KEY TO THE WORLD OF THE NET!

Study of NAIH on the safe and conscious internet use of children

(Promoting legally conscious internet use of children by means of fundamental rights protection measures)

2016

Objective of the study:
Awareness raising of children regarding potential risks of internet use, identifying future challenges, promoting the conscious internet use and exercise of rights by means of applying the results of theoretical and practical researches.

Co-authors:
Viktor Árvay (NAIH)
Mária Krisztina Bácskai (Office of the Commissioner for Fundamental Rights)
Nóra Belső (M.D. psychiatrist)
Dániel Eszteri (NAIH)
Laura Kozma (NAIH)
Ágnes Lux (UNICEF)
Petra Márkus (NAIH)
Attila Mátyásfalvi (NAIH)
Sára Ránki (linguistic expert)
Borbála Csekeő Reményiné (Blue Line Child Crises Foundation)
Bence Ságvári (sociologist, HAS Centre for Social Sciences)
Gabriella Sárközi (educational mediator)
Dániel Somfalvi (NAIH)
Katalin Somogyvári (NAIH)
Júlia Sziklay (NAIH)
Zsófia Tordai (NAIH)

Translator:
Balázs Mayer

Editor and reader:
Julia Sziklay

We want to give special thanks to Facebook Ireland Ltd. for supporting the English language translation and to the National Media and Infocommunication Authority for supporting the publication of the second edition of the study.

Second edition, Budapest 2016 ISBN 978-963-08-7155-6

Contents

1. Introduction

"The internet is not good and not bad either – it is solely a feature. A mirror. What emerges therefrom does not seem to be radically novel. Network life inherits many nuisances and diseases of the social existence.[1]"

(Dr. László Ropolyi)

The rapid development of IT, internet and telecommunication technologies have brought about radical changes in the world almost in all aspects of life in the recent decades. The information society is based on the nearly unlimited abundance and distribution of information. However, as defined by Prof. Manuel Castells "The network society, in the simplest terms, is a social structure based on networks operated by information and communication technologies based in microelectronics and digital computer networks that generate, process, and distribute information on the basis of the knowledge accumulated in the nodes of the networks.[2]" Into this world our children have been born and they consider it as a natural communication environment.

Without overestimating the available research data (e.g. European Values Study, 2008[3]) we can conclude that people communicating and socializing on the web – due to the amount of available information as well – are generally more curious and open to new things but less cautious than his fellow-beings that do not use the internet. Results of international researches[4] focusing principally on children also warn that the risk of evolvement of double morality among internet users is high – the frequent internet users' online standards are more lenient and less severe compared to those rules recognized by the same person in the offline world. This reflects in regular and frequent software downloads, in rough chat style, disgracing comments or even online harassments and in the abuses of fellow net users' personal data.[5]

[1] László Ropolyi: Internet use and the construction of network life, Information Society, VI(4), 39-46, 2006

[2] Identity and Change in the Network Society, Conversation with Manuel Castells (May 9, 2001) In.: http://globetrotter.berkeley.edu/people/Castells/castells-con4.html

[3] György Csepeli – Gergő Prazsák: Internet users attracted by the values in.: What do Hungarians appraise? Hungarian results of the European Values Study, 2008, ed.: Gergely Rosta- Miklós Tomka, OCIPE Hungary-Faludi Ferenc Academy, Bp., 2010, p. 187-204.

[4] For example Isabelle Michelet: Our Children at Risk Online: The Example of Thailand., ECPAT International Bangkok, 2003

[5] *"frequent and for long internet user kids lack empathy and the ability to read faces, they cannot detect subtle signals which are not communicated verbally or in writing and this evokes several conflicts in the offline communication."* in.: Katalin Parti- György Virág: The cyberkid and the bicycle. Specialities of internet use of Eastern European children, Criminology studies 48., OKRI Bp., 2011, p. 43.

The new culture develops novel behavioural forms which we, adults, need to recognize, understand as well as to prepare the so-called "Z generation"[6] to dangers arising out of them, too. (Y generation: born between 1976-1995, Z generation: born between 1995-2009). Fortunately lots of programs, campaigns and organizations deal with potential online threats to children in Hungary, as well. It must be noted, however, that the "network of networks" offers numerous advantages to children. In the essay tasks on internet usage in secondary grammar school admission tests in Hungarian language of 2013 14 year-old pupils provided replies like "The internet is very important and useful to mankind as you can find there everything easily. You can have access there to information or vital documents. Even though a clear majority of people – mainly teenagers – spend their spare time browsing social networking sites instead of studying". Moreover responses included that "We can acquire information and keep in touch with others far away more simply but probably we gain access to more unhelpful information than useful on getting online." [7]

In the USA the internet became the major source of information in 2010 among young adults in case of Hungarian children aged 14-19 this ratio is 48 %.[8] There are no space or time limits, reproduction and other costs, the search and store of any kind of information is a "piece of cake". The internet can serve as an excellent arena for constructive entertainment, capacity building or contacting if used in a cultured and safe way.

According to the findings of a Hungarian comparative study of 2010 examining the habits of youths aged 10-18 the main purpose of everyday internet use, based on a boy-girl category distribution, is primarily the social contacting (47-53%), entertainment (46-37%), games (29-6%) and lastly the studying (5-4%). Although users who go online at least weekly the principal focus is on studying (40-50%), entertainment (37-45%), social activities (32-35%) and games (43-26%). Search engines related to studying are used almost everybody, using electronic dictionaries and the Wikipedia is also common. Visiting thematic link collections, sites containing education materials or sample tests as well as language related websites (maturity and higher education admission tests) are more sporadic. Internet culture has a real effect on the habits of youths in all aspects of life.

[6] Online market research on the retail internet use ordered by NMHH, 2014 http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf 12-02-2016 Levente Székely: Internet boots on school desk, from: New Youth Review, Winter 2010, 79-87.pp.
[7] Source: own research
[8] 65% of those interviewed cited online news site as a source of information, this figure is almost the double of those in 2007. Source: Pew Research Centre study, 01-04-2011 in: http://mashable.com/2011/01/04/internet-surpasses-television-as-main-news-source-for-young-adults-study/

New words are created (e.g. trolls, delebs, liking), new communications forms are being used (electronic messaging instead of writing letters, blogs instead of diaries, MMS in place of postcards etc.), worldwide events (either cultural – for instance a new novel or song dedicated to youths or new fashion goods) affect them right away – all these influence their thinking and behavior. We emphasize, however, that these changes are inevitable but not condemnable at all. Awareness, caution, critical approach and analysing attitude are absolutely advantageous in this field

The objective of the present study is to contribute to the appropriate and up-to-date analysis of the topic from a fundamental law - primarily a data protection - perspective and, according to our intentions, to improve the online culture of children by practical means. The approach, i.e. the fundament of data protection, is based on human dignity which, pursuant to the Hungarian legal interpretation is inviolable and unrestrictable. If a child, using the internet, takes over these stable values he will not do anything to hurt the dignity of others, what's more, will deliberately take a stand against disturbing and offensive phenomena in his vicinity and thus his vulnerability could be significantly reduced.

We are convinced that introducing individual data protection education courses and providing state-of-the-art and practical knowledge in the teacher training is inevitable today so as to students turn into trained and conscious users of modern IT technologies and help them become confident digital citizens. To this end, in March 2016 I initiated at the ministry responsible for education and the teacher training centres to insert data protection training programmes into teacher education to which the NAIH offers its experience, knowledge basis as well as international networks with pleasure.

The success of the first edition of the "Key to the internet!" publication of 2013 clearly indicates that among Hungarian experts dealing with children – teachers, child protection specialists, NGOs – there is a great need to exchange the best practices and knowledge. Therefore we published the second, extended and updated 2016 edition of the above-mentioned publication; in this regard we wish to express our special thanks to the National Media and Infocommunications Authority.

Dr. Attila Péterfalvi, President of NAIH

2. Presenting of NAIH

The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) commenced its operation on the 1st of January 2012, however, it has been resuming the legal protective activity of the former data protection commissioner operative between 1995-2011. Pursuant to the Fundamental Law of Hungary and the effective legal instrument the NAIH, as a state body, supervises the enforcement of the rights to the protection of personal data (data protection) and access to public information and information of public interest (freedom of information). It receives complaints from citizens and in case of well-founded suspicion of severe data breaches it initiates data protection administrative procedures where it may order the blocking or destruction of data processed unlawfully and may prohibit the unlawful data processing or even may impose a financial penalty up to 20 million HUF.

The internet is an extraordinary scope of processing of personal data and data of public interest with regard to the incredible high number of information, the data processing activities and data subjects as well as the power of unlimited publicity. The protection of children's personal data has always been a priority for all of us dealing with data protection issues since, due to their age and lack of proper life experience, they are more vulnerable and the consequences of infringements may severely affect their personality and mental development. Hence our DPA has to pay more attention to internet-related data processing activities affecting minors. Beyond remedying infringements and raising awareness of data subjects and the public the prevention and the dissemination of information are also of utmost importance.

Apart from *Key to the world of the net!* we published, as member of the international ARCADES consortium, more teaching materials for teachers in 2015 (European Handbook on Privacy and Data Protection for Schools, Data Protection Handbook for Teachers). The publications can be freely downloaded from our website (www.naih.hu).

3. Hungarian case law

A. Case law of the Hungarian DPA

The Data Protection Commissioner – then as of 1st January 2012 the NAIH – always received a lot of complaints in relation to internet abuses. Even in default of knowledge concerning the age of the aggrieved party we can conclude that in case of the violation of inherent rights – violation of the honour and human dignity, defamation, abuse somebody's likeness and recorded voice, violation of the privacy of correspondence and private information, legal disputes arising out of the violation of inherent rights in the course of data processing and data process – the aggrieved party may launch a civil lawsuit against the offending party. A judicial establishment of the violation of law, provision of restitution, a cease and desist order as well as a damage claim may also be initiated. In case of offences of defamation, libel or misuse of personal data the proceeding begins by virtue of a denunciation lodged with the competent authority. In addition the aggrieved party may ask for the removal of comments and contents infringing his/her inherent rights.

Most complaints are received in accordance with personal data or photos disclosed on social networks by users and misused by third parties. Online registrations on behalf of a third party, however, without his/her consent and knowledge shall be deemed as a misuse of personal data. The same applies to defamatory profiles.

According to the position of NAIH publicity shall be interpreted in a small scale in conformity with the logical structure of social networks. Third parties who are not registered may get to know personal data entered into the system only with the support of a registered member. This kind of publicity, however, may not lead to an unlimited exploitation of personal data since the collection, organization and processing of personal data disclosed on the website qualifies always as data processing. Registered users may process the disclosed data only for specified purposes, for the implementation of certain rights or obligations, but may transfer to third parties only with the consent of the data subject or upon authorization of law.

And now a couple of concrete cases from the practice of the Data Protection Commissioner:

- A photo of the petitioner, to be found on iwiw (the first Hungarian social network site), has been used without his consent and knowledge as an esoteric book cover. In view of his unfamiliarity with the topic of the book as well as his desire not to appear on the front cover page of the publication right before his dissertation defense, the disclosure infringed the data subject's rights anyway. (2534/P/2009)

- A mother appealed to the Data Protection Commissioner because a photo of her child had been posted on Facebook and, instead of the name, a derogatory term was visible. The question was how to get this photo removed from the site and how to call persons having disclosed the photos to account? The servers supporting the site operate outside Hungary hence the Commissioner lacked the proper jurisdiction to investigate the submissions launched against the social site. Even though it shall be noted that Facebook has a subsidiary in the territory of the European Union (Ireland, Dublin) therefore submits to the jurisdiction of the EU law and, consequently, the data protection regulations adopted by the EU, and forming the basis of the Hungarian data protection legislation as well, also apply to them. As a photo of a child constitutes personal data, the disclosure thereof would have been lawful only with the consent of the child or his/her legal representative. The data subject (or his/her legal representative) may ask for the removal of the photo from the customer service of Facebook (clicking on the button "report a photo" to be found beneath the image) and, depending on the circumstances, a civil suit or a criminal proceeding may also be initiated (ABI-7949/2012/P).
- A parent uploaded some photos of his student daughter to a social site and someone copied the images with the name to a public website where defamatory remarks appeared with the pictures. The mother approached the operator of the site multiple times to have them erase all personal data of his daughter from the site. The operator of the site published also these requests containing names and addresses and replied to the letter publicly in a cynical, abusive and vulgar tone, moreover disclosed several comments from users which also severely violated the good reputation of the entire family of the applicant (ABI-7041/P/2010).
- The complainant submitted an application for a beauty competition called Miss MyVip on the MyVip social network and uploaded photos to her application form. A friend of her called her attention that she had been found on a disreputable site along with pornographic images that defamed 9 other girls as well. The request sent to the editor of the site for deletion remained unnoticed (ABI-4900/2010/P).

- Photos of the complainant’s daughter of 16 had been removed from the site www.myvip.com and uploaded to a disreputable site along with the girl’s full name, place of domicile, age and phone number. She was receiving threatening letters and vexatious phone calls as well as indecent commentaries were attached to her images. To her request for cancellation she got the mere reply only that *“never in a thousand years you are gonna’ be removed from here”* (ABI-4865/2012/P).
- In a similar case a parent approached the Commissioner on behalf of his daughter of 15. Personal data and photos of his daughter to be found on a social site had been uploaded to a disreputable site along with the girl’s full name, place of domicile, age and derogatory comments had been added. The petitioner has not appealed to the operator of the site requesting for deletion because the operator himself urges the users to breach the law this way: *“Send in chicks of 16 or younger preening themselves online! Do specify myvip or iwiw domain addresses! Should you have been posted on the site and hence you have become sad, send a message and perhaps we will remove your photos from the site. Since we are jerks and inclined to disobey the more you are buggering us around the more certain you are going to succeed!”* (ABI-4841/2012/P)
- Another petitioner received an email through iwiw from an unknown person along with a link to a certain disreputable website containing also his photos with names and obscene comments. The complainant was receiving numerous vexatious messages to his iwiw email-box from visitors of the other site (ABI-1243/2010/P).

In view of the repeated complaints the Commissioner filed charges against a person unknown in virtue of the misuse of personal data violating the provisions of the Penal Code. Photos appearing on the operated websites were taken over from other social sites that, in most cases, enabled the disclosure of individuals via personal identifiers (name, phone number, place of domicile, location on a social site). Purpose limitation is one of the most important data protection principle thus the use of likeness and other personal data without permission qualifies as unlawful data processing. The determining factor in using public databases is the initial intention for the publication of data. The disclosure of a dataset, for the purpose set forth in a legal regulation or in accordance with the provisions of data subjects, may not lead to the use of information by data controllers to the effect other than the original purpose. (The practice of the judiciary also affirms this aspect. The

Capital Tribunal in its judgement in 2009 explained that the publication of a photo in a closed system - on a social site - does not allow for use and disclosure without permission on different places and under different circumstances.) The DPA has approached the companies having registered the respective websites due to the violations of law committed on the website, however, the managers of the companies were unable to identify the person who uploaded the disputed contents. Since the real user of the domain name is different from the company listed in the whois registry an investigation would be required to detect the person or company abusing the personal data. Unfortunately the XIII. District Police Headquarters terminated the investigation in its decision.

The justification of the decision included that the collection and organization of pictures and data qualify as data processing thus the offending conduct is formally factual, however, significant conflict of interest cannot be established. The decision of the Police was repealed by the Prosecutor's Office since even the reasoning of the decision points out that it can be suitable to conclude another criminal offence, e.g. defamation (though this is a private crime rather than a public one).

The Commissioner examined the above cases in the course of a so-called investigation procedure. As of 1st January 2012 through the NAIH has been empowered to launch a more formal administrative procedure, pursuant to the regulations of the Administrative Procedure Act, instead of the informal investigation procedure, in the course of which it is authorised, in case of establishing a violation of law, to impose a financial penalty from 100.000 up to 20 million HUF.

The NAIH investigated in 2013 the data processing activity of Generál Média Publishing Ltd. in the course of a data protection administrative procedure since test registrations affirmed that on the dating websites www.love.hu, www.szeretlek.hu and www.talalka.hu there were approximately 3500 data sheets where the age of registered users were between 10 and 15 (and "of course" lacked the necessary prior permission of the legal representative or subsequent approval). The NAIH in its decision imposed a data protection financial penalty of 3.000.000 HUF on the operator of the dating websites and, additionally, ordered the erasure of illegally processed personal data (alternatively the subsequent acquisition of the necessary statements of legal representatives) as well as to modify the data protection practice respecting the registration in order to comply with the law. According to the view of NAIH especially the dating websites in social networking sites carry a real risk as we have experienced during test registrations: in the days following the registration several vexatious, more or less implicitly sexual oriented letters were received in the mailbox of the owner which can be qualified as undoubtedly illegal, harmful and age-mismatched content (NAIH-5951/2012-H).

In the press – either online journal or news site – personal data disclosure of children's name, place of birth or mother's name published temporarily in the birth heading raises concerns from a data protection point of view. (NAIH/2015/503/2/V)

Another case relates to children beauty contests where complainants approached the NAIH respecting modelling, fashion photography and other events organised through the website of a model agency. On the basis of the content of the website the organizing company cannot be identified and verified, the firm in question cannot be contacted, what's more, there is no privacy policy on the homepage. Investigation is still underway. NAIH/2016/330/V

B. Case law of the Ombudsman

The institution of a parliamentary ombudsman has been existing in Hungary as of 1995 that has been called, from 1st January 2012 in line with the EU terminology Commissioner for Fundamental Rights. As an independent body he is liable only to the Parliament during his 6 year term and consequently prepares annual reports of his activity. His major responsibility is to investigate, ex officio or upon complaints, abuses with respect to fundamental rights and, for their remedy, make recommendations or initiate actions against authorities (excluded the activity of the Parliament, courts of justices, Constitutional Court and the Public Prosecutor's Office as well as infringements taken place before 23rd of October 1989).In the absence of a special children's rights ombudsman in Hungary the Commissioner for Fundamental Rights performs the duties concerning children's rights to which he pays particular attention. Every year he conducts thematic investigations in the framework of special projects in this area of law. As of 2008 there exists a single website on children's rights (http://gyermekjogok.ajbh.hu/), from 2011 in turn a Facebook site (https://www.facebook.com/Gyermekjogok), too. Individual complaints over children's internet use – as they imply primarily data protection aspects – do not fall into the competence of the ombudsman, however, he has the power to launch ex officio series of comprehensive thematic inspections in the context of special children's rights project. Thus, in 2015, he examined the topic of education of media literacy in Hungary.

The European Commission Recommendation of 2009 on media literacy urges that media education and media literacy be introduced into the education system and as many potential actor be involved as possible in Member States. The objective and essence of media literacy education is to prepare minors to the critical media consumption, to become conscious consumers so that they can distinct between news and views. Education experts warn that, depending on local, personal and school conditions, difference in children's IT literacy brings about problems. In the context of the 2013 National Core Curriculum on Education (hereinafter referred to as NAT) media literacy knowledge is explicitly incorporated into the school subject of visual culture where the development of critical thinking, media violence, the interpretation of the phenomenon and the awareness raising thereof, the impact of online presence on personality development, personal relations, study, work and free time activities. A thorough ombudsman survey revealed, however, that a true view can be mirrored only by local education curricula qualifying as real practice. It is decided upon locally whether skills are being taught as a subject in its own or as attached to another subject. Teaching staff may decide as to whether the subject "movie and media studies" is taught individually or as part of literature, IT, drawing or visual culture. As this happens regularly in an integrated form, in the framework of other subjects, the number of hours of training of the subject in question increases by the timeframe which is prescribed by the Core Curriculum for teaching media studies. In practice the time dedicated for teaching disappears and it is not made use of.

In the Hungarian teacher training system we have the following university programmes for improving media literacy and studying special knowledge: BA in Motion picture and media studies, MA teacher in Motion picture and media studies, MA teacher in Movie, motion picture and communication (unitary teacher training). These programmes have been developed to teach motion picture and media studies introduced in primary and secondary schools. Training and certification requirements, however, do not contain information on dangers of the internet, online abuses as well as treatment thereof. According to the survey in Hungary a very limited number of media teachers are properly qualified as much as 20-30 %. There are shortcomings in compulsory qualification requirements for media teachers, as a result, in formal training media studies are taught by teachers who are interested or who have been assigned with it, regardless of whether or not they possess professional qualifications as the Hungarian legislation enables employing teachers in this field who do not have appropriate qualifications. Due to the low number of courses, the integrative presence as well as the low number of properly qualified and skilled teachers in schools and educating media awareness is not realised appropriately and effectively in many cases in the education system. The relatively low number of teaching courses and the lack of qualified teachers has adverse effects because, according to the findings of the survey, children using online media often are not aware of the risks thereof, not everyone knows the privacy settings, in case of harassment they do not know where to turn for help.

The “Alarm-clock-course” children’s rights project of the Hungarian UNICEF Committee addresses the topic of online safety separately. In accordance with the findings of UNICEF children are very interested in the theme and they have preliminary knowledge on the risks of online media and the conscious use thereof. Pursuant to a 2014 survey of UNICEF titled “You are entitled to your rights!” half of children questioned already experienced media contents they did not understand and each third minor has been subject to online harassment. In these cases half of children (53%) tried to defend themselves whilst a quarter of them (26%) quickly closed the session and only every tenth minor asked for help (11%). 47% of minors believed the internet was unsafe. Only 21% of minors (each fifth) considered the online world as undoubtedly safe. Breakdown of opinions as follow: 11% considered the internet as fully safe, 10% rather safe, whilst 32% both safe and unsafe, 22% rather unsafe, 25% absolutely unsafe. 96% of minors aged 10-18 have mobile phones, 88% of them have online social profile. Particularly interesting is that 78% of children aged 10-12 have online media profile; however, officially they are permitted to have it only above the age of 13. 8 minors out of 10 know that several people use the internet for annoying children. 8 minors out of 10 were already involved in discussions on the online safety. Half of children encountered online contents they did not comprehend. In such cases two-thirds of minors closed the window but 18% of them remained and started to browse the site and only 14% asked for help in order to grasp the information experienced. The evaluation of the domestic media literacy education cannot be dissociated from the availability of digital equipment and digital competences which indicates the capabilities relating to the use of ICT technologies.

Although the practical implementation of these technologies has not been part of the ombudsman investigation it is worth noting that in Hungarian schools the opportunities and circumstances in terms of digital tools differ remarkably nowadays. In the year of 2011 the digital public education was monitored in 27 countries – including Hungary – in the context of the ESSIE project on the basis of more than 190.000 questionnaires. According to the findings of the survey the number of PCs has doubled in European education institutions since 2006, however, there are high differences in the field of use of IT tools and digital competences. In accordance with the Hungarian country report the access to PCs comes near the European average, even though, the self-confidence of teachers in using IT appliances in all school years is under the European average. To sum up, Hungarian schools typically belong to digitally well-equipped institutions, this type is characterized by low-grade appliances, slow internet speed or the lack of broadband connection. According to the surveys nearly half of the students have access to mobile internet in schools therefore the improvement of digital IT systems of schools would be even more needed because hence students would face more filtered and controlled contents during classes. Thereby, in accordance with the position of the Fundamental Rights Commissioner, a crucial precondition for implementing full scale media literacy education are the existence of digitally well-equipped education institutions whereby the existing inequalities and shortcomings need continuous development and improvement. The investigation of the Fundamental Rights Commissioner also pointed to the fact that there is a clear correlation between the education of media literacy and the level of awareness raising on the one hand and the lately ever growing phenomenon of cyberbullying on the other hand where minors and young adults would need clear guidance and the education of media literacy could contribute the most effectively in tackling these challenges according to experts. In cyberbullying cases children have very limited knowledge and are not aware where to turn for help. In the meantime neither the NAT nor the training and certification requirements of teacher training subjects encompass competences in handling cyberbullying cases. In the teacher training we still lack capabilities in handling and transferring knowledge on media literacy and on the active and safe use of the media. Though the use of the internet and various digital devices as spare time activities (games, social contacting) begins even earlier. Dangerous activities for minors like cyberbullying, careless posting of contents and photos, internet addiction and irresponsible data processing happens too often. In these cases children behave as a result of their age characteristics, even though, the protection and guidance provided by adults as well as the setting of the frameworks is not sufficient. A distinguishing feature of cyberbullying is that the roles of the insulting person and that of the victim can reverse hence, during the process, the awareness-raising of responsibility and providing assistance are equally important. Reflecting the theme also allows for the children to resolve conflicts and that assistance and attention become basic principles. Another relevant consequence of the investigation is that the real public space shall not set apart from the community of the cyberspace and if you encounter violence in any of them then, in the process of providing remedy, you have to address both in conjunction with one another.

Smartphones with internet access raise further problems in this field as parents are less capable of supervising, filtering or blocking the use of the diverse apps for their kids. The investigation revealed that in the majority of public schools there is filtering software for harmful or unlawful unwanted contents therefore pupils usually surfing online under teacher supervision. However, relating to filtering software, a problem was that there is no proper recommendation to be used in public schools, what's more, the burden of costs and maintenance is disputed. As a result, schools mainly opt for the drastic limitation of internet access at schools. With appropriate teacher guidance, however, there is no need for filtering software; though problems arise after school courses at home or public spaces; using mobile internet gives rise to greatest perils since it is practically uncontrollable for teachers and parents as well. Given the above there is particular need for information and situational descriptions which enable the youths to identify problems, moreover, for processes and methods which would support the online safety of children. In the meantime, however, experts agree that the most powerful protection is secured if parents also use the internet and openly discuss their experience with the minors. On the other hand it would be important to shift the focus to the public and interactive approaches, to information on remedies in the field of harmful or illegal contents or cyberbullying. For this reason it is inevitable for teachers to shape their approaches, to extend their toolkits as well as to gain knowledge which are based on practical experience rather than didactic education. Civil organisations, alternative schools, educational bodies and youth development workshops could contribute to these objectives. The NAT drafts media awareness education as follows: *"The purpose is that pupils become responsible actors in the media-driven, globalized world: to grasp the language of the traditional and novel media. Educating media awareness, by enhancing critical attitudes and activity-orientation prepares for the involvement in participatory democracy and to pursue a rational and value-based everyday life also influenced by the media. Pupils get familiar with the functioning and mode of action of the media, the relation between the media and the society, the distinction methods between real and virtual as well as public and private contacting, in addition, with the legal and ethical importance of these distinctions and the above-mentioned media features. ...Digital competences encompass the self-confident, critical and ethical use of contents transmitted and made available by the technologies of information societies in the fields of personal relationships, work, communication and free time activities. This is based on the following capabilities and activities: recognition (identification), retrieval, evaluation, storing, creation, presenting and change of information; the creation and sharing of digital contents and communication cooperation via the internet."* To sum up the above, the professional requirements drawn up in the NAT illustrate merely external and formal expectations though in the public education system as a whole simply the pure intent rather than the results of media education can be perceived.

Consequently the Fundamental Rights Commissioner stated that the absence of properly trained and skilled teachers, incomplete, truly theoretical and practically controversial transfer of knowledge on media literacy education, the lack of comprehensive government researches surveying the effectiveness of media literacy education and that of analyses on target setting bring about faults which are closely connected with children's rights to protection and care as well as with the right to education. The current situation may, indeed, result in the imminent danger of breach of law. In order to tackle the above difficulties the Fundamental Rights Commissioner called on the competent Minister to initiate a wide-ranging review of the domestic media literacy education, to begin enhancing the specialized skills and competences of teachers and to take the necessary measures in order to increase the number of well-trained instructors. In addition, to launch an overview of the current target system of NAT and that of the teacher training so as to insert the knowledge on cyberbullying into the training and certification requirements.

C. Case law of the Hungarian Police

(special thanks to Dr. Sándor Gömbös p. major-general Dr. Henrik Szabó p. lieutenant-colonel, Mr. Zsolt Szabolcsi p. captain for providing all the relevant information to this chapter!)

"The Public Prosecutor's Office of Budapest I. and XII. District indicted four persons for child pornography – said the Budapest Capital Public Prosecutor's Office in an interview. They attended a home party in 2013-ban in Budapest XVII. District and recorded that two fellows of them had sexual intercourse with a drunken 15 year-old girl. The young boys sent the video recording to multiple friends. 3 of the accused boys are juveniles, that is to say, under the age of 18…According to the Penal Code any person who obtains or have in his possession pornographic images of a person or persons under the age of eighteen years is punishable for a felony by imprisonment not exceeding three years. Who, however, produces, offers, supplies or makes available pornographic images of a person or persons under the age of eighteen years is punishable by imprisonment between one to five years." http://index.hu/belfold/2016/03/10/hazibulin_eroszakoltak_meg_a_15_eves_lanyt/, 10.03.2016.

A remarkable proportion of criminal offences relating to minors and the internet which got into the scope of the Hungarian police are instrumental offences: this means that a less severe offence needs to be committed to reach a more serious result

The first stage is the attainment of personal data from social networking sites which, in this regard, are considered chief 'sources'. On the one hand simple passwords given by minors could be very risky; although they merely wish to contact their fellows and play with each other. On the other hand, given their naivety, upon contacting with adults they may frivolously reveal vital information on themselves or their background. In other cases perpetrators pretend to be minors in order to mislead the children.

Problematic could be some games distributed through social sites which are produced aiming at collecting personal data about minor users. Young play games, watch videos and browse certain webpages on their classmates' advice; nonetheless they lack proper command of foreign languages, what's more, they are not prepared to protect themselves against harmful codes either. Usually the curiosity wins so they download programmes essential to open the required content not considering that by doing so they "pave the way" for a Trojan application collecting personal data to get onto their PCs or mobile phones. These softwares gather information on minors separately promoting a black market to criminals interested in committing sexual-oriented crimes. Once a new game has spread within a community the Police regularly receives complaints claiming that the sites of the children had been compromised or modified. In addition this offense usually remains unrevealed because the child habitually hiddens the case not knowing that s/he has become a subject of a dangerous or mass incident.

The second instance is the utilization or exploitation of the information obtained. Blackmails under the desire for gain or intended to force someone to child pornography are typical. Social sites offer an excellent platform to offenders as there you can a find a place for all ages, moreover, useful data may be acquired on potential victims in advance:

Accessing to the personal data may happen by contacting the recipient intentionally or in a tricky way when a link or a spam is sent to him "accidentally". This links to a page which copies the entry page of a social site or an instant messaging service (for example "Messenger") and enables the user, following the insertion of the relevant password, to enter the real homepage. In possession of the password gained this way a data collection will take place for a while after which, depending of the purpose, will follow a blackmail by putting into perspective the uploading of an image or video recording. This recording may come to effect through a popular method, namely via a Trojan application, that turns on the webcam by remote control without the knowledge of the user and the events coming about in the room are recorded by the offender. Recordings are made typically of naked individuals after bathing, dressing or at masturbation. At the beginning, as the first step, the blackmailer modifies the password of the real user then proves the victim, by entering a neutral comment, that he has acquired full control over his PC. Subsequently the blackmailer puts into perspective the disclosure of the derogatory recordings on a social site where parents, classmates and friends can see the victim. It happens nowadays by virtue of a pre-compiled scenario when the victim is evidently warned that if he were to ask for help from others the recordings would be disclosed. The consequence is, based on international experience, all the same. Youngs become victim of blackmailers for months without anyone being aware the unpleasant situation they got into. Parents tend to realize the possible trouble as a result of a general moodiness and a long-lasting and continuous depression. Though, due to the lapse *of time and shame, the reasons 'are not revealed' and, unluckily, these situations often lead to lies and, because of hopelessness, to suicide.*

Challenging can be also that, on social networking sites, teens tend to mark and verify unknown people with the mere purpose to enhance the circle of friends as much as possible. In the course of the registration process it would be desirable not to upload, beyond the basic personal data necessary for registration, additional personal information (address, date of birth, mobile phone number, and favourite style of music or interests). Intimate images can clearly bring about substantial detriments e.g. in the field of higher education or job search. The provocative photos may result in the commitment of more serious crimes (crimes against sexual morality, theft, robbery, burglary).

We have to be more cautious upon disclosing family photos as well as, by their parents doing so, children could become victims of crimes (and vice versa, images published by kids can raise the attention of burglars). According to police findings several perpetrators visit social networking sites for this purpose and select their victims based on personal information posted online: they pretend being in love, offer hostess or model agency work or Western European schools which young girls are likely to succumb to.

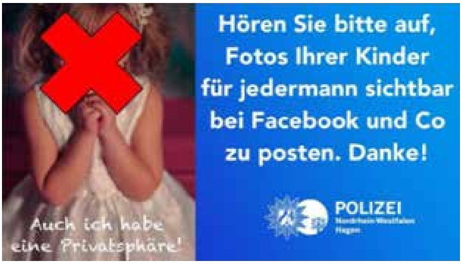

Hören Sie bitte auf, Fotos Ihrer Kinder für jedermann sichtbar bei Facebook und Co zu posten. Danke!
POLIZEI
Nordrhein-Westfalen
Hagen
Auch ich habe eine Privatsphäre!

Figure 1: A public call of the German police to parents in October 2015

Identity theft is extremely unpleasant and may even cause a life-long injury. This may happen if a perpetrator creates a pseudo-profile page by misusing a user's stolen IDs on a social networking site and hence discloses degrading images/texts, insults others or even commits a crime hiding behind the victim's personality. This is possible for the criminal if he is in possession of personal data, images capable of committing an identity theft which can be obtained from a profile site provided with all relevant data.

Chat programs offer the possibility of anonymity therefore the good faith and innocence of children can easily be exploited: consequently perpetrators obtain sensitive information/photos from them, make appointments with them or force them to watch insulting contents. The legal case of 'indecent exposure' often does not come into effect in this regard as the images are acquired or watched with the consent of the data subject; and the offenses, due to the logging being switched off, cannot be attested.

Lots of information is unknown to children, what's more, in many cases they cannot really assess the weight of their actions. As a consequence they may unwittingly and easily become offenders of infringements or even crimes during internet surfing. Children often do not consider that a 'good joke' intended to be directed to a narrow circle and dis- closed (written, uploaded) on the internet shall be regarded as being available to anyone and herefore implies a great audience. Due to this improvidence they, despite their intentions, may commit the crime of 'defamation or libel before the public at large' namely the internet - chat and social forums, blogs or other chat areas as file sharing sites - qualify as being 'public at large' set out by law.

Inspecting a correspondence belonging to another person is equivalent to the crime of 'mail fraud'. A typical case of it is when the user gets his password stored by the PC at school or in a public netcafé or he forgets to log out from his electronic mailbox thus the person, subsequently occupying the same PC workstation and deliberately inspecting the correspondence left open, could simply become a potential perpetrator.

The online sharing of images recorded at school events or received from classmates can violate the right of personal data protection. *Recording, uploading and sharing images of beatings and blackmailings by means of cameras could be more serious acts since, in these cases, the abuse of personal data occurs as an aggravating circumstance beyond the original violent crime.*

Youngs utilize IT devices to maintain friendly contacts and broaden their knowledge with respect to sexuality as well. If, however, somebody wishes to satisfy his sexual desires by downloading photos taken from a minor below the age of 18 irrespective of age, sex and interests qualifies as a criminal conduct. *There are even cases when couples (similarly to adults) record the intimate intercourses that are to be considered also as a criminal offense even if the recordings are made about themselves with the consent of each other. Based also on a true story that a girl, 16, wished to entertain her boyfriend and enhance his libido by "performing a show" by means of the built-in webcam of her laptop on MSN in the course of which she was masturbating. By doing so she committed a crime. The action of the girl, the disclosure, is punishable with an imprisonment ranging from 2 to 8 years whilst that of the boy up to 3 years, respectively. Certainly these actions need to be weighed on a case by case basis. Obviously it is quite different when the recordings are made, and subsequently shared, during parties. Currently the legal background is not satisfactory. Even more serious is that youngs are incapable of handling these issues properly as firstly it is a joke, secondly being not involved is 'embarrassing', thirdly certain images are major money-making opportunities.*

In connection to child pornography it shall be noted that there are usually misunderstandings in Hungary concerning the term "teens" compared to the Hungarian usage of "tini" (teenager) to be found on special sites. In view of the sexually oriented websites and the 'sex industry' the expression "teen" means that images/videos of youngs, young adults, between the age 18 and 20, that is to say, precisely below the age of 20 are being disclosed which, however, is not punishable. This is a typical reaction to an existing demand. The detection of cases respecting child pornography meets occasionally legal obstacles. Successful detections could be achieved primarily in virtue of the supervision of websites, the download of contents shared by the user on peer-to-peer networks and the supervision of data traffic. Although it is quite difficult to implement these actions as the uploading of such images or videos is usually a prerequisite to access these forums or contents. We have even found a webpage where a preliminary personal contacting had also been set with a view to 'eliminate' police constables and committing such crimes is forbidden even to covert agents.

Unfortunately, on account of aggressive advertisements, the visiting of certain sites accidentally is also not rare. Moreover the servants of sex industry create specific keywords, thus misleading the ignorant net user, when the latter encounters a label e.g. 'PTHC Inc.' that means 'pre-teen hard core included', that is to say, containing hard sex events involving teenagers rather than the naming of a company.

4. Online behaviour of the Hungarian children

(Author of this chapter is Dr. Bence Ságvári sociologist)

A. GENERAL TRENDS

According to the surveys of recent years minors go online at an increasingly early age, the majority between 8 and 10 years depending mainly on the age and the availability of high quality "devices" (e.g. desktop PCs, mobile appliances etc.) in the household. In the fall of 2015 pupils of 7th grade started going online at the age of 8 whilst those of 11th grade at the age of 10 on average which, of course, does not mean that there are no kids who begin the online activity 1-2 years earlier or later.

In the age group surveyed the time spent with online surfing can be measured on weekdays in hours rather than in minutes. The real time consumed, however, depends largely on the age. The highest portion (27%) of pupils of grade 11th go online for more than 4 hours a day whilst the younger children usually spend 1 hour a day and roughly one-third of pupils go online less or never at all on schooldays (31%). The same applies to each tenth 11th grade student thus the slight difference between the two age groups refers to divergent internet using habits. A remarkable increase can be observed when finishing primary schools and advancing to secondary schools.[9]

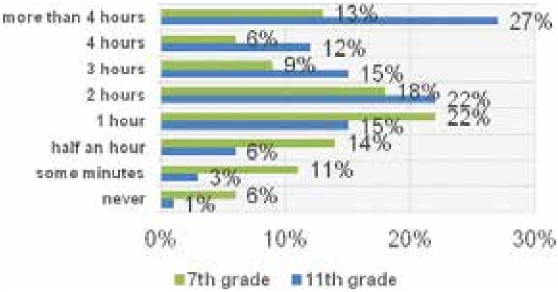


Figure 2: Time spent with online surfing on average schooldays (broken down by both age groups surveyed)

[9] This chapter is based on a representative survey, by analogy of the Hungarian primary and secondary schools, ordered by the International Children's Safety Service (NGYSZ) and produced by the ITHAKA Nonprofit Co. Ltd. in autumn 2015. The research covered pupils of 7th and 11th grade (2x1200 individuals) who completed the questionnaires at schools. The results relate, from a strict statistical point of view, to these two age cohorts not to the younger people "in generally". In accordance with the slightly lighter though more practical interpretation, however, the findings can be more or less generalised to younger people aged 13-18.

It is not surprising that both age groups go online more frequently on weekends. By that time the ratio of younger people surfing online more than 4 hours a day is the highest. Although there a clear difference between these two age groups on out-of-school days can be observed. On weekends almost a half of kids elder than 15 use the internet more than 4 hours a day whilst the same ratio of children aged 13-15 is only 31%.

Time spent online depends, beyond age, on two additional factors: polls show that girls and children having an own device surf the web more than the average does.

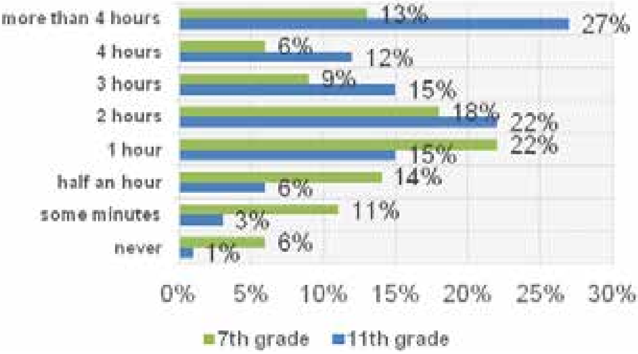


Figure 3: Time spent with online surfing on average out-of-school days (broken down by both age groups surveyed)

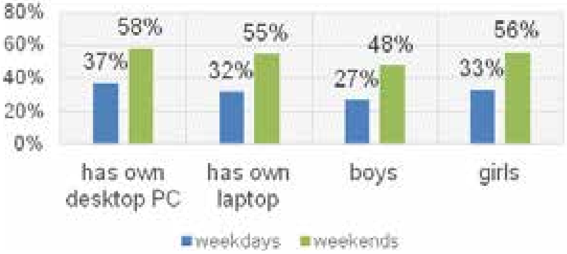


Figure 4: Ratio of children using the net more than 3 hours a day on weekdays and weekend (among those having and not having an own PC surveyed as well as broken down by sex)

The principal location of using the net is at home and at school even though the portion of children using the net when travelling is increasing. 30% of pupils of 7th grade and 61% of those 11th grade claim to use the net often during the journey. Appliances exclusively in own ownership or in own rooms can obviously increase the time spent online remarkably. Whereas there is no significant difference between the two age groups concerning smartphones, then in the rooms of the younger people we can find mobile devices more likely than desktop PCs. Among pupils of 7th grade each third while among those of elder grades every fourth possesses tablets. It is interesting, however, that they possess own laptops in a far greater proportion (43%) than their younger fellows (36%) do. That is to say, this slight margin of several years produces systematic differences in the access to the “digital environment” of the youth.

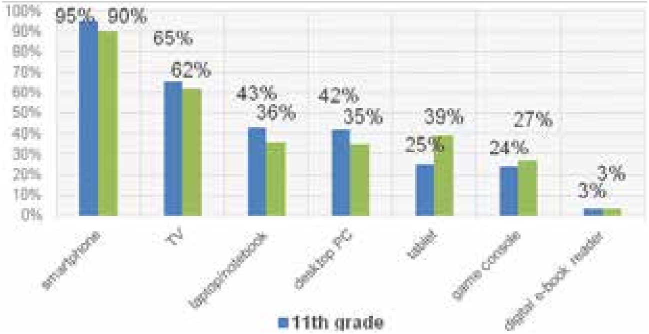


Figure 5: Devices in own ownership or room (the ratio of those who have devices in their ownership or their own room, broken down by both age groups surveyed)

In the past recent years the mobile phone (smartphone) has become the most chief platform in this age group. The most popular activity is, accordingly, listening to, and downloading of, music as well as chatting and browsing social networking sites. 78% of those aged 13-15 and 90% of those aged 16-18 often listen to music online and merely 9% and 2% of those, respectively, never do so. Moreover, 80% of the younger and 92% in the elder group use the device for chatting. In practice, there are almost no children aged above 15 who have declined to use social networking sites frequently (96%) whilst 77% of the younger group belongs to this circle. Though this later is a quite high percentage, the major difference between the two age groups can be discovered respecting the use of social sites: whereas almost all the elder group members (11th grade) use community sites then those belonging to 7th grade this ratio is (still) only 13%.

Chatting, reading news and browsing for information is somewhat more frequent among the elders. As for school tasks the distinction is relatively little: in both age groups approximately half of pupils search for learning materials on the net. By contrast, searching for out-of-school things online is much more common in case of minors aged above 15, two-thirds of whom browse something like these quite often in contrast to 48% of younger pupils doing so. Online games, however, played either alone or together with others, are more popular among younger children: nearly half (49%) of the latter group whereas more than half (57%) of the former group spend their free time with it regularly. In both types of games nearly four kids out of ten elder ones belong to frequent players. Online telephony as well as composing blogs or micro blogs is also more popular among the younger people albeit in these cases the divergence is not so huge at all. To sum up, about 40% of youth surveyed use the net for online telephony whereas one-third write blogs. Online dating, however, being one of the parents' worst nightmares does not appear to be as widespread as presumed before: 13% of younger children and 21% those of elders' dates regularly, consequently, an overwhelming majority of them never do so.

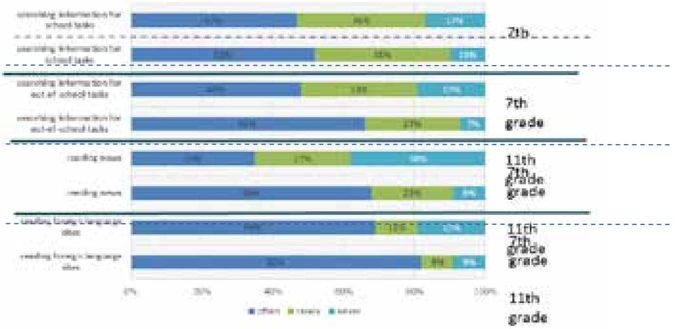


Figure 6: Internet use: obtaining information and knowledge (broken down by both age groups surveyed)

Browsing foreign language sites is relatively common in both age groups, where elder groups have some "advantage" over their younger fellows.

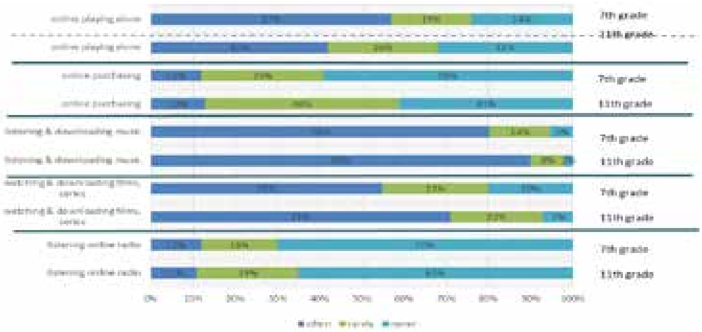


Figure 7: Internet use: entertainment and transaction (broken down by both age groups surveyed)

Watching and downloading of films and series is the second most popular online entertainment activity following listening to music: 71% of elders and 55% of younger people spend their time this way. By contrast, online shopping is not so common, though, frequent shopping does not necessarily mean daily orders. From this point of view, the fact that 12% of those aged between 13-15 and 13% of those elder often goes online for shopping cannot be regarded as a low percentage, particularly in light of the reality that nearly half of the elder ones sometimes, though rarely, order goods via the internet. Although 59% of children aged 13-15 and 41% of those elder than 15 never act this way. The least popular online entertainment activity among those listed (and the second least popular after online dating) is by all account the listening to online radio with which more than two-thirds of younger people never spend time.

B. SOCIAL NETWORKING SITES

The use of the internet among the younger people is equal to being active on community sites. News articles, information, serious and entertaining contents reaching out to them are obtained through sharing of friends' postings. Examining merely the time these people spend on networking sites clearly shows the importance of this activity for them. 36% of those aged 16-18 spend on community sites at least 3 hours even on weekdays, on weekends this ratio is as much as 56%.

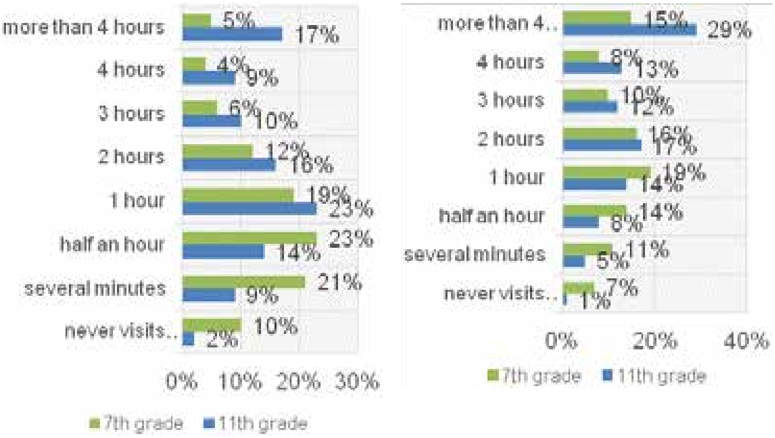


Figure 8: Time spent on community sites on average school as well as out-of-school days

As illustrated above, the age difference of some years between the two age groups surveyed affects the use of community sites to a greater extent. The frequency of use among 13-15 year-olds is much less intense; what's more, in this generation each tenth person questioned never visits such sites on weekdays, many of them spend purely half a minute or not more than half an hour on social networking sites. On out-of-school days the situation is, of course, different, though merely 15% of them are present on these sites for more than 4 hours.

Some years ago social networking sites corresponded to several giant service providers: users typically chose either iWiW or MySpace or Facebook. This online "choice" has altered remarkably nowadays. The prominent role of Facebook is obviously beyond doubts, however, sites offering diverse and distinct services have appeared and become more admired. Thus, it is no coincidence that you can barely find younger people in both age groups who have not signed up to any community site. Or, looking at the other side of the coin, merely 8% claimed not having registered to any service provider.

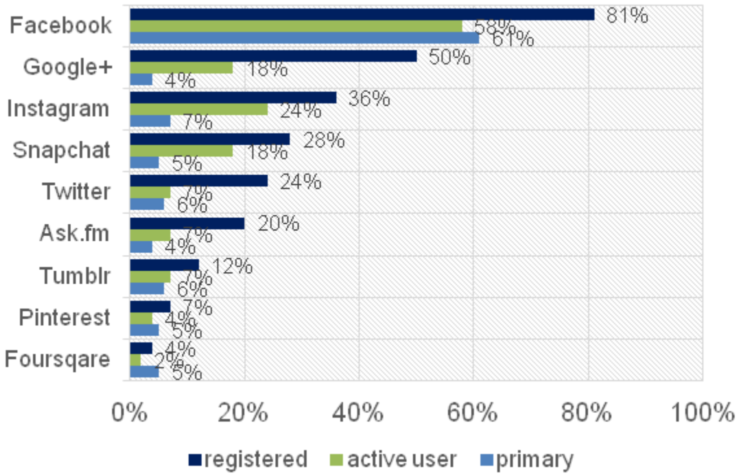


Figure 9: The attractiveness of various community sites (among 7th and 11th grade pupils)

Although 81% of younger people is signed up to Facebook, only 61% of them consider it being his primary community site. Though even less (58%) regard themselves active Facebook users. As for the registration, the second most attractive social networking site is the Google+ to which many people sign up presumably relating to the Gmail service or the Android system smartphone as the number of active users is much more low and very few people use it as a primary service. By contrast, 36% of those surveyed has registered to the Instagram and 24% of people questioned use it actively. Similar popularity can be discovered in case of Snapchat, however, with somewhat smaller attractiveness. Theoretically Twitter also has got many followers but the ratio of active users is even smaller like in case of Ask.fm.

The younger people are registered, on average, almost on three (2.8) community sites, 18% of them are real "omnivorous" having registered to five or more sites. Data shows that girls usually sign up to these sites in greater proportion. The difference is relatively high respecting the Instagram (registration rate is 43% of girls and 30% of boys) and the Tumblr (registration rate is 17% of girls and 9% of boys). The Google+ is, surprisingly, more popular among boys. Another decisive factor is the age: evidently the elders are present on community sites in greater percentage. The difference for the Facebook is 8 percentage point (77 and 85%), for Snapchat is even higher (21 and 34%) and relatively significant for Tumblr, too (9 and 16%).

C. NUMBER OF CONTACTS

It is not easy to obtain precise data on the number of contacts on community sites. In the course of the research we enquired after the number of contacts of the user questioned in relation to the social networking site visited by him primarily. The average has got 521 contacts on their main networking site whereas 15% has got 1.000 or more contacts. Pupils of 7th grade have got much less connections on average (326) than elders have (668). Besides – similarly to former trends –, girls have got more contacts on average on social sites as boys have (536 and 509).

	7th grade	**11th grade**
boys	310	638
girls	341	706

Figure 10: The average number of contacts among boys and girls (broken down by both age groups surveyed)

As shown in the table above, the difference between boys and girls appears in the breakdown based on age cohorts, too. Accordingly, girls of 11th grade have got, on average, the most contacts.

One of the most important handling method and the safest way to use and share of the numerous contacts if users create various friend groups (thus, for example, the entitlements for friends can be processed easier). However there are few people taking advantage of this opportunity: half of the younger people (52%) never apply such arrangements of contacts, 43% arranges only a circle of friends into groups and merely 4% use arrangement schemes relating to each contact l. The more contact a user has got, the more likely it is that he will organise them into groups. A clear distinction can be observed between those having the fewest contacts (less than 50) and all other groups.

D. ACTIVITY

As we have seen, a huge proportion of "today's young people" spend hours every daily surfing on community sites with this free time activity having an even more prominent place on weekends. But what exactly is covered by the term surfing on social networking sites? According to polls, on the one hand, there is no huge difference between younger and elder age cohorts regarding the use pattern; on the other hand, passive use patterns take the lead for popularity. Here, too, the trend observed concerning the use of mobile phones and internet is true that elders, practically, are more active in every use pattern, save the games. Nevertheless, in both age groups the highest percentage of people frequently watches and like the posts of their contacts. The majority of younger people (including adults) are consumers (or distributors) of contents (news articles, images, videos) created by others on networking sites. A rather smaller number of users produce their own creative or less creative contents.

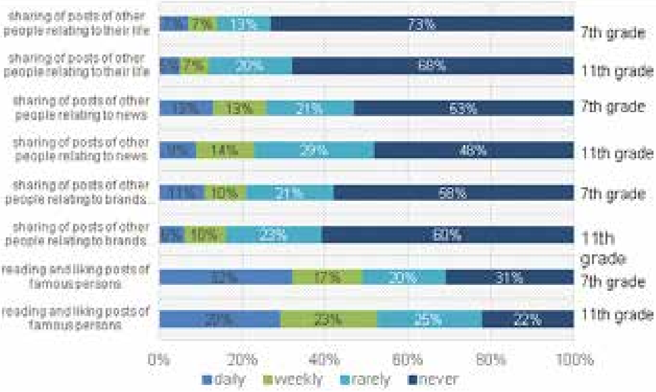


Figure 11: Activity on social networking sites I. (broken down by both age groups surveyed)

Almost one-third of those questioned usually reads posts of "famous people". "Managing" own profiles are less widespread: neither the updating of the status nor the uploading of images and videos are conducted frequently by the younger generation. In both cases nearly one-third of them deal with their own profiles weekly or more often. Activities respecting school duties are somewhat more frequent; in addition, 58% of the elders use community sites for this purpose on a weekly basis (as well).

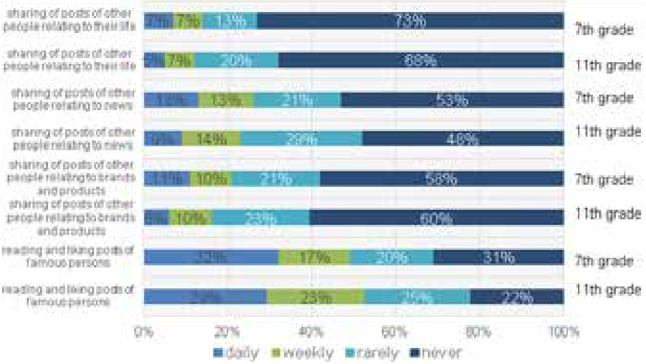


Figure 12: Activity on social networking sites II. (broken down by both age groups surveyed)

Sharing the posts of others is not popular at all, whether private comments, news or information on fashion brands.

Community sites are important forum for contacting with friends, too: 60% of 11th grade pupils communicate with friends several times a day and just 2% of them never use the site for this purpose. Younger people use this communication channel rarely, however, 42% of them chat with their friend more times a day.

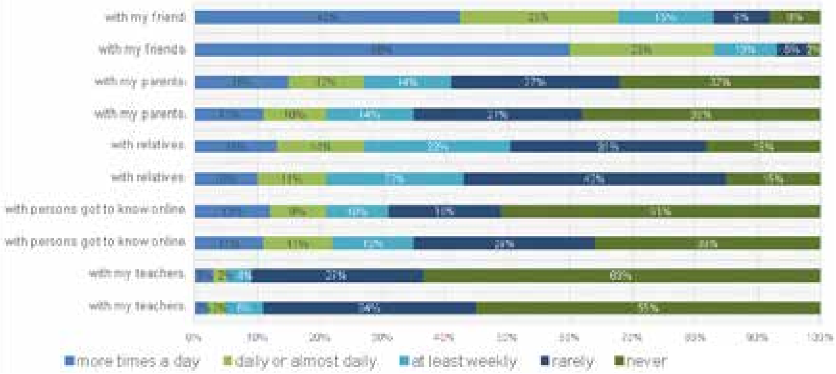


Figure 13: How often do you contact with the persons below on social networking sites? (broken down by both age groups surveyed)

The communication is not so vivid with other groups on the community site but plays an important role. The majority of younger people keep contact even with their parents to some extent through this channel. What's more, 15% and 11% of them, depending on age groups, evidently maintain continuous daily contact with parents on these sites. A rather smaller group of people keep contact also with their teachers; however, every tenth student uses this option at least on a weekly basis.

5. Children's rights online

The following rights or regulations can be directly enforced in an online environment in accordance with the Convention on the Rights of the Child (New York, 20 November 1989) and the promulgating Hungarian Act LXIV of 1991 (excerpts):

Article 1: For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

Article 3: In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.

Article 5: States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.

Article 8: States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name and family relations as recognized by law without unlawful interference. Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection, with a view to re-establishing speedily his or her identity.

Article 12: States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child. For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law.

Article 13: The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice. The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

a.) For respect of the rights or reputations of others; or *b.) For the protection of national security or of public order (order public), or of public health or morals.*

Article 16: No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks.[10]

Article 17: States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health.

To this end, States Parties shall:

a.) Encourage the mass media to disseminate information and material of social and cultural benefit to the child and in accordance with the spirit of article 29;

b.) Encourage international co-operation in the production, exchange and dissemination of such information and material from a diversity of cultural, national and international sources;

c.) Encourage the production and dissemination of children's books;

d.) Encourage the mass media to have particular regard to the linguistic needs of the child who belongs to a minority group or who is indigenous;

e.) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18.

Article 19: States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury

[10] The executive summary of the study 2012 of the French ombudsman (Children and screens: Growing up in a digital world) concludes that the spread of internet – and particularly portable devices becoming more and more cheaper and smaller – has been remarkably growing whilst the hazards affecting the children are well-known and there is no single strategy elaborated either by the legislation or the administration or professionals. While the negative impacts of excessive TV watching by little kids is indisputable the modern and fashionable child education includes the use of smaller iPads, iPods and smartphones offered by parents to their – even infant – children. As children are born into the digital world and for them it is hardly separable from the real world, you have to define the term of "digital privacy" with respect to Article 16 of the New York Convention of the Rights of the Child. From.: http://crin.org/enoc/ resources/infoDetail.asp?id=30126, 14-03-2013

or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child. Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement.
Article 29: States Parties agree that the education of the child shall be directed to:

> *a.) The development of the child's personality, talents and mental and physical abilities to their fullest potential;*
> *b.) The development of respect for human rights and fundamental freedoms, and for the principles enshrined in the Charter of the United Nations;*
> *c.) The development of respect for the child's parents, his or her own cultural identity, language and values, for the national values of the country in which the child is living, the country from which he or she may originate, and for civilizations different from his or her own;*
> *d.) The preparation of the child for responsible life in a free society, in the spirit of understanding, peace, tolerance, equality of sexes, and friendship among all peoples, ethnic, national and religious groups and persons of indigenous origin;*
> *e.) The development of respect for the natural environment.*

Article 31: States Parties recognize the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts.
Article 34: States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:

> *a.) The inducement or coercion of a child to engage in any unlawful sexual activity;*
> *b.) The exploitative use of children in prostitution or other unlawful sexual practices;*
> *c.) The exploitative use of children in pornographic performances and materials.*

In addition to the general children's rights we need to advocate the rights relating deliberately to data processing. The provisions of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Privacy Act) shall be applied to all data processing activities undertaken in Hungary and to data transfers from Hungary to foreign countries. In case of online data processing activities the exact location of this processing is not always clear (for instance the server is located in the US) but it is beyond doubt that if a Hungarian or a foreign child, the latter living in Hungary, gets into contact with an internet trade company offering its services in Hungarian language, the Hungarian law shall apply.

The data subject is the natural person on whom the personal data and information is directly collected or any natural person directly or indirectly identifiable by reference to these personal data. Concerning internet data processing activities the user usually consents to the processing of his personal data voluntarily, in the absence of external coercive forces – the cases of compulsory data processing are always regulated by law (as of 2014, for example, university admissions will be made exclusively electronically).

A special category of personal data are the sensitive (special) personal data; this includes, according to law, personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and personal data concerning sex life, personal data concerning health, pathological addictions, or criminal record. Special data may be processed, beyond legal authorization, when the data subject has given his consent in writing.

The statement of consent of minors over the age of sixteen – contrary to the preceding rules – shall be considered valid without the permission or subsequent approval of their legal representative.

Basic principles of data processing in the Privacy Act as follow:
Section 4

- Personal data may be processed only for specified and explicit purposes, where it is necessary for the exercising of certain rights and fulfilment of obligations. The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness.
- The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Person-

al data may be processed to the extent and for the duration necessary to achieve its purpose.

- In the course of data processing, the data in question shall be treated as personal as long as the data subject remains identifiable through it. The data subject shall - in particular - be considered identifiable if the data controller is in possession of the technical requirements which are necessary for identification.
- The accuracy and completeness, and – if deemed necessary in the light of the aim of processing – the up-to-dateness of the data must be provided for throughout the processing operation, and shall be kept in a way to permit identification of the data subject for no longer than is necessary for the purposes for which the data were recorded.

Data subjects are entitled to request for information, rectification and – in certain cases – erasure, objection and to refer the case to the NAIH or the court for remedy. The court is empowered to even award compensation to the data subject on grounds of infringement of his privacy rights.

Implementation of the data protection provisions

In case of children the general principle – children's interest is the most ultimate one – may, in theory, collide with the privacy rights of minors. This may take place particularly throughout the child welfare processes when regulations on mandatory data processing operations empower doctors, teachers or any other actor in the child welfare system to transfer even the most intimate data of minors in the course of an administrative procedure (e.g. in case of domestic violence or the pregnancy of a minor-aged mother).

General data protection principles can imply a different meaning in case of a minor becoming a data subject: at the supervision of fair data processing or the control of up-to-dateness of data the relevant age of the subject has to be taken into account indeed as well as one shall be cautious that data processing at younger age which might have been deemed as legitimate could entail different meanings at a later age in case of an elder child or a juvenile[11] (e.g. the case of photos taken for the purpose of medical research).

[11] Working document 1/2008 on the protection of children's personal data

By virtue of commenting online or misusing personal data civil rights violations or crimes can also take place – though they are typical instances where traditional ways of enforcement of rights cannot work. If the server supporting the social site is functioning from outside Hungary jurisdictional difficulties may arise. It may happen that the offender remains unknown or he is not punishable due to minor age.

Mediation

Among infringements during the use of internet (e.g. harassment, defamation) some conflict resolution process may be useful in case of violation of the inherent rights which may be invoked by the parties both in the course of pending procedures and prior to the commencement thereof. Mediation is a special method aimed at resolving conflicts by hiring a third neutral party as mediator. The mediator, in the framework of the process, helps to clarify the problem and to find a solution which is satisfactory for both parties. Mediation can also be an excellent means for the aggrieved party to discuss his injuries with the offender and to consider the pecuniary and non-pecuniary damages occurred. Basically there are two types of mediation at schools: the classical type, where the participants try to discuss their problems with the collaboration of a third neutral party and the other kind of restorative negotiation for compensation, when some infringement was committed and the perpetrator claims responsibility for rendering compensation. The classical school mediation is currently not regulated by law but there is no need for teachers and heads of institutions to have a separate regulatory framework in place for the purpose of incorporating the peaceful communication techniques and conflict resolution methods in their everyday work. Although the scheme of restorative conflict resolution was transposed into the disciplinary procedure by the legislator. Pursuant to Section 32 of Ministerial Decree 11/1994. (VI. 8.) MKM of the Functioning of Education Institutions as of 2008 there has been an opportunity to organise a consultation procedure in primary, secondary schools and student dormitories in the framework of which the events having led to the infringement may be explored and a solution may be sought to redress the injury. During the procedure participants may get to know the reasons having led to the breach, the damage caused, the interests of the aggrieved party, an opportunity opens up for compensation and reintegration as well as parties may find an appropriate solution for their problems. In the course of the consultation procedure the parties practically create a mutual plan to overcome the dispute. Should the offender confesses to his action, that is to say, claims responsibility for the damage caused by him he may be involved in restitution *in integrum*. The perpetrator discusses the means for restoration with the aggrieved party and an agreement will be concluded between them.

Finally there is an opportunity for mediation even in the criminal procedure. In accordance with the effective Criminal Code, if the juvenile offender shows repentance and has confessed to the misdemeanour offense till the indictment as well as has provided restitution by way of the means and to the extent accepted by the injured party within the framework of a mediation process then the imposing or implementation of the sentence may be suspended.

Studies show that compensation techniques can effectively help in preventing the development of future conflicts and the restoration of human relations – for example in a school class. Unfortunately it is a common experience that "perpetrators" committing bullying against their fellow classmate is often not one pupil but a gang of pupils or the whole class acting simultaneously or paralelly, but nonetheless mutually reinforcing each other.

6. Key topics

A. Age and maturity

A child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.[12] The Hungarian civil law reaffirms this rule[13] and adds that a minor shall be of limited capacity if he or she has reached the age of fourteen years and is not incompetent.

The position of the child can be examined both from a static and a dynamic perspective: the child is a person still being, both physically and mentally, immature though s/he is steadily progressing to adulthood.[14] In reality it is, however, not sure that a young adult, 19, and a child, 16, represent different levels of maturity. The fact that somebody is mature or immature for his/her age is influenced by several other factors for instance social, religious or ethnic affiliation, educational background, family background, real life experience to date (external effects), individual capabilities as well as the intention to study, read or to enhance the knowledge. The dichotomy maturity – immaturity presumes also relativity as we always relate to fellows.

In the Hungarian penal law the capacity for guilt begins at the age of 12 even though the legal capacity relating to legal age concerning civil law (the respective person may become a party to a contract or may make a legal statement) begins, however, at the age of 18. From that time on the parents' custody right ceases, marriage, employment, voting, travelling abroad without supervision, purchase of a vehicle or apartment, application for loan, consuming alcoholic drinks and smoking etc. become possible without parental consent. Prior to it (minority) most similar activities are either forbidden or bound to parental/guardian authorization. In most countries of the world people reach the legal age at 18 obtaining the opportunity for taking autonomous decisions expect Scotland (16), South Korea, British Columbia, New Brunswick, Newfoundland and Labrador, North-Western Territory, Nova Scotia, Nunavut, Yukon (Canada), Nebraska as well as Alabama (USA) (19), Indonesia and Japan (20).[15]

[12] Art. 1 of the UN Convention on the Rights of the Child, 20th November 1989

[13] Act V of 2013 on the Civil Code, 2:10

[14] Working document 1/2008 on the protection of children's personal data p.3.

[15] http://en.wik ipedia.org/wik i/Adult (04-11-2013)

Since children are still in development the exercise of their rights – including also the exercise of their data protection rights – must adapt to their physical and mental progress. Hence different jurisdictions make a clear distinction between the following age categories: under 12, between 14-18, between 12-16 and between 16-18.[16]

According to the Hungarian law – unless otherwise provided by specific legal provisions, including also the Privacy Act(!) – the legal statement of a minor with limited capacity shall not be deemed valid without the consent or subsequent approval of that person's legal representative. If and when minors of limited capacity become competent, they shall be entitled to make their own decisions concerning the validity of their pending legal statements.

Nonetheless minors of limited capacity shall, without the participation of their legal representatives, be entitled

a) to make legal statements of a personal nature for which they are authorized by legal regulation;

b) to conclude contracts of less importance aimed at satisfying their everyday needs;

c) to dispose of the earnings they acquire through work and undertake commitments up to the extent of their earnings;

d) to conclude contracts that only offer advantages and;

e) to donate a gift of common value.

Legal representatives shall be entitled to issue legal statements in the name of minors of limited capacity, except when the law requires the statement to be made by the minor with limited capacity himself/herself or when the statement concerns earnings acquired through work.

As regards any statement of a legal representative that effects the person or property of a minor, it shall be made with a view to the minor's opinion if he/she is of limited capacity.[17]

[16] Opinion 2/2009 (WP 160) of the Article 29 Working Party set up by the Directive 95/46/EC on the protection of children's personal data (adopted: 11th February 2009)

[17] Act V of 2013 on the Civil Code, 2:10-2:12

As far as children are concerned, one always has to take into consideration that the fundamental right of data protection refers to the child rather than his legal representatives acting merely in their behalf. A possible factor to be examined respecting the enforcement of rights is the opportunity of consenting to the data processing. The concept of parental consent takes into account the ultimate interest of the child and in a certain sense – at least dogmatically – is contrary to the philosophy of informational self-determination.[18] The Hungarian law requires the opinion of the minor child (below the age of 14) following that the parallel consent of both the child and his legal representative is needed (between the age of 14-16) and finally, regarding an elder minor, the exclusive consent of the child is sufficient (above the age of 16). Consequently, pursuant to the valid (new) Hungarian data protection regulations, in Hungary the statement of consent of minors over the age of 16 shall be considered valid without the permission or subsequent approval of their legal representative.[19] According to the new Data Protection Regulation in particular cases a minor, below the age of 13, may also make a valid legal statement without parental consent.

Besides the consent the right of participation is also a significant factor. Even though it is not sure that authorities are inclined to follow this rule that his/her wishes shall be taken into account during the whole process.[20] As, however, the child becomes capable of exercising his right of participation it may result in a mutual or even individual decision making. For instance in cases relating to the use of photos taken of them – whether the parent is entitled to disclose the picture of his child on a social site if the latter objects to it and finds it rather embarrassing. (Nowadays children are still not born when their parents already tend to disclose information on them – ultrasound images are being uploaded on 25% of fetus by parents –, after their birth they becomes stars of additional photos, videos and Facebook sites, a huge part of babies even receive an email address, four fifths of minors below the age of 2 living in developed Western countries already have digital footsteps.[21]).

An additional topic is the right of access to personal data which can be exercised either by the legal representative of the child or the representative and the child together, however, the child can exercise this right even against his legal representative (e.g. the teenager may ask for his general practitioner (GP) not to pass on medical documents –

[18] Children's Privacy On Line: The Role of Parental Consent, Working Paper of the IWGDPT, 26 March 2002

[19] Section 6(3) of the Act CXII of 2011 on Informational Self-determination and Freedom of Information (In- fotv.).

[20] Recommendation R(97)5 of the Council of Europe Committee of Ministers on the protection of medical data – 13th February 1997, points 5.5. and 6.3.

[21] http://index.hu/tech/2013/04/22/g yerekek _es_az _internet/, 05-15-2013

though in this case the GP may have discretionary power). In the UK teenagers above the age of 12 are entitled to exercise their right of access individually; in numerous countries the right of access of legal representatives to personal (medical) data of their teen daughters is restricted in case of abortion.[22]

Examination of the age is essential in the event of websites where an age limit is set for registration. It is well known that kids, during the registration, provide true data only if this does not prevent them from further use. In the course of TV broadcasting the age marks and parental oversight together could be adequate means in developing appropriate TV watching habits of children but in the online environment, unluckily, the harmful contents to kids cannot be filtered out simply since web contents are not as accurately ranked as TV programmes are. The only restrictions we can explore in the web are sites offering pornographic or "adult" contents for visitors above the age of 18. Videos, images and films depicting violence are usually not protected. Moreover the access to a pornographic site is also too simple for a minor because these sites generally offer two options: I am over/below the age of 18. Kids click on the button "above 18" and get easily to images, videos and films. Visiting other pages might be subject to a registration containing an age limit. In this case a precondition to proceed is – youngs realize this quickly – to provide a date of birth by which the registering person is considered to have completed the age of 18. The discernment of the minor is to be assessed as immature because s/he is willing, in exchange for alleged advantages, to disclose personal information on him/her incorrectly and does not think about the potential risk that by doing so s/he paves the way for abuses and unfair data processings.[23] Simply s/he is willing to try out the services of which s/he has been informed at school or from his/her friends – in vain there is a theoretical age limit of 13 e.g. on Facebook, according to the figures of Consumer Reports 5 millions of registered users are below 10.[24]

Finally the issue of liability with regard to compensation for damages, caused for instance by kids, arises. Pursuant to a judgement of the German Federal Supreme Court from November 2012 the parents are not to be blamed for the torrenting of their child of 13 (and for other offences committed on the web) provided that they have earlier properly informed the minor on the general terms and rules of internet use and basic information.[25]

[22] Opinion 2/2009 (WP 160) of the Article 29 Working Party set up by the Directive 95/46/EC on the protection of children's personal data (adopted: 11th February 2009)

[23] Children's Privacy On Line: The Role of Parental Consent, Working Paper of the IWGDPT, 26 March 2002

[24] http://index.hu/tech/2013/04/22/gyerekek_es_az_internet/,15-05-2013

[25] Parents are not liable for torrenting of their children from.: http://index.hu/tech/2012/11/23/a_szulo_ nem_felelos_a_gyerek_torrentezeseert/, 08-03-2013

B. Anonymity – easier with a mask?

Identity associates with the perception of the "complete ego" through roles, behaviour patterns and values. Personality development is a result of socialization and evolves in the course of human interactions. According to the Latin proverb *"Nomen est omen*", that is to say, everybody carries his destiny in his name. On the web users tend to keep a low profile by using nick- and pseudonyms posting comments via single use email addresses whilst they are terrified about that someone "recognizes" them and obtains their personal data whereas they voluntarily disclose these data on social sites to the whole world.[26]

Online identity or online personality, however, is a group/community identity created by internet users which is used in networks and on websites. Lot of users, concealing their real names, use pseudonyms so as to revealing their true identity as much as they want. Online identity, implying in most cases the anonymity as well, raises several questions in particular concerning the quality of personal relations established in the virtual world. When an online anonymous individual gets into interaction in a social sphere s/he holds a mask covering his personality. Anonymously anyone can communicate anything to the world which probably fails to correspond to reality (including age, sex, address, username and so on). In this event the user hides behind a false mask that tells a lot about his fears and lack of self esteem.

For the purpose of preventing internet abuses and criminal offences the termination of anonymity shows an increasing trend. In South Korea[27], where the internet penetration rate is the best in the world, the rule that anonymity in case of websites counting more than 100.000 visitors a day ceases and everybody must use his real name when commenting has prevailed for a year. In China[28] this habit has appeared on major websites but this idea also came up in France[29], Brasil[30] and in several US states[31].

The most important argument in terminating anonymity is that if the user takes the risk for all of his comments and clicks with his name and, as a result, he may be subject to an impeachment he transforms from a troll to a civilized human being. Although a more telling business argument is that by abandoning anonymity, it becomes much

[26] http://index.hu/tech/2010/08/10/a_nev_a_vegzet_az_interneten/, 10-04-2013
[27] http://w ww.koreatimes.co.kr/w ww/news/biz/2008/10/123_32121.html, 18-04-2013
[28] http://index.hu/tech/blog/2010/05/05/peking_megszuntetne_a_netes_anonimitast/, 18-04-2013
[29] http://w ww.v3.co.uk/v3-uk/news/1944812/french-outlaw-anonymous-web-posting, 18-04-2013
[30] http://realtimesociety.blogspot.hu/2006/11/proposal-to-control-net-access.html,18-04-2013
[31] http://betanews.com/2008/03/11/anonymous-web-posting-may-become-illegal-in-kentucky/, 18-04-2013

easier to gather information from users and to send them targeted advertisements based on their browsing habits.

Disadvantages of real names to be used mandatorily are obvious: it could lead to the termination of intimate anonymous blogs and everybody would come off badly who has good cause for insisting to remain anonymous, let's say, because he is interested in a hobby or belongs to a minority (e.g. homosexual) the disclosure of which could be harmful to him. Anonymity could also provide safety for instance in the event of identity theft or other forms of abuse. What's more there are signs that the termination of anonymity is fostered by political and business interests rather than the desire for improvement.[32]

In view of this the Council of Europe's 'Internet Strategy 2012-15' sticks to the principle declared by the Committee of Ministers in 2003 stating that internet users have the right to decide, against the online surveillance and for the sake of freedom of expression, whether or not they wish to reveal their identity.[33]

C. Personal distortion

(Author of this subchapter: Dr. Nóra Belső M.D. psychiatrist)

"I am wondering how I could "discourage" him from studying, from showing interest in the everyday life of the family, how come that he feels no shame for failing his school exams: only the internet and some strategic game and the players thereof, his virtual friends, he realizes them only. If I enquire after him and his businesses and I wish to help him I get a rejection. I am in despair...
I guess your son has become an internet addict over the years. Based on your letter I cannot give reasons but the divorce of parents, university studies of mummy and his introverted nature might all have induced this perception of isolation that directed him towards virtual relations. I think the relation between the minor and the PC should be settled – and not exclusively by limiting the time spent before the screen!"

(Prof. Dr. Jenő Ranschburg: The agonies of puberty, questions and answers)[34]

[32] http://index.hu/tech/2010/08/10/a_nev_a_vegzet_az_interneten, 10-04-2013
[33] Principle 7of Anonymity of the Declaration of the Committee of Ministers on freedom of communication on the Internet: "In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and cooperating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police."
[34] Saxum Publishing 2011, p. 107.

Since the 90's relatively new topics have emerged in the bibliography of psychological and psychiatric studies including the behavioural addictions and the abnormally extensive PC usage, the pathological internet addiction and lately the pathological usage of social media and the related addictions. With the IT technologies and web presence developing such psychological problems and pathological behavioural patterns have increasingly been inspected by experts. This phenomenon affects the entire population – particularly children – hence the relating bibliography embraces paediatric journals, family-community-sociological periodicals and studies analysing psychiatric as well as neurological brain imaging examinations.

Of course the internet usage encompasses advantages seeing that various activities needed much resources and extensive work before, (gathering information, research, data collection, organisation, etc.) thus saving time for the user. Although the pathological changes of behaviour, the improper usage can cause detrimental effects, typically psychological disorders.

Recent psychological literature analyses the impact of the facebook-phenomenon on human relations, the personality of individuals, as well as the changing operation and structure of communities. Modern functional brain imaging techniques are already being used by experts to discover how different contents and different online behaviours influence the various segments of human brain. These psycho-neuro-cognitive examinations serve as evidence for previous practical observations, that is to say, the use of internet, what's more that of the social media can cause, from a medical aspect, a real addiction to people liable to it, indeed. We can call for the attention, in this regard, to examinations aimed at analysing the development and neurological structure of the human brain using the net and seek answer for the question: will anatomy and/or functionality of the neuron network in the brains of youth actively using the web differ from that of the preceding generation? One thing is certain: younger and younger minors are inclined to use the net and the extensive use of tablets and smart phones are tending to supersede obsolete PCs and semi-smart phones. Consequently the development of moving, speech and communication could be neglected which may cause health risks as well.

Numerous medical expert groups are examining the relationship between the time spent before the PC and the evolution, progression and healing process of different diseases (abnormal obesity, sedentary life, malnutrition, lack of open air, ophthalmology implications, smoking, epilepsy etc.), that clearly show the medical significance of the topic.

From a psychological, psychiatric point of view several factors should be considered:

1. Time spent with internet, social media (online surfing; browsing; continuous searching for, and reading of, particular contents; posting, chat etc.)
2. Internet games (abnormal passion for playing, gamblings, etc.)
3. Psychological impacts via online available social media (retrograde effects)

Points 1 and 2 refer to addictional implications whereas point 3 summarizes the (psychological and psychiatric) impacts of social media on the individual. All three factors have a remarkable impact on the relation between the individual and the environment and, in the framework of the evolving interactive processes; the relation of the individual to himself and to the world completely alters. Should this process become pathologic, social damages, psychological and psychiatric disorders may occur.

Forms of appearance are as follows:

- Personality distortion (with special regard to hiding behind the mask of anonymity)
- Abnormal and addictional behaviours, evolution of online deviances
- Evolution of addictology or abnormal behavioural forms (behavioural addiction)
- Other interaction with psychological, psychiatric symptoms, comorbidity (disease association).

The development of the features and functioning of the personality is a life-long interactive process which is genetically determined though external factors (patterns, impacts, cognitive skills, experiences etc.) could also be decisive. Numerous studies inspected the personal distortion effects as well as those personal attitudes that are likely to induce abnormal and pathological behavioural patterns with regard to the internet use. Experts share the view that negative impacts of the internet may evolve, with a higher probability, among individuals with an immature personality (minors) or who show personal disorder.

As a result minors are more endangered at every age and life situation since their mental and personality development could become malfunctional if they fail to acquire the command of proper internet usage. The study process consists of multiple elements: the behaviour of the parent and/or the sibling, fellow children (sample tracking) and the active study process (from parents, teachers). Consequently the habits of parents and other people concerning the internet usage are determining. In the childhood, when the development of personality is still in progress, the abnormal development of the personality (instead of the phenomenon of personality distortion) can be detected. It brings about intermediary negative effects such as disorders relating to studying and school advancement, the damage and disorders of interpersonal relations and finally either a personal distortion or an abnormally functioning personality will be emerging (the latter means pathological features in personality). Upon the individual becoming an adult he will be experiencing malfunctions therefore additional signs of distortion could be anticipated both in the social integration and operation as well as the internal relations inside the person concerned.

Direct aspects of internet usage distorting personality:

- time spent before the PC (time schedule, negligence of priorities, decrease in other performances)
- change of friend contacts (net friends instead of ‘flesh-and-blood’ relations), lose of ‘real’ friends
- virtual space and time (divergence from the experiences and challenges of real life as well as from the reality)
- incapableness of perceiving certain contents (roughness, sex) – consequences may include abnormal adaptation, deficient fixation, subsequent pathological reactions, human relation disorders
- change of communication (poorer quality): deterioration of speaking skills, changing metacommunication, declination in the recognition of non-verbal gestures, deterioration of emotional expressiveness and the realization of emotions
- consequently uncertainty, anxiety and fears may appear in real environment that result in social withdrawal and isolation (simultaneously misleading ‘strengthening’ could arise in the virtual or anonymous environment – for instance by harsh tone, aggressiveness)

What advice can we give with a view to defeat distorting effects?

- Internet habits of parents and other persons shall also be considered
- Time limits shall be set for the respective user contents
- Rules and opportunities shall be explained to minors in compliance with their maturity

- They shall be warned against possible risks
- Positive impetus and alternative programs (the internet is not a babysitter!) shall be offered in order to 'drive' them from the PCs (excursions, sport, extra courses etc.)
- In more serious cases individual or family psychotherapy

The pathological or addictive behaviours are closely related with the above discussed online deviancies and several key issues. These psychological effects, affecting children online, give rise to psychological reactions (fear, anxiety, remorse, desires etc.) inside them. Although it shall be emphasized that minors could also become irritating and can show deviant behaviour. It is about a two-way 'opportunity'. Internet commenting, telling, annoyance, encompassment could cause severe bruise to the victim. As a result, the withdrawal, the isolation as well as the putative or real fear from valued relations and communities could intensify along with the increase of the anxiety which can drive the children towards online positive relations and friends. The more deficient (in terms of emotions, safety and confidence) the minor's life is, the more serious the negative impacts affecting the minors become. Due care shall therefore be taken to the two- way trust parent-child relationship since this could be the only way in which the child is likely to share all detrimental effects (slight ones are expected to remain unnoticed even in a friendly contact). Children have to be educated on these perils stressing these risks are, unluckily, not single cases and if such were to happen to him he could not be blamed for it *('It is not your fault!').*

The risk of the evolution of an addictological disease relating to the internet (behavioural addiction) can be anticipated mainly at those persons who are inclined to it. The inclination is brought about by the family anamnesis (abnormal gambling passion among first-degree relatives, drug addiction, and other psychiatric problems), the structure and functioning of the family (divorced parents, insults inside the family, abnormal patterns, emotional negligence, and lack of impetus) as well as the individual sensitiveness (temperament and the features of the personality, interest). The term 'addiction' refers to the pathological passion, desire, as well as the physical and psychical symptoms arising from the withdrawal of the substance the person has become dependent on and the long-term changes in behaviour. Addictions and passions can be categorized by their objects. As a consequence the individual can be an internet addict and besides may be addicted to particular contents or to certain devices' (addiction to mobile phones, to tablets etc.).

One can get accustomed to social media as well. Surveys confirm that the social site-addiction is a situation which can be easily defined and activates the brain's reward system which has led to its widespread distribution. In 2012 a Norwegian research group published its findings obtained by means of the Bergen Facebook Addiction Scale (BFAS) which had been created by them.[35] By introducing the scale in Hungary this simple self-observation method would be easily available.

Presumably minors facing such problems may encounter other addictions or abnormal behaviours in their adulthood moreover the chance of the occurrence of life-threatening anxiety and depression may rise.

In these cases the education is very important and also the approach of professionals (psychologist, addictologist), what's more, the running of self-help associations and the personal experiences of people struggling with the same problems would be highly advisable.

Interactions and comorbidity may occur with almost any psychiatric disease. In addition to abnormal internet usage, abnormal anxiety may occur more frequently which can lead to diseases (generalized anxiety disorder, social phobia, panic disorder, mixed anxiety and depressive disorder) after a sufficiently long time including also mood changes and mood disorder. There are still no available data on the frequency of comorbid depression but it is likely that the combined incidence rate is very high. Co-occurrence with certain hidden disorders also shows high rates, as in these conditions it is much easier to hide behind the mask of anonymity "to prevail" (personality disorders, sociopathies, anorexia and sexual identity disorders etc.) In such cases, where the medical history or family anamnesis is avail- able, the psychiatrical consultation is inevitable.

Summing up the psychological-psychiatric examinations we can conclude the conscious and purposeful use of the internet can avert numerous psychiatric and social dam- ages. The abnormal use of the internet may produce severe mental disturbances but existing psychiatric disorders can also cause and sustain the problematic behaviour of the user. Most effects induce the development of fear and anxiety, which form the basis for many psychologicalproblems.

The abnormal and harmful operations influence interactively, particularly as regards the development of children's personality; in this process the patterns as well as the studying process and its quality are significant. For these reasons it is of utmost importance to study the topic in a complex way and to disseminate the recommendations and contact details of protective authorities, organizations and self-help groups facing with similar problems. It is also important to draw the attention to the fact that in case of severe

[35] Cecilie Schou Andreassen: Developement of a facebook addiction scale1, 2, 2012, 110, 2, 501-517. © Psychological Reports 2012 Department of Psychosocial Science University of Bergen, The Bergen Clinics Foundation, Norway

mental disorders (addiction, social isolation, and threatening behaviour) it is inevitable to seek for professional help![36]

D. Public spaces – unknown friends

From among the internet features – because of its rapid expansion and impact on privacy – the role of social networks evolving as virtual communities shall be emphasized. By virtue of internet-based social networks strangers and acquaintances get in touch with each other via a common feature with the objective of building connections or providing services. Basic criteria of an internet-based social network[37]:

- users can create a public or semi-public profile site for themselves,
- the contact among users is secured,
- users can get to know the social network of their own and their friends.

The first networking site of this kind has been operating, as of 1995, in the US named classmates.com which aims at collecting classmates, colleagues and fellow soldiers. The first site where users were capable of creating profile sites and could review their contacts was the SixDegrees in 1997 (the name refers to the theory of 'Six degrees of separation' according to which we can get linked with anyone on Earth by inserting up to five persons, as intermediaries, between us); in 2000 the site was, however, shut down due to financial loss. From 2003 on such social sites emerge worldwide, however, currently the most popular among them is definitely the Facebook, from the 4th of October 2012 it has got altogether 1 billion registered users. The reported number of users today is 1.71 billion (www.statista.com) · The use of Facebook is free; one can join easily without invitation via a simple registration. Users create a personal profile, can get in touch with acquaintances, groups and fan clubs, can exchange messages and organize events, and can share news, information, websites and videos through the message wall. Profiles of other people in your net- work are shown in detail whilst users belonging to other communities are hidden; this, however, depends on the users' settings as well. In August 2011 the

[36] "We define social network sites as web- based services that allow individuals to (1) construct a public or semi-public profile within a bounded system (2) articulate a list of other users with whom they share a connection and (3) view and traverse their list of connections and those made by others within the system". In Boyd, Danah M. and Ellison, Nicole B: Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, Publisher: Morgan Kaufmann Publishers, 2008, Volume 13, Issue 1, 210. o.

[37] http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/-, 11-01-2014

Facebook improved its data protection scheme (by introducing Activity Log that makes it easy to see the things for users they have posted on and control the privacy of that content, for example to remove tags of photos). The data protection scheme has ever since been developed, which changes were triggered by feedback from users and regulators. In 2012 Facebook further moved towards inline tools, introduced Privacy Shortcuts and a new Request and Removal Tool for managing multiple photos users are tagged in. In 2013 Facebook changed its default privacy setting for teens aged 13 to 17 who join Facebook, the initial privacy choice of their first post will be set to "Friends" instead of "Friends of Friends". They also enabled teens to post publicly for status updates, photos, check-ins and other types of content they share. Moreover, teens will also be able to opt-in to Facebook's 'Follow' feature. On 30th January 2015 the terms of use was amended again as a result of which numerous data protection authorities (hereafter: DPA) launched investigations. In the process initiated by the Belgian DPA the court procedure led to a conviction of Facebook because the service provider followed up the internet using habits of users unlawfully. If somebody (either an internet user without registration to the networking site) got to a website where a supplementary (e.g. "like" or "share" Facebook-related button) had been placed then the Facebook places, without prior notice, a small identification application (a so-called DATR cookie) onto the PC of the user by means of which it will be able to track down the browsing habits, that is to say, to observe the user's behaviour. In Germany the Düsseldorf Provincial Court (Landgericht Düsseldorf) fined a large fashion company for 250.000 EUR (approximately 80 million HUF and, as alternative punishment, 6 months' imprisonment of the CEO of the company) in 2016 since personal data of customers, from the website of a retail clothes shop associated with them, were forwarded, without prior notice, to the company by pushing the Facebook "like" button.[38]

The publicity of profiles of social sites is dependant on service providers (SPs); it ranges from total publicity through publicity for registered users only as far as situations where the limits can be set separately. The 'user existence' begins with the provision of minimal scope of the personal data including: name, age, place of residence, interests, an informal introduction and any other which the individual considers as being important on himself, usually it is also expected to upload a photo. The formal legality of data processing cannot be challenged; however, a mass publication of millions of personal data may lead to a vulnerable privacy in relation to the global youth on the one hand.

On the other hand it paves the way towards online forms of abuses (sexting, grooming, and online bullying). An awareness-raising film clip from the USA shows

[38] http://www.reuters.com/article/us-facebook-like-germany-idUSKCN0WB1OI, 11-03-2016

persuasively how easy teenager girls are dating, deceiving their parents and getting into potentially perilous situations, with “unknown friends” in spite of having discussed over the threats and risks thereof in the family earlier. (https://www.youtube.com/watch?v=-6jMhMVEjEQg)

European surveys revealed that social networking is particularly popular among the young: 38% of minors between 9-12, whilst 76% of teenagers between 13-16 are members of a network community (one third of minors between 9-16 is dedicated to Facebook – a sign clearly showing the frivolity of the age limit of 13) and young users tend to become even incautious: they render access to their personal data for strangers in an ever growing rate (even to place of residence, phone number). In 2014 the number of individuals – both children and adults – chatting online further increased as a primary consequence of spreading of smartphones. 95% of younger people aged 14-19 use texting while 74% sound chat apps. 96% of them visit Facebook and 93% of them browse YouTube at least on a weekly basis (this ratio is for parents – aged 40-49 – 71% and 59%).[39]

Meanwhile two-thirds of Hungarian children aged 9-16 possess an own profile at least on one community site; rather girls and elder teenagers visit regularly these sites. One-third of kids have 50-100 contacts whereas one-third possesses 100-300 contacts and 13% have even more. 55% of all kids surveyed claimed having a public (i.e. accessible to everyone) profile on community sites. 22% made their profiles partially public whereas merely 16% applied privacy settings, as a result, only their friends having access to their profiles.[40]

Personal data circulating in the cyberspace without any control can be exploited regardless of the data subject’s original intentions or his will. Digital dossiers can be produced any time about the data subject without his knowledge *(digital dossiers aggression)*[41] listing e.g. his hobbies or the names of his girlfriends. (According to recent news from New York Police Department the number of murders decreased due to a social media observation project launched by the police in October 2012 where the actions of teenager gang members were tracked in order to crack down on them in time[42]). The data subject loses control over his information collected from profiles, that is to say, these information tend to pursue a life in full independence. Considering that the data content of diverse

[39] EU Kids Online - Social Networking, Age and Privacy; Researches by Sonia Livingstone, Kjartan Ólafsson and Elisabeth Staksrud in.: http://eprints.lse.ac.uk /35849/ 13-06-2013

[40] Bence Ságvári: On the EU survey of Kids Online in Hungary in.: w w w2.lse.ac.uk/.../EUKidsOnline/.../Hun-gary%20webpage.pdf, 07-03-2013

[41] G. HOGBEN (ENISA), ENISA Position Paper No.1 Security Issues and Recommendations for Online Social Networks, October 2007, p. 8.

[42] http://index.hu/tech/2013/02/26/csokken_a _bunozes_a_facebook_miatt/, 26-02-2013

social networking sites can be simply linked, it becomes easy to understand what extent of potential hazards (control of a would-be employer, blackmail etc.) these social sites can bring about without proper security settings.

Images uploaded by users expand remarkably, not only the so called profile pictures but also photos uploaded to albums and shared with others. That could be perilous since conclusions (secondary information) can be drawn from them relating to the personality of the user, his social contacts and his pecuniary situation. Hence annoyance may arise in virtue of a neutral image by removed from its habitual environment. The biggest danger is that images and the relating secondary information provided by users effortlessly enable the linking of profiles and data stored in SPs' systems (let's say linking a specified social site's profile with the information of an allegedly anonymous or pseudonymous dating website).

Most social sites enable users to attach supplementary information to uploaded images with the objective to, for instance, name the people depicted on the image, specify the link granting direct access to their profiles or add e-mail addresses etc. (the so-called tagging). This also facilitates the linking of several profiles. A quite sensitive situation in this regard is when the person affected is not a registered user of the social networking site. In such cases SPs are inclined to send 'notifications' to these non-users advising him on his the tagging by the user and invites him to join – as the individual tagged cannot do anything more without a registration except for viewing the image. According to the view of the NAIH this practice, in pursuant to the effective legal provisions, qualifies as being a spam sending on the part of the SP while, in the absence of consent, abuse of personal data on the part of the user. So the difficulty is that users have the opportunity, in relation to their own personal data, to choose between the information they wish to disclose and those which they don't, whilst in case of tagging information published by others on us the right to informational self-determination is fairly limited, if any (the privacy policies of numerous SPs do not contain regulations in this regard).

The issue of (data) security cannot be ignored either: several abuses occur when 'creating' profile sites on behalf of another party, uploading (even compromising, unpleasant) photos or other information. The point of the ECJ judgement in the Lindqvist case[43] was that even personal data of people participating in ecclesiastic charity work cannot be disclosed bona fide on a website without their consent. What's more people usually forget that all personal data once disclosed online can never be deleted from the web once and for all. Particularly it is the case with respect to the above-mentioned secondary data col-

[43] C-101/01 Lindqvist [2003] ECR I-12971

lecting. The ultimate erasure of full profiles is difficult, what's more often impossible since the user profile can be deleted, usually, easily secondary contents cannot be (entirely) erased (images, comments or messages present in others' profiles etc.). There are already existing automatic programmes which would enable the complete deletion, the so-called virtual suicide, though the use of these softwares are blocked or restricted by most SPs.

Usually it is not unambiguous what a deletion practically means: the effective and prompt erasure or only making the required content inaccessible and data retention for a definitive time period. For example at Facebook users can deactivate their account or they can ask for full deletion. When the user decides to delete the profile, it immediately becomes inaccessible for others. For 14 days the account is deactivated, during this period of time the content is hidden from the site and the user can cancel deletion - a significant percentage of users in fact do cancel deletion. If the user does not cancel the deletion, the deletion of the account begins. Most deletions can be completed within a day, but some heavily used accounts may require more time. Facebook has a statutory requirement to delete all personal data held in an account within 40 days, with the exception of data that a user may have contributed to a group.

The difficulties reaffirm and verify the apprehension that the internet does not forget; data shared earlier cannot be erased any more - ultimately the user loses his rights to dispose over his personal data.

We shall also bear in mind that all data about us being disclosed online can be obtained by data miners as well. The easiest method is the collection of email addresses which may result in filling our mailbox with spam messages. The acquaintances of users can be effortlessly tracked down via their contact network thus making it possible to attain personal data from anyone. Hungarian users seem unwilling to take the relating data protection concerns seriously that is clearly indicated by the huge increase of number of users on a daily basis as well as the addiction-like alignment of juvenile users to Facebook (a permanent topic in Hungarian teenager users' conversations *'how long I have been active on Facebook' and 'what exciting information I have discovered about my friends there').*

E. Harmful contents

Getting in touch with contents which are disclosed online and which cannot be considered as being explicitly illegal but, however, according to the assessments of the general public and/or experts (teachers, psychologists) may have detrimental effects on the physical/mental development of minors – carried out either by the child or the supervising adult[44] - could be extremely perilous. Typical cases include sites fostering violent or pornographic behaviours, committing suicide, drug consumption or abnormal nutrition.[45]

The president of the Hungarian Nurses' Association lodged a petition with the Fundamental Rights Commissioner complaining about a radio programme, dealing with the sexual education of younger people, which revealed that the first hit in the Google search engine for the word "*sexual education*" boasts a demonstration link of an incestuous, homo- and heterosexual video stream which, however, was "meant for fun". The Fundamental Rights Commissioner, lacking official powers to act, was able to provide information on the opportunity of reporting illegal/adverse online contents on the Internet Hotline site of the National Media and Infocommunications Authority.

Major problem is that the access to harmful contents is not always subject to a deliberate behaviour, i.e. the user may open such webpages accidentally or even despite his will (inserting a neutral key term for example "girls" and the hits appear without selection, additionally we can discover cheap pornographic e-books even in an online bookshop that seems, at first sight, to be reliable, however certain sexual topics are illustrated in the Wikipedia surprisingly fully). Through web browsing we can get to harmful sites in a similarly easy way. According to the comparative figures of the 2014 EU Kids Online survey 20% of European children aged 11-16 using the net may face sites calling for hatred, 13% for anorexia, 11% for self-destruction; 12% of them are exposed to cyberbullying (the negative trend compared to the data from 2010 is significant).

[44] In case of the starved-to-death baby of Agárd "investigators were trying to find out, by analysing a PC found on the spot, with whom the parents had been keeping contact and what kind of internet pages they had been visiting. Police officers were also examining whether or not the parents had been keeping contacts with anybody who might have given them instructions in relation to the starvation of the minor." In.: http://index.hu/belfold/2013/04/22/vizsgaljak _az _agardi_szulok _beszamithatosagat/, 22-04-2013

[45] A recently completed survey involving 800 students revealed that children, wishing to study nutrition facts, prefer the internet as a reliable source whilst other minors who put a great value on the healthy nutrition consult rather their family members in this regard in.: Nikoletta BÖRÖNDI-FÜLÖP: Inspecting the nutrition habits of youth in the South Transdanubian region, 2012 PhD thesis, phd.ke.hu/fajlok /1348561429-borondi-fulop_n_ _ tezisek.pdf, 01-03-2013

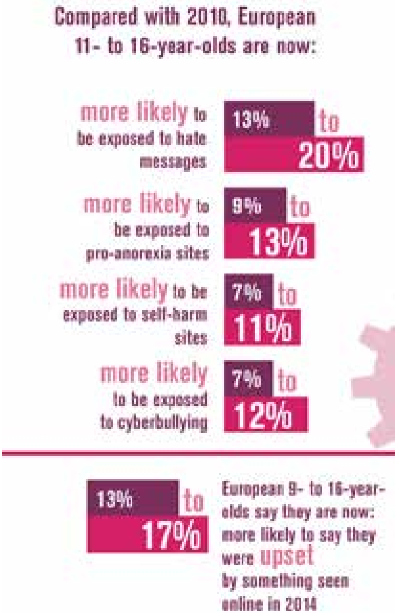


Figure 14: https://lsedesignunit.com/EUKidsOnline/ 17.02.2016.

What to do? On the one hand minors shall be prepared for the existence of such sites. In the event of an accidental encounter s/he should leave the site immediately instead of inspecting it thoroughly. In other cases s/he should be able to judge its content (e.g. there are several unscientific and deceptive articles circulating in the web concerning nutrition, physical/mental health as well). It is the best if the child reveals his negative experiences later voluntarily to his parents or to a reliable adult (a prerequisite for it is, however, the confidence that the child would not fear of a potential punishment).

A second solution could be a technical one: content filtering softwares can repel the unwanted occurrence of such sites. Multiple filtering methods can be used with a view to select between adult- and child-related contents:

- the real time filtering analyses of the target site by means of text or image recognition algorithms and blocks the access to pages which contains the features included into the filter;
- other filters block webpages put onto “black lists” or servers or only enable the browsing of websites put onto “white lists” thus constituting a safe children playing field;

- other filters apply the “labelling method”, that is to say, they use labels placed by SPs, users or undertakings – similarly to age limit labels of films.

Unreasonable filtering and overblocking bring more disadvantages. In all cases the intrusive (“push-type”) pop-up windows shall be banned in comparison to on-demand (“pull-type”) sites similar to unsolicited spams which destruct email correspondence. Although the unwanted browsing windows also include harmless ones (e.g. ads) this aggressive technology enables the redirection of the unsuspicious user to destructive websites which he did not wish to visit and the attempts to close the respective site induce the opening of multiple sites. Another important thing is to enhance the useful contents for children and to teach them their usage. The more interesting and useful pages the children will find, the less they will search for sites dedicated exclusively for adults.[46]

In several countries central internet censorships operate, for instance in China, in Saudi Arabia or Vietnam the central filtering includes sites which are undesirable for religious or political reasons or otherwise with pornographic contents. In the event of certain illegal contents European countries also apply site blockings (Germany: holocaust denial, Norway: child pornography, USA: community internet access points). In Hungary, due to the respect for freedom of thoughts and speech, only the voluntary filtering was accepted till 2012; this has been modified by Section 77 of the new Act C of 2012 on the Penal Code (hereinafter referred to as: new Penal Code) imposing a novel judicial measure – the order for irreversibly rendering electronic information inaccessible:

(1) Data disclosed through an electronic communications network shall be rendered irreversibly inaccessible:

a.) the publication or disclosure of which constitutes a criminal offense;
b.) which is actually used as an instrument for the commission of a criminal act; or
c.) which is created by way of a criminal act.

(2) The order for irreversibly rendering electronic information inaccessible shall be issued even if the perpetrator cannot be prosecuted for reason of minority or insanity, or due to other grounds for exemption from criminal responsibility, or if the perpetrator had been given a warning.

[46] László Drótos: Referatum of Bayer Judit: The freedom of the net: difficulties in regulating internet con- tents in light of freedom of speech (excerpts from the publication) in.: http://tmt.omik k.bme.hu/show_news. html?id=4633&issue_id=479, 02-04-2013

This new legal instrument is meant, according to the detailed explanation of the draft, to be applied in order to remove the sites with child pornographic contents complying with the provisions of Article 25 of Directive 2011/93/EU.[47]

F. SEARCH ENGINES – the online "gatekeepers"

It is about customized presentation of information in online traffic control services. Hungarian users generally use the search engine of Google without any exceptions (93-96%) – ratio of queries conducted by Google reached as much as 99% in 2014 –, whereas they do not even think that the hit list does not exclusively reflect to their demand for information; possibly there could be other aspects of the search results. Google operates with the term of "subjective relevance" relating to the user upon presenting the search hits when, based on previous search habits, creates a priority list of six categories (*vital – useful – relevant – slightly relevant – off topic and useless*) which is, of course, influenced by the enormous financial contributions paid by advertisers as well. From the point of view of economic the order is of great importance – particularly in case of dominant platforms –, as the customer typically clicks on the first five advertisement hits (consider hotel bookings).

Online surfing children should be taught not only for searching practices (selecting appropriate search words, how to enter them etc.) but also for the proper use of various services as well as for the right assessment of information received. Thus, the phenomenon already known from US schools could be avoided that the teacher should be forced to read again and again the same analysis, consigned to the class, in twenty different homework making use of the substantially same low-grade source.

G. ONLINE LINGUISTIC PROFILING

(Author of this subchapter: Sára Ránki linguistic expert)

The novel achievements of the communication technology brought about new forms of crime. Detecting online criminals is a difficult task both on domestic and international level. The linguistic expert assists law enforcement agencies, among others, by the method of linguistic profiling. A branch of criminal linguistics is a science that,

[47] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

contrary to common beliefs, means text evaluation rather than graphology. We create a profile (this is called socio-demographic feature) by trying to find out his age, sex, education background, mother tongue and number of authors based on the text originating from him. In addition, linguistic profiling can include content evaluation as well: the expert receives a letter lacking signature (anonymous) or showing a pseudonym; in this case we should carry out a linguistic profiling in order to find out the target person. It might occur that we know whom to look for; in this case linguistic profiling is meant for comparative examination with a view to establish the real author of the diverse texts. Criminal linguistics (or forensic linguistics) is not a novel science in the professional international literature though domestically it is. However first studies came up in the '60s, it has just become a real practice or profession only now. This is an applied linguistics science, benefits in practice from the conclusions of the general linguistics, in this case assisting in investigating of crimes.

In the theme of forensic linguistics Police Officer Lt. Col. Jolán Szilák described already in 1979 how important is the examination of reality items in letter composed anonymously or with a pseudonym. During the evaluation of anonymous letters reality items should be searched in the textual system: it is the duty of the investigating officer to inspect the data and facts in the text whereas the subsequent inspection aims at exploring the hidden content of the writing. In such cases the expert compares the textual words with the hidden content as well as with his own knowledge and, as a result, draws consequences on the author. In another study Ms Szilák investigated one hundred letters from previously unknown (later exposed) authors with a view to discover the reality in personal and locality names. It is important to note that letters written on false names fall into the same category as those written anonymously. Results of this investigation as follow: false names are partly common, ordinary surnames e.g. Tóth or Nagy, the same applies to false, invented street names: Main Square or Kossuth street etc. There are different types of name inventions: some people mix up elements of his real name with false items. Others benefit from phonetic similarities or differences by keeping, for instance, the first syllable or first vowels of the name: Szalay-Szabó or Gábor-János. We also can find "expressing" names: this mirrors the opinion of the author on the topic in question. Sometimes people conceal themselves behind others' names (Ms Szilák believes that males take up female names more rarely than vice versa). Others borrow names from famous persons or at least from their own circles. Naming localities or streets after anonymous or invented persons is also interesting. In such cases consequences may be drawn to the education, occupation or place of residence of the author. There are anonymous authors who write in representation of individuals exposing contrary socio-demographic features than he does, for example elders in the names of youngsters or intellectuals in the names of workers. Ferenc Nagy in his publication titled Forensic textual linguistics (1980) explains that the deliberate alteration of the text is a one-way street, that is to say, educated people can pretend being undereducated though vice versa it does not work. The final conclusions of the study reveals that all invented names, addresses as well as texts contain reality items which provide information beyond the author's purpose. For this very reason misleading attempts do not exclude the determination of the author's personality.

In the digital world, initially, the decryption of mobile phone messages led to problems. The limitation of the length of characters forced the language to introduce short and understandable contents. As a result, SMS messages became abbreviations so as to deliver as much information to the recipient as possible. Most acronyms contain phonemes of English words, expressions or numbers. For instance the 'lol' (laugh out loud) is an abbreviation for "laughing out loudly". The 'b4' (before) indicates something "before". The 'btw' (by the way) displays something "not relevant". Nowadays online games have their own language, too. The most remarkable features of communication are the velocity as well as brevity. You have to communicate with fellow players because who types quickly hardly plays. The majority of online games are truly team games: if someone wishes to be involved, he must know the language of the game world. Digital world provides opportunities not only for criminals for hiding but facilitates also the work of law enforcement officers. A human being can be featured a real data matrix, for instance long range satellites are capable of evaluating the shadow of people creating their pattern of movements. The examination of internet language and linguistic behaviour has not yet been taken.

Analysing chat rooms, the comparative examination of Facebook profiles as well as examination of hate crime are meant to assess texts relating to online criminal offences. A clear distinction shall be made between texts created and published online. Texts created online may be subject to online linguistic evaluation whereas texts published on online channels, being rather everyday scripts, are closer to the so-called linguistic norm and these should be examined fairly by traditional textual linguistic methods. These include e-mails, blogs, ads and several homepages.

The online language usage, known also as digital linguistic identity, fundamentally differs from the everyday language. Yet, this kind of language regime can be characteristic. What make it unique are the various elements of the language rather than the wording which is somewhat general in the online world. Let's think of suffixes or the structure of the sentence. We faced comparative profiling cases where the various texts could be recognized by the fact that a certain type of suffix was exclusively used by a certain author, what's more, always poorly. This was a distinguishing feature that helped to establish that 14 out of 30 letters were written by the same author. Why is our linguistic behaviour revealing? Because nobody is so conscious in his language habits as to changing the frequently used linguistic elements. Average user wishing to be seen as silly uses "ly" instead of "j". This is a typical distortion technique as people often think of the language that if I do not write it correctly I can pretend to be a different individual. In addition, according to our non-representative observations it is obvious that, regardless of education, age or sex, we would give the same nickname to a "fellow perpetrator". This also confirms that education or, in this event the age, are not a precondition in language usage. Investigating naming habits would be of crucial importance in combatting online crime against children because a thorough examining of nicknames could lead to the profiling of users of pornographic sites. When decoding online pseudonyms you have to take into account that the individual cannot derive from himself, there is always something unique in our nicknames. For instance, the date of our birth, the name of our child or that of the street we are residing in. We can observe that users on various sites can identify each other by their nicknames. Not only the slang of sexual crimes but also that of other criminal activities (weapon or drug traders etc.) could be subject to assessments. In the light of experience acquired so far the secret language of different criminal gangs can be measured. Inventing the "secret language" has a dual purpose: on the hand a linguistic separation from the society (so that we cannot understand them) whereas, on the other hand, the identification of criminal group members (so that they can understand each other). Thus the various criminal gangs have developed a secret language relating to their activity. We presume that the online and offline criminal languages differ from each other to some extent; the investigation thereof would be useful.

The internet is a safe arena for those who do not wish to reveal themselves. It renders anonymity. People committing crimes online think they cannot be identified. Nonetheless nobody can hide as his linguistic activity clearly exposes him disclosing at least his age, sex or intentions. A man of 45 cannot "speak" in a way as a boy or girl of 15 does. We use the language more customarily than merely creating a language practice atypical for our generation.

During profiling the gender linguistics can be beneficial. Examining the linguistics of different sexes is of great importance not only in linguistic studies but also in other human sciences as well. Stereotypes are true: females express themselves more emotionally than males do. Men, however, are much more focused than women are therefore they write more briefly.

We are presenting an example for decoding pseudonyms. The investigating authority enquired whether the texts published under two nicknames (Sebinoka Hai and Solomon Cedar) originate from the same person and whether the person behind the nicknames is a paranoid schizophrenic individual. The linguistic expert cannot establish whether the person in question has a paranoid schizophrenic personality as it is not a linguistic issue. Though, he can determine whether the texts or pseudonyms have references in the real world. If not, then we can declare that the author displays a different linguistic behaviour from the general average. The presumed person hiding behind both nicknames chose women sending them threats to the life.

Sebinoka Hai: the word "hai" can be found in dictionaries and means shark. The term "Sebinoka" puzzled me. I could not find this expression in any dictionaries. The term "sebino" is to be found on an Italian page describing a special type of dolls. (Human shaped realistic puppets with human hairs.) The ending "ka" may refer to a Hungarian diminutive (babácska, small doll). In the Hungarian language it is common to attach a Hungarian ending to a foreign word, e.g. chat +"l", csetel. Decoding "Sebinoka Hai" to a "puppet-eating shark" and being aware of the case coincides with the issue.

The "Solomon Cedar" was not a piece of cake. This term can be found only in the English edition of the Holy Bible: "So Hiram gave Solomon cedar-trees and cypress-trees [according to] all his desire." King Solomon had a temple built from cedar-trees. Endeavour to, and contact with, God and divinities also appears in persons showing different linguistic behaviours. All this sustain that the linguistic activity of the person, hiding behind both nicknames, may differ from that of everyday usage. Texts examined confirmed this view.

We assume that cyberbullying has its own special language. The person signing in often has an anonymous or invented profile; as a result, the identification of the perpetrator is difficult. Internet language is characterised by abbreviations as well as the use of simple wording and internet slang. However, we cannot discover the accompanying linguistic features (supra-segmental tools like tone of voice, intonation, pitch) that can revise an interaction. We cannot encounter additional direct elements related to speech in the online communication: no mimicry, no gesticulation. These are, however, replaced by emoticons which, being icons expressing emotions, are constant companions of online conversations. Their presence emphasizes the content and meaning of a message, intensifying or replacing the text in question.

In the context of online grooming personal meetings following online dating repeatedly lead to tragic consequences, however, the communication style of adult criminals, pretending to be young boys, may reveal the real identity of the dating partner.

Internet enables concealing but nobody can escape his own "language".

H. Possible trends of future developments

The amazing dynamics makes the development of the online world scary – through the manifold development all relevant components of the web (e.g.: hardware, software, network, societal expectations) always change.

Besides the hardware environment dedicated to visualize the online world also the design is being improved a lot over the past decade. The more complex and cooler- looking device, the "widget" has become a key element of fashion. One of the most important cult-object among youth has become the smarter, more expensive and designed mobile phone. While in the early years of the internet era we were browsing internet sites in front of a desktop PC's screen, today we are already capable of instantly sharing, via the screen of a smart phone, our photos taken in the street along with our geographical location on a social networking site. The progress is steady, more and more simple devices are becoming smart and going online. Very soon we will be walking in the streets wearing glasses that will display images, seen on the street, simultaneously on the internet as well; we will have watches that take our pulses in every two minutes and, comparing the results with online databases, will not only predict diseases but also call our GP; we will have game consoles that, perceiving our entering the room, will offer us newer and newer games. In the future smart devices will be equipped, besides a permanent internet access, with numerous sensors by which the gadget will be capable of monitoring its environment (e.g.: accelerometer, camera with facial recognition, depth gauge, laser scanning, GPS sensor, noise measurement and analyses).

An additional challenge will arise when all devices around us go online and communicate autonomously thus the fridge in our kitchen notices if it has run out of fresh milk so it is high time to place a self-automatic order via a tablet…

The term **"Internet of Things" ('IoT')** means that all devices in our personal environment communicate online and individually, that is to say, our fridge will realize the shortage of fresh milk, consequently, you should place and order via a tablet. (Such smart fridge already exists which can be contacted any time through the HomeChat application. Since the smart fridge can, by means of a mounted camera, take pictures as well, we can control the content of the fridge through a smart phone or a tablet without having opened its door. A software oversees the freshness of meals inside the refrigerator, too, and immediately warns if a product has expired. According to marketing ads smart fridges also take care of our health: by means of an app called "healthy diet suggestions" it can set up a daily and weekly diet based on the personal features and data (weight, sex, height, BMI index) of the user. In South Korea there is an oven already in place which recommends recipes and, then, adjusts the baking temperature and duration needed for the selected menu. Via the chat programme we can request meal suggestions based on raw materials provided by us finally it sends the potential variations through the recipe selecting window.

The data will be collected by few multinational companies which, by virtue of their overwhelming datasets *(big data)* and complex algorithms will categorize the consumers and probably will also be able to predict our behaviour – in other words they will think and take decisions for us – initially only step by step, later more autonomously.

Another potential risk is that these smart devices are quite vulnerable from a data security point of view meaning they can easily be hacked. Not only hardwares enlarge dynamically but also sharing channels get better. On account of the acceleration of mobile internet we do not even need to get off the tram to share videos. The disclosure methods of contents have expanded rapidly as well; in the early stages of internet we were sending our personal data only in email circulars, today hundreds of millions of users gather on social sites and we can forward our videos by double-clicking to millions. Development does not stop here, more and more thematic networking sites emerge and these thematic webpages are increasingly targeting juveniles. What's more, in ever more user-friendly systems minors can establish a micro community as well. (In the Netherlands a social site developed by a minor and dedicated to fellow minors has been investigated by the Dutch DPA). However, the real challenge, in light of the children, lies in the marketing activities which form the basis of social sites that observe this age segment as the most lucrative one. Social networking sites are more and more tending to concentrate on behavioural advertising; they make attempts to seize the minors by monitoring their contents and activities and provide them with targeted ads.

Among community applications capable of revealing our privacy the most intrusive ones come to the front, solutions requiring permanent activities and services aiming at sharing images and videos are expanding.

From a software development point of view more and more programmes, created by individual IT experts and available in mobile platform application shops, endeavour, regardless of privacy, to obtain the personal data of minors. Improvements intended originally to satisfy adult users' demands – with a view to be available everywhere, to arrange our businesses without queuing – are now targeting, in terms of advertising, a more profitable generation, the minors. It became to a greater extent fashionable to adjust the various online services to children's needs. Having a look at the offers of online application stores, they abound with programmes dedicated to minors. Small kids can play painting on their tablets; they can get the virtual cats talking on smart phones or can fondle virtual lions on a game console. Application producers seduce minors with other creative methods into the virtual environment as well – a huge amount of games produced to minors pose the most imminent danger; these are free of charge, at least from a virtual aspect. Children fundamentally pay for them with their personal data, in worse cases parents' purses will have to be opened, too. There are plentiful games where one has to pay little in exchange for small advantages or additional playing levels. Seducing "micropayments" apply psychological methods by which even adults of greater life experience will be misled…

The online community experience has turned into an expectation towards each application. Nowadays a minor plays all games against friendly or strange players online and the most developed version of the application is that he, by disclosing the personal data of his acquaintances, can invite other players. In most games we can share our advancements and results, however, in addition we can insult each other on live phone call online or disclose personal data to strangers. An additional threat is that mobile applications require or disclose more and more personal data. Most applications demand access to all contents stored on our mobile phones, contacts, online profiles created on social networking sites, geographical locations. From this enormous database our whole life can be explored better.

Beyond hardwares and softwares the societal factor also compels individuals to reveal their personal particulars, of course. The driving force among minors is tending to be more powerful to come up with astonishing and amusing attractions in the online environment. This requires surprising and spectacular disclosures that implies the total revelation of the privacy of us or of our fellows. As a result of the vibrant development of the online world parents having grown up in a different world rather than this digital era (X and Y generations) cannot be aware of its risks, therefore they cannot supervise and teach their children (Z generation). Of course, the industry could also do its best so that the new techniques take into account basic data protection concerns; however, these considerations are usually overridden by economic factors. Enhancing the involvement of states is a global tendency nowadays but the effective technologies often lose the battle against the futile strategy development and rapid industrial progress.

Adults, who are responsible for raising the younger generation, bear the liability to call the attention of minors to the risks as it should not be forgotten that the kids have been socialized already in the online community, it has become a daily routine for them to share the relevant and irrelevand stories.

7. Mapping of problems – online deviancies

"Should you fail to post, then nothing happened!" motto governs the everyday life of younger people. They live on various online platforms evidently, consider virtual unknown people or "half contacts" as being friends, consequently, they are too open respecting their own and others' private life and do not feel the gravity of their behaviour until risks and threats are approaching them.

New deviancies emerging in the information society may range from the "somewhat uncomfortable" feelings leaving behind bad impressions to actions constituting crimes.[48] One possible reason of the new deviancies could be the anomy caused by the new living conditions. The term anomy (anomia) literally, stands for a standard deficiency, broadly speaking a situation when there are no general, customary norms or values for new life circumstances or the common societal practice differs from the norms recognized by the society.[49] Beyond the virtual anonymity the seemingly tolerant community sanction is another risk factor since the deviant behaviour, in the virtual space, may face the only consequence that the person, conducting unusually, will be excluded from the group, in contrary to real world where the infringement may have more serious outcomes. Not only mild sanctions in the cyberspace but also the slight consequences in the real world enhance these deviancies. The anonym online life leads to the evolution of a certain double morality which implies a more liberal interpretation of the offline societal rules, that is to say, some users remain traditionally law abiding, however, during the internet communication he follows a different guideline.[50]

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 young open up to the outer world blindly. Girls, at best, upload photos of them in bikinis, reveal their actual location and the place where they head for 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 required: "Inhibitions of children, evolved instinctly 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 chan-*

[48] Adler F., Muller, G.O.W. & Lufer, W.S., Criminology, Osiris Publications, Budapest, 2002. pp. 34-35.

[49] Gönczöl K., Kerezsi K., Korenik L.&Lévay M. (ed.) Criminology-Professional Criminology Complex Publications Budapest, 2006. p. 104.

[50] Zoltán Szathmáry: Criminality in the information society, Constitutional criminal dilemmas in the information society, PhD thesis, Budapest 2012. pp. 64-65.

nels… 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".[51]

The purpose of cyber intimidation (cyberbullying) used as an "umbrella expression" is to achieve "negative powers" over the victim by the perpetrator. Intimidation is carried out through electronic devices online (email, sms, chat, mobile apps, blogs, posting on community sites.

One form of cyberbullying – beyond slander, defamation, hate speech, organised exclusion, misuse of personal data, blackmail, invasion of privacy as well as violating human dignity and personality rights – is intimidation. In addition, particular examples include malicious acts which are not illegal, however, are capable of destroying and harming the prestige, self-confidence, position and/or social status of the victim.

A. Cyberbullying

Due to modern technical devices, the widespread expansion of internet and the lack of information we can find cases of cyberbullying in relation to children aged 10-16 more and more frequently. Cyberbullying always begins for personal reasons and the offender deliberately "tortures" his victim for a longer period, repeatedly via the use of information and communication technologies (internet, cell phones, laptop, videocam etc.)

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.*

[51] Dr. Tibor Peszleg: Internet and pedophily from: Police Studies Review, December 2004 in: http://www.remet.hu/cms/index.php?option=com_content& task=view&id=16&Itemid=4,12-02-2013

> *(2) Any person 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.

In comparison to the figures from 2010, in 2014 12% of European children aged 11-16 are predicted to encounter cyberbullying (the shift is significant compared to that of the previous 7%).[52] Consequences of cyberbullying could be quite serious: according to an EU survey 55% of children who had fallen victim of a bullying earlier complained about depression, 35% of them injured themselves and 38% considered suicide as a final solution.[53] What's more, internet use and the online presence tend to start at an increasingly earlier – at the age of 8-10 –, consequently children may face harmful and inappropriate contents or actions.

Online and offline intimidation frequently go hand in hand as bullying commenced online can resume in the classroom or in the street thus the victim cannot escape.

Children globally indicated that cyberbullying poses a serious risk in their life; however, adults do not always perceive the severity of this phenomenon. A little portion of online bullying materialises or continues in real life. According to a UNICEF research in the USA children using violence at school have probably also become a victim of an online bullying earlier. 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

[52] http://europa.eu/epic/news/2014/20140805-cyberbullying-harm-european-children_en.htm (2016.01.14.)
[53] https://lsedesignunit.com/EUKidsOnline/index.html?r=64 (2016.02.22.)

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.[54] Unfortunately the number of fatal victims of cyberbullying 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.[55]

B. Internet memes

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 degrading campaign. The difference between memes and cyberbullying is that the aggrieved party is usually a strange person 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

[54] http://www.sg.hu/cikkek/61147/missouri_buncselekmeny_lett_az_online_zaklatas http://www.foxnews.com/story/0,2933,312524,00.html, 04-06-2013

[55] In the fall of 2012 in Ireland two completed suicides happened within weeks, fellow schoolmates had been harassing the victims anonimously on the same website from: http://www.thejournal.ie/erin-gallagher-funeral-655978-Oct2012/, 08-03-2013

became a real “meme celeb “following his resignation, often depicted in a rather indecorous manner) but sometimes ordinary people – rarely children – also come up. This happened to a young girl, 11, from California in 2010 who shared YouTube videos on herself and her music preferences online. Her appearance brought about aversions from an internet com- munity that’s why they decided to “punish” her: they posted faked information on the alleged sexual intercourse between the girl and a famous singer. The mother of the girl gave credit to this and raised stink whilst the minor, in despair, sent a threatening video message to the community. As a consequence they obtained the contact details (phone number, email addresses) of the family and the bullying campaign began including also death threats. The girl, in a subsequent video message, cried for getting her off, however, during the messaging, the angry father entered her room and expressed his opinion with some grim words. In revenge the father was accused of raping his daughter publicly on the web and, though he was cleared of the charges, later the father died of heart attack while the girl has been in need of a psychiatric treatment since then. US experts’ queried advice in these cases is clear: you should not pick up the gauntlet and react to the abuses online because this invokes only hysterical revenge from the members of the online community.[56]

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 sportlers this way.Recently a young British boxer has been spotted by a user on Twitter who, under the nickname Jimmibob88, hurling various insults at the athlete and taunting his results. The very temperamental sportsman offered blood money of 1.000 GBP on the 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 in the internet indicating that he can catch him any time he wants. The troll retreated and pleaded for forgiveness. On Twitter the ratings

[56] http://know yourmeme.com/memes/events/jessi-slaughter, 27-02-2013

#keyboardwarrior and *#jimmybrownpants* converted into the most popular hashtags due to this issue.[57]

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"*[58] Trolls expressing their extremist opinions anonymously certainly do not promote civilized inter- net style and can generally influence all users into an unwanted and wrong direction.

D. Sending erotic photos (sexting)

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

Based on survey figures from 2014, 22% of teenage girls and 18% of teenage boys sent already erotic images of themselves. Additionally, 15 %- of them sent such pictures to persons whom they have not ever met before. Major purpose of boys was clearly sexual whereas in case of girls pressure appears as motivation, however, in many cases they regard sending and receiving such contents purely as fun.[59]

In most sexting cases "detected" erotic images have been recorded by the models themselves or, upon mutual consent, by the partners but later the recordings come to an independent life.

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 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 in anger or revenge may refer to juvenile relationship behavioural patterns characterized by emotional abuses and violence.

[57] Sports Trolls Heap Abuse on NBA Star After Big Miss in.: http://mashable.com/2012/11/14/sports-trolls-gasol-miss-nba/,14-03-2013

[58] http://bleacherreport.com/articles/1034961-san-francisco-receiver-kyle-williams-receivers-death-threats-on-twitter,18-06-2013

[59] http://nobullying.com/sexting-statistics/ (04-02-2016)

Though we should not take the consequence, this attitude is typical to young generations only but, exploiting their technical opportunities, teenagers' emotional life and their gradually impulsive behaviour explain why they surely do not consider long-lasting consequences.

"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 an illegal pornographic picture arises but also – in case of age differences – the delict of abuse with personal data; even though there is no uniform approach even in the US as regards the detection and handling of the reason of the phenomenon. The only complicated factor is that data subjects take and forward these pictures on their own about themselves, 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. Cyberbullying and sexting equally verify that attitudes to privacy turned to the wrong direction as while cyberbullying 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."

A case getting within the scope of the NAIH evidently illustrates the above things: a girl of 14 and a teen boy of 16 took erotic images of each other. The boy, for hyping purposes, disclosed the pictures in a closed group of a community site comprising almost all classmates. The father of the girl learnt the case and reported it to the police. During the investigation the boys were interrogated as suspects as the girl never consented explicitly to the taking of the images and the pictures have been disclosed by everyone. A legal issue to be decided upon whether the images, beyond viewing them, have been forwarded to others since in this case the conditions for the misuse of personal data have been met (the sole viewing of the image does not constitute data processing). The young boys, confronted visually, showed disinterest and behaved unintelligibly during the process; merely the parent was upset because of the case.

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.

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 porno- graphic 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 “of him” an attractive photo, begins to date with teenager girls, they become friends quickly, the girl takes “the boy” into her confidence and, on his request, she possibly sends additional pictures of herself, in clothes at best, at worst nude or semi-nude images.

In the course of internet paedophilia offenders really use the internet as a means 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. (In many cases the pictures are modified, for instance – through image editing software – a foreign head is added to a nude body.)

Finally, we must talk about a novel form of child exploitation which is the **virtual pedophily by means of webcams** being more secure and cheaper for the offenders. In 2013 one thousand pedophiles were identified within a week by the Terre des Hommes Dutch children’s rights organisation; for this action a 3D model was used which resembled a 10-year-old Philippine girl. The virtual girl called Sweetie waited for the men in chatrooms; during the experiment, lasting for two and a half months, more than 20.000 males contacted her online and demanded some sort of sexual service and many of them would have been willing to pay for it. 1.000 pedophile identities could be determined usually by personal particulars used in the social networking media; the database was handed over to the Interpol. The civil association produced a documentary on the action as well; the participants said it had been a disturbing experience even after years combatting child prostitution watching closely what demands are expressed by pedophiles to a 10-year-old girl. The investigation unveiled the most sexual predator had been American followed by Britons and Indians; pedophiles were caught from altogether 71 countries. They seemed to be ordinary young or middle-aged men; in the film appeared a 35-year-old father of two kids from Atlanta who offered 10 dollars to Sweetie for taking off her clothes.[60]

F. Online meshing (grooming)

„I could go home from the child protection institute to my grandma at the age of 12" –tells Brigi, a girl of 14, who has been in Esztergom for two years, she will be "released" this summer. Once being at home she met a man of 45 on the Facebook who marked her by the profile picture and she replied with pleasure as she was very happy being considered by somebody as very beautiful for her age of 12. From that on they chatted many times and, finally, the man persuaded her to move to him. Brigi departed at night by bicycle. "What was his convincing argument? Well, by him I could live independently. I could have a house and a kitchen on my own and I would be the queen by him. And, if demanded, he would take the cocoa to bed in the morning." Brigi was found fully accidentally by her brother in the bus stop waiting, then the grandma called the police that went to place agreed on before with Brigi as meeting point. At this point it was found out that the girl had already been sold abroad. She was taken to Esztergom immediately for defence reasons."[60]

For the time being there is no proper Hungarian term for it, the phenomenon could be described by the words meshing or catching.[69] With social sites expanding dating practices have simplified 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 year-old man, or even elder who search for potential victims to satisfy his 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 take them into their confidence, obtain personal

[60] http://kronika.ro/szines/ezer-pedofilt-fogott-a-virtualis-kislany, (05-02-2016)

information from them, involve the youngs into online sexual games and ultimately they draw the minors on to a personal meeting. 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 tell about it. Due to the shame involved s/he generally will ask for help too late or never ever.

A Canadian girl of 13 met an elder man via video chat in 2009 who, after numerous compliments and flatterings, persuaded her to show her brusts. Then the man started to blackmail the girl: if she refused to show more from her body he would send the topless images to everybody. In 2010 the police commenced an investigation because the pictures reached numerous people. Following hardship and continuous online bullying for 3 years the little girl committed suicide[61].

G. „Flaming"

"Flaming" is a type of online bullying carried out in online forums, practically a kind of online "war", assault, a flow of furious and obscene comments on public forums (often online political, religious or ideological dispute). Intentionally intimidating and hostile off-topic comments are disseminated in public forums, on social networking sites, in personal blogs, chatrooms, on e-mail messaging systems or video sharing sites (for instance YouTube). The perpetrators – "flamers" – usually disclose "defamatory" contents of others as a response to their anger, sadness, degradation or lack of self-confidence. Whereas some people release degrading information targeted specifically or address other individuals' racial, sexual, religious orientation or financial situation others insult fellow netizens without good reason, purely for fun.

Several insulters target particularly seemingly vulnerable net users from whom they obtain and exploit personal particulars with pleasure.

If degrading or insulting contents are published of somebody the worst reaction is to respond to it with fury, anger or disappointment as this is the main purpose of the criminal. Should someone fall victim to "flamers" s/he can report it to the site administrator that, as a result, deletes the challenged contribution or bans the user from the site.[62]

[61] http://hvg.hu/plazs/20160126_Otven_lajkert_folteszek_magamrol_egy_fel (23-02-2016)
[62] http://nobullying.com/what-is-flaming/ (27-01-2015)

H. Online games for children

The professional literature considers only the passion for gambling as a single addiction, the obsession with PC and online games is still not registered as a single disease, even though numerous psychological surveys are engaged with the topic. An American study revealed that “serious” online players spend an average 23 hours a week in a certain game field and both the best and worst experience of one-third of these players is associated with the game.[63] Game addiction is categorised by experts primarily as a symptom: if implies truly serious consequences, is uncontrollable and not simply a manifestation of the healthy and normal game activity typical for childhood then it may indicate definite disorders of behaviour and other psychological diseases.[64]

In Hungary, pursuant to Section 1(6) of the Act XXXIV of 1991 (Gaming Act), persons under the age of 18 shall not participate in online gambling as a general rule with the exception of lotteries organised sporadically. All other online games, not constituting gambling, can be accessed by anybody.

Playing means fun of course, and children can learn and obtain many skills with the help of online games which may be useful in terms of developing their proficiency. They can enhance their historical, economic and biological knowledge by playing with special role-play games; however, there are some stumbling blocks worth emphasizing. Firstly, it should be recalled that the main concern of producers and distributors of games is making profit; this can be (legally) achieved by selling more and more expensive products, urging the buyers to additional purchases and “keeping” the users for as long as possible. In 2011 in Germany alone approximately 2 bn euros were spent for PC game softwares; a huge proportion of them being minors. More and more, basically free, games collapse or fail to satisfy without buying special “accessories”.Additional German figures show that in 2011 consumers spent, for virtual accessories alone, 233 million euros, 100 million euros more than in the previous year.[65] Purchasing accessories is generally easy: with a premium rate phone call or sending an SMS as well as paying with bank card (often using the parent’s phone and bank card) and the child under pressure purchases multiple times, only the final statement at the end of the month reveals the expenses of more hundred euros. Even

[63] Nicholas Yee: The Psychology of Massively Multi-User Online Role Playing Games: Motivations, Emotional Investment, Relationship and Problematic Usage. In: R. Schroeder and A. Axelsson (ed.): Avatarts at Work and Play: Collaboration and Interaction in Shared Virtual Environments. London – Springer Verlag, 2006

[64] Andrea Vida: The effects of information and communication culture onteenagers: http://xenon.bibl.u-szeged.hu/~vidaa/holi/03/szenvbet/vidaa.pdf (24-03-2013)

[65] In der Kostenfalle – Kinderspiele im internet, Sendung vom 11.Dezember 2012, http://www.zdf.de/ZDFmediathek/beitrag/video/1794584/#/beitrag/video/1794584/Kostenfalle-Kinderspiele-im-Internet

if the website administrator pledges to limit the purchasing obligation of accessories to 1-2 times a month, you can easily find loopholes to evade these commitments.

Inventors and administrators of games are inclined to assert that the minor user has learnt and accepted the end user agreement and terms & conditions of the game drawn up by the developer unilaterally. In case of more relevant online games users are entitled to sign up only above a certain age. Although the system can, lacking direct control, be easily evaded by kids. In numerous known cases transactions are performed with the password of the parent. For instance, in the United Kingdom a boy of 5 asked for his father's password to upload a free game, though a payment was needed for additional accessories and, due to inappropriate settings, parents had to pay a lot.[66]

Online games with a PC, playing console or smartphone can usually be played involving numerous participants (so-called multi-player games); in this case, however, we can have access to other individuals' personal data as well. Players create a customised virtual personality called avatar that will be their online alterego. The participant plays in the virtual game worlds by instructing the 3D – mostly humanoid – avatar. Due to the close relationship between the player and his digital alterego the avatar can be regarded as personal data of a given user: by means of the virtual behaviour, the nickname or other personal features the individual hiding behind the avatar can be undoubtedly identified.

Regular players are prone to be present in multiple online universums simultaneously; however, their playing style and personalities created by them may resemble each other very much.

Prior to entering the game, therefore, the privacy policy shall be learnt as this document contains useful information on the person having access to our personal data, the purpose of data processing as well as third parties to whom these data are transferred.

PC games can be grouped in many ways:

- according to appearance: textual (e.g. visual novel), graphic or mixed;
- according to genre: action, adventure, stretegic, simulation, role-playing games.

The most popular gaming software among Hungarian children is an online role-playing game that can be categorised into the so called MMORPG *(Massively Multiplayer Online Role-Playing Game, that is to say, an online role-playing game involving numerous users).*

[66] http://index.hu/tech/cellanaplo/2013/03/18/oteves_gyerek_610_ezret_koltott_appokra/, 2013-04-28

Upon signing up to online games one has to provide a username, e-mail address and date of birth. The geographically nearest server to the user is set automatically by the software based on the IP address of the internet connection. In jurisdictions where a minimum age is determined by law, usually, a confirmation is required on the age of majority of the player.

Some services may be used free of charge whereas others are subject to payment. If a credit card is used for online payments it is advisable to regularly monitor the relating statements. We must contact the game administrator immediately if a suspicious transaction has been made.

We can specify the privacy settings depending on the game environment, the developing company and the feature of the game. In more specific games we usually have the opportunity to restrict the settings so as to nobody will have access to our profile or personal data save the system administrator. This security level, however, does not facilitate the multi-player game or the community aspects of online adventures, consequently, several players ignore these restrictions thus granting access for others to their profiles. The username created can be protected in the following ways:[67]

- strong password difficult to unveil;
- HTTPS (Hypertext Transfer Protocol Secure), the settings of the web application that encrypts personal data and the communication during the game (if this is possible);
- restricted privacy settings and,
- disclosing as little sensitive personal data as possible (e.g. avoid using infos on place of residence, school or workplace);
- if the legal disclaimer of the service enables you are advised to create a profile with a pseudonym or nickname; this will be interconnected with community sites by administrators in order for players to inform each other on the commencement of the game. In this case, however, it is useful to study the privacy policy and legal disclaimer of the social networking site as well.

The privacy policy and legal disclaimer are accessible on the screen or on a link during the registration process or before uploading a programme upon specifying our

[67] http://campuslet.unideb.hu/dokumentumok/tanulmanyok1/Csoportkepzo_tenyezok/Virtualis_es_valosagos_csoportok_internetes_szerepjatekokrol/Balku_Anett_Virtualis_klanok_Csoportkepzodes_egy_internetes_szerepjatekban_SzakdolgozatMA.pdf, 25-03-2013)

personal settings. Thus we see the data controller, the scope of our personal data collected and processed, the destination of data transfers and the way our data are processed as well as where to turn with complaints. Gaming companies disclose our personal data in an excessively wide range with third parties for various purposes (legal obligation, monitoring diverse illegal activities, troubleshooting, game development, ensuring payment process, communication among players, sending promotion leaflets). As a result, our personal data can be accessed by contracting programmers, financial institutions, online hosting or distribution services, customer services relating to technical or game support, internet service providers, researchers, marketing businesses, market researchers, execution agents and other public bodies. Players shall make sure, however, whether the company or the game developer enacted special regulations on liability, what's more, whether they specified data security rules in service agreements which are essential in case of disclosure of personal data.[68]

At first it may appear surprising though in single online games with extremely detailed virtual reality simulations (typically the MMORPGs) some players may become inclined to insult and exploit each other or even carry out an activity with direct adverse financial effects on others. This phenomenon is described by the legal profession as *„virtual crime"* including criminal actions both against person and property of players.

In virtual communities criminal actions against property are committed in relation to things of commercial value for a player community. This is the virtual property the definition of which is different from that determined by civil law. Online role-playing games simulate virtual markets which may truly impact on the actual economy.[69] Misuses of virtual property items – particularly in Far East countries like China, Japan and South-Korea – are frequently reported by the media. For example, this was the case when a Japanese man abused the confidence of his fellow player and, using his login data, entered their joint role-playing game with the avatar of the genuine user and, afterwards, sold the house and all movables therein to a third person on eBay for 50.000 JPY.[70] In this event the crime seemed to be realize since a "theft" was committed against the avatar and his owner and his virtual property items were sold for real money.

It is worth noting concerning the above case that if, according to the general terms & conditions accepted by the user and attached to virtual simulation software (online game), virtual commodities can be sold on markets outside the virtual world, then the

[68] http://www.priv.gc.ca/information/pub/gd_gc_201211_e.asp (15-04-2013)

[69] Edward Castronova: On Virtual Economies. Gamestudies.org, December 2003 http://www.gamestudies.org/0302/castronova/

[70] Slasdot.org: Japanese Man Arrested for Virtual Theft. (14.02.2003.). http://www.slashdot.org/articles/03/02/14/0523248.shtml?tid=127

beneficial interest over the goods constitutes valuable rights. The unlawful deprivation of beneficial interest over such commodities can give rise to the suspicion of crime against property as the termination of the right brings about pecuniary disadvantage or *"damnum emergens"* to the aggrieved party.[71]

A different approach is applied if the owner of the virtual assets consents himself to the destruction of his commodities or gets into a situation knowingly – even in the game – that his goods may be subject to damage. A good example, from the beginning of 2014, was a space war played in a sci-fi role-play gaming community consisting of millions of users as a result of which as much as 70-114 million USD pecuniary loss emerged in the virtual assets of users.[72] In this case the voluntary willingness to take risks from the aggrieved party provides grounds for the preclusion of punishability.

The criminal policy draws distinction between punishable acts and so-called *"griefing"* actions. This latter includes, for instance, the recurring and continuous killing of avatars directed by weaker players *(corpse camping)*, unjustifiable attacks on fellow company members *(friendly fire)*, the self-motivated murder of monsters prior to others and thus hampering their development *(kill stealing)*, quick repeating of meaningless statements in the shared chat room of the game *(flooding)*, hindering other players in movements etc. What these actions have in common to purposefully annoy fellow users and hence reduce the game experience. The administrators of most virtual communities crack down hard on griefers because they insult directly the users thus having a potentially adverse effect on the software market. At first and generally a warning is addressed to owners of avatars bothering fellow players followed by partial or final exclusion from the community in case of additional abuses.[73]

In each document attached to online role-playing games there are rules that govern the relation among players on the one hand and between the players and the game administration on the other hand. These documents and contracts stipulate regulations on the general code of conduct for users. These embrace e.g., banning the use of deceiving programmes and hacks as well as disturbing fellow players. Maintaining law and order is vested in system administrators. This regulation scheme is usually adequate to settle tensions in the virtual world. Beyond the self-regulating mechanisms of various commu-

[71] Dániel Eszteri: From World of Warcraft to Bitcoin: Evaluation of the situation of the individual, the economy and the property in virtual communities from the point of view of the civil and criminal law. PhD thesis, PTE Faculty of State and Law Sciences. http://ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-vedes-ertekezes.pdf (02.02.2016.)

[72] HVG.hu: An online war brought about an enormous damage beyond the internet as well within 24 hours, (30.01.2014.) http://hvg.hu/tudomany/20140130_hatalmas_karokat_okozott_egy_netes_haboru

[73] Katalin Parti: Actual Policing in Virtual Reality – A cause of moral panic or a justified need? From: Ja Jin Kim (ed.): Virtual Reality. InTech ISBN 978-953-307-518- 1

nities the chat, channel or software administrators can also clamp down on perpetrators; this is generally the most objective and effective solution. If, however, deviancies go further, a firm response from law enforcement agencies may be needed.

Although this may sound somewhat surprising but the most effective solution for the online protection of kids is playing together with his parents or the family – of course to a reasonable extent!

I. Other forms of personal data abuses

The online world has become an integral part of our everyday life. We exist, to a great extent, in the virtual environment where we can keep contacts with our beloved friends effectively, order goods and services easily, follow and comment on world events. The online world has infiltrated into our life increasingly, mainly in virtue of the, at first sight, cheap or free services. These services are factually not free of charge; we pay for them with our personal data and the cheaper the price is the more personal data we provide. According to the study of the European Network and Information Security Agency (ENISA) in case of services with similar prices customers prefer the more secure ones in terms of data protection, however, as the prices differ one-third of clients opt for the cheaper services even if they, in exchange for, waste their personal data.[74]

From Section 21(1) of the Act C of 2012 on the Penal Code the term "unlawful" has been omitted, consequently each illegal or from the original purpose differing data processing activity, failure in ensuring the security of data processing, or violation of the obligation to report, which are deemed to infringe the provisions of Privacy Act, committed for unjust enrichment or causing substantial injury of interests qualify as misdemeanour.

In January 2011 a complainant filed a petition on the children's rigths section of the ombudsman's website claiming that an email exchange service (Freemail) sends **unsolicited email messages (spams)** to minors containing penis enhancement advertisements. He thinks the defence tactics of the service provider arguing that the age of users are processed based on statements provided upon registration has to be rejected since the validity of personal data rendered have not been verified, what's more, those declarations cannot be considered as legal statements. Conversely, it consitutes the mass violations of children's rights if the dissemination of such ads is carried out based on such data. Due to

[74] Study on monetising privacy An economic model for pricing personal information http://ww w.enisa.europa.eu/activities/identity-and-trust/librar y/deliverables/monetising-privacy

competence limits the ombudsman forwarded the complaint to the Hungarian Content Industry Association (MATISZ) and the Hungarian Commercial Advertisement Association as well. The President of MATISZ outlined in his reply that between 2002-2003 both in the USA and Europe legal regulations governing spams were enacted, however, spams account for about 90-95% of global e-mail correspondence today hence the effective solution to the problem still has to emerge. The disinterest and ignorance of users also contribute to this phenomenon because a remarkable proportion of networks responsible for disseminating spams are consisting of contaminated PCs. In the USA the most effective solution for combatting these challenges are the detection and shutdown of botnets accountable for spreading spams as well as the prosecution and conviction of developers and operators of infectious botnet-components.

In Hungary the principal government body liable for handling spam issues is the National Media and Infocommunications Authority operating a hotline (https://e-nmhh.nmhh.hu/e-nhh/4/urlapok/esf00101/). Particularly messages from unknown senders or those composed in a foreign language, similar to the complaint cited above, could deceive the recipient, additionally, the sender must have been driven either by material benefit or the purposeful infection of the PC of the addressee (mainly also for financial benefit). The best response is the fast deletion of the message without reply; attachments must not be opened, of course as they might contain harmful codes (which could even destroy the PC). Should anyone is addressed by an unwanted job offer or a prize etc. it must be in all probability a deception. There are spam filters on the side of the service provider (on mailing servers) and you can upload spam filters on the clients' side (on your own PC), too; among others the complex defence packages of modern antivirus softwares contain such components, there it is advisable to install these tools. Even though you should be aware that neither spam filters of the service provider nor those on the client's side are capable of eliminating all spams.

Besides phishing, the information acquired can be exploited for multiple purposes including harassment, defamation, libel, blackmail, identity theft abusing that it could be out of control who is hidden behind a profile, i.e., who is the real perpetrator, as well as the majority of SPs urge users to disclose more and more data with in order to be able to improve "applicability", at the same time, fail to call the attention to the risks implied. What's more, on the one hand, SPs are powerless to such actions while, on the other hand, they exclude their liability in advance.

Most SPs enable for users to link their profiles with external sites, programmes, applications (XSS, cross site scripting), however, these outer programmes can easily be infected with harmful contents (viruses, worms, Trojans). The danger lies in the fact that most social sites are vulnerable to such threats since the third party, supplying the programme, is not controlled appropriately. Moreover these perilous contents can spread, due to the contact networks, faster and resulting in greater damage. The risks of these hazards are unpredictable; they may range from compromising the profile to losses caused by phishing.

Finally we can conclude that auction sites are very popular nowadays where some points can be raised in terms of data protection. According to the information provided to NAIH by a popular web auction and shopping site operator abuses are revealed if the customer care is approached; the case will be cleared up either with the support of the investigative authority or by means of a prosecution. Concerning point one in many cases "the user requests the revocation of his bid claiming that the bid was made by his child or his child put on goods for sale. This time users request information what to do, how statements made online can be revoked." Terms and conditions of auction sites explicitly stipulate, however, that the online marketplace is open to users above the age of 18 though SPs cannot check it. As a result the IT awareness of parents should be enhanced since their usernames can be used by children below 18 only if they are stored without adequate protection measures. The number of these kinds of submissions is relatively low: annually approximately 10 out of 150-200 cases affect this issue in Hungary. Regarding the second case a real fraud will be committed when a user, having registered as a vendor puts on – sometimes not existing – goods but fails to sell them and collects the money on a bank account. In such cases of fraud final judgments have already been passed. The affected company does not have any information on the age of persons having committed the crime; in addition it is unaware whether a minor (who, in theory, should not be admit- ted to auction sites) would have become a victim of an abuse. "*We already encountered cases where the offender claimed his minor child had uploaded products for sale just for fun– in this case the statement of the adult could be contested since the bank account number to which he could expect the price of the commodity had been handled by the father; so the minor can be considered as being a victim.*"

In case of defence against auction frauds we should beware of vendors with few feedbacks, aware of the contents of scores, not buy extremely cheap goods and avoid vendors who registered with an invalid home address or phone number and take over goods – particularly of greater value – always personally.[75]

[75] http://w w w.penzcentrum.hu/vasarlas/tizezreket_buk hatnak _a _g yanutlan_vasarlok _tamadnak _az _at veros_ netes_boltok.1035976.html,15-05-2013

8. Best practices – international examples

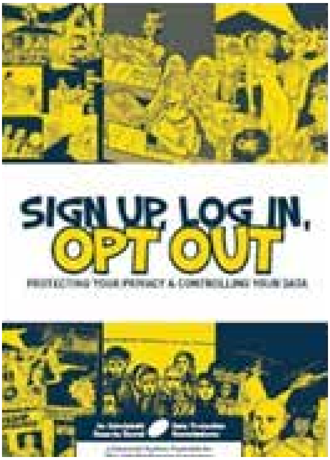
A. Portugal, Project Dadus

In 2008 the Portuguese DPA envisaged the introduction of data protection in the education plans of schools. The first phase of the long-lasting structural programme, named Dadus Project and dedicated to children aged 10-15, was elaborated with the support of the Ministry for Education. (The name Dadus is very similar to the English "data".) Dadus is a young boy who lives as an average teenager whilst experiences events of data protection importance. The project is divided into thematic units and each unit contains a summary, addressing teachers in a complexed manner while the students in a simple "Dadus – style" that is to say, in a weekday "child language". From the website (http://dadus.cnpd.pt) teachers can download project leaflets, summaries; pupils can browse news, legal norms whereas parents can obtain practical advices and share their experiences and opinions in a forum. On the Dadus Blog pupils can directly discuss topics raised by Dadus and can publish school studies. The site includes – teaching entertainingly – numerous interactive games, illustrations as well as various tips and funny contents. The Dadus Project was launched symbolically on the European Data Protection Day, on 28th January, 2008. Previously regional conferences had been organized nationwide where the project was proposed and different leaflets, documents were handed over to the teachers. The education institutions welcomed the initiative; teachers registered immediately and began to deliver data protection lectures soon. The effectiveness of the project is clearly visible through numbers: 1.450 teachers registered, about 32.000 visitors consulted the Dadus site, shortly nearly 40.000 members logged into the Dadus blog, the members of forum of parents in turn almost reached 2.000 users. For the academic year 2008/2009 competitions were organized to student in order to enhance the participation as well as more and more new documents and games were invented. As a positive effect of the Dadus Project people in Portugal – mainly parents and teachers – take significantly better care of online perils affecting children. Earlier parents thought they would not have been able to tackle with these challenges, primarily due to the lack of infocommunication knowledge; in turn teachers experienced problems at schools to be resolved on a daily basis. The main objective is to enhance the awareness among minors by educating them to take autonomous decisions responsibly concerning their fundamental rights. Acknowledging the importance of having privacy issues in the school curricula, the Portugese Ministry of Education decided, in 2012, to officially introduce in the curricular contents of the discipline" Information and Communication Technology" data protection matters. This means that all pupils between 12-14 are learning mandatorily the main issues concerning data protection and privacy. In view of these new developments, the DADUS Project is being restructured in order to provide a more focus support to this new reality. The themes are being reorganized and more materials will be available for teachers and pupils to work in the classroom. The electronic platform will keep playing a central role for information, as well.

B. Ireland, "Private I, Public Eye"

In the past years the Irish DPA has intensively dealt with data protection issues of the youth.[76] Among the initiatives to promote awareness of data protection and privacy is- sues among the younger age group include:

- CSPE Resource Booklet (a coloured education leaflet of 92 pages for education purposes)
- Video Clip Competition (two video clip competitions were initiated to students in the topic of privacy - result can be seen on www.youtube.com/dataprotection
- Young Social Innovators 2008 - Survey
- Privacy Survey 2010: "The I in Online"
- Officefor Internet Safety- Updated Parental guidesfor Internet Safety (aparents'guidetonewmediatechnologies/to social networkingwebsites/ tocyberbullying)

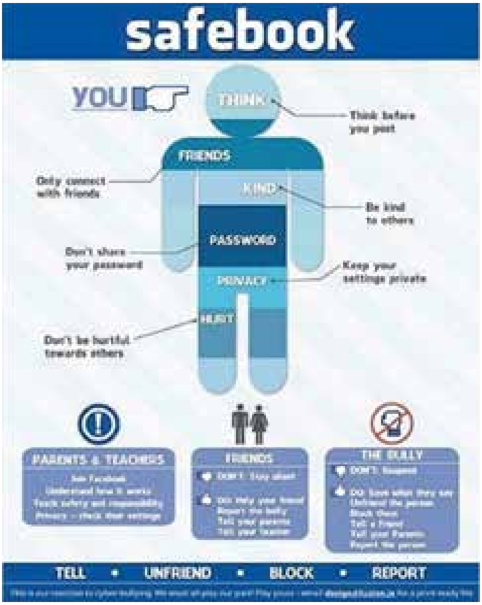


[76] http://dataprotection.ie/viewdoc.asp?docID=520

The Irish Ombudsman for Children, Mrs. Emily Logan consulted the topic of online bullying with over 300 children and young people between 10 and 7 years of age pupils with diverse socio-cultural background nationwide. The over- all aim of the consultation was to hear children's and young people's views and ideas about what ac- tions are needed to deal effectively with bullying in schools. *"It is estimated that there are at least 7,000 primary school and 3,700 post-primary school students who find it difficult to go to school every day as a result of being bullied frequently and that at least a further 24% of primary school students and 14% of post-primary school students have experienced bullying, albeit to a lesser extent."* In her summary report Mrs. Logan emphasized that schools have to handle the issue of preventing online harassment more frequently; pupils have to be taught that they are responsible for their online words and actions and serious consequences may follow thereof; additionally children have to be informed where to turn for help. (http://w w w.oco.ie/assets/files/OCO-Bullying-Report-2012.pdf)

The Irish Ombudsman for Children commenced another project named "Stay safe!" that intends to render fundamental information to primary school pupils, their parents and teachers mainly on the topic of assault and the prevention thereof includ- ing also the defence against cyberbullying. The programme was resumed by the "Cool school" project which was dedicated to up- per classes.

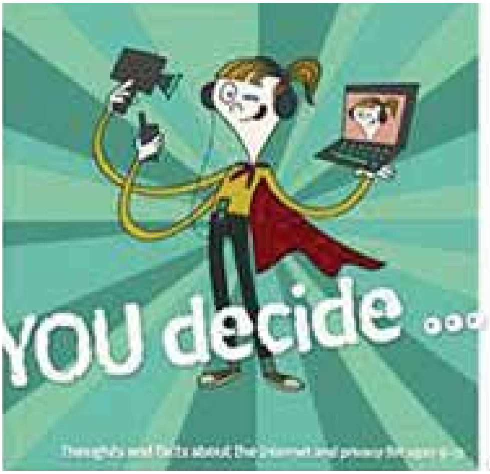
An Irish communication agency, the Fuzion Communications gives advice to children in pictures on social networking sites (http://www.thejournal.ie/safebook-how-to-stay-safe-online-657753-Nov2012/).


safebook
YOU
THINK
Think before you post
FRIENDS
Only connect with friends
KIND
Be kind to others
PASSWORD
Don't share your password
PRIVACY
Keep your settings private
HURT
Don't be hurtful towards others
PARENTS & TEACHERS
FRIENDS
THE BULLY
TELL • UNFRIEND • BLOCK • REPORT

C. Scotland, “Respect Me!” – “You don’t have to like me… agree with me… or enjoy doing the same things I do… But you have to respect me!”

The Trinity College Anti Bullying Centre’s “Respect me” program has been supported by the Scottish Ombudsman for Children’s Rights as well. The aim of the project launched by the Scottish Government in 2007, promoted also by the Scottish Association for Mental Health and LGBT Youth Scotland, is to overcome the (mainly online) harassments and to elaborate the most appropriate prevention programmes; to this end free trainings are organised nationwide on local levels. The project includes awareness and information campaigns to youths. In 2013 they launched the first ever respect me Anti-Bullying Awards to celebrate some of the amazing projects and initiatives being carried out at a local level across Scotland. (http://w w w.respectme.org.uk/What-do-I-do-if-a-child-tells-me-they-are-being-cyberbullied.html)

D. Norway, “You Decide”



“You decide” project is a co-operation be- tween the Norwegian Board of Technology, the Norwegian Data Inspectorate and the Centre for ICT in education. The aim of the project is to increase young people’s knowledge of privacy and to raise their con- sciousness about the choices they make when they use digital media such as the Internet and mobile phones. The project has developed two packages with teaching material: one aimed at secondary schools and one at the oldest children in primary school (ages 9-13). Each package consists of a brochure with facts, real life examples and topics for discussions/tasks. The leaflets dedicated to primary school students contain mostly drawings and some easier tasks for younger minors. The materials dedicated to secondary school students consist of more images and gets straight to the point. This also includes tasks, however, instead of the vocabulary attempts to clearly explain the legal terms (major considerations: everyone shall have the right for privacy which shall be respected; the internet will never be totally anonymous; do not share private contents for fun; how to share private contents; what to do against cyberbullying; who may know what of you via the net; who observes in the net). Throughout the project a number of films that highlight the subject have been developed. These films are meant to stimulate the debate in the classroom. Emphasis has been put on creating reflection and discussion, and not on rules. The project asks open questions, so that each individual can reflect on his or her own boundaries. If you have knowledge about the consequences of the different choices you make, you can also take responsibility for your actions. The Norwegian You Decide project has been adopted in about 16 countries.

E. Poland: "Your data-your concern" programme[77]

In 2009 the Polish Data Protection Agency (GIODO) produced an education leaflet for students and teachers with the collaboration of the Education Centre of Gliwice and under the auspices of the Ministry of Education and Children's Rights Ombudsman. The primary purpose has been to introduce data protection themes and privacy issues into the teachers training programme and into the curricula of primary and secondary schools in Poland. "Your Data-Your Concern!" includes training programmes and offers education materials and model presentations for teachers and encourages them to become familiar with privacy issues of pupils aged 7-16.

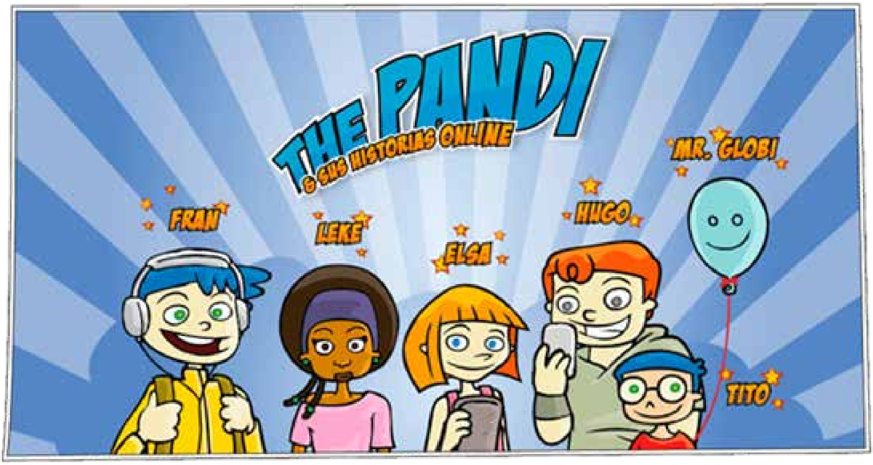
F. France: "More rights for your personal data"[78]

On the website of the French Data Protection Agency (CNIL) a separate subpage you can find an online version of a teenager magazine titled "More rights for your personal data", and additional special topics are discussed (e.g. geo-location, the online protection of personal data) as well as methodological practices and various education materials are explained.

[77] http://www.giodo.gov.pl/324/id_art/763/j/en/
[78] https://www.cnil.fr/en/more-rights-your-personal-data

G. SPAIN, “PANDI PROJECT[79]

The Spanish Data Protection Agency (AEPD) has created a subpage on its website dedicated to younger people (and their open-minded parents) based on a campaign called “Pandi” that follows the adventures of a friend circle in the form of comics. The cartoon teaches the children about the importance of data protection and the critical thinking. The website encompasses six education materials with basic skills and situation exercises in the following themes: personal data and privacy; rights, obligations and major online threats; digital personality and online reputation, social networks; images on web 2.0: e-mail, chat, message sending; ads, purchase and online entertainment; identity theft, online bullying and sexting.



H. New Zealand, Youth Privacy Kit

In 2009, the Privacy Commissioner started a project to find out what young New Zealanders think about privacy and to develop guidance material produced by young people for young people. The project began with a focus group of 15 secondary school students. Under the umbrella of “safety”, the student’s three key ideas behind the materials were awareness; consent; and appropriate use of information.

[79] http://www.tudecideseninternet.es/menores-v2/?q=node/176

They believed that the best way forward for young people to start to think about privacy was for us to encourage people to do a presentation, for instance to school assemblies. They were also keen to see teachers or senior students using the material in class. The students discussed what aspects of privacy caused them most concern and what advice people their age and younger needed to help them make choices about what was happening to their information. To improve awareness and the proper use of information they outlined a concept called "Youth Privacy Kit" (w w w.privacy.org.nz/youth) which includes the following elements:

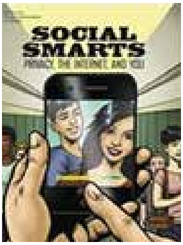
- notes guiding you how to present the topic to schools on data protection,
- privacy stories with discussion points, stories can be played and conversed later,
- a short film aims to get students thinking about what happens to their personal information,
- activities,
- a quiz with true/false questions on data protection,
- mini brochures,
- posters
- as well as a link to footage of the official launch of the kit and the "inaugural presentation".

Each part is aimed at mobilizing the youth: think over, play and experience the diverse situations then discuss what should have been done and how could have been overcome the abuse with personal data. Give advice to each other and share their positive and negative opinions with regard to different situations.

YOUTH PRIVACY

I. Canada, graphic novel and tips

The Canadian Privacy Commissioner created a variety of resources and tools designed for educators and parents including Presentation Packages for Parents and Teachers, Fact Sheets and Other Resources, Discussion Topics, Tools and Videos. (http:// w w w.priv.gc.ca/youth-jeunes/index_e.asp)



The colourful graphic novel dedicated to youngs – the Hungarian ver- sion can be found in the Appendix! – illustrates how many personal information we share without will or undetected in the internet. Devel- oped with feedback from youth, it tells the story of a brother and sister who learn (sometimes the hard way) about the privacy risks related to social networking, mobile devices and texting, and online gaming.

The Canadian Commissioner also published 12 tips for parents to help them limit the risks to their children's personal information, while allowing the minors to make the most of their time online:

- It's important to know the Internet spaces your kids frequent and the devices they use to go online!
- Try the spaces out!
- Keep up with the technology!
- Make restricting privacy settings a habit!
- Make password protection a priority!
- Emphasize the importance of protecting mobile devices!
- Remind your kids that what they post on the Internet is not always private!
- Teach your kids to think before they click!
- Stress the importance of knowing your real friends!
- Teach your kids that their personal information is valuable!
- Let your kids know that you are there if they make a privacy mistake!
- Set a good example!

Besides the Commissioner issued a school education plan in which he analyses 12 subjects, presenting each one briefly and setting issues for discussion:

- Think before you click!
- Do you take into account of your privacy settings?
- Do you mark only your real friends?
- Choose an appropriate password!
- Protect your online identity and take care of your personal data in the online world as well!
- Take care on online game sites!
- Beware of messages received from foreigners!

- Parents on Facebook
- Mobile applications
- Internet dating sites
- Sexting
- Cyberbullying

J. United States of America

In 1998 a new law was adopted in the United States of America a law on the online protection of personal data of children (minors below 13) with a view to prevent unlawful data processing[80] (Children's Online Privacy Act, COPPA). The law imposes additional obligations on data controllers of website providers that provide online or commercial services to children whereas the compliance with the law is supervised by the Federal Trade Commission (in the USA no supervisory authority exists with general powers and functions with regard to data protection) ex officio and upon complaints. The law encompasses websites which collect personal information on children during the provision of services. This includes not only homepages dedicated to children (e.g.: online toy shop or website of a cartoon offering online games) but also sites providing commercial or online services to the public if the services could be taken by minors as well and website providers are aware that services are in fact taken by minors. Website providers must:

- Obtain verifiable parental consent, with limited exceptions, prior to any collection, use, and/or disclosure of personal information from persons under age 13.
- Provide a reasonable means for a parent to review the personal information collected from their child and to refuse to permit its further use or maintenance.
- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected.
- Only verifiable active consent from the data subject is acceptable.
- Registrations with false date of birth data must be filtered. For example:

[80] Children's Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2581-728, enacted October 21, 1998).

a) at entering the date of birth users should have the right to set an age below 13 thus minors will not be forced to give a false information as well as the SP will be informed that a minor wanted to register;
b) even at entering the date of birth there should not be indications that children below 13 may not register or only with prior parental consent;
c) the site should ban the respective IP address for a while if the user's retreat is intended only to modify his age;
d) online purchase should be made exclusively by a nominative credit card;
e) if, upon the age provided, the user proves to be a minor then the reply should not be merely a denial but the child should be informed the services of the site may be utilized if he asks for his parents to register [it is also possible by law that SP may require the child to give him the parent's email address which certainly will be deleted following the unsuccessful or denied request].

- Employees of the SP shall attend a thorough data protection course as well as the SP shall adapt its internal policies to the legal requirements.

The law specifies multiple possibilities in obtaining a verified parental consent which are divided into 2 categories depending on the services of the site:

- 1. If the service foresees the disclosure of personal data of the minor to third par- ties (e.g.: social networking site, blog etc.) SPs shall use a more reliable method of consent, including:
  a) getting a signed form from the parent via postal mail or facsimile;
  b) accepting and verifying a credit card number in connection with a transaction;
  c) taking calls from parents, through a toll-free telephone number staffed by trained personnel;
  d) email accompanied by digital signature.

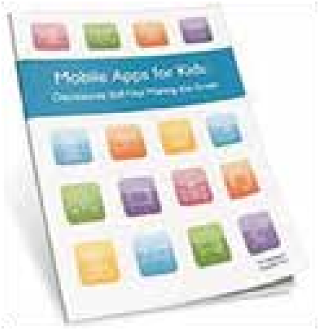
- 2. If the service foresees the processing of personal data of the minor solely for internal purposes and the transfer to third parties is excluded then, besides the above options, parents shall be entitled to give consent to the data processing via the following methods:

a) the parent consents to the data processing via e-mail and specifies a postal mail or facsimile number from which the SP may require a confirmation,

b) the parent consents to the data processing via e-mail; in a short period thereafter the parent will be required to confirm the registration.

In addition to the above the law stipulates stricter rules for the transfer of personal information (including intra-company transfers as well) as well as subcontracting data processors. The parent shall be noticed on every data processors hired and on each data transfers not fully coherent with the original purpose.[81]

In 2011 the FTC issued a staff report of kids' mobile apps whereas in December 2012 a new staff report was released that examined the privacy disclosures and practices of apps offered for children in the Google Play and Apple App stores.[82] The users (both parents and children) are not being noticed that identifiers of mobile phones and tablets (unique identifiers consisting of numbers and letters) are transmitted secretly by vendor companies to market researchers, social sites and marketing agencies that, as a result, could potentially develop detailed profiles of the children based on their behaviour in different apps.



The majority of apps examined failed to inform users on what data are being collected on them in spite of the fact that identifiers had been transmitted, in most cases, to third parties, too. 17% of apps entitled children to buy virtual goods for real money up to 30 USD. (http://www.ft .gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing)

K. EU practices

From EU projects the Safer Internet program[83] shall be mentioned first and foremost which was launched by the European Union in 1999 and currently 30 countries are

[81] http://www.coppa.org/comply.htm, 2013.04.15.

[82] http://www.ftc.gov/opa/2012/12/kidsapp.shtm, 2013.04.22.

[83] http://www.saferinternet.hu

involved (Hungary joined in 2009). From 2004 on the project has been called Safer Inter net Plus. All NGOs and law enforcement agencies are covered in all countries which can collaborate very effectively by virtue of mutual dialogue and cooperation. The Hungarian member of the consortium is the National Children's Safety Service, the Blue Line Children Crisis Foundation and the National Network Security Centre. The aim of the project is to make the internet and online technologies safer, particularly for children, and to tackle with unlawful and/or harmful contents. The most important achievements include the running of hotlines and help lines through which anybody may report or ask for help. Participating organisations do their best to increase the awareness among users; the self- regulation is stressed when promoting the safe online background. They fight unsolicited and harmful contents by means of filtering systems, information exchange, child welfare measures and close cooperation with the police and law enforcement authorities. The Safer Internet Day (5th February) is celebrated worldwide with special programmes, conferences and school lectures.

The handbook titled **"Web We Want"**[84] and edited by teenagers to teenagers was published in February 2013, on the Day of Safe Internet, by the Insafe network. The publication examines, among others, the rights and obligations and urges the readers to think about the behaviour of himself and fellow people. Its equivalent –Handbook to teachers – has been elaborated by teachers to teachers. (The publications are freely available.) It helps teachers to bring in online activities of students into the school curricula by interactive study programmes and tests which are in line with the national competence framework system. Each task covers topics and related goals in a well structured manner. The various points drawn up in the publication enable students to comprehend better the advantages as well as the challenges of the internet and to learn skills needed for their future life and career.

[84] http://www.webwewant.eu/hu/web/guest/about

The EU Kids Online research series (www.eukidsonline.net) has summarised, on the one hand, results of already accessible research materials and, on the other hand, has set up a new database stemming from a survey in autumn 2011 covering as much as 25 countries. The survey deals, beyond the two basic term of risk and adverse effects, with the inclination to adverse effects as well. The most remarkable findings of the research regarding Hungary are still valid; it is regrettable that a similar report has not emerged since then.

- *Analysing the complex web of risky online activities among Hungarian children, between 9-16, 37% of them have experienced at least one out of the five most risky activities – they experienced an average 0,74 cases. 12% have encountered one, and only 0.5% of them had experiences with multiple risks. The most widespread risky activity is the online dating which has already been done by 25% of kids. Afterwards comes the browsing of perilous contents (16%). Despite the preconceptions regarding the internet browsing pornographic contents is far less prevalent: every 10th kid has experienced it. Sexually motivated messages and activities are far rarer similarly to the online bullying (6-6%).*
- *Experiences with risky actions grow evidently in conformity with the age – the turning point is at the age of 14 and 15 when the number of affected kids increases suddenly. Ac- cording to the regression analysis other demographic valuables influence this theme in less degree; in this regard the qualitative features of internet use are far more important and the some psychological off- and online factors. The frequent and diverse internet use as well as the common risk-seeking behaviour enhances the chance of testing risky activities.*

- *Generally 10% of children reported bad experiences during browsing the net. Concerning the 4 behaviour types that were examined in more details it is very variable to what extent those have been perceived as harmful. The highest ratio comes up relating to bullying (72%), followed, with more lower extent, by facing sexual images, videos (30%) and experience with sexual messages and behaviours (29%). The lowest ratio (9%) of bad experiences was encountered relating to children having gone to an offline meeting with someone first met online. Summing up and also observing the severity of bad experiences 5% said they had been bothered or upset by someone in the past.*
- *The internet addiction – based on own confession of kids or the opinion of parents – seems not to be widespread among Hungarian minors.*
- *Data shows that children who collected bad experiences could handle the cases actively and reduce the harm. Though fatalist aspects also occur in the responses frequently, 40% of persons affected chose exclusively an active strategy (discussed the issue with someone, took precautionary measures etc.) and merely 10% used solely passive means (for instance suspended internet activity for a while).*
- *Solely 24% of minors between the ages of 11-16 considered the assertion false that they would be more familiar with the internet than their parents. 30% rather agreed with this figure whereas the remaining 46% definitely claimed they were more experienced online compared to their parents. That is to say, in case of almost every second minor the parent, in terms of IT knowledge, is in a detrimental situation compared to his child.*
- *Around half of the Hungarian children are able to bookmark websites, find information on how to use the internet safely, block messages from unwanted persons, delete their browsing history and change privacy settings (45%) on social networking sites. Only 38% are capable of blocking unsolicited messages and less than one third felt himself skilled to compare di- verse websites with a view to obtain the required information. Finally only every fifth minor knew how to modify the filtering settings on his PC.*
- *In relatively small number of cases when some online risks or perils affected a kid factually harmfully (taking into the volume of this research) active reactions from their part could be detected which apparently contributed to solving the problem. This survey, of course, cannot provide sufficient information on the long lasting, real and complex effect mechanisms of these*

cases. Therefore our findings may only indicate that the problem exists and the reactions are quite di- verse, the majority of kids – by their own admissions – can handle the challenges relatively well.

- *More than one quarter of parents questioned do not use the internet. 43% use the internet frequently, on a daily basis. One in four Hungarian children's, aged between 9-16, parents surely do not use the internet whilst their children do. Here we can find a gap in terms of computer literacy and knowledge. Parents not using the web can be located, to a high extent, in smaller towns (below a population of 10.000 and 2.000) and in lower income households.*
- *The less restricted activities include instant messaging as well as watching videos and video clips. On social sites about half of the kids are allowed to create an own profile without pernission.*
- *Two thirds of parents (75%) regularly talk to their children about what they do on the internet. This conversation between the parents and kids depends, to a rather large extent, on whether parents use the web.*
- *Parents with a higher computer literacy can, of course, assist their children in either searching for useful contents or ensuring safer internet use.*
- *More than half (52%) of parents of kids who use the internet (also) at home habitually check what their children do online, nearly 40% also watch the child's online profile on a social networking site while 35% controls the contacts in instant messaging programmes. Incoming/outgoing messages – either emails or instant messages – of kids are inspected by 23% of parents.*
- *Around two third of children got support from their friends when they had difficulties in finding something on the internet. 24% helped when a bothering or annoying online content was encountered.*
- *Teachers generally do not fall behind, however, kids receive more support from parents than from educators."* [85]

[85] Bence Ságvári: On the EU Kids Online research in Hungary from: http://w w w.lse.ac.uk /media@lse/research/ EUKidsOnline/ParticipatingCountries/NationalWebPages/Hungar y%20webpage.pdf, 07-03-2013

9. “Hungarian recipe”

Based on international examples we would like to bring forward some easy and cheap initiatives and ideas for interested adults and children so that, in our expectation, they could give rise to contemplations about the internet and to develop empathic skills that could promote sophisticated internet use.

Stories

The class or a minor group reads out or plays true or invented stories in relation to violation of privacy/data protection rights then they discuss the emerging problems from different points of view (drama pedagogy). They evaluate the behaviour of participants and the consequences thereof as well as draw conclusions on what could have been done better or in another way.

“Privacy diary”

Students are tasked with keeping a diary for a shorter period (1 week-1 month) thus recording on what happened to them within the given period:

- In what range they disclosed personal data concerning their private life?
- What has another person (acquaintance, unknown person) written or told about them?
- Have they revealed their name, phone number or email address to anyone online?
- Have they logged into a website?
- Have they downloaded or uploaded files to the PC?
- Have they used their mobile phones for online applications? etc.

Once the diaries have been composed, the class/group would be requested to discuss and evaluate the findings freely.

Creating a portrait and a profile of a third party

Using the collected diaries children should collect all personal information available of themselves and/or of a well-known person then they should create a profile. Everybody should analyse independently whether the online profile corresponds with the real person’s personality.

The second task is to choose a close acquaintance (family member, classmate or teacher) and to create a profile on the person concerned by means of all available online sources (images uploaded to the internet, marked favourite activities, shared websites, clubs, spare time activities). This should be presented to the model person and students should observe his/her reactions; whether there are some information that the person is unwilling to hear or see on himself though previously he shared this specific information with everywhere voluntarily.

Privacy-oriented examination of artistic works implying serious privacy violations: (examples)

Films:

- Rear Window, 1954, Alfred Hitchcock
- The Net, 1995, Irwin Winkler
- The Game, 1997, David Fincher
- Gattaca 1997, Abdrew Niccol
- Truman Show 1998, Peter Weir
- Enemy of the State, 1998, Tony Scott
- Minority report, 2002, Steven Spielberg
- Changing Lanes, 2002, Roger Michell
- The lives of others (Das Leben der Anderen) 2006, Florian Henckel von Donnersmarck
- My dear spied friends (Drága besúgott barátaim) 2012, Cserhalmi Sára
- The Social Network, 2010, David Fincher
- Trust, 2010, David Schwimmer
- Cyberbully , 2011, Charles Binammé
- Caught in the Web ,2012, Chen Kaige
- Disconnect, 2012, Henry Alex Rubin
- Identity Thief, 2013, Seth Gordon
- Selling Innocence, Pierre Gang, 2004

Novels:

- Thomas Mann: Mario and the magician
- George Orwell: 1984
- Heinrich Böll: The Lost Honour of Katharina Blum
- William Golding: Lord of the Flies
- Natascha Kampusch: 3096 days

Poems:

- Attila József: A Breath of Air!
- Dezső Kosztolányi: I have been recorded into several books
- Gyula Illyés: One sentence on tyranny

Internet glossary

ban: excluding/prohibiting one or more persons from a concrete channel (consequently the user will not be able to sign in again even after the change of his nickname.)
banner: "banner advertising", the most frequent means ofinternet advertising ("Button"= advertisement in more little pixel size than that of banner).
bookmark: Possibility offered by the browser pro- gramme to mark the internet site visited in order to facilitate the return there to.
botnet: "robot network", network of zombie computers that, by virtue of various viruses and Trojan softwares, get under control of a cracker. Fol- lowing that the powers of the PC will be used for his own purposes in most cases without the knowledge of the owner or the user of the PC. These PCs governed by bots are used by spam senders (zombie PCs are capable of sending even 25.000 spams/hour) and other criminal gangs with maliciously (tort, intimidation etc.).
browsing: search inthernet, visiting numerous sites by starting from one webpage through multiple sites when finally getting to unknown pages (surfing).
browser: a programme intended to search for, and inspection of, information on different websites.
bug: error or malfunc- tion in programmes (resulting in e.g. "frozen" screen or total system collapse).
cache: swiftly operating automatic data storage with a view to temporarily store the frequently used data.
chat: two or more people conversing with each other online where the chat room is provided by chat programmes.
clicks and mortar: a mixture of traditional and virtual commercial activity.
cloud computing: a common feature of daily growing IT services where the services are provided neither by the user's PC nor by the company's central PC but by a remote server which can be located anywhere in the world. The most frequent cloud computing facilities include the online mailing systems, web hosting sides, developer environments, virtual work stations (e.g.: Gmail, Dropbox). A benefit for customers thereby is that cost effective and personalized IT solutions are offered to them, but the application raises privacy concerns since the movement of data is not really traceable.
cookie: short data files that are placed by the homepage visited on the client's PC – theoretically with the consent of the user. Its objective is to facilitate and make the respective info communication (ICT) and online service more comfortable. Several types of cookies exist; however, they can be arranged into two categories. Temporary cookies are

placed for an interim session (e.g.: during on- line banking for authentication) whilst permanent cookies (e.g.: language settings on a website) remain on the PC until they are erased by the user.

CTCP: Client-To-Client Protocol, direct data ex- change between two PCs.

cyber bullying/bullying: "online bullying", transmission or disclosure of text/image contents via internet, mobile phones and other modern technologies which are capable of humiliating another person. The harassment is directed against an intended victim recurrently against whom s/he is unable to protect him/herself.

deleb: dead celebrity

domain name: a unique identifier of a website.

e-commerce: "electronic commercial service"

electronic signature (e-signature): authentic signature produced via IT methods and approved by law.

grooming: online dating by giving a false identity

hashtag: searching for similar comments on Twitter

hoax: chain letters, rumors spreaded via e-mails, "false news"

intexticated: sending messages during driving a car

lamer: negative attribute, often used by users indicating their unfamiliarity with specific topics and requesting patience should they ask or say pointless things.

meme: disseminating digital files (mainly images) online in order to make others to enjoy a painful or even a false/manipulated image/ video (meming).

msg (private): separate conversation that can be followed only by the chatting partners; many people wrongly call it private channels but if we wish to exchange messages with our partner we do not need to be present at the same channel.

netiquette: ethical norms in the internet

nick: a unique username chosen by the user

off topic: far from the general subject of a discussion

op or @: before the name of a user: a person (or a bot) who is authorized to act as operator on the respective channel due to his reliability (may exclude others from the channel).

plugin/social plugin: "like" and "share" buttons

pop-up window: a new window opening up automatically when you download a website, usually containing information from the webpage downloaded (campaigns, advertisements).

post: leaving a message on an image board or a website.

smartphone: "smart mobile phone", mobile phones capable of installing and using external applications.

sexting: messaging with erotic text/image contents közvetíti, ahogy éppen játszik).

teamspeak: communication by voice so as to hear there- actions of fellow participants (receive only) as well as to enable us to comment.

topic: "theme", headline of the channel

torrent: fast download shared with numerous PCs during which the downloaded file is split up into multiple smaller files and these files are being downloaded by multiple PCs simultaneously (used primarily for illegal downloading of music, movies).

troll: provoking, anti-social utterance, kind of "verbal insulting"

ufriend: rejection of a person

URL: Uniform Resource Locator, standardised internet domain informing on the location of the document.

viber: an installable programme similar to Skype that enables free (or very cheap) internet telephoning and sending of messages to friends who have also installed the programme.

website: combination of homepages to be located under the same domain name in close relation to each other.

webpage: "website", document appearing in the browser as a complete site. It may contain texts, hyperlinks, images, voice, animations, videos and active programmes starting when the site appears. The "home" is usually the starting point and the index of the website from where we can access to almost all contents of the page. The website is regularly the site which appears when entering a domain name.

Where to call for help in Hungary?

Where?	Contact	In what
National Authority for Data Protection and Freedom of Information www.naih.hu	1125 Budapest, Szilágyi Erzsébet fasor 22/C. Tel: +36 -1-391-1400, e-mail: ugyfelszolgalat@naih.hu	If I have questions concerning my constitutional rights with regard to data protection or the publicity of data of public interest (freedom of information) or my informational rights have been violated or may be violated.
Commissioner for Fundamental Rights www.ajbh.hu	1051 Budapest, Nádor utca 22. Tel: (06-1-) 475-7100 e-mail: panasz@ajbh.hu or specially or children kerdesemvan@obh.hu	If the activity or negligence of a public authority violates or may directly violate my fundamental rights.
National Media and Infocommunications Authority www.nmhh.hu	1133 Budapest, Visegrádi u. 106. Tel: (06-1) 468 0673 e-mail: info@nmhh.hu	If I want to submit a complaint against telecom SPs (e.g. complaints concerning mobile phone, internet or postal services, reporting of unsolicited electronic advertisements and spams) as well as complaints against media content providers (e.g. complaints concerning TV or radio programmes, so called downloadable media contents, contents published in written or electronic press and other internet contents).

National Media and Infocommunications Authority Internet Hotline	1015 Budapest, Ostrom u. 23-25. e-mail: internethotline@ internethotline.hu	If I want to submit a complaint on illegal or harmful contents that can affect minors it is possible to report them on the site of Internet Hotline (http://internethotline.hu/tart/ index/31/ Bejelentes) and in email (internethotline@ internethotline.hu) in 9 categories (content disclosed without valid consent, paedophile content, harassment, racist, xenophobe content, violent content, content promoting drug consumption, content fostering terrorist attacks, phishing sites as well as contents perilous to kids).
Blue Line Child Crisis Foundation www.kek-vonal.hu	Tel.: 116-111 vagy 06 1 354 1029 e-mail: kek-vonal.hu chat: http://chat.kek-vonal.hu	If I, as a child, feel that I got into trouble, I am bullied online, I found bothering sites or messages or, as a parent, I worry that my kid have had bad experiences on the internet and I wish to resolve the situation discussing it with somebody.
International Child Welfare Service www.gyermekmento.hu www.saferinternet.hu	H-1066 Budapest Teréz krt. 24. Tel: +36 1 475 7000 Fax: +36 1 302 4136 ngysz@gyermek-mento.hu	Either if you wish to deliver a lecture to pupils, teachers, parents or social workers at schools on safer internet use, the large opportunities the internet is offering, on simple and effective methods how to avoid possible risks and threats or if you want to be involved in such courses.
Government Incidence Response Centre www.biztonsagosinternet.hu	bejelentes@biztonsagosinternet.hu https://www.facebook. com/biztonsagosinternet	If I want to submit a complaint on illegal or harmful contents that can affect minors it is possible to report them on the site http://biztonsagosinternet. hu/bejelentes. The main scope of activity encompasses fighting against pedophile contents, harassment, racist, violent content, content promoting drug consumption as well as contents disclosed without valid consent.