

Tordai Zsófia:¹

Online intimidation and its potential solutions from a data protection expert's point of view

The online world has become an integral part of our daily life. We exist in a virtual reality in a substantial part of our life where we can keep in touch with our loved ones effectively, order goods and services easily, follow and comment on world events. The online world has been increasingly penetrating into our life while purchasing these services – sometimes unknowingly –, threatening our private life and thus suffering our personal data.

The fast development of technology had a particularly important role in the emergence of the new 'Z generation'², which members exist and communicate in the online world. Its members, during the late 90s and after the millennium were born in the digital era, where it would be unimaginable to exist without Web 2.0 smartphones and other digital communication tools. Another term used for the 'Z generation', invented by Marc Prensky is 'digital aboriginals'³.

Members of the 'Z generation' grew up in a new world where the learning habits changed gradually, inducing problems in the education system, mainly in the field of teaching methods. It becomes harder and harder for teachers to transfer knowledge to the students who are used to fast flow and reception of information. They are capable of dealing with various tasks (*multitasking*).

They are tending to read less while playing more with PC games as well as visiting the social media increasingly. By the development and increased speediness of communication devices they are affected by different online circumstances: they receive more information, process and think of them differently than the members of the 'X and Y generations'.

The number of digital devices has been increased in the households and adolescents are already living online. The attraction of the virtual domain has already reached the youngest generation, by now teenagers are surfing online extensively. The changes generated by technological development are visible at adolescents whom, truly are difficult to approach however, in some cases they are mature enough to receive and process information, and in other cases they are a little more childish. This is called

¹ Data protection expert, NAIH.

² Annamária Tari: *Teenagers in online mode: sought on the Z generation*.

<http://www.dehir.hu/eletmod/kamaszok-online-uzemmodban-teriteken-a-z-generacio/2012/09/27/>

(Downloaded 16th February 2016)

³ Marc Prensky: *Digital Natives, Digital Immigrants*. 2001, In: *On the Horizon*

(MCB University Press, Vol. 9 No. 5, October 2001), 1. p.

[http://www.marcprensky.com/writing/Prensky%20-](http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf)

[%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf](http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf) (Downloaded 16th February 2016)

‘mosaic-like maturity’ which signals the effects of consumer society and information age that cannot be modified and avoided either.

The emotional operation and mental capabilities of the “Z generation” are often distant from each other. Despite the rapid technological development, the emotional capacity of a child progresses in its own psychological pace, they are unable to align to the accelerating world. Consequently, they understand a lot but are incapable of processing everything. They spend a lot of time in the narcissistic online world, receiving emotional experiences that affect their social relations in real life, even changing their relation with family and parents. Real ties conflict with virtual relations and the addictive effects of their online status.

The Internet is a special sphere of personal data processing, with regard to the huge extension of information, data processing and the enormous number of data subjects as well as the power of unlimited publicity. Protection of children’s personal data is a priority for data protection experts as they, concerning their age and lack of experience, are more vulnerable and the potential infringements have serious detrimental impacts on their personal development. As a consequence, data protection authorities (hereinafter referred to as DPAs) have to take special care of online data processing involving children. Prevention and information play a vital role as do the reconciliation of past violations and the awareness-raising of data subjects involved and the publicity.⁴

The rapid development of IT technologies and the online presence are responsible for more and more psychological problems and adverse patterns of behaviour. The phenomenon affects the entire population, but particularly, incautious children.⁵

Certainly, several changes are to be considered forward-looking, as a result, various former complicated work processes (collection of information, research, data collection, organization) have been accelerated thus saving time for the user. Although the pathological changes in behaviour, the improper use of the Internet can induce detrimental effects and cause serious psychological problems.

Children start using the Internet at ever younger ages and the extensive use of tablets and smartphones marginalise the outdated PCs, simultaneously overshadow the development of physical activities, speech and communication skills, leading to real health risks.

Several factors should be taken into account from a psychological point of view:

⁴ National Authority for Data Protection and Freedom of Information: *Key to the world of the net!*. Budapest, 2013, 47-48. pp.

<http://naih.hu/files/projektuzet-angol-web.pdf> (Downloaded 16th February 2016)

⁵ Árpád Mihalik – Éva Szabó – Péter Kovács: The parental control of the children’s computer- and internet use. In: *Applied psychology*. 14(1):47-58., 2014, 48. p.

http://ap.elte.hu/wp-content/uploads/2014/05/APA_2014_1_Mihalik_Szabo_Kovacs.pdf (Downloaded: 16th February 2016)

1. time spent online and with social media (surfing, browsing, looking up 1-1 single content continuously, reading, posting) – can go to the expense of real experience;
2. online games (pathological playing addiction, gambling) – may lead to addiction;
3. psychological effects induced by widespread social media usage – social platforms, improper use of dating websites by minors and negative impacts thereof.

All three factors do have impacts on the relationship between the individual and his/her environment and in the framework of established interactive processes the individual's relation to him/herself and to the outer world fundamentally changes. Inasmuch this phenomena becomes pathologic, social damage as well as psychological disorders may arise.

Researchers agree that problems can occur in persons who are either still immature (children) or have personality disorders. It follows that kids are vulnerable at all ages and situations since their personality development might take a wrong direction if they become familiar with the Internet in an inappropriate way. The learning process consists of numerous steps: parents and/or siblings, the behaviour of peers (following patterns) and the active learning (from parents, teachers).

Best practices to protect against personality distortion factors:

- the Internet using habits of parents and external environment should be observed,
- time limits shall be set for the various platforms,
- rules and opportunities shall be explained to children according to their age and mental capabilities,
- minors should be warned for possible threats,
- children should be diverted from computers via positive inputs, alternative programs (the Internet shall not be a babysitter!)
- in more serious cases a family or individual psychotherapeutically care is advised.

The majority of impacts lead to the emerge of fear and distress which form the basis for several mental problems. The more deficient (emotion, safety, trust) the life of the minor is, the higher is the negative effect on the child. The pathological and detrimental factors impact interactively, particularly on the personality development of minors, the patterns and the learning process are of great importance in this regard. Moreover, great care must be taken of the continuous forming of the trust based, two-way, parent-child relationships, since it is the only way to be expected that their children will share bad experience with their parents.

I. Mapping of problems – online deviancies

New deviancies emerging in the information society may range from the “somewhat uncomfortable” feelings leaving behind bad impressions to actions constituting crimes.

Another endangering risk factor beyond the apparent anonymity is the seemingly mild community sanction since the abnormal behaviour in the virtual world may lead only to the exclusion of the perpetrator from the community whereas, in the real world, such conduct can involve more serious consequences. Past the mild sanctions of the cyber communities the mild assessment of the society also enhances these deviations. The anonymous online life leads to dual morality which implies the weak interpretation of social norms, i.e. a huge majority remains traditionally compliant but during his Internet communication follows altered rules.⁶

In the online world people lose their inhibitions and can contact strangers more easier, individuals present their opinions or expose information more bravely, either taking on himself or anonymously. And the majority of the youngsters open up to the outer world blindly. Girls, at best, upload photos of themselves in bikinis, reveal their actual location and the place where they head to have a party or that they will be at home alone in the weekend. In accordance with the findings of Police Major Dr. Tibor Peszleg the sense of danger in children during online surfing is lower than necessary: “Inhibitions of children, evolved instinctively or by virtue of family education, are being demolished. Subsequent to the Internet chatting comes the personal meeting during which the juvenile could become a victim of a crime. These risky dating possibilities include the Internet chat rooms, mailing forums, IRC channels.....In my work I already encountered a minor who met an adult in a chat room, at the personal meeting had a sexual intercourse with that person and consumed drugs together as well. The child was away from home for days and even after did not even perceive the peril of what has happened. In the course of the interrogation came out the fact that this had not been the first ‘chat’ relationship”.⁷

a. Cyber bullying

Due to modern technical devices and the widespread expansion of Internet we can find cases of cyber bullying in relation to children aged 10-16 more and more frequently (mostly) due to the lack of education on this subject. Cyber bullying always begins for personal reasons and the offender deliberately “tortures” his victim for a longer period.

The new Hungarian Penal Code establishes the following statutory provisions for harassment (Section 222): (1) Any person who engages in conduct intended to intimidate another person, to disturb the privacy of or to upset, or cause emotional distress to another person arbitrarily, or who is engaged in the pestering of another person on a regular basis, is guilty of a misdemeanour punishable by imprisonment not exceeding one year, insofar as the act did not result in a more serious criminal offense. (2) Any person

⁶ Zoltán Szathmáry: *Doctoral dissertation: Crime in the Information Society, criminal constitutional dilemmas in the information society*. Budapest, 2012, 64-65. pp.
<http://ajk.pte.hu/files/file/doktori-iskola/szathmary-zoltan/szathmary-zoltan-vedes-tezisek.pdf> (Downloaded 16th February 2016)

⁷ National Authority for Data Protection and Freedom of Information: Id. 47-48. pp.

who, for the purpose of intimidation: a) conveys the threat of force or public endangerment intended to inflict harm upon another person, or upon a relative of this person, or b) giving the impression that any threat to the life, physical integrity or health of another person is imminent, is guilty of a misdemeanour punishable by imprisonment not exceeding two years.

The key element is harassment, though the actions can differ: for instance someone sends threatening or degrading emails day and night, sends messages on a social site, posts intimidating comments or insults his fellows in his blog. An unpleasant situation happened anywhere that was recorded by a cell phone equipped with a camera, can be learned the same day by mass of people on a popular social networking site. The insulting offense committed by a fellow youngster via an ICT gadget is directed repeatedly against a targeted victim from whom he is unable to defend him/herself. In the course of rough joke and bantering young people, typically between the ages of 13-17, discredit each other on diverse platforms.

Perpetrators are mostly other minors and juveniles. The anonymity of the offender could be more scaring for the kids since it can enhance the impression of being unprotected thus causing more serious injuries. As psychological or physical harassment at school ceases after getting home, in the event of an online bullying the victim remains victim at home as well. Internet annoyance takes place publicly with the approval of apparently multiple witnesses compared to offline insulting. The prevalence of smart phones limits the supervisory and regulatory powers of parents thus the peril affecting children increases.

An example for the above is highlighted through a suicide case committed by an American girl, M.M., in 2006. The tragedy happened because, according to the prosecution, a mother and her daughter were collaborating to deceive the victim, 13, on MySpace where they made her believe that she was dating with a boy, 16, in the course of a continuous e-mail correspondence. The girlfriends later got into conflict with each other, the deceit came to light and M.M. hung herself in utter bitterness. The public has been shocked by the prosecution initially failing to bring charges against the suspected mother since they could not find a count of indictment capable of complying with the action of online bullying. Finally the mother was brought to court on account of conspiracy and illegal use of PC networks. Since the issue took place on MySpace, the liability of the social site was also raised. After the case Mr. Matt Blunt, Governor of Missouri, signed the Act on the Punishment of Online Bullying that was officially promulgated the 28th of August 2008 and stipulates that online insulters or vexatious persons may be fined up to 500 \$ or sentenced to custody up to 90 days. Unfortunately the number of fatal victims of cyber bullying increase every day and, hearing media coverages, typically girls aged between 13-15 are driven to suicide due to the malicious and generally anonymous remarks.⁸

b. Internet memes

⁸ National Authority for Data Protection and Freedom of Information: Id. 48-50. pp.

Dispatching digital files or references originally for marketing purposes nowadays consists of circulating faked news embarrassing videos or images. These could express artistic contents or courtesy but often end up in rough smear campaign. The difference between memes and cyber bullying is that the aggrieved party is usually a stranger whom the Internet community generally “picks out” based on some negative features or attitudes. Generally these subjects are well known personalities, (e.g. Pope Benedict XVI became a real “meme celeb “following his resignation, often depicted in a rather indecorous manner) but sometimes ordinary people – rarely children – also come up.⁹

A fresh graduate Hungarian man expressed his special thanks to his senior colleagues (including also the Prime Minister) for granting him an office job on his Facebook site in May 2013 – soon he became featured in numerous insulting memes as a result of unveiling his name and photo. Due to his personal message originally directed to his friends a fresh graduate has become a victim of a public degrading campaign. We can see from the above story how irresponsible seniors can be, we could imagine the impact of such harms on adolescents.

c. Provoking comments (troll)

The troll, according to the Internet slang, is a person who distributes his irrelevant messages provocatively to an online community (e.g. on an Internet forum, in a chat room, blog or a mailing list) or pushes forward his position violently aiming at provoking harsh reactions from other users or else disturbing and hindering the communication. The English sentence “Do not feed the trolls” (abbreviated as DNFTT) suggests that users should ignore these persons.

Among trolls nowadays it has become “fashionable” to outrage famous athletes this way. Recently a young British boxer has been spotted by a user, under the nickname Jimmibob88, on Twitter who hurled various insults at the athlete and taunting his results. The very temperamental sportsman offered blood money of 1.000 GBP on Twitter to anyone who reveals the name and address of the troll. Soon he found the offender; what’s more, he even posted a photo of his house on the Internet indicating that he can catch him any time he wants. The troll retreated and pleaded for forgiveness. On Twitter the ratings #keyboardwarrior and #jimmybrownpants became the most popular hashtags due to this issue.

Trolls evidently unleash passions: both the abuses and the backlashes are made in a brutal style; even death threats are very frequent. Following a poor match athletes can expect even such messages: “I hope you, your wife, kids and family die, you deserve it.” Trolls expressing their extremist opinions anonymously certainly do not promote civilized Internet usage and can generally influence all users in an unwanted and wrong way.¹⁰

d. Sending erotic photos (sexting)

⁹ Id. 50. p.

¹⁰ Id. 51. p.

Sexting means circulating erotic images or videos via infocommunication tools, which grew to be trendy among youth in recent years.

In most 'detected' sexting cases erotic images had been recorded by the models themselves or, upon mutual consent, by the partners but later the recordings started to spread uncontrollably. The obvious circumstance that may result in abuses is that multiplied images can be forwarded without any further permission or limits. Another significant inspiration, beyond irresponsibility, could be the vengeance usually in cases when once an affair comes to an end, the one party – mostly the male – discloses the pictures taken of his girlfriend.

Some views argue the reason for this behaviour could be that today teenagers are sexually promiscuous and send erotic messages just for fun. Others are on the opinion that youth make experiments during which they take wrong decisions. Researchers, however, agree that distributing erotic images because of anger or revenge may refer to juvenile relationship behavioural patterns characterized by emotional abuses and violence. It would be wrong to assume that this attitude is only typical of youngsters, however due to their possession of digital opportunities their emotional life and impulsive actions became the main reasons why they avoid to consider the long-term consequences of these actions.

The ethical assessment of the new forms of sexting is not the subject to this chapter, however, it should be noted what unlawful acts could emerge in this regard. Obviously the abuse with illegal pornographic picture arises, as well as – in case of age differences - the delict of abuse with personal data. Unfortunately, even in the US there is no inconsistent approach regarding the detection and handling of the root causes of this phenomenon. The only problem comes from judging the circumstance that in many cases data subjects take and forward these pictures of their own free will thus, i.e. sexting destructs certain principles of impeachment related to legal matters to be protected. Another feature which, however, is meaningful in this chapter is the revaluation of users' relation to privacy. Cyber bullying and sexting equally verify that attitudes to privacy turned to the wrong direction as while cyber bullying means the total ignorance towards the privacy of another person sexting implies the entire revealing of the user's privacy and the voluntary renunciation to protect thereof.

These new trends clearly show not only the changes in moral but also the attitudes of people concerned – including children – to certain protected societal values.¹¹

The above mentioned events are clearly illustrated in the following example: a 14 year-old girl and a 16 year-old boy took erotic photos of each other. The boy shared the pictures – out of pride – in a closed group of a social media site including almost the whole school class. The girl's father learnt the case and reported it to the police. The police interrogated the boys in the class and found that all the boys processed the photos unlawfully (since the girl never consented explicitly to the processing of the pictures that would have been a legal basis for processing). Point of law: did the class members who

¹¹ Id. 52-53. pp.

got access to the photos commit the crime of misuse with personal data. From a data protection point of view we should emphasize that the sole access to the data does not constitute processing of personal data but any further action does (for instance forwarding, in the present case).

Experts of the Authority (who heard the case) were astonished that— pursuant to the police reporting – the suspected youngsters had been totally indifferent in the course of the procedure.

Therefore we can conclude that today's children do not deal with online privacy the same way as offline privacy. One may wonder, whether these children would have posted their photos printed out from the social site, on the school billboard with an adhesive tape. The answer is clearly no, I presume.

This demonstrates that the perception of risk amongst youngsters in the online world has still not evolved while, in the offline world they may easily realise the effects of their actions.

e. Internet paedophilia

A paedophile is an adult person who, due to his personal distortion, feels sexual desire towards minors. The social opinion of paedophilia is extremely negative and several forms thereof are penalized by the penal law as well:

- sexual abuse: any person who engages in sexual activities with a person under the age of fourteen years, or persuades such person to engage in sexual activities with another person; or

- child pornography: any person who a) obtains or have in his possession pornographic images of a person or persons under the age of eighteen years, b) produces, offers, supplies or makes available pornographic images of a person or persons under the age of eighteen years, c) distributes, deals with or makes pornographic images of a person or persons under the age of eighteen years available to the general public, or d) persuades a person/persons under the age of eighteen years to participate in a pornographic production.

Therefore offenders certainly strive to hide their activity. The Internet is an excellent forum to satisfy these paedophile desires anonymously. It involves not only individual but also organized crime activities since acquiring and forwarding pornographic pictures of children is much faster and simpler on the net. A not unusual example: a male in his forties registers on a social networking or dating site pretending to be 18 years old, uploads an attractive photo of himself, begins to date with teenager girls, they become friends quickly, the girls take 'the boy' into their confidence and, on his request, they possibly send additional pictures of themselves, in clothes at best, at worst nude or semi-nude images.

In the course of Internet paedophilia offenders really use the Internet as a channel to commit a sexual abuse by dating, establishing contacts or obtain the pornographic pictures by severely violating the real intentions or interests of the aggrieved party.

From a data protection perspective it could be problematic that in many cases the injured party himself, willy-nilly, facilitates the acquirement of pornographic images by uploading pictures voluntarily. Moreover an expert shall be appointed to testify that on a certain pornographic image the child in question is observable or not. (In many cases the pictures are modified, for instance – through image editing software – the head of a stranger is added to a nude body.).¹²

f. Online meshing (grooming)

For the time being there is no proper Hungarian term for it, the phenomenon could be described by the words meshing or catching. The expansion of social sites simplified nowadays' dating practices and as a result, children accept the friendship of people they have not ever met before, only because the individual is an acquaintance of a friend or they share some common field of interest. We shall also bear in mind that a person concealing behind a photo and pretending to be a 14 year old boy may be actually a 30 or 40 years-old man, or even elders who search for potential victims to satisfy their sexual desires on the web. Most perpetrators hunt for their young victims (boys and girls equally) on social sites with a well-founded strategy for months. They get into the victims' confidence, obtain their personal information, involve the younger people into online sexual games and and in extremist they persuade their victims to meet them in person.

Children initially – in virtue of the well-founded confidence – do not recognize what is going on; they will not get disappointed that the person who in the beginning pretended to be a fellow youngster really deceives them. The excitement or curiosity is much higher. If, after all, a personal meeting takes place between them the minor will not speak about it. Due to the shame involved s/he generally will ask for help too late or never ever.¹³

g. Flaming

'Flaming' is a form of cyber bullying exercised in widespread Internet forums where insulting and hostile comments, not directly linked to the main topic are being sent deliberately via public channels such as public community sites, personal blogs, chat rooms, e-mail messaging systems or famous video sharing sites like YouTube.

The term 'flaming' refers in Hungarian to some sort of discrediting someone in the online world, in practice, a written manifestation of oral, emotional and, frequently sexual harassments. Perpetrators – the 'flamers' – generally publish defamatory contents as responses to their fury, sadness, degradation or lack of self-confidence.

¹² Id. 53-54. pp.

¹³ Id. 54-55. pp.

Actually it can be considered as an online ‘war’, assault, quarrel: angry, offensive and obscene comments on public forums (often political, religious, ideological disputes).¹⁴

Whereas some individuals share purposefully degrading contents or target the racial, sexual, religious identity or pecuniary situation of people, others insult net users solely for fun, without reasonable grounds.

Several offenders clearly address seemingly vulnerable Internet users; if the former managed to acquire personal information of them – giving rise to more serious concerns – they would make use of it against the latter.

Anybody, spending some time in the online world, can fall victim of the flaming. The negative reactions given to ‘flaming’ raise the interest of perpetrators by which they learn that they have achieved their goals and succeeded in infuriating the targeted people.

Their purpose is to intentionally provoke innocent users and by sharing offensive and degrading contents, to invoke negative emotions in the individuals involved: fury, indignation, worry, fear or degradation.

Neither the detailed character of ‘ordinary’ offenders nor the ‘flamers’ can be illustrated precisely as anyone can become perpetrator regardless of age, sex, origin or family status: some for fun, others from envy and others as an act of revenge responding to previous insults.

In case of disclosing insulting contents the worst response of the victim is to react to it, particularly, if the victim’s behaviour reveals anger, fury or disenchantment since the major purpose of ‘flamers’ is to provoke. For this reason – though it is quite difficult to act so – the best practice is to ignore these contents because perpetrators, following 2-3 unsuccessful attempts, cease insulting the targeted person and switch for another individual.

When problems strike, it is essential for victims to know they are not let alone. Unfortunately cyberbullying became an ‘everyday practice’ today. If someone falls victim to ‘flamers’, it can be reported to the service provider of the site who deletes the insulting content in question or bans the offender user from the site.¹⁵

II. How to avoid becoming a victim to cyberbullying – different roles?

„If you are not posting, it has not happened!” this slogan directs the Y-generation. The youth take for granted that they are living in the online world, refers to unknown virtual

¹⁴ <http://www.kek-vonal.hu/index.php/hu/szolgaltatasok/internetbiztonsag/395-internetes-zaklatas>
(Downloaded the 27th January 2016)

¹⁵ <http://nobullying.com/what-is-flaming/> (Downloaded the 27th January 2016)
<http://www.wisegeek.com/what-is-flaming.htm> (Downloaded the 27th January 2016)

people as ‘friends’ and as a consequence they reveal all of their secrets to strangers; they do not perceive the risks until the above mentioned online threats reach them.

The Innocenti Research Centre of UNICEF¹⁶ produced a report of the online safety of youth in 2011. According to the survey the debates conducted on information and published online are varied. Some think disclosing personal information is a normal behaviour nowadays. Basically, if a teenager does not publish any personal information then his fellow schoolmates tend to consider him strange or crank. Disclosing personal data has become commonplace and part of their culture for them today and the kids do not consider it dangerous. Worldwide researches show that young people are more convinced of their online safety than their parents.

The reason for this is that the online world creates a different and new lifestyle on infocommunication devices which previously was not available and, therefore, the younger generations cannot enquire about it from their parents and grandparents. Challenges of the Internet should be discovered by children and parents together.

Surveys also revealed that in case of online harassment young people do not rely on their parents at first since, according to their views, they do not know and understand the online world. Besides, they fear of being deprived of their smartphones or parents limiting the use of Internet, or they are anxious about the insulter threatening them or concerned about shame or indignity. There is growing evidence that the most powerful protective aspect would be the parents using the Internet, discussing the online experience with the children openly which, according to the studies, the young people would not object to. Smartphones with online access are on a raise however, new problems in this regard since parents are much less capable of supervising, blocking or monitoring the use of different apps. That’s why it is of utmost importance to involve the young people and to make them aware the risks and perils so as to they can help other children as well as, in case of troubles, they approach their fellows at first. Teenagers need information and protocols to identify the problems, methods and processes which they can apply. Last but not least, with a view to enhance the online safety of children, parents should also be supported in improving their digital skills.¹⁷

In Hungary several organisations are playing an active role in developing digital literacy through numerous programmes and events.

¹⁶ ITHAKA Research & Consulting: EU Kids Online II: *International research at the children's Internet usage, the risks and hazards, The results of the research in Hungary*. 2011.

http://ithaka.hu/wp-content/uploads/2012/07/ITHAKA_NMHH_EU_KIDS_PPT_v1.0.pdf (Downloaded 16th February 2016) PowerPoint Slides

¹⁷ Report of the Commissioner on Fundamental Rights on the state of play of teaching media recognition, Budapest, 2016, 15.

[p.\[http://www.ajbh.hu/documents/10180/2500969/Jelent%C3%A9s+a+m%C3%A9dia%C3%A9rt%C3%A9s-oktat%C3%A9s+helyzet%C3%A9r%C5%91+497_2016/41838d72-616e-45bf-8b51-e744c4fa1b59?version=1.0\]\(http://www.ajbh.hu/documents/10180/2500969/Jelent%C3%A9s+a+m%C3%A9dia%C3%A9rt%C3%A9s-oktat%C3%A9s+helyzet%C3%A9r%C5%91+497_2016/41838d72-616e-45bf-8b51-e744c4fa1b59?version=1.0\)](http://www.ajbh.hu/documents/10180/2500969/Jelent%C3%A9s+a+m%C3%A9dia%C3%A9rt%C3%A9s-oktat%C3%A9s+helyzet%C3%A9r%C5%91+497_2016/41838d72-616e-45bf-8b51-e744c4fa1b59?version=1.0); (Downloaded: 9th February 2016)

The Digital Knowledge Academy (<http://digipedia.hu/>) is a civil society that intends to give examples and information to both parents and children on the conscious usage of digital devices.

The National Authority for Data Protection and Freedom of Information (NAIH), within the scope of its official duties pays particular attention to the conscious Internet use of minors and to enhance privacy knowledge. In this field the NAIH launched its long-term awareness-raising campaign in 2013. It's first outcome was the "The key to the World of the Internet" teaching material published in September 2013 (<http://naih.hu/key-to-the-world-of-the-net-.html>).

The book illustrates the risks of the online world and smart devices as well as social community sites, highlights events occurred but also contains tips for children to protect themselves against threats.

In summary we can conclude that it is a common concern to monitor the activity of our children in the online world and joint action is needed for prevention and to address problems.