else's name;
- dead calls;
- offensive voice messages;
- sometimes, offensive text messages are sent to mobile phones through websites using names and phone numbers of people who have nothing to do with them, but they end up being accused of being the sender;
- another technique of electronic harassment is to create websites that target specific individuals or groups by inviting others to post hate messages; harassment also happens when another player in an online game attacks the "avatar" icon that reflects a child's virtual self, e.g. by shooting it, stealing its virtual possessions or forcing it to behave in an undesirable way.

Such behaviours can make children and young people feel lonely, unhappy, afraid and insecure. They lose confidence and may not want to go to school or meet with friends. Moreover, in extreme cases, persistent and intense harassment can lead to terrible consequences such as suicide attempts.

Bullying and harassment, either by electronic means or in the school yard and the playground, **are socially unacceptable behaviours**. Parents, teachers and children must be sensitised and ready to react. Unlike traditional bullying, cyberbullying can affect a child even when he or she is physically not in the same place as the perpetrator. The offender may, for example, send intimidating messages to the child's e-mail or mobile phone **from anywhere, at any time** of day or night.

To protect children from such inappropriate behaviours, we should:

- Familiarise ourselves with the children's environment – get to know **their friends**, their friends' parents, their teachers and their classmates.
- Be alert for **signs that children have become the target of cyberbullying or online harassment**, e.g. emotional distress, sudden avoidance of friends, not wanting to go to school

or undertake their favourite activities, a drop in school performance or comments that reflect disturbed relationships.

- Explain to children – as they often **avoid mentioning uncomfortable encounters** on the Internet or their mobile phone – that if something unpleasant happens, it is not their fault and they should report this directly to us.
- Teach children **never to answer mean or insulting messages**. If they receive such messages or others they do not understand, if they see improper images on the Internet, if they receive such images on their mobile phone or if they are bullied, they should immediately inform us.
- **Investigate if the offender** of a child who is harassed or bullied **is in his/her immediate environment**. Often the perpetrator is a classmate, friend or acquaintance who wants to harass or intimidate the child for some reason (or simply "for fun", without thinking about the possible consequences). In such a case, we should talk directly with the offender's parents, as well as with the school administration.
- **Promote** in the family and in the school **an environment that does not tolerate bullying and harassment**. We need to teach children that anonymity on the Internet is not tantamount to approval of irresponsible behaviour. We all leave digital footprints online, so we have to behave politely, and adhere to rules and morality, just like in the real world. We should remember that even our own children are not always angels.
- Teach children their **rights and responsibilities** and how to respect the rights of others.
- Be in **constant dialogue with children,** so they feel safe to discuss their concerns with us.

All that glitters online is not gold

The Internet provides great opportunities for bargain transactions, but, as in the real world, it is **open to both trustworthy companies and crooks**, who will try to sell us items of questionable quality. Therefore, is it important to remember certain rules:

- Minors should never make purchases **without a parent's supervision**. Websites whose legitimacy and reliability we cannot be sure of should be avoided.

- **We should always type in the web address ourselves** – this refers to the addresses of online shops, banks and organisations whose sites we want to visit. This way we can be sure to land on the genuine website, and not a fake one. We need to make sure that the address appearing in our browser starts with "http**s**: //" (the "s" stands for a "secure" connection). Finally, if we do not want to give our regular credit card details, we can use a prepaid one for online transactions.
- We need to explain to children that **they should never take part in online quizzes or competitions** in which they are asked for their personal details, **if they haven't asked us first.** This way we can double check the validity of such actions, as well as familiarise ourselves with the terms of use of personal information. Such activities may have the sole purpose of fooling children into inadvertently subscribing to services which have excessive charges, start bombarding them with ads or even exploit them in commercial questionnaires or campaigns. There are also fake competitions aimed at "phishing" sensitive personal data, in order to financially harm the child's family.
- In the same way, it is essential to teach children **not to fill in online forms** without our consent. This way we can locate and carefully read important information (such as terms of use or privacy policy) which clearly describes how the requested data will be used.

Online ethics, respect towards intellectual property

Online anonymity allows many people to believe that, when in the virtual space, they can break the ethical rules which guide us in the real world. Nevertheless, if we want the Internet to be a positive resource, we should all behave responsibly and ethically towards its services and towards other users:

- We need to **treat other Internet users in the same we want them to treat us**. We should not blame or insult anyone online thinking that we are only joking, because joke may not be accepted and may hurt the person it is aimed at. It is worth discussing this with children.
- As in the real world, on the Internet children should know that if they violate specific rules connected with sanctions, they are

not invisible – they **can be located** anywhere **through the digital footprint** they (like all of us) leave.

- We should teach them to only **visit legitimate sites**. In this way, they will also avoid the possibility of viruses infecting their computer.
- We need to explain to children that they cannot forward e-mails they have received and find unacceptable, as this is synonymous to sending **unwanted mail (spam)**.
- We should explain to them the **importance of intellectual property** through examples. We can ask how they would feel if someone used their creations without their permission. We can explain that they cannot simply copy text from online materials and use it for their homework, because this is tantamount to stealing: it may be illegal and in no way helps them develop cognitive and critical skills, qualifications that they will certainly need in the future. The term "copyright" does not mean "the right to copy".
- We need to explain to children that **they cannot simply "download" software, music, videos** or anything else from the Internet that is **protected by copyright**, because this is a violation of the law. There are many websites that provide their users with free materials, such as tracks by young musicians who want to become known to the public.
- We should, again, explain that children **cannot publish on the Internet photos or videos in which their friends or other people are portrayed** if these people have not given their consent. Each of us owns the intellectual property rights to our own image, and this must be fully respected.

Malware and unwanted messages

Daily activities, such as the use of USB storage devices, opening e-mail attachments or downloading programmes from the Internet, can pose risks. These are mainly related to the distribution of malicious software (so-called malware) aimed at damaging our computer, stealing our personal information or bombarding us with unwanted advertising material. We must, therefore, be careful. The following tips will help us avoid dangerous situations:

- We should install an **antivirus** programme and a **firewall** on our computer. Upon installation, **antivirus** software checks all our computer files along with e-mail attachments. If viruses are detected, it informs us immediately and, in most cases, isolates or repairs the infected files. Such a programme can also be used to filter web pages. Antivirus software must be constantly updated. It is widely available on the market or offered by Internet service providers. A **firewall** is a device or software that prevents or blocks unauthorised access to our computer. It checks all incoming and outgoing files and, if a suspicious one is detected, it deals with it, ensuring our computer's safety.

- We need to teach children **not to open e-mails from people they do not know or e-mails they are not expecting** (even if they seem to have been sent by friends or acquaintances), as such messages may contain viruses. The account of someone the child knows may have been hacked to send viruses to other users.
- We must teach them **never to activate links they find in e-mails**, even if these e-mails come from people they know. Such links may lead to websites which steal personal data or install computer viruses. We need to teach children to always type the address of a website they want to visit themselves.
- We should teach them **never to answer any such e-mails as described above**, as in this way they confirm the validity of their email address.
- We need to teach children to **"Bookmark" websites or save them in the "Favourites" tab**. This way, when they want to revisit them, they will be able to find them very easily and avoid being led to websites unsuitable for their age, for example by typing an incorrect address.
- We should explain to children that they have to protect their e-mail address by **avoiding unnecessary disclosure** on websites they visit. The same goes for the e-mail addresses of members of their family, friends or third parties.
- When children publish their e-mail address, **they can "transform" it** by using characters that trick the tracing engines. For example, instead of john.smith@xy.com, they can type john DOT smith AT xy DOT com. We can also teach them to use their imagination when establishing their usernames. The stranger such aliases are, the harder it is for an engine to guess them and to start sending spam.

- Children should avoid **suspicious websites**, and if they accidentally access such a site, they should leave immediately. If windows pop-up, asking them to agree to anything, they must never press any buttons inside them and close them immediately (an easy way to do that is to simultaneously press "Alt" and "F4").

Excessive Internet use

We should prevent Internet "dependence", which can lead to addition, by **immediately taking into consideration relevant signs** and asking experts for help. We, better than anyone else, know our children's everyday habits and can instantly see **changes in their behaviour**.

Thus, if we notice the following symptoms:

- irritation when the child is offline;
- using the Internet much more than intended;
- sudden school failure;
- sleep disorders and changes in sleep habits / fatigue and drowsiness;
- reduced physical activity;
- disturbance in interpersonal relationships;
- change in the child's habits, such as neglecting friends or favourite hobbies;
- negligence of personal hygiene;

we should immediately seek help from experts, e.g. by calling a relevant helpline for parents and professionals or for children and youth.

The time children spend online **should not affect their family life**, their schoolwork, their hobbies, their friends and their sleep. We should also teach them to take **regular breaks** from the computer in order to rest their eyes.

Filters and parental control

Even very young children can benefit from surfing the Internet by visiting websites for recreational or educational purposes. However, the web provides all kinds of content, not always suitable for the children's age. Thus it is essential – especially for younger children and for those who are just starting to use the Internet – to install special filters and activate parental control mechanisms.

Filters are programmes that **regulate access** to information or services online according to set criteria. They can be installed on a user's computer, on a server owned by an organisation (e.g. a school), or on the devices of an Internet service provider. They work in a variety of ways: they can alert us of problematic web pages, record the movements of a user on the Internet, block suspicious websites and even shut down the computer entirely.

The primary goal of filters for the protection of minors is to provide a **reliable barrier** preventing access to content which is unacceptable, which is considered dangerous, or which may cause problems in children's development. At the same time, such a solution should not block content which is appropriate for children and youngsters. For example, a filter that aims to block websites concerning sex should not block those referring to the city of Essex (EsSEX). In other words, it should be smart enough to block content using sophisticated methods that recognise which web pages are harmful and which are not. Moreover, a filter should not be more restrictive than necessary so as not to block innocent content. For instance, a too-restrictive filter could block research on World War Two history, as such activity would probably lead to web pages with descriptions of violence.

As far as parental control is concerned, filters deal also with outgoing data, which makes it possible e.g. to prevent children from publishing personal information such as names, home or school addresses, credit card information, etc. This type of filtering is very important for the protection of young users and there is software widely available both on the Internet and on the traditional market for this purpose.

Important tips for filters and parental control

→ Create a **separate user account for each child** via our computer's operating system (e.g. Windows, Linux, macOS), then activate parental control options according to the age of each child. If we do not know how to do this, we can ask the help of a specialist, for example at the shop in which we bought the computer.

→ Make the most of the **parental control** options offered by our computer's operating system. In this manner, we will be able to protect children's privacy and online safety, set and monitor the time they spend on the Internet, define the websites they are able to visit or select the games they are allowed to play.

→ "**Bookmark**" the child's favourite websites or add them to "**Favourites**" (both options are available in our browser).

In this way, children will visit their favourite pages without having to re-enter the address or going through search engines.

- → Use **filters**, which can be valuable tools to protect minors from harmful content. However, we must always remember that they **can act only complementarily** and, probably, are really effective only for younger children. Any filter that can be enabled can also be disabled by clever young users, often skilled in covering their tracks. Only if we know how to handle the computer and the programmes it contains, will we be able to detect such actions.
- → Remember that **no programme can replace our guidance**. Technical means are not panacea and sometimes, if they are not combined with common sense, they can create a false feeling of security. Educational supervision at home, in line with the one carried out at school, along with communication and risk awareness, is preferable to technological barriers as it contributes to the proper education of minors, as well as to their understanding the problems they face and developing critical thinking in dealing with them. This is why we should be there next to the child, especially in the case of younger children, when they use the Internet. It is a great way to instantly discuss any issue that arises and to cultivate trust.

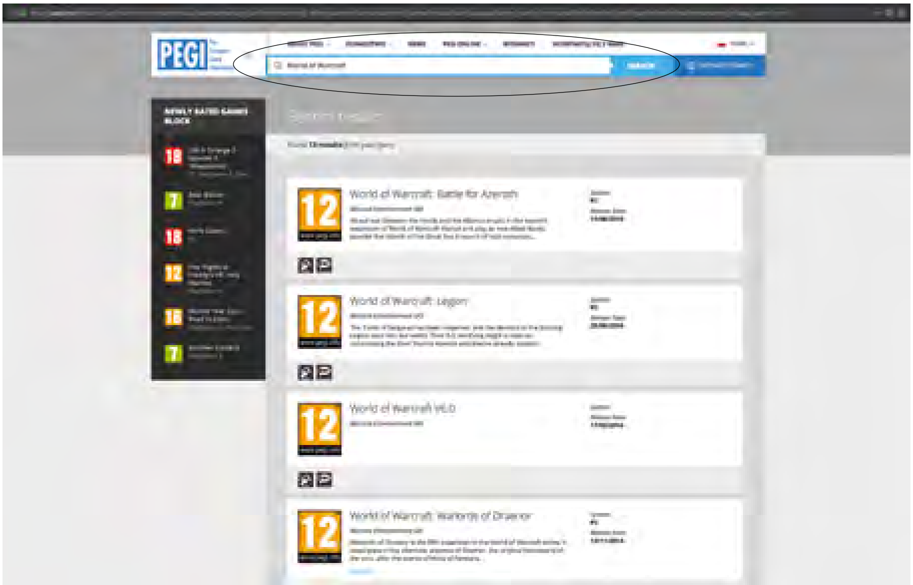
Selecting appropriate games for each child

In order to protect minors from inappropriate games, the PEGI – Pan European Game Information – system was created. It consists of two parts: age labelling and content descriptors. Most commercially available electronic games have a PEGI label on the front and back of the DVD box.

- → **Age labels** – there are 5 labels: PEGI 3, PEGI 7, PEGI 12, PEGI 16 and PEGI 18. They indicate the minimum age at which a game's content is considered appropriate.
- → **Content descriptors** – there are 8 descriptors: bad language, discrimination, drugs, fear, gambling, sex, violence and in-game purchases.

Although the PEGI information aims to act as a guide and provide a simple recommendation to buyers, it should be taken into account for the safety of children. We can find **the classification of a game** by looking up its title on the PEGI website (pegi.info)[1].

Figure 1: Looking up a game's classification on the PEGI website


PEGI
12
World of Warcraft: Battle for Azeroth
12
World of Warcraft: Legion
12
World of Warcraft V4.0
12
World of Warcraft: Warlords of Draenor

For example: if we type in *World of Warcraft*, a list of 13 available versions of the game will appear, with the age label and content characterisation for each. The above Figure 1 is a screenshot of the PEGI website, where we can see four (out of the total of thirteen) results with the age label 12 and two content characterisations for violence and bad language.

Basic tips for a child's use of electronic games

- Make sure, before buying a game, that its contents are appropriate for the child (PEGI rating system).
- Set rules on the time the child can spend playing.
- Spend some of our leisure time playing with the child. If the complicated virtual environment scares us, we can ask the child

[1] With age marks and content descriptors along with their descriptions, consistent PEGI guidelines can be found in previous chapter ("Safe gaming"). This information is also included available on the PEGI website (pegi.info).

to help us understand how the game works. He/she will be happy to show us!

- Keep track of the child's habits when playing. This will allow us to immediately identify signs of excessive engagement or "dependency".
- Discuss the content of the games. Which elements resemble reality, which do not, and what does the child particularly like in these games?
- Teach the child to be responsible concerning the use of personal data – during online gaming, as well as in general Internet use.
- Encourage critical thinking. Children are a very profitable target group for Internet advertisers. Thus, they should always be alert in order to distinguish information from advertising within the virtual environment of the games.
- When the child plays online games with multiple users, we should:
  - choose websites with strict rules and supervisors;
  - teach them not to give any personal information to other players;
  - teach them not to agree to meetings in the real world with players they only know online;
  - encourage them to immediately tell us about harassment, bullying, use of inappropriate language, nasty content or invitations received from other players to meet in the real world.
- Keep the child away from a game if the way it evolves makes us or the child uncomfortable.

Proper use of the mobile phone

Mobile phones are now a widespread means of communication. Almost all commercially available devices offer a range of services beyond the conventional phone, such as sending and receiving text messages (texting), taking and sharing photos, sending and receiving multimedia messages (MMS), playing music, etc. They also provide full Internet access.

As the mobile phone is a personal tool, exercising parental control over a child's use of this device is not so straightforward. Indeed, many children view it as an indicator of social status and cannot imagine their lives without this tool.

Problems which may arise from careless or improper use of the mobile phone are quite serious: the possibility of uncontrolled access to inappropriate material, harassment of the child by malicious people or paedophiles, phone theft and the abuse of the personal data stored in its memory, or inadvertent exposure to advertising material to which the child does not know how to react are a few examples. As a result, in relation to smartphones **we must take the same safety measures as when using the Internet**. Here below are some general tips. We should:

→ Agree with the child on rules they should follow when using the mobile phone, especially when they are using online services.

→ Tell them about potential risks, especially those related to personal contacts, and train them to recognise them.

→ Teach the child not to reply to messages which they receive from strangers or which seem odd.

→ Teach the child not to give their mobile phone number or personal information to people they do not know and do not trust.

→ Directly ask the child whether they are being harassed via their mobile phone if we suspect this to be happening. If this proves to be the case, we should save the messages, note down the date and time of the calls, and contact our mobile operator or the police.

→ Teach the child to follow the rules of good behaviour when using their phone.

→ Tell the child not to leave their mobile phone in public view and not to keep it in their hand when this is not necessary. They should also not place it in their pocket or in a backpack they cannot see at all times.

→ Warn the child against giving their phone to strangers who ask to make an "urgent" call. Yet, if such a situation becomes threatening, the child should opt for giving the phone, even if it ends up being stolen. Their personal safety and integrity are much more important. Also, we can immediately report the theft.

→ Make sure the child knows that, before taking anyone's picture, they must obtain that person's permission. They should never photograph strangers.

- → Teach the child not to use their mobile phone to send or post photos which depict personal moments, and which could result in a problematic situation either today or in the future.
- → Remind the child that they should never send their photos to strangers via their mobile or upload them onto the Internet. Under no circumstances should they send photos of others if these people do not know about this and have not consented to it.
- → Make sure the child never answers advertising messages or messages from unknown senders. Under no circumstances should they forward these messages to other people.
- → Teach the child to protect their personal information and never to enter their mobile phone number in forms / applications (on- or offline). If they wish to do so, they need to inform us, so that we can deal with this process and check how the requested data are to be used. Entering their number could mean that the child consents to a contract with a company or organisation which administers the form / application.
- → Explain to the child that they should be very careful about the content they download onto their mobile phone. Find out if they share such content via their phone (or on the Internet) with their friends. This is important as downloading certain material may be illegal under the copyright law.
- → Teach the child to disable Bluetooth when they are not using it, and to keep it switched off in public places, as the data stored in their phone may be stolen.

Acronyms and emoticons

In chat rooms, social networks, e-mails or even on mobile phones, abbreviations of words or phrases (acronyms) are often used. These are mainly in English and are spelled with capital letters. The following table lists some common acronyms used by children in online communications, so that we can be aware of their meaning.

Table 1: Popular acronyms used by children in online communication

^5	High 5
24/7	24 hours a day, 7 days a week
ANW	Anyway
ASAP	As soon as possible
ASL or A/S/L	Age, Sex, Location
AFK	Away from keyboard
B/C	Because
B4N	Bye for now
BBL	Be back later
BRB	Be right back
BTW	By the way
C	See?
CU	See you
CUL	See you later
F2F	Face-to-face
FAQ	Frequently asked questions
JJ	Just joking
GL	Good luck
GM	Good morning
G2G / GTG	Got to go
IDK	I don't know
L8R	Later
LMIRL	Let's meet in real life
LOL	Laugh out loud
LU4E	Love you forever
NP	No problem
PAL	Parents are listening
PAW	Parents are watching
PLS	Please
POS	Parent Over Shoulder
S^, S'UP	What's up?
SRY	Sorry
THNX	Thanks
TTYL	Talk to you later
W8	Wait
WB	Welcome back
WTGB	Want to go private?
WYCM	Will you call me?

In turn, emoticons are icons that are meant to symbolise certain facial expressions and emotions. They are composed of characters which, when read with the head tilted 90 degrees to the left, are reminiscent of the “smiley” pictogram. So, for example, the emoticon :-) denotes a smile. In Table 2 below, some of the emoticons widely used in electronic communications are presented.

Table 2: Selected emoticons widely used in online communication

:–) smiling	:–(sad
;–) winking and smiling	:–O surprised
:–p tongue out	0:–) angel
:–* kiss	:–# keeping a secret
%–I confused	>:–(angry
8–) wearing glasses	QQ tears

Creating a family / classroom agreement on Internet use

It is important that children understand and follow general rules regarding responsible, healthy and safe use of the Internet, mobile phone and other interactive technologies. In this respect, it is a good idea to discuss with them the following 16 rules and to rank them (all the rules are equally important, yet it is always interesting to hear children’s thoughts). We can do this either individually with each child or as a group activity within the class. Then, together, we can sign and date the agreement, and place it in a commonly accessible space.

1. On the Internet, I never reveal **personal details**, such as my real name, my home address, my phone number or the name of my school. I treat the personal details of members of my family, my friends and other people the same way.
2. If, when online, I read something that bothers me, seems suspicious or too good to be true, **I inform my parents / teacher**.
3. I **treat** other Internet users in the same way I would like them to treat me.
4. I **do not** jokingly **blame** or **insult** anybody on the Internet, because this may be misunderstood.

5. I can have fun in the **virtual world**, but I always remember it differs from the **real world**.
6. In the real world, I **never meet** people I know only through the Internet, as these people are really **strangers**.
7. I always **cross-check the information** I find on the Internet with other sources, such as books, newspapers and magazines.
8. I never make **online purchases** unless there is **a parent next to me**, and I never shop using websites I am not sure are legitimate.
9. I take **regular breaks** from the computer and the Internet to rest my eyes.
10. I **do not ask** others to **reveal** personal information on the Internet.
11. I am not interested in **adult content**, I surf websites that are appropriate for my age.
12. Copying from the Internet may be illegal. I **do not just copy text** from materials I find online and use it for my homework, because this is tantamount to stealing. Before using any material, I always make sure I have the author's **permission**.
13. I do not **download music and movies** from Internet sites, unless I'm sure that the websites are trustworthy, that the music and movies are offered for free, and that by downloading them I am not in breach of other people's intellectual property rights. Legitimate websites clearly state whether their services are free or require payment.
14. When I go online on someone else's computer, I **do not go on websites that require my passwords**, especially if the Internet connection is not protected. Otherwise, there is a risk my personal details might get stolen.
15. I do not forward any e-mails I received and find unacceptable, because this is synonymous to sending **spam**.
16. I **protect my passwords** and I do not reveal them to anyone, not even my best friends. I regularly change them – I do this immediately if I suspect that someone may have stolen (intercepted) them.[2]

[2] The author proposes to prepare a contract based on the above document signed by children and adults.

Concluding remarks

Interactive technologies have opened new horizons regarding both knowledge and communication. It is up to each of us to know their positive aspects and to protect ourselves from potential dangers. And, as parents and teachers, we have an obligation to provide children with information so they, too, can use these technologies without any unpleasant surprises.

Children must be actively involved and, through proper education, learn what they can and should not do online. When we advise them, it is important that we explain our reasons. For example, when we tell them not to open e-mails from an unknown source, we should say this is because such a message may contain viruses.

Children need to understand that they have to treat people online as they do in the real world: with respect and good manners. It is also important that they learn to evaluate for themselves which information found on the Internet is accurate and which is false, as well as what is good and what is bad.

Last but not least, it is crucial to develop trust within the family and in the school. In this way, when they are in need, children will come to their parents and teachers for help knowing that they will always receive support in their online activities.

Additionally, the role of the state is imperative. There is a need to introduce proper laws and measures that will safeguard the well-being of minors in the digital world, both on a national and global scale. Without adequate control systems, the world of violence, pornography, gambling and other unacceptable online content and activity will continue to be available to all children.

Home

Cybersafety – practical aspects of school's activities in programs eTwinning and Erasmus+

Adam Stępiński, Jolanta Gradowska

For teachers and students participating in eTwinning and Erasmus+ projects, the issue of cyber security is a priority. In addition to the tasks that are part of their work within the project, they undertake numerous initiatives at school and beyond, which promote the responsibility of the young generation on the Internet. These activities take the form of contests, performances, films, posters that provide participants with proven online behaviour and how to proceed in the event of a threat.

Keywords:
cybersafety
eTwinning
Erasmus+
educational projects

Home

The Internet in the lives of young people

Young people, children and teenagers are able to fully utilise the rapid development and potential of the Internet. They do not remember a time when this important component was not a part of their lives, and their online presence is just as important to them as meeting friends in real life or going to the cinema. In today's world, it is not surprising to see a 3-year-old efficiently operating a tablet or looking for cartoons on YouTube. The Internet has become an integral part of the social life of children and young people, it accompanies them in their daily activities and is a source of entertainment.

From conversations with teenagers we can learn that they use the Internet every day and stay online from two to even a dozen or so hours (Wrońska, Lange, 2016). Young generations do not ask where mobile phones or laptops come from – these devices are an inherent part of their lives.

Already at the beginning of the 21st century, Marc Prensky called the youngest Internet users "digital natives" and older ones – "digital immigrants" (Prensky, 2001, pp. 1–6). For contemporary teenagers, the Internet is the most important medium as they grew up with it. While a few years ago it was said that children were born with a mouse in their hands, nowadays they grow up with their thumbs on the on-screen keyboard of a smartphone.

The most popular online pursuits of children and young people include watching videos and using social networking services. Further down the list are such activities as doing homework, searching for information or downloading music (Gursztyn, 2014, p. 6). The web's resources open up great opportunities to young people, but at the same time they out many negative elements in this environment. These are, among others, cyberbullying, phishing, hate speech, private message disclosure, misuse of personal data, excessive use of the Internet and Internet addiction, imprudent publication of photographs, videos and other material, promotion of self-destructive behaviour, copyright infringement, plagiarism, damaged online reputation, sexting and dangerous contacts with unknown users.

The list of threats is much longer and is constantly changing along with the development of new technologies. Keeping up with the evolution of the web and online interests of the young generation seems to be an impossible task. Therefore, there is a need to continuously raise awareness regarding these issues both among students and their parents and teachers. It is important to understand that we do not need to be experts in new technologies in order to be able to talk with children about their online activity. Parents and teachers should teach young generations responsible behaviour in cyberspace and constantly make them aware of online risks.

For over two decades, the Foundation for the Development of the Education System has promoted such activities by organising wide-ranging events aimed at raising students' awareness, as well as by improving teachers' professional skills and indirectly influencing parents.

eTwinning as a community of informed Internet users

Since the beginning, eTwinning has treated students' cybersafety as a top priority. Cooperation conducted as part of eTwinning projects between preschools and schools takes place in virtual reality. Having in mind the ubiquity of the programme (over 630,000 teachers and more than 200,000 schools in Europe, including almost 60,000 teachers and over 16,000 schools in Poland)[1], eTwinning project teams focus on the online safety of project participants, as well as on the promotion of responsible behaviour, awareness raising and dissemination of knowledge on this topic in and outside of schools. "Students and teachers use the Internet to work together across borders – to exchange information and learning materials. eTwinning broadens the range of pedagogical opportunities offered to students and teachers, motivates them to learn and opens them up to Europe"[2]. Project participants work together on previously planned activities using a variety of synchronous and asynchronous communication tools.

In order to ensure safety, teachers registering on the eTwinning portal are verified by national support services, which prevents persons who are not education professionals from registering. New users have access to the eTwinning Live platform which enables them to search for prospective partners from other countries and participate in various forms of in-service training (for example, webinars and learning events – two-week online workshops devoted to project work). eTwinning Live

[1] www.etwinning.net/en/pub/index.htm [access: 20.12.2018].

[2] etwinning.pl/czym-jest-etwinning [access: 20.12.2018].

also offers the opportunity to create one's own event (and invite other teachers to participate in it), to cooperate and take part in a discussions in thematic forums, to join one of the many groups of teachers, and to set up a project previously agreed on with partners from other countries. For several years, it has also been possible to carry out a project without foreign partners, within so-called domestic eTwinning.

After the national support service has accepted the submitted project outline, teachers gain access to the TwinSpace platform, which is a closed space dedicated to cooperation within the project. TwinSpace is not accessible for random Internet users. Here, teachers create accounts for their students, giving them logins and passwords generated by the system. When inviting students to TwinSpace, teachers must obtain consent for students' participation from each child's parent or legal guardian. The same rule applies to the publication of photographs. It is recommended to use avatars, icons or figures representing a given person. Before inviting students, teachers are recommended to read the answers to the five questions on eTwinning and TwinSpace eSafety available on the European eTwinning Portal[3]. New eTwinning users should also become familiar with the code of conduct, which will facilitate effective cooperation and eliminate possible inappropriate student behaviour within the project[4]. In accordance with the eTwinning code of conduct, all inappropriate content and spam e-mails must be reported. Comments must be addressed to specific individuals and relate to a specific post. One should also respond quickly to direct threats and incitement to violence due to differences in skin colour, ethnic and national origin, religion and sexual orientation. Inappropriate graphic content is immediately removed. The code of conduct also focusses on intellectual property and rules governing the management of private information and confidential data.

Three very helpful infographics have also been developed to clearly explain how to protect oneself online, how to select new online contacts and how to properly assess content to be published[5].

[3] bit.ly/2WSC8lf [access: 20.12.2018].

[4] bit.ly/2MvMBzD [access: 20.12.2018].

[5] bit.ly/2FTvFiG; bit.ly/2AmojnD; bit.ly/2Uf2zmE [access: 20.12.2018].

From the home page it is possible to add project pages (tabs), publish materials in three categories (images, videos, files), create new discussion forums, plan chats or videoconferences and manage participants in the project. Teacher administrators can change user roles (student – student administrator), invite new people to join the project, reset students' passwords, export member lists and delete project members. It is possible to contact multiple participants at the same time and each one individually. A very interesting setting is the role of a "guest" who can only observe the work progress but cannot add anything to it. This makes it possible to invite the head teacher who can, for example, verify if the project complies with the rules of online safety.

In the "Trends / Issues / Policies and Practices" section of the European eTwinning portal, the topics concerning user rights and responsibilities, privacy and data protection, as well as copyright are discussed in the form of questions and answers[6]. The web page also features a link to the Code of EU Online Rights. It is a very interesting document that can be used as source material for classroom discussion and project work on e-safety. Other extremely important topics discussed in the form of questions and answers are:

- social networks and social media;
- challenges of online communication outside eTwinning;
- Safer Internet Day[7].

eTwinning projects and cybersafety

The eTwinning programme sets only minimum requirements. To create a project, all that is needed is a computer with Internet access. The tools offered are simple and safe for students, who can use them without worrying about outside interference and access to inappropriate content. Together with colleagues from the same school, a teacher can run a number of projects – this depends only on their willingness, time and ability.

When starting a project, teachers introduce students to the principles of safe online work. This is done at schools. Dedicated classes

[6] bit.ly/2YN7IRR [access: 20.12.2018].

[7] bit.ly/2uFvCkg [access: 22.12.2018].

are conducted during which all participants share their knowledge about the rules of safe Internet use. This topic is often included in specific project tasks carried out together with partners. For example, students create posters, e-safety glossaries, comic books, videos, animations and presentations featuring the most important tips concerning safe online work. Apart from practical learning of safety rules, such task organisation ensures students have fun, which boosts their motivation to work in the project.

A very common practice applied at the beginning of an eTwinning project is to formulate netiquette rules, i.e. guidelines on how to relate to one another, comment on peers' work, and upload materials, photos and videos. All students vote in favour of or against individual proposals, thus creating a jointly developed code of conduct and attitudes to be adopted in the project work. In this way, apart from influencing students' attitudes, the principles of democratic behaviour, discussion and joint selection of proposals to be accepted by all participants are promoted.

Students and teachers involved in eTwinning projects are also often the driving force behind broader cybersafety awareness-raising campaigns at their schools. When holding arts exhibitions in school corridors, working on screenplays for performances and videos about student online behaviour and then staging them, they are, on the one hand, promoters of desired behaviour on the Internet, and, on the other, they warn their peers against recklessness, showing the consequences of irresponsible activities.

Examples of eTwinning projects devoted to cybersafety

eTwinning projects devoted to online safety are often the result of observations made by teachers who see real problems faced by their students. This was the case with the project entitled "Being aware, feeling e-safe"[8] carried out by the Franciszek Łuszczki Primary School in Lubenia, Poland and Liceul de Arte "Ionel Perlea" in Romania.

Initially, students exchanged posts in order to get to know one other. To introduce themselves, they used, among others, the Voki application. Each student had an avatar and it was not necessary to publish photos.

[8] bit.ly/2T460ck [access: 02.04.2019].

During the project, the participants jointly developed a netiquette, which they committed to follow during their work. They also prepared slogans on e-safety aimed at promoting safe online behaviours, organised and conducted a competition for a poster promoting safe Internet use, and developed materials for thematic crosswords and quizzes with LearningApps. During their work, participants used, among others, the Tricider application to prepare slogans promoting e-safety and Google Drive documents to develop questionnaire forms.

The main goal of the project was to propagate rules for the use of online resources. Students developed their digital and IT skills, and through cooperation with foreign partners significantly enhanced their social and civic competences, the ability to work in a team and to communicate in a foreign language. They also learned how to create their profiles on social media, how to protect e-mails from phishing and how to behave in the case of experiencing cyberbullying.

Since the project had an interdisciplinary character, the didactic materials developed in its course can be used when teaching various subjects. They are adapted to teaching classes while using modern technologies and can be given to students to work on them independently at home.

As part of the project, Safer Internet Day was organised at the two schools and a classroom wall presentation with thematic posters was prepared. In addition, a quiz for students of grades 4 and 5 was staged to test their practical knowledge of the Internet and the safe use of electronic media. The "Being aware, feeling e-safe" project was presented during a webinar held by the "Bringing e-safety into eTwinning projects" group. It was awarded the National and European Quality Label, and in 2017 it won the "Our eTwinning project 2017" competition.

Another example of a project promoting cybersafety is "Digital citizenship: Better eSafe than Sorry"[9]. It was carried out by IES San José in Spain, Michael College in the Netherlands, Hristo Smirnenski Primary School in Bulgaria, Herskind Skole & Børnehus in Denmark and Collège Paul Gauguin in France. The main goal of this project was to provide an answer to the question whether we know how to use the Internet

[9] bit.ly/2Ap6Db7 [access: 20.12.2018].

safely and responsibly. Other objectives included: the promotion of the use of new technologies in the field of digital security, improving participants' language skills, improving the effectiveness of group work, becoming familiar with and respecting cultural differences, and obtaining tips on how to behave in the case of cyberbullying and information manipulation. The crowning of the project was the creation of documents regulating the use of and access to new technologies at the schools.

Within the framework of the project, experts were invited to schools to share their knowledge with students and suggest certain courses of action. Particular attention was paid to the uncontrolled use of mobile devices by students. Project tasks focussed on responsible use of the Internet, promotion of appropriate standards of behaviour on social media, and rights and responsibilities of young users.

Methodology focussed on project-based learning and cooperation between students was applied during the project. Teachers divided their students into international task groups. Project participants carried out a survey among their peers on online safety and the use of modern devices. Each team dealt with a different topic. When all the information was collected, the participants had to present the results of their work to other groups. Thanks to using the resources posted on the webwewant.eu portal, students were able to work on the following topics: rights and responsibilities of Internet users, netiquette, social media, privacy and copyright. They also took part in Safer Internet Day 2016. With the support of Chaval Spain, they gained access to a series of fun exercises using the SmartPRIVAL application.

Project participants developed several online questionnaires, which were available in the project section of TwinSpace. The Spanish group took part in the Digital Natives Forum initiative of the Spanish ministry of education. Its main objective was to raise awareness of responsible use of IT tools. In the course of work, a group of students was selected to act as tutors who passed on their knowledge and skills on cybersafety to their peers.

Meanwhile, teachers produced a comprehensive Digital Action Plan, bringing together the most important issues relating to e-safety in schools. The first stage involved a needs analysis in the project's thematic area. Then concrete solutions were developed in reaction to the observed problems along with tips on how to behave in different situations. To develop the Digital Action Plan, materials available on the esafetylabel.eu portal were used. The suggestions developed are contained in two documents, which any school can add to its annual work plan: "Rules for acceptable use of the Internet by school staff" and "Rules for acceptable use of the Internet by students".

A very interesting part of the project was the comparison of several countries which showed the differences in approach to the Internet among young Europeans. Thanks to Google Forms, many informative observations were made. Teenagers in different countries use their smartphones for the same purposes and spend comparable amounts of time online. The most popular social networking sites are Facebook and Twitter, although Spaniards also use the WhatsApp messenger. All project participants were confronted directly or indirectly with the problem of cyberbullying, and learned how to react in difficult situations, how to solve problems and whom to turn to for help.

Within the framework of the project, police officers and experts in the field of modern technologies gave lectures on cybersafety to students and parents. A parents' association was involved in disseminating the results. Its efforts revealed that older generations' level of knowledge about new technologies and related risks varies greatly. While most parents were aware of the scale of young people's being bullied on the Internet, only few knew which institutions could help them in crisis situations. Efforts made within the project "Better eSafe than Sorry" were awarded with a silver e-Safety Label.

Another example of an eTwinning project that focussed on e-safety was "Take care of me – take care of you", which in 2018 took second place in the European competition for projects addressed to children aged 4–11. In the school year 2017/2018, 107 students from five countries (Poland, Portugal, France, Ukraine and Italy) took part in the project. The main topics covered by this initiative were: cyberbullying, the causes of aggressive online behaviour among young people, and the promotion of responsible attitudes during online activity. In addition to traditional ways of presenting oneself at the beginning of the project (forum, photos, videos), the participants also created quizzes for their peers with the use of LearningApps[10].

[10] bit.ly/2UeLjOr [access: 20.12.2018].

Another task was to prepare a logotype of the project working in international teams. Using the Padlet application, students worked on the definition of cyberbullying. They collaborated with comic book creators to prepare stories on the topic. They also recorded videos on cybersafety, which was very rewarding for them and motivated them to continue their work.

Safer Internet Day

Each February, eTwinners take part in Safer Internet Day. It promotes safe access to online resources for children and young people, while parents, teachers and educators become more familiar with methods allowing them to make positive use of online resources. The idea behind Safer Internet Day, similarly to other eTwinning initiatives, is to highlight the strength of cooperation focussing on digital safety at both international and local levels. As part of this event, thematic educational activities, talks, happenings, awareness-raising campaigns and competitions are organised. Some schools publish special newspapers. Polish initiatives can be entered into a nationwide competition for the most interesting celebrations of Safer Internet Day[11].

Many schools operating within the eTwinning network use the educational and promotional materials they receive to help them to prepare for the celebrations. The organisers also provide access to online educational tools: multimedia materials, e-learning courses, lesson scenarios, guides and brochures.

In 2018, the theme of Safer Internet Day was "Create, connect and share respect: a better Internet starts with you!". Many teachers involved in eTwinning took part in a MOOC devoted to online safety. The aim of the course was to equip participants with necessary knowledge and useful tools that would enable them to counteract online abuse, hate speech and radicalism, cyberbullying or blackmail with intimate photographs[12].

eSafety Label

Teachers running eTwinning projects can apply for an eSafety Label, which is awarded as part of a pan-European initiative aimed at ensuring

[11] bit.ly/35Vcxw7 [access: 22.12.2018].

[12] etwinning.pl/dzien-bezpiecznego-Internet-2018 [access: 22.12.2018].

safe access to online technology within teaching and learning processes. The eSafety Label website helps teachers, head teachers and network administrators assess the online security of their schools, develop and implement an action plan and, in the final phase, share good practice examples with other schools.

The eSafety Label project was launched on Safer Internet Day 2012. From the very beginning, many eTwinning project participants from different European countries have been actively involved in the work of the team which contributed to the development of an assessment form indispensable in evaluating the level of a school's online safety and to identify areas for improvement[13].

In order to be awarded an eSafety Label, it is necessary to become acquainted with the resources featured on the portal and register the institution, which is the starting point for an accreditation process. Then, in cooperation with other schools, a baseline analysis is conducted which makes it possible to draw up a plan for development and implementation of specific solutions.

The Label is awarded for 18 months and a new accreditation process begins one year after the award. This makes it possible to continuously improve the online safety of the school. There are four levels of the Label: iron (basic online safety level), bronze (minimal awareness of online safety), silver (more advanced approach to online safety) and gold (outstanding practice in all areas of online safety and education on online safety)[14].

Recently it became possible to join eSafety Champions as part of the eSafety Label project. The eSafety Champions initiative lasts 28 months and aims at the exchange of knowledge and good practices by teachers and schools wanting to develop students' habits of responsible use of modern technologies. eSafety Champions participants take part in a series of online training courses, webinars and a three-day course at the Future Classroom Lab in Brussels. They will also develop materials for a MOOC addressed to thousands of teachers across Europe[15].

[13] www.esafetylabel.eu/about [access: 22.12.2018].

[14] www.esafetylabel.eu/esafety-label [access: 22.12.2018].

[15] www.esafetylabel.eu/esafety-champions [access: 22.12.2018].

Promotion of eTwinning schools that focus on e-safety

The eTwinning programme recognises eTwinners – both teachers and institutions – promoting eSafety. Since 2018, institutions have been able to apply for the eTwinning School Label.

One of the criteria to be met in order to be awarded an eTwinning School Label is the presentation of the school's activities related to the promotion of knowledge regarding safe Internet use. The verification is based directly on issues contained in the assessment form related to the eSafety Label award procedure and requires that school representatives answer a series of questions that make it easy to assess whether the institution has adequate knowledge of eSafety and carries out targeted and systematic actions in this respect. The questions included in the application form relate to three areas:

- → infrastructure (personal data protection, ICT equipment management, school network security);
- → e-safety policy (copyright awareness, social media presence, online safety standards);
- → good practices (curricula including e-safety, information meetings for parents, consultations).

In accordance with the guidelines, a school applying for the Label presents specific activities confirming the informed, safe and responsible use of Internet resources by students and teachers not only within the framework of eTwinning projects, but also in everyday activities at school and outside of it.

The eTwinning School Label is a tool that helps to maintain high standards of eSafety in the eTwinning programme and enables schools, teachers and students participating in it to develop further, thanks to identifying elements for improvement and providing support in this area.

eTwinning publications

In eTwinning publications, much attention is paid to cybersafety. A good example is a brochure published in 2016 entitled *Growing digital citizens. Developing active citizenship through eTwinning*, which features the descriptions of three projects dedicated to online safety: "Better e-Safe than Sorry", "Medienkoffer" and "Net is the Key". The ideas presented there can serve as a source of inspiration for teachers who want to work on this topic[16].

The guide *Człowiek, komputer i Internet* [*Man, Computer and the Internet*] is a compendium of knowledge for beginners embarking on their adventure with computers and the virtual world. From this publication they can learn how to effectively search for resources on the Internet, how to publish content, what learning and self-development opportunities online courses offer, what to pay attention to when shopping on the web and how to behave in order to be safe online[17]. The guide is very popular among new eTwinning project participants, as the level of knowledge of modern technologies in the teaching community in Poland is not yet very high.

Another eTwinning publication entitled *Korzystanie z telefonu komórkowego w szkole. Zarządzanie szansami i zagrożeniami* [*Using a mobile phone at school. Managing opportunity and risk*] presents many aspects of the use of mobile phones by children and youth. It addresses the following issues: the role of smartphones in the life of young people, violence and pornography, and opportunities for learning and teaching with the use of mobile devices. The last chapter of the book, which presents practical exercises for different age groups showing how to creatively use mobile phones[18], is particularly noteworthy. After reading this guide, it is possible to form an objective opinion and decide whether using mobile phones during classes and in project work is worthwhile.

The Web We Want[19], which has been developed over the past few years by students, teachers and e-safety professionals under the auspices of the European SchoolNet, deserves special attention.

[16] bit.ly/2Ym5yvV [access: 22.12.2018].

[17] issuu.com/frse/docs/digital-world [access: 22.12.2018].

[18] issuu.com/frse/docs/telephone at school [access: 22.12.2018].

[19] www.webwewant.eu [access: 22.12.2018].

Teachers participating in eTwinning projects and their students contributed greatly to the development of this publication.

Within it, teenagers from several European countries created a handbook for their peers, and teachers and specialists – a methodology guide containing lesson plans and ideas for interesting activities that can be conducted with students both in class and during an educational project. The chapters of the handbook and the methodology guide are devoted to the following topics: rights and responsibilities on the Internet, the nature of online information, children and young people's activities in the virtual world, online identity, and the importance and protection of privacy. The lesson plans propose specific tasks and ideas to encourage young people to develop creative and critical thinking so they can find fulfilment in the world of the future and acquire skills needed for their careers. All these materials are in line with the European reference framework for key competences[20], which is an indicator of the ways in which knowledge and skills can be expanded in EU Member States.

The Web We Want portal, which is run in several languages, provides an opportunity to use these materials in international online projects (e.g. eTwinning), during lessons at schools and in projects involving students' visits to partner institutions (e.g. Erasmus+).

The "Bringing eSafety into eTwinning projects" group

More than a dozen specialist groups (eTwinning groups) promote the exchange of experiences and good practices between teachers participating in eTwinning projects. The aim of these groups is to expand the knowledge and skills of their members. One such group, "Bringing eSafety into eTwinning projects", comprises over 3300 members. Its main objectives are to:

- → provide support for teachers in the area of safe use of electronic media and online resources by students (especially in the scope of eTwinning projects);
- → develop teachers' skills regarding preparation of their own teaching materials for the promotion of e-safety;
- → enable European teachers to share knowledge, good practices and proven solutions.

[20] Council Recommendation of 22 May 2018 on key competences for lifelong learning; bit.ly/2Ks3Lho [access: 15.03.2019].

In addition to a forum where current issues and work topics are discussed, the group has developed detailed rules for eTwinning netiquette, a TwinSpace safety guide, copyright guidelines, and a bank of resources and materials to be used in projects and in everyday schoolwork. The group has organised five thematic webinars, during which invited specialists presented a network of educators who promote online awareness among young people, introduced the publication *The Web We Want* and discussed the issue of online identity. Group members held many live events, during which they presented examples of good practices and projects devoted to cybersafety.

"Week with e-safety" online course

For several years, Polish teachers have received support in the development of knowledge and skills related to the safe use of electronic media by means of participating in the online course entitled "Week with e-safety". It is offered on the Moodle platform, which provides an opportunity to participate in thematic forum discussions, express opinions by means of voting, create a dictionary on cybersafety, share ideas for specific e-safety tasks, lessons and projects, participate in live sessions (chats and videoconferences), as well as read texts and view audiovisual materials[21].

The course lasts seven days and is task-based. It is divided into several modules. The first is devoted to Internet-related threats. It covers such topics as cyberbullying and cybercrime, dangerous contacts and content, sexting and student safety online. Another module deals with excessive Internet use and dependence on electronic media. The remaining sections deal with data privacy and protection, intellectual property, social networking sites, computer security, types of malware, mobile device parental control and cookies. A separate part features exercises prepared on the LearningApps platform. These can be used as homework, as tasks to be completed individually on a computer at school or on a multimedia whiteboard with a group of students. The latter form of work in particular contributes to increasing students' motivation and interest.

[21] etwinning.pl/e-safety [access: 22.12.2018].

Teachers taking part in the course devote an hour or two a day to becoming familiar with the materials and completing the prescribed tasks. Participants have a round-the-clock access to the Moodle platform, training materials and tasks. If necessary, they can be assisted by a coach available on the help forum. It often happens that individual eTwinners specify among themselves the details of new eTwinning projects (both Polish and international ones) in which eSafety forms an important part.

Cybersafety in Erasmus+ projects

As is the case with eTwinning, many projects carried out as part of Erasmus+ Key Action 2: Strategic partnerships in the field of education are either fully or in part devoted to online safety. They offer students the opportunity not only to collaborate online, but also to meet and interact in the real world.

In the years 2014–2016, students from the Piotr Skarga upper secondary school in Grójec, along with partners from Greece, Norway, Sweden and Austria, worked on the project entitled "Safe Internet for all". It addressed risks associated with the Internet and promoted safe methods of working in virtual reality, in accordance with netiquette and ethical principles. The thematic scope of the project covered the following issues: Internet dependence, threats caused by excessive use of computers, protection against viruses and spam, netiquette and ethics on the Internet. Each topic was developed by one project partner, which resulted in the creation of several guides for young people using the Internet. The topics were handled in cooperation with experts, academic lecturers and non-governmental organisations. The students from Grójec invited an expert from the Alter Centre for Personal Development who introduced them to the issues of cyberbullying and cyberstalking. During five international exchanges, the students discussed subsequent thematic modules, and, after each trip, presented these issues to their peers during workshops. In addition to the guides, they also developed a brochure entitled *How to get addicted in 7 days*, an Android application, videos and presentations[22].

[22] bit.ly/2YCEjbl [access: 22.12.2018].

Another Erasmus+ project with a similar theme – "Camouflage and security in the virtual world" – was carried out in the years 2015–2017 by the School Complex in Pobiedziska together with partners from Bulgaria, Greece, Cyprus and Portugal. The main objective of the project was to raise e-safety awareness among students, teachers, parents, local and national-level education policy-makers, as well as local communities. Since e-safety is a key issue in schools in the digital era, project coordinators set themselves the task of equipping students with competences that would, in the future, facilitate their work and daily lives.

A guide was produced that can be used by any primary school in Europe. Project partners also exchanged examples of good practices. The University of Coimbra (Portuguese project partner), which has extensive experience in international research and projects on cyberviolence, provided training for teachers. During the two years of project work, three meetings were held: to kick-off cooperation (Portugal), to focus on mobility (Cyprus) and to sum up the project (Greece)[23].

By enabling schools to participate in Key Action 1: School staff mobility, Erasmus+ supports teachers in improving their professional skills. Thanks to participating in courses and training on cybersafety organised abroad, school staff learn about modern educational methods that contribute to promoting responsible use of Internet resources among the young generation. Through its database of available courses[24], Erasmus+ helps schools to find training on e-safety best suited to their needs and aids pan-European efforts to promote safe use of online resources, such as Safer Internet Day[25].

In May 2018, the Polish National Agency of Erasmus+ organised a conference in Zakopane entitled "School in the world of changes and new technologies". Participants of one of the workshops – "Cybersafety in schools: effective strategies for action" – become acquainted with different types of activities that contribute to the young generation's better functioning on the Internet, learned how

[23] camouflage-project.eu [access: 22.12.2018].

[24] www.schooleducationgateway.eu [access: 04.03.2019].

[25] bit.ly/2FORPBt [access: 22.12.2018].

to incorporate an e-safety strategy into school practice, and discovered effective ways to motivate children and young people to use electronic media responsibly.

To sum up, it is worth emphasising that for teachers and students participating in eTwinning and Erasmus+ projects on cybersecurity is a top priority. In addition to the tasks that are part of their work within the project, they undertake numerous initiatives both in and outside of school to promote responsible online behaviour of the young generation.

Conclusion

The Internet is a multifaceted environment which falls outside systematisation and definition. The dynamic development of technology and the continuous emergence of new services and solutions cause all attempts to describe the activity of young people online to be closely related to the analysis of changes in the communication processes. As a result, they will require constant updating and supplementing. This challenge relates to the diagnosis of both the opportunities arising from the Internet's development and the risks it can bring to the lives of children, youth and their careers.

Taking into account the specificity of the subject matter discussed, it was paramount for this publication to select the authors – top Polish and international experts dealing with the presence of digital media in the lives of young people – and topics in a way which would fully present the multidimensional character of new information and communication technologies, today serving as an indispensable tool for entertainment and education as well as an element of relationship-building.

Many research communities focus their attention on the impact digital technology has on different areas of young people's lives. This is why educators, media experts, sociologists, gaming experts and psychologists specialising in the prevention of risky behaviours are among this book's authors. The Internet, which forms an integral part of young people's daily life, must be considered holistically. Both formal and informal education has a very important preventive role to play in this area. It should contribute to equipping children with comprehensive competences allowing them to use the full potential of the web. In the diagnosis of the topic, we cannot ignore the role of parents and carers, i.e. those who are young people's first guides in the world of online solutions and processes. These aspects aim to prepare children to use the Internet effectively and in an informed way, as well as to deal with risky situations related to new technologies.

However, education should be addressed not only to young people, but also to society as a whole, especially concerning the law, which is based on a specific system of values. The law stands for the introduction of standards that ascribe value to human activity, also online. It thus affects society and serves as a signpost for acceptable and unacceptable behaviour. It is important to disseminate knowledge of the rules governing online activity as part of the prevention of online transgressions and offences.

It seems that the greatest challenge for the parents and carers of children and teenagers who are active online is to properly analyse their needs and skilfully manage the development of their media competences. All of this, while maintaining appropriate vigilance, will make it possible to arrive at a proper diagnosis of potential problems as well as a quick response to threats resulting from the specificity of digital media.

The key to ensuring the youngest users' online safety is the willingness of adults to familiarise themselves with the world into which children migrate. Knowledge about new trends, learning about the changing communication habits of today's teenagers, and tracking new services, solutions and activities of network experts will not only allow us to hold smarter conversations with young people about threats related to the Internet, but also enable us to become aware of the great opportunities offered by the web.

The intention of the authors of this publication was not to leave readers feeling threatened, but to persuade them to explore the Internet together with children. Discovering the potential of the web as a family and paying attention to risky behaviours that children can exhibit online can bring many benefits. It can also be valuable for teachers to use technology during class, to show students its practical applications and to facilitate learning through interaction. This way technology becomes a means to an end, and not an end in itself, stripped of its developmental and civilisation-building potential. The existence of this potential is made clear by numerous initiatives, such as those carried out within the eTwinning and Erasmus+ programmes.

We are convinced that a comprehensive approach to the presence of digital technology in the lives of children and young people will make it possible to better shape the media competences of this group – in terms of both creative use of the Internet and skilful avoidance of cyberthreats.

Agnieszka Wrońska,
Rafał Lew-Starowicz,
Anna Rywczyńska
(editors)

Bibliography

→ Aarseth, E., Bean, A. M. et al. (2017). Scholars' open debate paper on the World Health Organization ICD-11 Gaming Disorder proposal. *Journal of Behavioral Addictions*, *6*(3), 267–270.

→ Adachi, P. J. C., Willoughby, T. (2013). More than just fun and games: The longitudinal relationships between strategic video games, self-reported problem-solving skills, and academic grades. *Journal of Youth & Adolescence*, *42*(7), 1041–1052.

→ Adamski, A. (2000). *Prawo karne komputerowe*. Warszawa: Wydawnictwo C.H. Beck.

→ Adamski, A. (2001). *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*. Toruń: Wydawnictwo Towarzystwa Naukowego Organizacji i Kierownictwa "Dom Organizatora".

→ Aftab, P. (2003). *Internet a dzieci: uzależnienia i inne niebezpieczeństwa*. Warszawa: Wydawnictwo Prószyński i S-ka.

→ Aiken, M. (2016). *The Cyber Effect: An Expert in Cyberpsychology Explains How Technology Is Shaping Our Children, Our Behavior, and Our Values – and What We Can Do About It*. New York: Random House Publishing Group.

→ Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *The Journal of Social Issues*, *33*(3), 66–84.

→ Anderson, C. A., Shibuya, A., Ihori, N., Swing, E. L., Bushman, B. J., Sakamoto, A., Rothstein, H. R., Saleem, M. (2010). *Violent Video Game Effects on Aggression, Empathy, and Prosocial Behavior in Eastern and Western Countries: A Meta-Analytic Review. Psychological Bulletin*, *136*(2), 151–173.

→ Andrzejewska, A. (2009). Świat wirtualny – kreatorem rzeczywistości. In: J. Bednarek, A. Andrzejewska (ed.), *Cyberświat – możliwości i zagrożenia*. Warszawa: Wydawnictwo Akademickie "Żak".

- → Andrzejewska, A. (2012). Rola forów internetowych w życiu dzieci i młodzieży. In: S. Bębas, J. Plis, J. Bednarek (ed.), *Komunikacja w cyberświecie*. Radom: Wyższa Szkoła Handlowa w Radomiu.
- → Andrzejewska, A. (2018). Wyzwania i zagrożenia przestrzeni cyfrowej dla edukacji i aktywności zawodowej. In: S. M. Kwiatkowski (ed.), *Kompetencje przyszłości*. Warszawa: Wydawnictwo FRSE.
- → Andrzejewska, A., Bednarek, J. (2018). Zagrożenia w cyberprzestrzeni dla nastolatków w społeczeństwie wiedzy. In: W. Ratajek (ed.), *Edukacja i człowiek w czasach nowych technologii. Szanse, nadzieje i zagrożenia*. Wrocław: Wydawnictwo Humanistyczne Via Ferrata.
- → Andrzejewski, A. (2018a). "Lajki" i "Followersi" na portalach społecznościowych sposobem na poszukiwanie własnej tożsamości. *Problemy Opiekuńczo--Wychowawcze*, No 1.
- → Andrzejewski, A. (2018b). Fora internetowe źródłem informacji dla młodzieży o stosowaniu substancji psychoaktywnych – na przykładzie polskiego serwisu Hyperreal.info. In: J. Bednarek, A. Andrzejewska (ed.), *Cyberprzestrzeń – Człowiek – Edukacja. Rodzic, dziecko, nauczyciel w przestrzeni wirtualnej*. Kraków: Oficyna Wydawnicza Impuls.
- → Ansari, A. (2016). *Modern Romance. Miłość w czasach Internetu*. Gdańsk: Wydawnictwo Józef Częścik.
- → Antonovsky, A. (2005). *Rozwikłanie tajemnicy zdrowia. Jak radzić sobie ze stresem i nie zachorować*. Warszawa: Instytut Psychiatrii i Neurologii.
- → Aronson, E. (ed.) (2000). *Człowiek – istota społeczna*. Warszawa: Wydawnictwo Naukowe PWN.
- → Aronson, E., Wilson, T. D., Akert, R. M. (1997). *Psychologia społeczna. Serce i umysł*. Poznań: Zysk i S-ka.
- → Balicki, A., Pyter, M. (2017). *Prawo oświatowe. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.
- → Barani, K. (2009). Rola więzi online w życiu społecznym człowieka. In: B. Szmigielska (ed.), *Psychologiczne konteksty Internetu.* Kraków: WAM.
- → Barron, F. (1969). *Creative person and creative process*. Oxford: Holt, Rinehart & Winston.
- → Batorski, D. (2015). Technologie i media w domach i w życiu Polaków. Diagnoza Społeczna 2015, Warunki i Jakość Życia Polaków – Raport. *Contemporary Economics*, *9*(4), 373–395.
- → Baumgartner, S. E., Valkenburg, P. M., Peter, J. (2010). Assessing causality in the relationship between adolescents' risky sexual online behavior and

their perceptions of this behavior. *Journal of Youth & Adolescence*, *39*(10), 1226–1239.

- Bąk, A. (2015). *Korzystanie z urządzeń mobilnych przez małe dzieci w Polsce. Wyniki badania ilościowego*. Warszawa: Fundacja Dzieci Niczyje.
- Bean, A. M., Nielsen, R. K. L., van Rooij, A. J., Ferguson, C. J. (2017). *Video game addiction: The push to pathologize video games. Professional Psychology: Research and Practice*, *48*(5), 378–389.
- Beardsley, E. (1971). *Privacy: Autonomy and Selective Disclosure*. *Yearbook of the American Society for Political and Legal Philiosophy*, *XIII*: Privacy, 65.
- Bediou, B., Adams, D. M., Mayer, R. E., Tipton, E., Green, C. S., Bavelier, D. (2018). Meta-analysis of action video game impact on perceptual, attentional, and cognitive skills. *Psychological Bulletin*, *144*(1), 77–110.
- Bednarek, J. (2009). Teoretyczne i metodologiczne podstawy badań nad człowiekiem w cyberprzestrzeni. In: J. Bednarek, A. Andrzejewska (ed.), *Cyberświat – możliwości i zagrożenia*. Warszawa: Wydawnictwo Akademickie "Żak".
- Bednarek, J. (2014). Społeczne kompetencje medialno-informacyjne w kontekście bezpieczeństwa w cyberprzestrzeni i świata wirtualnego. In: J. Bednarek (ed.), *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*. Warszawa: Wydawnictwo Difin.
- Bednarek, J., Andrzejewska, A. (2018). Zagrożenia dla nastolatków w społeczeństwie wiedzy. In: W. Ratajek (ed.), *Edukacja i człowiek w czasach technologii. Szanse, nadzieje i zagrożenia*. Wrocław: Wydawnictwo humani styczne Via Ferrata.
- Ben-Ze'ev, A. (2005). *Miłość w sieci. Internet i emocje*. Poznań: Dom wydawniczy Rebis.
- Bendyk, E. (2004). *Antymatrix. Człowiek w labiryncie sieci*. Warszawa: Wydawnictwo W.A.B.
- Bennet, S., Maton, K., Kervin, L. (2008). The "digital natives" debate: A critical review of the evidence. *British Journal of Educational Technology*, *39*, 775–786.
- Bergh, J. van den, Behrer, M. (2012). *Jak kreować marki, które kocha pokolenie Y?* Warszawa: Wydawnictwo Samo Sedno.
- Bębas, S. (2018). Zagrożenia dla dzieci i młodzieży w świecie wirtualnym. In: W. Ratajek (ed.), *Edukacja i człowiek w czasach nowych technologii. Szanse, nadzieje i zagrożenia*. Wrocław: Wydawnictwo Humanistyczne Via Ferrata.
- Borucka, A. (2011). Koncepcja resilience. Podstawowe założenia i nurty badań, Resilience. Teoria – badania – praktyka. In: W. Junik (ed.), *Resilience*. Warszawa: Parpamedia.

- Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.
- Braciak, J. (2004). *Prawo do prywatności*. Warszawa: Wydawnictwo Sejmowe.
- Branicki, W. (2013). *Przyjaźń w relacjach zapośredniczonych przez technologię*. In: M. Sokołowski (ed.), *Nowe media i wyzwania współczesności*. Toruń: Wydawnictwo Adam Marszałek.
- Broekman, F. L., Piotrowski, J. T., Beentjes, H. W. J., Valkenburg, P. M. (2016). A parental perspective on apps for young children. *Computers in Human Behavior*, *63*, 142–151.
- Byrne, S. et al. (2012). Caring for mobile phone-based virtual pets can influence youth eating behaviors, *Journal of Children & Media*, *6*(1), 83–99.
- Caplan, S. E. (2010). Theory and measurement of generalized problematic Internet use: A two-step approach. *Computers in Human Behavior*, *26*(5), 1089–1097.
- Carr, N. (2010). *The Shallows*. New York: W&W Norton & Company Inc.
- Carrier, M. L., Spradlin, A., Bunce, J. P., Rosen, L. D. (2015). Virtual empathy: positive and negative impacts of going online upon empathy in young adults. *Computers in Human Behavior*, Vol. 52, 39–48.
- Cassidy, R. (2013). Partial convergence: social gaming and real-money gambling. In: *Qualitative research in gambling. Exploring the production and consumption of risk* (pp. 74–91). New York–London: Routledge.
- Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers.
- Connor, K. M., Davidson, J. R. (2003). Development of a New resilience scale: The Connor – Davidson resilience scale (CD-RISC). *Depression and Anxiety*, *18*(2).
- Czabała, J. (1988). *Rodzina a zaburzenia psychiczne. Koncepcje i studia nad percepcją interpersonalną*. Warszawa: Instytut Psychoneurologiczny.
- Czopek, J. (2016). Bezpieczeństwo i ochrona prywatności młodzieży w internecie w kontekście edukacji medialnej. *Zeszyty Naukowe Wyższej Szkoły Humanitas. Pedagogika*, 12, 67–73.
- Davidow, B. (2013, 10th of June). Skinner Marketing: We're the Rats, and Facebook Likes Are the Reward. *The Atlantic*.
- Delors, J. et al. (1996). *Learning: the treasure within*. Paris: UNESCO.
- Dolev-Cohen, M., Barak, A. (2013). Adolescents' use of Instant Messaging as a means of emotional relief. *Computers in Human Behavior*, *29*(1), 58–63.
- Dopierała, R. (2013). *Prywatność w perspektywie zmiany społecznej*. Kraków: Zakład Wydawniczy "Nomos".
- Dye, M. W. G., Green, C. S., Bavelier, D. (2009). *Increasing speed of processing with action video games. Current DirERctions in Psychological Science*, *18*(6), 321–326.

- Edosomwan, S., Sitalaskshmi Kalangot, P., Kouame, D., Watson, J., Seymour, T. (2011). *The History of Social Media and its Impact on Business*. *The Journal of Applied Management and Entrepreneurship*, *16*(3).
- Eichenbaum, A., Bavelier, D., Green, C. S. (2015). *Video games. Play that can do serious good*. *American Journal of Play*, *7*(1), 50–74.
- Fikkers, K. M., Piotrowski, J. T., Valkenburg, P. M. (2017). A matter of style? Exploring the effects of parental mediation styles on early adolescents' media violence exposure and aggression. *Computers in Human Behavior*, 70, 407–415.
- Fish, M. T., Russoniello, C. V., O'Brien, K. (2014). The efficacy of prescribed casual videogame play in reducing symptoms of anxiety: a randomized controlled study. *Games Health Journal*, *3*(5), 291–295.
- Freud, Z. (1976). *Poza zasadą przyjemności*. Warszawa: Państwowe Wydawnictwo Naukowe.
- Gainsbury, S. M., Hing, N., Delfabbro, P. H., King, D. L. (2014). A taxonomy of gambling and casino games via social media and online technologies. *International Gambling Studies*, *14*(2), 196–213.
- Gajda, J. (2006). Hipermedia szansą wzbogacenia tradycyjnych form multimedialnego kształcenia otwartego na odległość. *Pedagogika Mediów*, 1/2.
- Gajda, A. (2008). What if Samuel D. Warren hadn't Married a Senator's Daughter: Uncovering the Press Coverage That Led to the Right to Privacy. *Michigan State Law Review*, Vol. 07–06, 3–38.
- Galanciak, S. (2015). Zamiast zakończenia. Humanistyczne przesłanki pedagogiki medialnej. In: M. Tanaś, S. Galanciak (ed.), *Cyberprzestrzeń – Człowiek – Edukacja. Cyfrowa przestrzeń kształcenia*. Kraków: Oficyna Wydawnicza Impuls.

- Galanciak, S. (2015). Zamiast zakończenia. Humanistyczne przesłanki pedagogiki medialnej. In: M. Tanaś, S. Galanciak (ed.), *Cyberprzestrzeń – Człowiek – Edukacja. Cyfrowa przestrzeń kształcenia*. Kraków: Oficyna Wydawnicza Impuls.

- Galanciak, S. (2017). Realne wspólnoty medialne? Media w roli narzędzia integracji kulturowej i społecznej. In: S. Galanciak, M. Siwicki, J. Czarkowski (ed.), *Na krawędzi. Szkoła przed ekranem*. Warszawa: Wydawnictwo Akademii Pedagogiki Specjalnej.
- Galanciak, S., Siwicki, M. (2018). Cyberwypalenie. Syreni śpiew wśród cyfrowych pokus. *Problemy Opiekuńczo-Wychowawcze*, *2*(567).
- Galas, B. (2018). Społeczna przestrzeń edukacji cyfrowej w świetle dyskursów współczesnej socjologii. In: M. Tanaś, S. Galanciak (ed.), *Cyberprzestrzeń, człowiek, edukacja. Mistrz i uczeń w cyberprzestrzeni*. Kraków: Oficyna Wydawnicza Impuls.

- Gámez-Guadix M., Borrajo, E., Almendros, C. (2016). Risky online behaviors among adolescents: Longitudinal relations among problematic Internet use, cyberbullying perpetration, and meeting strangers online. *Journal of Behavioral Addictions*, *5*(1), 100–107.
- Garmezy, N. (1991a). Resilience in children's adaptation to negative life events and stressed environments. *Pediatric Annals*, 20.
- Garmezy, N. (1991b). Resilience and vulnerability to adverse developmental outcomes associated with poverty. *The American Behavioral Scientist*, 34.
- Gaś, Z. B. (1998). *Psychoprofilaktyka. Procedury Konstruowania Programów Wczesnej Interwencji*. Lublin: Wydawnictwo UMCS.
- Gaś, Z. B. (2006). *Profilaktyka w szkole*. Warszawa: Wydawnictwa Szkolne i Pedagogiczne.
- Gęsicki, J. (2010). Zmiany prawa oświatowego a reforma edukacyjna. In: J. Bielecki, A. Jacewicz (ed.), *Edukacja z perspektywy przemian kulturowo-społecznych wczoraj – dziś – jutro*. Białystok: Wydawnictwo Niepaństwowej Wyższej Szkoły Pedagogicznej.
- Giddens, A. (2004). *Socjologia*. Warszawa: Wydawnictwo Naukowe PWN.
- Giddens, A. (2006). *Socjologia*. Warszawa: Wydawnictwo Naukowe PWN.
- Giddens, A. (2008). *Konsekwencje nowoczesności*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
- Gnambs, T., Stasielowicz, L., Wolter, I., Appel, M. (2018). *Do computer games jeopardize educational outcomes? A prospective study on gaming times and academic achievement*. *Psychology of Popular Media Culture*, advance online publication.
- Goban-Klas, T. (2005). *W stronę społeczeństwa medialnego*. Warszawa: Wydawnictwa Szkolne i Pedagogiczne.
- Goban-Klas, T. (2006). *Media i komunikowanie masowe*. Warszawa: Wydawnictwo Naukowe PWN.
- Goffman, E. (2005). *Piętno. Rozważania o zranionej tożsamości*. Gdańsk: Gdańskie Wydawnictwo Psychologiczne.
- Goldstein, J. (2015). Applied entertainment: Positive uses of entertainment media. In: R. Nakatsu, M. Rauterberg, P. Ciancarini (ed.), *Handbook of digital games and entertainment technologies*. Singapur: Springer.
- Goldstein, J., Buckingham, D., Brougére, G. (2004). Introduction: Toys, games and media. In: J. Goldstein, D. Buckingham, G. Brougére (ed.), *Toys, games and media* (pp. 1–8). New Jersey: Taylor & Francis Group.
- Gorman, T. E., Gentile, D. A., Green, C. S. (2018). Problem gaming: A short primer. *American Journal of Play*, *10*(3), 309–328.

→ Granic, I., Lobel, A., Engels, R. C. M. E. (2014). The benefits of playing video games. *American Psychologist*, *69*(1), 66–78.

→ Graves, L. E. F. et al. (2010). The physiological cost and enjoyment of Wii Fit in adolescents, young adults, and older adults. *Journal of Physical Activity & Health*, *7*(3), 393–401.

→ Gursztyn, J. (2014). Online? Offline? Internet w życiu młodych ludzi. In: *Bezpieczeństwo dzieci online. Kompendium dla rodziców, nauczycieli i profesjonalistów*. Warszawa: Naukowa i Akademicka Sieć Komputerowa, Fundacja Dzieci Niczyje; bit.ly/2VdS9QJ [access: 2.04.2019].

→ Hamari, J., Järvinen, A. (2011). Building customer relationship through game mechanics in social games. In: *Business, Technological, and Social Dimensions of Computer Games: Multidisciplinary Developments* (pp. 348–365). IGI Global.

→ Hawkins, J. D., Catalano, R. F., Miller, J. Y. (1992). Risk and protective factors for alcohol and other drug problems in adolescence and early adulthood: Implications for substance abuse prevention. *Psychological Bulletin*, *112*(1).

→ Heffler, K. F., Oestreicher, L. M. (2016). Causation model of autism: Audiovisual brain specialization in infancy competes with social brain networks. *Medical Hypotheses*, 91, 114–122.

→ Helsper, E., Eynon, R. (2010). Digital natives: where is the evidence? *British Educational Research Journal*, 36, 502–520.

→ Herring, S. (2008). Questioning the generational divide: Technological exoticism and adult constructions of online youth identity. In: D. Buckingham (ed.), *Youth, identity, and digital media*. Cambridge: MIT Press.

→ Hopson, L., Lee, E. (2011). Mitigating the effect of family poverty on academic and behavioral outcomes: The role of school climate in middle and high school. *Children and Youth Services Review*, *33*(11).

→ Jackson, L. A. et al. (2012). *Information technology use and creativity: Findings from the children and technology project. Computers in Human Behavior*, *28*(2), 370–376.

→ Jansz, J. (2005). The emotional appeal of violent video games for adolescent males. *Communication Theory*, 15, 219–241.

→ Jew, C. L., Green, K. E., Kroger, J. (1999). *Development and validation of a measure of resilience. Measurement and Evaluation In Counseling and Development*, *32*(2).

→ Jones, C. (2012). Networked learning, stepping beyond the net generation and digital natives. In: L. Dirckinck Holmfeld, V. Hodgson, D. McConnell (ed.), *Exploring the Theory, Pedagogy and Practice of Networked Learning* (pp. 27–41). New York: Springer.

→ Kabali, H. (2015). *First exposure and use of mobile media in Young children*. AAP National Conference and Exhibition, American Academy of Pediatrics.

→ Kabali, H. K. et al. (2015). Exposure and Use of Mobile Media Devices by Young Children. *Pediatrics*, *136*(6); bit.ly/2OxRDe6 [access: 20.03.2019].

→ Kacprzak, K., Leppert, R. (2013). *Związki miłosne w sieci*. Kraków: Oficyna Wydawnicza Impuls.

→ Kamieniecki, W., Bochenek, M., Lange, R. (2017). *Raport z badania "Nastolatki 3.0"*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.

→ Kardefelt-Winther, D. (2017). *How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? An evidence-focused literature review*. UNICEF.

→ Kato, P. M. (2010). Videogames in health care: closing the gap. *Review of General Psychology*, *14*(2), 113–121.

→ Kelvin, P. (1973). A social-psychological examination of privacy. *British Journal of Social and Clinical Psychology*, 12, 248–261.

→ Kerckhove, D. de (1997). *Powłoka kultury. Odkrywanie nowej elektronicznej rzeczywistości*. Warszawa: Mikom.

→ Khoury-Kassabri, M., Benbenishty, R., Astor, R. A., Zeira, A. (2005). The contributions of community, family, and school variables to student victimization. *American Journal of Community Psychology*, *34*(3/4).

→ Kirwil L. (2011). *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo – część 2. Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9–16 lat i ich rodziców*. Warszawa: Szkoła Wyższa Psychologii Społecznej.

→ Klimek, M. (2015). Bezpieczeństwo teleinformatyczne i bezpieczeństwo informacji w przedsiębiorstwach budownictwa inżynieryjnego. *Zeszyty Naukowe Uniwersytetu Przyrodniczo Humanistycznego w Siedlcach*, 105, 95–102.

→ Ko, C.-H., Yen, J. Y., Liu, S. C., Huang, C. F., Yen, C. F. (2009). The associations between aggressive behaviors and Internet addiction and online activities in adolescents. *Journal of Adolescent Health, 44*(6), 598–605.

→ Konopczyński, M. (2007). *Metody twórczej resocjalizacji*. Warszawa: Wydawnictwo Naukowe PWN.

→ Konrath, S., O'Brien, E., Hsing, C. (2010). Changes in dispositional empathy in American college students over time: A meta-analysis Personality and Social. *Psychology Review*, *15*(2).

→ Kopff, A. (1972). Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne). *Studia Cywilistyczne*, XX.

- *Korzystanie z urządzeń mobilnych przez małe dzieci w Polsce. Wyniki badania ilościowego* (2015). Warszawa: Fundacja Dzieci Niczyje.
- Kotarbiński, T. (1975). *Hasło dobrej roboty*. Warszawa: Wydawnictwo Wiedza Powszechna.
- Koutromanos, G., Sofos, A., Avraamidou, L. (2015). The use of augmented reality games in education: a review of the literature. *Educational Media International*, *52*(4), 253–271.
- Kowert, R., Domahidi, E., Quandt, T. (2014). The relationship between online video game involvement and gaming-related friendships among emotionally sensitive individuals. *Cyberpsychology, Behavior & Social Networking*, *17*(7), 447–453.
- Krauze-Sikorska, H., Klichowski, M. (2013). *Świat Digital Natives. Młodzież w poszukiwaniu siebie i innych*. Poznań: Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza.
- Krznaric, R. (2014). *Empathy: Why It Matters, and How to Get It*. London: Random House.
- Krzystanek, K. (2007). *Postawy rodzicielskie a reakcje chłopców na agresywną grę komputerową*. In: I. Pufal-Struzik (ed.), *Agresja dzieci i młodzieży: uwarunkowania indywidualne, rodzinne i szkolne*. Kielce: Wydawnictwo Pedagogiczne ZNP.
- Kubacka-Jasiecka, D., Passowicz, P. (2014). Dorastanie we współczesności. Postawy, wartości i doświadczanie czasu a kryzysy rozwoju pokolenia po transformacji. *Psychological Journal*, *20*(2).
- Kühn, S., Gallinat, J. (2014). Amount of lifetime video gaming is positively associated with entorhinal, hippocampal and occipital volume. *Molecular Psychiatry*, 19, 842–847.
- Kühn, S. et al. (2014). Playing Super Mario induces structural brain plasticity: Gray matter changes resulting from training with a commercial video game. *Molecular Psychiatry*, 19, 265–271.
- Kühn, S., Kugler, D. T., Schmalen, K., Weichenberger, M., Witt, C., Gallinat, J. (2018). Does playing violent video games cause aggression? A longitudinal intervention study. *Molecular Psychiatry*; bit.ly/2C6nQUS [access: 6.03.2019].
- Kulesza, J. (2012). *Ius internet. Między prawem a etyką*. Warszawa: Oficyna Wydawnicza Łośgraf.
- Kurzweil, R., Grossman, T. (2004). *Fantastic Voyage: Live Long Enough to Live Forever*. New York: Plume.

- Kutner, L., Olson, Ch. K. (2008). *Grand Theft Childhood: The surprising truth about violent video games and what parents can do*. New York: Simon & Schuster.
- Kwiatkowska, D., Dąbrowski, M. (2012). Dojrzałość technologiczna uczniów w świetle wyników badań ankietowych. *E-mentor*, *1*(43); bit.ly/2SFdod9 [access: 23.07.2018].
- Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.
- Leary, M. (2003). *Wywieranie wrażenia na innych. O sztuce autoprezentacji*. Gdańsk: Gdańskie Wydawnictwo Psychologiczne.
- Leary, M. R., Kowalski, R. M. (1990). Impression Management: A Literature Review and Two-Component Model. *Psychological Bulletin*, 107, 34–47.
- Lew-Starowicz, R., Lorecka, K. (2013). *Włączenie cyfrowe – droga do reintegracji społecznej*. Warszawa: Wydawnictwa Uniwersytetu Warszawskiego.
- Lewis, C., Wardrip-Fruin, N., Whitehead, J. (2012). Motivational game design patterns of 'ville games. In: *Proceedings of the International Conference on the Foundations of Digital Games* (pp. 172–179). New York: Association for Computing Machinery.
- Li, J., Theng, Y. -L., Foo, S. (2014). Game-based digital interventions for depression therapy: A systematic review and meta-analysis. *Cyberpsychology, Behavior & Social Networking*, *17*(8), 519–527.
- Lieberman, D. A. (2009). Designing serious games for learning and health in informal and formal settings. In: U. Ritterfield, M. Cody, P. Vorderer (ed.), *Serious games: Mechanisms and effects* (pp. 117–130). New York: Routledge.
- Livingstone, S., Smith, P. K. (2014). Annual Research Review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55, 635–654.
- Luthar, S., Cicchetti, D., Becker, B. (2000). The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work. *Child Development*, *71*(3).
- Lyons, E. J. et al. (2014). Engagement, enjoyment, and energy expenditure during active video game play. *Health Psychology*, 33, 1174–1181.
- Makaruk, K., Włodarczyk, J., Michalski, P. (2017). *Kontakt dzieci i młodzieży z pornografią – Raport Badań*. Warszawa: Fundacja Dajemy Dzieciom Siłę.
- Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *The Journal of Social Issues*, *33*(3), 5–21.
- Markey, P. M., Markey, Ch. N., French, J. E. (2014). Violent video games and real-world violence: Rhetoric versus data. *Psychology of Popular Media Culture*.

→ Martončik, M., Lokša, J. (2016). Do World of Warcraft (MMORPG) players experience less loneliness and social anxiety in online world (virtual environment) than in real world (offline)?. *Computers in Human Behavior*, 56, 127–134.

→ Mason, S. G., Bohringer, R. et al. (2004). Real-time control of a video game with a direct brain-computer interface. *Journal of Clinical Neurophysiology*, 21, 404–408.

→ Mayer, R. E. (2014). *Computer games for learning: An evidence-based approach*. Cambridge.

→ Mayor, F., Bindé, J. (2001). *Przyszłość świata*. Warszawa: Fundacja Studiów i Badań Edukacyjnych.

→ McDool, E., Powell, P., Roberts, J., Taylor, K. (2016). *Social Media Use and Children's Wellbeing*. Bonn: Institute of Labor Economics Working Papers.

→ McDowell, J. (2000). *Wyobcowane pokolenie*. Warszawa: Oficyna Wydawnicza Vocatio.

→ Mead, G. H. (1975). *Umysł, osobowość, społeczeństwo*. Warszawa: Państwowe Wydawnictwo Naukowe.

→ Mead, M. (1978). *Kultura i tożsamość. Studium dystansu międzypokoleniowego*. Warszawa: Państwowe Wydawnictwo Naukowe.

→ Meerkerk, G. J., van den Eijnden, R. J. J. M., Franken, I. H. A., Garretsen, H. F. L. (2010). Is compulsive Internet use related to sensitivity to reward and punishment, and impulsivity?. *Computers in Human Behavior*, *26*(4), 729–735.

→ Moos, R. H. (1979). *Evaluating educational environments: Procedures, measures, findings, and policy implications*. San Francisco: Jossey-Bass.

→ Morbitzer, J. (2013). *Przedmowa.* In: J. Morbitzer, E. Musiał (ed.), *Człowiek. Media. Edukacja*, Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej.

→ Morbitzer, J. (2014). O wychowaniu w świecie nowych mediów – zarys problematyki. *Labor et Educatio*, 2.

→ Mrazek, P. J., Mrazek, D. (1987). Resilience in child maltreatment victims: A conceptual exploration. *Child Abuse and Neglect*, 11.

→ Nielsen, R. K. L., Grabarczyk, P. (2018). Are Loot Boxes Gambling? Random reward mechanisms in video games. In: *DiGRA '18 – Proceedings of the 2018 DiGRA International Conference: The Game is the Message*. DIGRA.

→ Nikken, P., Jansz, J. (2006). Parental mediation of children's videogame playing: A comparison of the reports by parents and children. *Learning, Media and Technology*, *31*(2), 181–202.

→ Nikken, P., Schols, M. (2015). How and why parents guide the media use of young children. *Journal of Child & Family Studies*, 24, 3423–3435.

- Olson, D. H. (1991). Commentary: Three-dimensional (3D) Circumplex Model and revised scoring of FACES II. *Family Process*, *30*(1), 74–79.
- Olson, D. H., Russell, C. S., Sprenkle, D. H. (1983). Circumplex Model of marital and family systems VI: Theoretical update. *Family Process*, 22.
- Palfrey, J., Gasser, U. (2008). *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic.
- Parente, A., Parente, R. (2006). Mind-operated devices: Mental control of a computer using biofeedback. *CyberPsychology and Behavior*, *9*(1), 1–4.
- Peng, W., Lin, J. -H., Crouse, J. (2011). Is playing exergames really exercising? A meta-analysis of energy expenditure in active videogames. *Cyberpsychology, Behavior and Social Networking*, *14*(11).
- Piaget, J. (2012). *Jak sobie dziecko wyobraża świat*. Warszawa: Wydawnictwo Naukowe PWN.
- Pilich, M. (2009). *Ustawa o systemie oświaty, komentarz*. Warszawa: Wolters Kluwer Polska.
- Pogue, D. (2008, 28th of February). How Dangerous Is the Internet for Children? *New York Times*.
- Pope, A. T., Bogart, E. H. (1996). Extended attention span training system: Video game neurotherapy for attention deficit disorder. *Child Study Journal*, *26*(1), 39–50.
- Postman, N. (2005). *Technopol. Triumf techniki nad kulturą*. Warszawa: Państwowy Instytut Wydawniczy.
- Prensky, M. (2001). *Digital Natives, Digital Immigrants*. Bingley.
- Prensky, M. (2001a). Digital natives, digital immigrants. Part 1. *On The Horizon*, *9*(5).
- Prensky, M. (2001b). Digital Natives, Digital Immigrants. Part 2. Do they really think differently?. *On the Horizon*, *9*(6).
- Pryciak, M. (2010). Prawo do prywatności. *Wrocławskie Studia Erazmiańskie, IV: Prawa człowieka – idea, instytucje, krytyka*.
- Przybylski, A. K., Weinstein, N. (2017). A large-scale test of the Goldilocks Hypothesis: Quantifying the relations between digital-screen use and the mental well-being of adolescents. *Psychological Science*, *28*(2), 204–215.
- Pyżalski, J. (2012a). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*. Kraków: Oficyna Wydawnicza Impuls.
- Pyżalski, J. (2012b). The Digital generation gap revisited: constructive and dysfunctional patterns of social media usage. In: A. Costabile, B. Spears (ed.), *The impact of technology on relationships in educational settings*. New York: Routledge.

- Pyżalski, J. (2016). Od paradygmatu ryzyka do paradygmatu szans – prospołeczne i prorozwojowe używanie internetu przez dzieci i młodzież. In: M. Tanaś (ed.), *Nastolatki wobec internetu*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.
- Pyżalski, J. (2017). Młodzi internauci a edukacja medialna – dlaczego musimy odejść od miejsca, w którym jesteśmy. In: W. Skrzydlewski (ed.), *Kultura – Edukacja – Technologia kształcenia* (pp. 225–238). Poznań: Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza.
- Pyżalski, J., Zdrodowska, A., Tomczyk, Ł., Abramczuk, A. (2019). *Polskie badania EU Kids Online 2018. Najważniejsze wyniki i wnioski*. Poznań: Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza.
- Radochoński, M. (1986). *Psychoterapia rodzinna w ujęciu systemowym*. Rzeszów: Wydawnictwo Wyższej Szkoły Pedagogicznej.
- Reykowski, J. (1979). *Motywacja, osobowość a postawy społeczne*. Warszawa: Państwowe Wydawnictwo Naukowe.
- Richardson, J. et al. (2017). *Internet Literacy Handbook*. Council of Europe; bit.ly/2nRDjU3 [access: 20.03.2019].
- Richardson, J. et al. (2019). *Digital Citizenship Education Handbook*. Council of Europe; bit.ly/2WTy4kW [access: 20.03.2019].
- Roessler, B. (2010). New ways of thinking about privacy. *The Oxford Handbook of Political Theory*.
- Romer, D. (2010). Adolescent risk taking, impulsivity, and brain development: Implications for prevention. *Developmental Psychobiology*, *52*(3), 263–276.
- Ronatowicz, W. (2014). Ryzykowne zachowania seksualne dzieci, młodzieży i młodych dorosłych w kontekście korzystania z technologii cyfrowych. *Rocznik Lubelski*, 40, part 1.
- Russoniello, C. V., Fish, M., O'Brien, K. (2013). The efficacy of casual videogame play in reducing clinical depression: A randomized controlled study. *Games for Health Journal*, 2, 341–346.
- Rutter, M. (2006). Implications of resilience concepts for scientific understanding. *Annals New York Academy of Sciences*, 1094.
- Ryś, M. (2007). *Rodzinne uwarunkowania psychospołecznego funkcjonowania Dorosłych Dzieci Alkoholików*. Warszawa: Wydawnictwo Naukowe PWN.
- Rywczyńska, A., Jaroszewski, P. (2018). *Internet zabawek – wsparcie dla rozwoju dziecka czy zagrożenie*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.
- Sartori, G. (2007). *Homo videns. Telewizja i postmyślenie*. Warszawa: Wydawnictwo Uniwersytetu Warszawskiego.
- Schwab, K. (2016). *The Fourth Industrial Revolution*. Geneva: Currency.

- Selwyn, N. (2003). "Doing IT for the kids": Re-examining children, computers and the "Information Society". *Media, Culture and Society*, *25*(3), 351–378.
- Selwyn, N. (2009). The digital native – myth and reality. *Aslib Proceedings: New Information Perspectives*, *61*(4), 364–379.
- Sęk, H., Cieślak, R. (2004). *Wsparcie społeczne, stres i zdrowie*. Warszawa: Wydawnictwo Naukowe PWN.
- Sherman, L. E., Payton, A. A., Hernandez, L. M., Greenfield, P. M., Dapretto, M. (2016). The power of the "like" in adolescence: Effects of peer influence on neural and behavioral responses to social media. Psychological Science, *27*(7).
- Siemieniecki, B. (2002). Kognitywistyka a media i kultura. *Kognitywistyka i Media w Edukacji*, 2.
- Sienkiewicz, P. (2015). Ontologia cyberprzestrzeni. *Zeszyty Naukowe WWSI*, *13*(9), 89–102.
- Siuda, P. (2015). Prywatność w Internecie – zarys perspektywy krytycznej. *Kultura – Media – Teologia*, 20, 36–56.
- Słysz, A., Arcimowicz, B. (2009). *Przyjaciele w internecie*. Gdańsk: Gdańskie Wydawnictwo Psychologiczne.
- Smahel, D., Brown, B. B., Blinka, L. (2012). Associations between online friendship and Internet addiction among adolescents and emerging adults. *Developmental Psychobiology*, *48*(2), 381–388.
- Solove, D. J. (2002). *Conceptualizing privacy. California Law Review*, *90*(4).
- Spitzer, M. (2013). *Cyfrowa demencja: w jaki sposób pozbawiamy rozumu siebie i swoje dzieci*. Słupsk: Wydawnictwo Dobra Literatura.
- Stachura, K. (2006). Nowe formy uspołeczniania online na przykładzie sieciowej towarzyskości. In: M. Sokołowski (ed.), *Oblicza Internetu: Internet jako przestrzeń komunikacji i dialogu*, Elbląg: Wydawnictwo Państwowej Wyższej Szkoły Zawodowej.
- Steinberg, L. (2007). Risk taking in adolescence new perspectives from brain and behavioral science. *Current Directions in Psychological Science*, *16*(2), 55–59.
- Stokes, B., Dols, S., Hill, A. (2018). *Cities remix a playful platform: Prominent experiments to embed Pokémon GO, from Open Streets to neighborhood libraries and local data*. Washington; playfulcity.net/pogo [access: 6.03.2019].
- Suchodolski, B. (1937). *Uspołecznienie kultury*. Warszawa: Wydawnictwo "Rój".
- Szewczuk, W. (ed.). (1998). *Przyjaźń. Encyklopedia Psychologii*. Warszawa: Fundacja Innowacja.
- Szmajke, A. (1999). *Autoprezentacja – maski, pozy, miny*. Olsztyn: Ursa Consulting.

- Szpunar, M. (2007). Alienacja i samotność w Sieci vs grupowość i kapitał społeczny w Internecie. Internet i jego wpływ na kontakty społeczne. In: M. Sokołowski (ed.), *Oblicza Internetu. Architektura komunikacyjna Sieci*. Elbląg: Wydawnictwo Państwowej Wyższej Szkoły Zawodowej.
- Śliwerski, B. (2012). *Pedagogika ogólna. Podstawowe prawidłowości*. Kraków: Oficyna Wydawnicza Impuls.
- Śliwerski, B. (2016). Czy sieć zastąpi szkołę i rodziców w edukacji i wychowaniu? – nowe wyzwania dla rodziców i systemu edukacji. In: M. Tanaś (ed.), *Nastolatki wobec Internetu*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.
- Tanaś, M. (1993). Medyczne skutki uboczne kształcenia wspomaganego komputerowego. *Toruńskie Studia Dydaktyczne*, *3*(II).
- Tanaś, M. (2005). *Technologia informacyjna w procesie dydaktycznym*. Warszawa: Mikom.
- Tanaś, M. (2007a). O potrzebie pedagogicznej refleksji nad kulturą i językiem mediów. In: M. Tanaś (ed.), *Kultura i język mediów*. Kraków: Oficyna Wydawnicza Impuls.
- Tanaś, M. (2007b). *Wychowanie a media.* In: B. Siemieniecki (ed.), *Pedagogika medialna*. Warszawa: Wydawnictwo Naukowe PWN.
- Tanaś, M. (2015). Prolegomena do pedagogiki medialnej. In: M. Tanaś, S. Galanciak (ed.), *Cyberprzestrzeń – Człowiek – Edukacja. Cyfrowa przestrzeń kształcenia*. Kraków: Oficyna Wydawnicza Impuls.
- Tanaś, M. (2016a). *Diagnoza funkcjonowania nastolatków w sieci – aspekty społeczne, edukacyjne i etyczne.* In: M. Tanaś (ed.), *Nastolatki wobec Internetu*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.
- Tanaś, M. (2016b). *Primum non nocere a internetowa przestrzeń wolności i aktywności nastolatków.* In: M. Tanaś (ed.), *Nastolatki wobec internetu*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.
- Tanaś, M. (2018). Analiza rozwiązań organizacyjnych i prawnych w wybranych krajach w zakresie zapobiegania i przeciwdziałania cyberprzemocy wśród dzieci i młodzieży. In: *Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży. Informacja o wynikach kontroli*. Kielce: Delegatura Najwyższej Izby Kontroli w Kielcach.
- Tanaś, M., Kamieniecki, W., Bochenek, M., Wrońska, A., Lange, R., Fila, M., Loba, B. (2016). *Nastolatki 3.0, Wyniki ogólnopolskiego badania nastolatków w szkołach*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.
- Tapscott, D. (1998). *Growing up digital. The rise of the Net Generation*. New York: McGrawHill.

- Tapscott, D. (2009). *Grown up digital. How the net generation is changing your world*. New York: McGraw-Hill.
- Tapscott, D. (2010). *Cyfrowa dorosłość. Jak pokolenie sieci zmienia nasz świat*. Warszawa: Wydawnictwa Akademickie i Profesjonalne.
- Tłuściak-Deliowska, A. (2017). *Dręczenie szkolne. Społeczno-pedagogiczna analiza zjawiska*. Warszawa: Wydawnictwo Akademii Pedagogiki Specjalnej.
- Trejderowski, T. (2013). *Terroryzm informatyczny*. Warszawa: ENETEIA Wydawnictwo Psychologii i Kultury.
- Trepte, S., Reinecke, L., Juechems, K. (2012). The social side of gaming: How playing online computer games creates online and offline social support. *Computers in Human Behavior*, 28, 832–839.
- UKE (2018). *Badanie opinii publicznej w zakresie funkcjonowania rynku usług telekomunikacyjnych oraz preferencji konsumentów. Raport z badania dzieci i rodziców*. Warszawa-Gdańsk: Urząd Komunikacji Elektronicznej.
- UNESCO (2015). *Global Citizenship Education: Topics and Learning Objectives*. Paris: UNESCO.
- Valcke, M., De Wever, B., Van Keer, H., Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers & Education*, *57*(1), 1292–1305.
- Valkenburg, P. M., Peter, J. (2011). *Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. Journal of Adolescent Health*, *48*(2), 121–127.
- van Dijk, J. A. G. M. (2012). The evolution of the digital divide: The digital divide turns to inequality of skills and usage. In: J. Bus, M. Crompton, M. Hildebrandt,
- G. Metakides (ed.), *Digital enlightenment yearbook 2012* (pp. 57–75). Fairfax, VA: IOS Press, Inc.
- Villani, D., Carissoli, C. et al. (2018). Videogames for emotion regulation: A systematic review. *Games for Health Journal*, *7*(2).
- Vitelli, R. (2018, 21st September). Video games, school success, and your child. Do video games affect school performance or are academic underachievers simply more likely to play video games?. *Psychology Today*.
- Voisin, D. R., Salazar, L. F., Crosby, R., Diclemente, R. J., Yarber, W. L., Staples-Horne, M. (2005). *Teacher connectedness and health-related outcomes among detained adolescents. Yournal of Adolescent Health*, *37*(4).
- Vygotsky, L. S. (1986). *Thought and language*, Cambridge. (MA): Harvard University Press.
- Wasylewicz, M. (2012). Komunikowanie się pokolenia sieci – szansą czy zagrożeniem relacji interpersonalnych. In: T. Lewowicki, B. Siemieniecki (ed.), *Cyberprzestrzeń i edukacja*. Toruń: Wydawnictwo Adam Marszałek.

→ Werner, E. E., Smith, R. S. (2001). *Journeys from Childhood to Midlife: Risk,* Resilience*, and Recovery*. Ithaca: Cornell University Press.

→ Whitty, M., Carr, A. (2009). *Wszystko o romansie w sieci*. Gdańsk: Gdańskie Wydawnictwo Psychologiczne.

→ Wigley, K., Clarke, B. (2000). Kids.net (NOP), London: National Opinion Poll. In: S. Livingstone, *Children's Use of Internet*; bit.ly/2YAPlIP [access: 20.03.2019].

→ Wojciszke, B. (2004). *Człowiek wśród ludzi. Zarys psychologii społecznej*. Warszawa: Wydawnictwo Naukowe "Scholar".

→ Wood, M. A., Bukowski, W. M., Lis, E. (2016). *The digital self: How social media serves as a setting that shapes youth's emotional experiences*. *Adolescent Research Review*, *1*(2), 163–173.

→ Woodman, D. (2015). *Youth and Generation*. London: Sage Publications Ltd.

→ Woźniak, J. (2018). *Seksting – niebezpieczna zabawa nastolatków.* In: A. Andrzejewska, J. Bednarek (ed.), *Rodzic, dziecko, nauczyciel w przestrzeni wirtualnej*. Kraków: Oficyna Wydawnicza Impuls.

→ Wrońska, M. (2015). *Od kultury nadmiaru poprzez kulturę wyrzucania do kultury medialnej.* In: M. Tanaś, S. Galanciak (ed.), *Cyberprzestrzeń – Człowiek – Edukacja. Cyfrowa przestrzeń kształcenia*, Kraków: Oficyna Wydawnicza Impuls.

→ Wrońska A., Lange R. (2016). *Nastolatek jako użytkownik Internetu – społeczny wzorzec konsumpcji.* In: M. Tanaś (ed.), *Nastolatki wobec internetu*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.

→ Wrońska, A., Lange, R., Bochenek, M., Niedzielska-Barczyk, D. (2018). *Dziecko w krainie smartfonów*. Warszawa: Naukowa i Akademicka Sieć Komputerowa.

→ Young, K. S., de Abreu, C. N. (2011). *Internet addiction: A handbook and guide to evaluation and treatment, Hoboken*. New Jersey: John Wiley & Sons Inc.

→ Zajada, A. (2014). Pokolenie X, Y, Z a fenomen turystyki. In: J. Śledzińska, B. Włodarczyk (ed.), *Międzypokoleniowe aspekty turystyki*. Warszawa: Wydawnictwo PTTK "Kraj".

→ Zeler, B., Żydek-Bednarczuk, U. (2009). *Homo communicans w świecie wirtualnym.* In: A. Kiepas, A. Sułkowska, M. Wołek (ed.), *Człowiek a światy wirtualne*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

→ Ziemska, M. (1975). *Rodzina a osobowość*. Warszawa: Wydawnictwo Wiedza Powszechna.

Netography

→ *A detailed description of the triennial Programme for International Student Assessment (PISA)*, www.oecd.org/pisa/aboutpisa [access: 27.03.2019].

→ Alux.com, 15 *Jobs that will disappear in the next 20 years due to AI*, bit.ly/2ErVSTm [access: 1.12.2018].

→ Armstrong, K. (2018). *Playing games with basic research*, bit.ly/2TsvXVy [access: 6.03.2019].

→ Backer, E. (2017). *A history of the selfie: a photo phenomenon*, bit.ly/2yueLBA [access: 20.03.2019].

→ Bartoszewska, A. (online). *Miłość w sieci – zabawa czy poważna sprawa?* bit.ly/2FvDwDo [access: 12.10.2018].

→ *Best Smart Home Devices And How IoT Is Changing The Way We Live* (2017). bit.ly/2G8C5d0 [access: 10.11.2017].

→ Bochenek, M., (2018). Rok pilotażu OSE. In: *Akademia NASK, O OSE*, akademia.nask.pl/projekt-48/o-projekcie.html [access: 17.07.2018].

→ Children's Online Privacy Protection Act (COPPA), bit.ly/1IJZNI0 [access: 20.11.2018].

→ Gursztyn, J. (2014). Online? Offline? Internet w życiu młodych ludzi. In: *Bezpieczeństwo dzieci online. Kompendium dla rodziców, nauczycieli i profesjonalistów*. Warszawa: Naukowa i Akademicka Sieć Komputerowa, Fundacja Dzieci Niczyje, bit.ly/2VdS9QJ [access: 2.04.2019].

→ IAB (2017), bit.ly/2SYoTMM [access: 23.10. 2017].

→ *International Civic and Citizenship Study* (ICCS), iccs.iea.nl/home.html [access: 20.03.2019].

→ Jarvis, J. (2018). Facebook hack: 50 million accounts exposed in latest data breach. *Evening Standard*, bit.ly/2xSLsKe [access: 8.11.2018].

→ Jędruszczak K. (2005). Modele i koncepcje prywatności w psychologii. *Przegląd Psychologiczny*, *48*(2), 199–200, bit.ly/2D7TWQt [access: 23.10.2017].

- Kamieniecki, W. et al. (2017). *Raport z badania Nastolatki 3.0*. Warszawa: Naukowa i Akademicka Sieć Komputerowa – Instytut Badawczy, bit.ly/2Xv6uNe [access: 25.10.2018].
- Kemp, S. (2018). *Digital in 2018: World's users pass the 4 billion mark*, bit.ly/2ZW6IKX [access: 25.10.2018].
- *Key Data on Education in Europe* (2012), bit.ly/2VDEFCp [access: 20.03.2019].
- *Kids & The Connected Home: Privacy In The Age Of Connected Dolls, Talking Dinosaurs, And Battling Robots* (2016), bit.ly/2h4a9tm [access: 20.03.2017].
- Office of the UN Special Representative of the Secretary-General on Violence against Children (2014). *Thematic Report: Releasing children's potential and minimizing risks: information and communication technologies, the internet and violence against children*, bit.ly/2DMf7Gb [access: 26.10.2018].
- Ogólne rozporządzenie o ochronie danych (2018), bit.ly/2vHVeNC [access: 20.03.2019].
- Pew Research Center (2018). *Teens, Social Media & Technology 2018*, pewrsr.ch/2L9CBbf [access: 16.11.2018].
- Prensky, M. (2009). *H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom*, bit.ly/2sVhBhS [access: 15.11.2018].
- Projekt ENABLE, bit.ly/2U2GDeJ [access: 20.03.2019].
- *The Digital Competence Framework 2.0*, bit.ly/2vxeWKn [access: 20.03.2019].
- United Nations Convention on the Rights of the Child (1989). bit.ly/1fGCcXV [access: 20.03.2019].
- What jobs will still be around in 20 years? Read this to prepare your future (2018, 26th of June). *The Guardian*, bit.ly/2tM3DOd [access: 9.12.2018].
- Witak, K. (online). *Sztuka (wszelaka) kochania w cyberprzestrzeni*, bit.ly/2uzyMpD [access: 08.10.2018].
- Zespół CERT Polska (2016). *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, Warszawa: Naukowa i Akademicka Sieć Komputerowa, bit.ly/3clyCRd [access: 31.10.2018].

Authors

dr Anna Andrzejewska
The Maria Grzegorzewska University

Adam Andrzejewski
The Maria Grzegorzewska University

dr hab., prof. APS Józef Bednarek
The Maria Grzegorzewska University

dr Sylwia Galanciak
The Maria Grzegorzewska University

prof. Jeffrey Goldstein
Utrecht University

Jolanta Gradowska
National eTwinning Support Service,
Foundation for the Development
of the Education System (FRSE)

Karl Hopwood
Independent esafety consultant,
Insafe Helpline Coordinator

prof. dr hab. Marek Konopczyński
Faculty of Pedagogy and Psychology,
University of Białystok

Filip Konopczyński
NASK (Research and Academic
Computer Network)

Home

Rafał Lew-Starowicz
Ministry of National Education

Janice Richardson
International Advisor at Insight

dr hab., prof. UAM Jacek Pyżalski
Adam Mickiewicz University, Poznań

Anna Rywczyńska
NASK (Research and Academic
Computer Network)

dr Veronica Samara
Senior Digital Skills and Internet
Security Advisor

Adam Stępiński
Mikołaj Kopernik
Secondary Grammar School
in Tarnobrzeg

dr hab., prof. APS Maciej Tanaś
NASK (Research and Academic
Computer Network)

associate prof.
Anne Mette Thorhauge
University of Copenhagen

dr Agnieszka Wrońska
NASK (Research and Academic
Computer Network)

Home

frse
Foundation for the Development
of the Education System

Erasmus+

European
Funds
Knowledge Education Development

Republic
of Poland

European Union
European Social Fund

Home

Home

NASK (Research and Academic Computer Network) works for the development and security of the network ICT. NASK conducts research on internet threats and techniques security and deals with education for safe and valuable use from the Internet by children and young people. Is the coordinator of the Safer Internet program in Poland and operator of the National Education Network – a government program for schools. As part of it by 2021 all educational institutions in Poland will receive free fast Internet, and students get access to constantly expanded educational content and tools.

NASK

Foundation for the Development of the Education System (FRSE) operates as the Polish National Agency of the Erasmus+ Programme implemented in the years 2014–2020 and as the Polish National Agency of the European Solidarity Corps. FRSE is also responsible for other European educational and information initiatives in Poland, such as eTwinning, Eurodesk, Eurydice, Europass, ECVET and EPALE. The Foundation also supports cooperation with countries in the East via the Polish-Lithuanian Youth Exchange Fund, the Polish Ukrainian Council of Youth Exchange, SALTO-EECA Eastern Europe and Caucasus Resource Centre. Since 2014, FRSE has been involved in the implementation of the Operational Programme Knowledge Education Development.

The Foundation organizes many educational events including competitions promoting projects' results. It coordinates the European Youth Week and coorganizes events in the framework of the European Day of Languages. It also conducts research. FRSE Publishing House issues, among others, such quarterly periodicals as Języki Obce w Szkole (Foreign Languages at School) and Europa dla Aktywnych (Europe for the Active).

Free copy

www.frse.org.pl

Home