



Hungarian National Authority for
Data Protection and Freedom of
Information

KEY TO THE WORLD OF THE NET!



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

2013

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)

2013

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)

NÓRA BELSŐ (M.D. PSYCHIATRIST)

LAURA KOZMA (NAIH)

ÁGNES LUX (OFFICE OF THE COMMISSIONER FOR FUNDAMENTAL RIGHTS)

PETRA MÁRKUS (NAIH)

ATTILA MÁTYÁSFALVI (NAIH)

BORBÁLA CSEKEŐ REMÉNYINÉ (BLUE LINE CHILD CRISES FOUNDATION)

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 publication of the present Study!

CONTENTS:

1. Introduction	1
2. Presentation of the National Authority for Data Protection and Freedom of Information (NAIH)	3
3. Case-law of the DPA, the ombudsman and the police	4
4. Advantages of the internet	15
5. Children's rights in online environment	17
6. Key topics	26
A. Age and maturity	26
B. Anonymity	30
C. Personality distortion	31
D. Public spaces	37
E. Harmful contents	41
F. Possible trends of future development	44
7. Mapping of problems – online deviancies	47
a. Cyberbullying	48
b. Internet memes	50
c. Provoking comments (troll)	50
d. Sending erotic photos (sexting)	51
e. Internet pedophilia	52
f. Online meshing (grooming)	54
g. Online games	54
h. Other forms of personal data abuses	59
8. Best practices (data protection supervisory authorities, ombudsmen)	61
a. Portugal	61
b. Ireland	62
c. Scotland	64
d. Norway	64
e. New Zealand	65
f. Canada	66
g. USA	67
h. EU practices	70
9. Hungarian “recipe”	74
+ Appendix (for children)	77

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.” (Dr. László Ropolyi)¹

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, 2008³) 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 researches⁴ focusing principally on children also warn that the risk of evolution 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, OCIFE 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., OKRIO 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. Fortunately lots of programs, campaigns and organizations deal with potential online threats to children in Hungary, as well.

The objective of this 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.

⁶ Y generation: born between 1976 and 1995, affected by an overwhelming impact of technology development, Z generation: the first global generation, teenagers of today who were born between 1995 and 2009.

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 (Infotv.)⁷ 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), receives complaints from citizens. 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 10 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. The prevention and the dissemination of information have therefore utmost importance whilst the remedy of infringements and the awareness raising of data subjects and the public are also fundamental requirements.

⁷ Act CXII of 2011 on Informational Self-determination and Freedom of Information – Hungary

3. CASE-LAW OF THE DATA PROTECTION SUPERVISORY AUTHORITY, THE OMBUDSMAN AND THE POLICE

Case-law of the supervisory authority

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 authorisation of law.

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

- A photo of a friend, to be found on iwiw (the first Hungarian social network site), of the petitioner 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 defence, 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 www.facebook.com (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).

- Another 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).

- In another case 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 the site www.puruttya.hu 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).

- In another case the photos of the complainant's daughter of 16 had been removed from the site www.myvip.com and uploaded to www.pedomaci.hu 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 www.pedomaci.hu 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 my-vip 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 bugging 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 the website puruttya.hu containing also his photos with names and obscene comments. The complainant was receiving numerous messages to his iwiw email-box from visitors of the site "puruttya" (ABI-1243/2010/P).

In view of the repeated complaints the Commissioner filed charges against a person unknown on 15th February 2011 in virtue of the misuse of personal data violating Section 177/A. (1) of the Act IV of 1978 on the Penal Code. The sites charged as follows: www.tundermacko.info, www.pedomaci.net, www.puruttya.hu, www.sunaszemle.hu, www.agyiszint.hu, www.napiszar.com (these domain names continually vary due to sanctions). Photos appearing on these pages 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 no. 2.Pf.21.792/2009/4. 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 Commissioner has approached the companies having registered the respective websites due to the violations of law committed on the website, however, the general managers 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 dated 28th July 2011. 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 to terminate the investigation was repealed by the V. and XIII. Prosecutor's Office since even the reasoning of the decision of the Police 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 though 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 10 million HUF.

The NAIH investigated the data processing activity of Generál Média Publishing Ltd. in the course of a data protection administrative procedure. The ground for it: 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 of 7th March 2013 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).

Ombudsman cases

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 usage, Commissioner for Fundamental Rights. The Parliament elects the Commissioner in order to protect the 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 pursuant to Act CXI of 2011⁸ determining his powers. Every year he conducts thematic investigations in the framework of special projects in this area of law (2008: children's rights awareness raising, 2009: violence against children – with special attention to violence in schools, 2010: the role of families and family replacement institutions, 2011: rights of children to physical and mental health in the broadest sense; 2012: child friendly justice). Besides the traditional functions of the ombudsman (complaint handling, investigations ex officio), the proactive protection of rights becomes more significant in the field of children's rights. 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.

In January 2011 a petitioner entered the homepage on children's protection rights who complained that a mailing system (freemail) had forwarded spams containing unsolicited advertising messages on penis enhancement to minor users. According to his position the defence argumentation of the site claiming that the age of users are handled in accordance with data provided at the time of registration cannot be accepted because

⁸ Act CXI of 2011 on the Commissioner for Fundamental Rights

the authenticity of information rendered had not been verified, what's more, they do not qualify as being legally valid statements. If the distribution of marketing messages is based on such personal data it is to be considered a crime, a massive violation of children's rights. For the limits of powers the ombudsman was unable to launch an investigation, however, the complainant forwarded his letter to the Hungarian Association of Content Industry (MATISZ) and the Hungarian Advertising Association as well. The president of MATISZ asserted in his reply that new provisions had been enacted in order to regulate spam messages in the USA and Europe between 2002 and 2003; nevertheless 90-95% of the global email traffic is made up by the sending of spam messages, that is to say, the effective solution for the problem is still to come. Apathy and ignorance of users also play some role since a considerable part of networks responsible for distributing spams consists also of infected PCs. According to MATISZ's knowledge the detection and disconnection of botnets, accountable for spreading of spams in the USA, as well as the capture and conviction of operators and developers of infectious botnet components is considered the most effective approach. A list is kept on the largest spam botnets generating traffic (<http://www.techrepublic.com/blog/10-things/the-top-10-spam-botnets-new-and-improved/1373/>).

In Hungary the National Media and Infocommunications Authority is competent principally in the cases relating to spam messages. They operate a website for reporting unsolicited spams (<https://e-nmhh.nmhh.hu/e-nhh/4/urlapok/esf00101/>). The MATISZ intends to solve the issue of spams and the control of companies dealing with online business marketing by establishing partner networks and within the media law (by self-regulation) with the objective to protect children's privacy. Partners to be involved: the National Media and Infocommunications Authority (www.nmhh.hu), the Direct Marketing Association (www.dimsz.hu), Association for Electronic Commerce (www.szek.org) as well as the Advertising Self Regulation Board (www.ort.hu). Regarding perilous (deceptive, malicious etc.) spams and the avoidance thereof the best defence is the enlightenment which is achieved via education centres, in Hungary the International Children's Safety Service (www.ngysz.hu) among the consortium members available on www.saferinternet.hu. In particular emails from unknown persons or composed in a foreign language may contain deceptive contents or the spam sender has been motivated by financial gain or the deliberate infection of the destination computer (mainly motivated also by intentional financial gain). The best defence method is the immediate deletion of the respective email message without being read and, as far as attachments and annexes are concerned, they must not be opened of course since they may contain harmful codes (which may destruct

the PC as well). If somebody were to be approached by an unsolicited email offering a job opportunity or a prize etc. it could probably be a deception aiming at obtaining as much money from the unsuspecting and naive victim as possible. Unfortunately a perfect means to filter/remove spams has not been invented as yet and presumably will not either. There are existing spam filters powered by SPs⁹ (on mailing servers) and clients (on own PCs); among others the complex defence packages of modern antivirus softwares contain such components therefore it is worth installing them. But you need to know that not each spam filtering system, powered either by SPs or clients, is capable of removing all spams.

- In another case the president of the Hungarian Association of Health Visitors submitted a petition to the ombudsman. In a programme of Radio Kossuth dealing with the sexual education of the youth emerged that the first hit of Google search engine, upon entering the term 'sexual education', brings forth an incestuous, homo- and heterosexual animation link. The ominous first hit is still available. The ombudsman, given his jurisdictional limits, could advice merely on how to report illegal/detrimental contents.

Police cases

At the request of NAIH the National Police Headquarters (ORFK) provided a brief overview of trends and features of serious internet-related crimes, known to the Hungarian Police, where children had been involved. A remarkable part of those actions are predicate offenses: accordingly to achieve a serious goal a minor offense should also be committed.

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. Youngs 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

⁹ SP = Service Providers

“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 hides 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 find a place for all ages, moreover, useful data may be acquired on potential victims in advance:

“The obtainment of some 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). One should also be precautionous when disclosing family photos since, by doing so, children can be victimized by their parents (and vice versa, information published by youngs may raise the attention of potential burglars). In accordance with police experience some perpetrators visit the social sites for this very reason and consciously choose their prospective victims by virtue of the disclosed data: pretending to search for love, offering hostess/artistic model jobs or Western European schools for which promises youngs easily go.

“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 disclosed (written, uploaded) on the internet shall be regarded as being available to anyone and

therefore 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.*

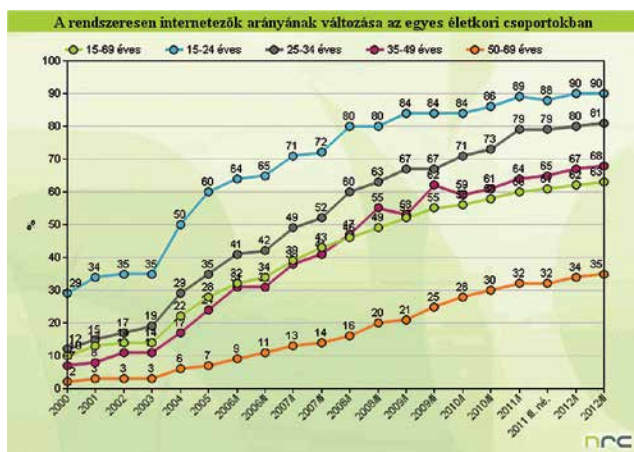
In connection to child pornography it shall be noted that there are usually misunderstandings in Hungary concerning the term “teens” compared to the Hungarian usage of “tini” (teenager) to be found on special sites. In view of the sexually oriented websites and the ‘sex industry’ the expression “teen” 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. ADVANTAGES OF THE INTERNET (INFORMATION SHARING, LEARNING, ENTERTAINMENT, SKILL DEVELOPMENT, NETWORK OF CONTACTS)

In Europe children, aged between 9-16, having access to the internet, browse the net for 1-5 hours a day, this ratio in Hungary is 2,5 hours a day (156 minutes). Children are online for an average of 1,5 days a month (39 hours), twice as much as their parents think. Domestic surveys carried out by the International Children's Safety Service revealed: almost all juveniles aged between 13-17 have access to the internet at home as well, they have mobile phones and half of them are in possession of even smart phones. Fashion trends advance towards smart phones which are clearly shown in Japan where the majority of the youth (60%) access the internet via a mobile net connection.¹⁰



Source: Internet penetration report 2011/Q3, NRC, Hungary, different age groups¹¹

The ‘network of networks’ offers several advantages to children as well. In relation to the Hungarian language admission essays of the year 2013 on internet usage among secondary schools’ pupils aged 14 the following typical replies have been given: *‘The internet is very important and useful to the mankind nowadays because you can find there everything. We get easily access to information, essential documents via internet. Though lot of people – mainly teenagers – browse social sites instead of studying’* or *‘We can obtain information*

¹⁰ <http://www.prherald.hu/2011/12/cyberbullying/> (report of Ágnes Romet-Balla of 29th January 2012)

¹¹ in.: <http://nrc.hu/hirek/2012/01/13/Internetpenetracio>, 23 April 2013

*more effortlessly and keep in contact more easily with friends who are far away from us but we receive probably more useless information than useful upon entering the internet.*¹²

Already in the year of 2010 in the USA the internet became the most significant information source among young adults¹³ and the same applies to European kids as well. There are no volume limits or time restrictions, copying or other additional costs, storage of, and search for, information in any format or quality is a ‘child’s play’. The internet could also be an excellent domain for constructive fun, skill development or making friendships if it takes place in a civilized and secure environment.

A Hungarian comparative study of 2010, examining the habits of children aged 10-18, concluded¹⁴ that the purpose of regular online attendance of youngs, in a male-female distribution, are primarily the community relations (47-53%), entertainment (46-37%), playing games (29-6%) and only finally education (5-4%). Although youngs who are online at least weekly the chief purpose is education (40-50%), entertainment (37-45%), community relations (32-35%) and playing games (43-26%). Almost everyone uses search engines for studying and using electronic dictionaries and Wikipedia is also very popular. Sites providing thematic links and education materials as well as pages offering language and other tests (e.g. secondary school graduation tests) are visited but rarely. According to the Hungarian results of an EU survey of 2011¹⁵, however, 60% of Hungarian children aged between 9-16 use the internet daily (mainly boys from Budapest), whilst 35% use the web once or twice weekly. The most popular activity is watching videos followed by the information collection for school tasks as well as visiting several social sites (especially girls). The second most popular category, nearly with the same value, includes the instant message sending, the online game as well as the sending/receiving emails.

Internet culture has an effect on the habits of children in almost all aspects of life, e.g. new lingual expressions are created (such as “deleb”, “liking”, “intoxicated”), novel communication methods are used (e-mails instead of postal letters, blogs in place of diaries etc.). All these phenomena heavily influence the younger people’s way of thinking and behaviour. We shall emphasize that these changes are natural consequences of the development of the “network society” and should not be condemned.

¹² Source: own collection

¹³ 65 % of respondents cited the internet resources as source of news, this ratio is almost the double of those registered in 2007. Source: Pew Research Center study, 01-04-2011 in: <http://mashable.com/2011/01/04/internet-surpasses-television-as-main-news-source-for-young-adults-study/>

¹⁴ LEVENTE SZÉKELY: Internet boot on the school desk from.: New Youth Review 2010/winter, pp. 79-87.

¹⁵ BENCE SÁGVÁRI: On the EU Kids Online research in Hungary from.: <http://webcache.googleusercontent.com/search?q=cache:0FNg25fSKjEJ:www2.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/NationalWebPages/Hungary%2520webpage.pdf+eukids&hl=hu&gl=hu, 2013-02-14>

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 2:

1. States Parties shall respect and ensure the rights set forth in the present Convention to each child within their jurisdiction without discrimination of any kind, irrespective of the child's or his or her parent's or legal guardian's race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status.

2. States Parties shall take all appropriate measures to ensure that the child is protected against all forms of discrimination or punishment on the basis of the status, activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members.

Article 3:

1. 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 4:

States Parties shall undertake all appropriate legislative, administrative, and other measures for the implementation of the rights recognized in the present Convention. With regard to economic, social and cultural rights, States Parties shall undertake such measures to the maximum extent of their available resources and, where needed, within the framework of international co-operation.

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 6:

2. States Parties shall ensure to the maximum extent possible the survival and development of the child.

Article 8:

1. 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.

2. 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:

1. 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.

2. 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:

1. 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.

2. 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 (ordre public), or of public health or morals.

Article 14:

1. States Parties shall respect the right of the child to freedom of thought, conscience and religion.

2. States Parties shall respect the rights and duties of the parents and, when applicable, legal guardians, to provide direction to the child in the exercise of his or her right in a manner consistent with the evolving capacities of the child. 3. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect

public safety, order, health or morals, or the fundamental rights and freedoms of others.

Article 15:

1. States Parties recognize the rights of the child to freedom of association and to freedom of peaceful assembly.

Article 16:

1. 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.

2. The child has the right to the protection of the law against such interference or attacks.¹⁶

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.

¹⁶ 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 separatable 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

Article 19:

1. 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 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.

2. 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 23:

1. States Parties recognize that a mentally or physically disabled child should enjoy a full and decent life, in conditions which ensure dignity, promote self-reliance and facilitate the child's active participation in the community.

Article 28:

3. States Parties shall promote and encourage international cooperation in matters relating to education, in particular with a view to contributing to the elimination of ignorance and illiteracy throughout the world and facilitating access to scientific and technical knowledge and modern teaching methods.

Article 29:

1. 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.

2. No part of the present article or article 28 shall be construed so as to interfere with the liberty of individuals and bodies to establish and direct educational institutions, subject always to the observance of the principle set forth in paragraph 1 of the present article and to the requirements that the education given in such institutions shall conform to such minimum standards as may be laid down by the State.

Article 31:

1. 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.

Article 36:

States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare.

Article 41:

Nothing in the present Convention shall affect any provisions which are more conducive to the realization of the rights of the child and which may be contained in:

a) The law of a State party; or

b) International law in force for that State.

Article 42:

States Parties undertake to make the principles and provisions of the Convention widely known, by appropriate and active means, to adults and children alike.

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 (Infotv.) 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 Infotv. as follow:

Section 4

1) 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.

2) The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose.

3) 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.

4) 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 juvenile¹⁷ (e.g. the case of photos taken for the purpose of medical research).

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.

¹⁷ Working document 1/2008 on the protection of children’s personal data

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 conflict resolution 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.*¹⁸ The Hungarian civil law reaffirms this rule¹⁹ 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 adulthood²⁰ 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 except 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).²¹

¹⁸ Art. 1 of the UN Convention on the Rights of the Child, 20th November 1989

¹⁹ Act V of 2013 on the Civil Code, 2:10

²⁰ Working document 1/2008 on the protection of children's personal data p.3.

²¹ <http://en.wikipedia.org/wiki/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 16-18.²²

According to the Hungarian law - unless otherwise provided by specific legal provisions, including also the Infotv (!) - 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.²³

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 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.²⁴ 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.²⁵ According to the new Draft Data Protection Regulation in particular cases a minor, below the age of 13, may also make a valid legal statement without parental consent (for example if s/he becomes victim of a sexual abuse).

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.²⁶ 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 become 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.²⁷).

²⁴ Children's Privacy On Line: The Role of Parental Consent, Working Paper of the IWGDPT, 26 March 2002

²⁵ Section 6(3) of the Act CXII of 2011 on Informational Self-determination and Freedom of Information (Infotv.).

²⁶ 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.

²⁷ http://index.hu/tech/2013/04/22/gyerekek_es_az_internet/, 05-15-2013

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 – 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.²⁸

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.²⁹ 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 10.³⁰

²⁸ 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)

²⁹ Children’s Privacy On Line: The Role of Parental Consent, Working Paper of the IWGDPT, 26 March 2002

³⁰ http://index.hu/tech/2013/04/22/gyerekek_es_az_internet/, 15-05-2013

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.³¹

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.³²

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 Korea³³, 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 China³⁴ this habit has appeared on major websites

³¹ 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

³² http://index.hu/tech/2010/08/10/a_nev_a_vegzet_az_interneten/, 10-04-2013

³³ http://www.koreatimes.co.kr/www/news/biz/2008/10/123_32121.html, 18-04-2013

³⁴ http://index.hu/tech/blog/2010/05/05/peking_megszuntetne_a_netet_anonimitast/, 18-04-2013

for months but this idea also came up in France³⁵, Brasil³⁶ and in several US states³⁷.

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 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.³⁸

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.³⁹

C. Personal distortion

- "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..."

³⁵ <http://www.v3.co.uk/v3-uk/news/1944812/french-outlaw-anonymous-web-posting>, 18-04-2013

³⁶ <http://realtimesociety.blogspot.hu/2006/11/proposal-to-control-net-access.html>, 18-04-2013

³⁷ <http://betanews.com/2008/03/11/anonymous-web-posting-may-become-illegal-in-kentucky/>, 18-04-2013

³⁸ http://index.hu/tech/2010/08/10/a_nev_a_vegzet_az_interneten, 10-04-2013

³⁹ Principle 7 of 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 co-operating 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."

- 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. Jenő Ranschburg: The agonies of puberty, questions and answers/⁴⁰

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 communi-

⁴⁰ Saxum Publishing 2011, p. 107.

cation 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 dysfunctional 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), loss 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.⁴¹ 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 available, the psychiatric 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 damages. 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 psychologi-

⁴¹ CECILIE SCHOU ANDREASSEN: Development of a facebook addiction scale^{1, 2}, 2012, 110, 2, 501-517. © Psychological Reports 2012 Department of Psychosocial Science University of Bergen, The Bergen Clinics Foundation, Norway

cal problems. 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 mental disorders (addiction, social isolation, and threatening behaviour) it is inevitable to seek for professional help!⁴²

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 network⁴³:

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 1.19 billion (last updated 10/30/2013)⁴⁴ 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

⁴³ "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.

⁴⁴ <http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/>, 11-01-2014

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 network 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 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 Autumn 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.

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).

European surveys revealed⁴⁵ 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).

⁴⁵ 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

⁴⁶ BENCE SÁGVÁRI: On the EU survey of Kids Online in Hungary in.: www2.lse.ac.uk/.../EUKidsOnline/.../Hungary%20webpage.pdf, 07-03-2013

Two third of Hungarian children aged 9-16 have their own profile on at least one social site, rather girls and elder children use these sites. A quarter of children have 50-100 friends, one third have 100-300 acquaintances whilst 13% of them have more. 55% of children surveyed had a public (visible to everyone) profile on a social site. 22% of them made it public partly while 16% used settings that enabled only their friends to discover their data.⁴⁶

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*)⁴⁷ 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 time⁴⁸). 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 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

⁴⁷ G. HOGBEN (ENISA), ENISA Position Paper No.1 Security Issues and Recommendations for Online Social Networks, October 2007, p. 8.

⁴⁸ http://index.hu/tech/2013/02/26/csokken_a_bunozes_a_facebook_miatt/, 26-02-2013

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 case⁴⁹ 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 collecting. 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.

⁴⁹ C-101/01 Lindqvist [2003] ECR I-12971

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 adult⁵⁰ - could be extremely perilous. Typical cases include sites fostering violent or pornographic behaviours, committing suicide, drug consumption or abnormal nutrition⁵¹ 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

⁵⁰ 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

⁵¹ 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

way. In accordance with a 2004 British survey 57% of children, between the ages of 9-19, surfing the web at least once a week already encountered pornographic contents (parents consulted thought of a remarkably less frequent number – merely 16%) and only 10% of them switched on the PC for that very reason. For 8% of minors queried the experience was rather insulting and disturbing.⁵²

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 unsuspecting user to destructive web-

⁵² UK Children Go Online, Surveying the experiences of young children and their parents by [S.Livingstone](#) and B. Bober, July 2004 in.: www.children-go-online.net, 24-05-2013

sites 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..⁵³

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.

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.⁵⁴

⁵³ LÁSZLÓ DRÓTOS: Referatum of Bayer Judit: The freedom of the net: difficulties in regulating internet contents in light of freedom of speech (excerpts from the publication) in.: http://tmt.omikk.bme.hu/show_news.htm?id=4633&issue_id=479, 02-04-2013

⁵⁴ 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.

F. 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 analysis).

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 above 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.

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.⁵⁵ 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

⁵⁵ In the Netherlands a social site developed by a minor and dedicated to fellow minors has been investigated by the Dutch data protection authority.

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 stories of their life in a status message or a photo.

7. MAPPING OF PROBLEMS – ONLINE DEVIANCIES

New deviancies emerging in the information society may range from the “somewhat uncomfortable” feelings leaving behind bad impressions to actions constituting crimes.⁵⁶ 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.⁵⁷ 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.⁵⁸

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 channels.....In my work I already encountered a minor who met an adult in a chat room, at the personal meeting had a sexual intercourse with that person and consumed drugs together as well. The child was away from home for days and even after did not even perceive the peril*

⁵⁶ ADLER F., MULLER, G.O.W. & LUFER, W.S., Criminology, Osiris Publications, Budapest, 2002. pp. 34-35.

⁵⁷ GÖNCZÖL K., KEREZSI K., KORENIK L.&LÉVAY M. (ed.) Criminology-Professional Criminology Complex Publications Budapest, 2006. p. 104.

⁵⁸ ZOLTÁN SZATHMÁRY: Criminality in the information society, Constitutional criminal dilemmas in the information society, PhD thesis, Budapest 2012. pp. 64-65.

*of what has happened.. In the course of the interrogation came out the fact that this had not been the first “chat” relationship”.*⁵⁹

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.

(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

⁵⁹ DR. TIBOR PESZLEG: Internet and pedophily from: Police Studies Review, December 2004 from: http://www.remet.hu/cms/index.php?option=com_content&task=view&id=16&Itemid=4,12-02-2013

people, typically between the ages of 13-17, discredit each other on diverse platforms. *“In the framework of ‘For Safer Internet Forum 2008’ the European Commission initiated a public consultation on public networks. Incoming responses revealed that through using social networks minors are generally threatened, besides violating their privacy and sexual grooming, mainly by online bullying.”*⁶⁰ 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 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.⁶¹ 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.⁶²

⁶⁰ ZOLTÁN SZATHMÁRY: *Criminality in the information society, Constitutional criminal dilemmas in the information society*, PhD thesis, Budapest 2012. pp. 68-69.

⁶¹ 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

⁶² In the fall of 2012 in Ireland two completed suicides happened within weeks, fellow schoolmates had been harassing the victims anonymously on the same website from: <http://www.thejournal.ie/erin-gallagher-funeral-655978-Oct2012/>, 08-03-2013

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 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 community 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.⁶³

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.

⁶³ <http://knowyourmeme.com/memes/events/jessi-slaughter,27-02-2013>

Among trolls nowadays it has become “fashionable” to outrage famous sportlers this way.⁶⁴ 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 #keyboardwarrior and #jimmybrownpants converted into the most popular hashtags due to this issue.⁶⁵

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”.⁶⁶ Trolls expressing their extremist opinions anonymously certainly do not promote civilized internet 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.

*“The findings of a research project, carried out during a national campaign in the US in 2008 aiming at the prevention of unwanted pregnancies among the youth, showed that 20 % of juveniles between the age 13 and 19 had already sent nude or semi-nude images of themselves. An additional interesting figure suggests that 25% of girls and 3% of boys gave affirmative responses to questions as to whether they had previously received an erotic picture which had not been supposed to be shared with them initially. 39% of teenagers circulate messages with sexual contents, 48% of them have already got such messages. In accordance with the outcome of a recent research these ratios increased, 65,5% of the youth between 13-19 made previously sexting”.*⁶⁷

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 in-

⁶⁴ 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>

⁶⁵ http://index.hu/tech/mem/2013/03/13/igy_kell_banni_egy_trollal/,14-03-2013

⁶⁶ <http://bleacherreport.com/articles/1034961-san-francisco-receiver-kyle-williams-receivers-death-threats-on-twitter>,18-06-2013

⁶⁷ ZOLTÁN SZATHMÁRY: Criminality in the information society, Constitutional criminal dilemmas in the information society, PhD thesis, Budapest 2012. p. 69.

dependent 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. 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.”⁶⁸

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

⁶⁸ ZOLTÁN SZATHMÁRY: Criminality in the information society, Constitutional criminal dilemmas in the information society, PhD thesis, Budapest 2012. p. 70.

forms thereof are penalized by the penal law as well:

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

Therefore offenders certainly strive to hide their activity. The internet is an excellent forum to satisfy these paedophile desires anonymously. It involves not only individual but also organized crime activities since acquiring and forwarding pornographic pictures of children is much faster and simpler on the net. A not unusual example: a male in his forties registers on a social networking or dating site pretending to be 18 years old, uploads “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.)

f. Online meshing (grooming)

For the time being there is no proper Hungarian term for it, the phenomenon could be described by the words meshing or catching.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 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.

g. 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. Professionals evaluate it primarily as a symptom: if it truly has serious consequences, is out of control and cannot be regarded as a manifestation of desire for games, which would have been usual and normal in the childhood, then it may refer to some behavioural disorders or other psychiatric crisis.⁷⁰

As far as gambles are concerned the law in Hungary is unambiguous: Section 1 (6) of the Act XXXIV of 1991 (hereinafter referred to as: Szjtv.) on Gambling Operations prohibits the participation of persons under the age of 18 in any contest of chance, with the exception of tombola. According to the practice of the Gambling Supervision Authority of the National Tax and Customs Administration (NTCA) “*currently only the Gambling*

⁶⁹ KATALIN BARACSI: Internet security in Hungary and in the European Union from: Civil Review 7th year, vol. 5-6., February 2012 http://polgariszemle.hu/app/interface.php?view=v_article&ID=478,08-03-2013

⁷⁰ ANDREA VIDA: Impact of information and communication culture on teenagers from: <http://xenon.bibl.u-szeged.hu/~vidaa/holi/03/szenyvet/vidaa.pdf> 24-03-2013

Operations Plc. is authorized by the NTCA to conduct lottery and betting operations as the state gaming operator which is available on the homepage of www.szerencsejatek.hu including also rules on bookmaking operations. Pursuant to Section 2(2) of Szjtv (2) all operations of gambling activities must be authorized by the state tax authority, save for the exception set out in the Act whilst, according to Section 9(1) of Szjtv a contest of chance may only be conducted on the basis of an approved game plan. Consequently the legal prohibition of participating of youth below 18 in gambling prevails currently at a single gambling operator; the detailed rules thereof are encompassed in different set of gambling rules and terms and conditions of participation. Pursuant to the game plan rules the involvement in online betting is in all cases subject to a preceding registration. Registration is possible exclusively to players above the age of 18 and with a permanent residence in Hungary; subsequently he has to upload his internal balance. Once, following the registration, the player has entered certain mandatory and optional personal data he gets a password and an identifier consisting only of numbers (or else he can opt for a password with characters) that enable the login and the participation. There are two types of registration: full and paper based version.

A) At full registration you have to fill in a form where the following personal data shall be indicated: name, place and date of birth, mother's name, bank account number, mailing and email address, additional data needed to betting as well as a declaration shall be made that the player is over 18 and accepts the terms and conditions of participation. Registration can be made either by phone or online.

B) Paper based registration (bankcard service agreement) can be made exclusively at lottery shops of the Gambling Operations Plc., at agents mandated by the Plc., or at the issuing bank office, upon showing the card and proofing identity if the registrant in an OTP Bank card holder and completed his 18 year of age.

Both types of registration enable access to all games and bettings offered by the Gambling Operations Plc. It shall be emphasized that one cannot take part in online gambling without a prior registration; there is no option for an ensuing or temporary registration. Moreover, according to game plans approved by the NTCA, people under the age of 18 as well as individuals whose valid personal data do not correspond to personal particulars given at the registration are not entitled to a prize; in this case organizers shall deny the payment. Should the player gives false data and receives a so-called higher prize – i.e. 200.000 HUF or above – he will not be able to collect it since the high prize will not be remitted to the internal account of the player but it will be transferred exclusively upon a personal request made at the lottery shop on the spot. The above rules can be consulted on the website of the organizer

as well as in the Terms and Conditions of Games whilst the Supervisory Authority monitors compliance. By now the NTCA has not encountered any abuses in the services of the Gambling Operations Plc. regarding the prohibition of online participation of minors in games.”

Playing is certainly a pleasant activity and children can improve and put into practice their knowledge by virtue of online games. Their familiarity with history, economics and biology can surely be enhanced by being involved in specific roleplays; however, there are certain setbacks that should be considered. First and foremost it shall be noted that the principal interest of game producers and game site providers lies in realizing profit, this can be (legally) achieved if they could put on market more and more expensive games, encourage users to additional purchases and “keep” the players in the game as long as possible. In 2011 just in Germany users, mainly juveniles, spent approx. 2 billion euros for PC game softwares. More and more, theoretically free, games freeze down or do not give pleasure if users fail to buy “accessories” – for instance installing a virtual courtyard costs a lot of real money – therefore, again in accordance with German figures, in 2011 users spent alone for virtual components 233 million euros, with 100 million euros more than in the preceding year.⁷¹ Purchasing these components is quite “easy”: by making a premium phone call or sending an SMS, often from the parent’s cell phone and as the child, under psychological pressure, purchases more frequently the expenditures reaching hundreds of euros will be revealed only at the month-end accounts. Even if the website provider promises to limit the possibility of purchasing components to few cases, these self-restricting pledges are usually not kept. What’s more, holding the players continuously in game is enforced by sanctions: those who “quit” prematurely may be excluded from the game for a while, for hours/days/weeks with the heavy financial consequence of losing the money invested so far. Vainly having paid for the admission fee or the components these purchases can go waste due to the expiry of the period of validity. Inventors and providers of games always assert that the child knows and understands the rules and also accepted them. We are aware of numerous cases when transactions are carried out by using the parent’s password. Lately a boy, 5, in Great Britain requested his father’s password in order to upload a free PC game, however, additional components were subject to charges and, by reason of improper settings, and the parents suffered a remarkable financial loss.⁷²

⁷¹ 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,08-03-2013>

⁷² http://index.hu/tech/cellanaplo/2013/03/18/oteves_gyerek_610_ezret_koltott_appokra/, 2013-04-28

Online games on PCs, game consoles or smart phones can be played habitually by involving multiple players (multiplayer games), though in such cases we process the personal data of others as well. It would be desirable to consult the terms and conditions on data protection of the game prior to entering the game since these rules determine who and under what conditions can have access to our personal data, for what purposes our data are processed and to whom they can be transferred.

PC games can be categorized into several groups:⁷³

- in terms of depiction: text (e.g. visual novel), graphic or miscellaneous
- in terms of type: action, adventure, strategic, simulation, role-plays

During the registration of online games a username, a mailing and an e-mail address, as well as a date of birth shall be given. Geographical information is needed to find the nearest server and players. Where a minimum legal age limit has been set generally a confirmation is required whether the player is over 18. Some services may be used free of charge, others are subject to payment. If we use the credit card for an online purchase we should be cautious and check out the reports frequently as well as we ought to contact the game provider should we encounter a transaction which is questionable. We can specify our data protection settings depending on the game, the game developer and the features of the game. At sophisticated games we generally have the option to limit the settings consequently nobody, except the provider, can learn the details of our profile or personal information. This level of security, however, does not promote multiplayer games or the community aspects of online adventures therefore numerous players reduces the limits of settings thus enabling others to see their profiles. The created username can be protected by applying the following methods:

- so-called “strong” passwords that cannot be easily identified by others;
- HTTPS (Hypertext Transfer Protocol Secure), settings of a web application which encodes the personal information and the communication during the game (provided this setting is enabled);
- restricted data protection settings and

⁷³ ANETT BALKU: Virtual clans – Clustering in an internet roleplay (university thesis), points 3.1.-3.2. Source: http://campuslet.unideb.hu/dokumentumok/tanulmanyok1/Csoportkepzo_tenyezok/Virtualis_es_valosagos_csoportok_internetes_szerepjatekokrol/Balku_Anett_Virtualis_klanok_Csoportkepzes_egy_internetes_szerepjatekban_SzakdolgozatMA.pdf 25-03-2013

- disclosure of minimal sensitive information (e.g. home address, school or work-place should not be released).
- Should general terms & conditions approve we can create profiles with a pseudoname or nickname which are linked with social sites by providers with the objective of enabling players to notify their online friends if the game begins. In this case it is advisable to consult the privacy policy and the legal statement of the respective social networking site as well.

The privacy policy and the legal statement are available during the registration for the online game or prior to installing a programme, on entering the personal settings on the screen or in the form of a link. This way we can see what sorts of our personal data are collected and by whom, where these data are transferred to, how the data are used and where we can direct our questions or enquiries. Providers are tending to disclose our personal data to third parties in a remarkably wide scope for diverse purposes (to comply with a legal obligation to which the provider is subject, to monitor diverse illegal activities, to resolve service breakdowns, to improve the games, to ensure payment mechanisms, to enable communication among players and to provide the players with various promotion materials). As a result our personal data can be learned by individual programme writers, under the scope of the contract, financial institutions, online hosting or distribution services, client service regarding technical assistance and game support, internet SPs, researchers, advertisers, market researchers, bailiffs and other public bodies. Players should make sure, however, whether the company or the game developer regulated the specific conditions with regard to liability, moreover whether data security rules have been included in the service agreements which are essential in the event of the disclosure of personal data.⁷⁴

It may sound astonishing but the most effective protection in the field of online games could be ensured when the child plays together with his parents or if the whole family were to play together!⁷⁵

⁷⁴ Source: http://www.priv.gc.ca/information/pub/gd_gc_201211_e.asp,15-04-2013

⁷⁵ <http://mediasmarts.ca/blog/game-tips-parents>,15-04-2013

h. 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.⁷⁶

From Section 219(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 Infotv., committed for unjust enrichment or causing substantial injury of interests qualify as misdemeanour.

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.

⁷⁶ Study on monetising privacy An economic model for pricing personal information <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy>

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 admitted 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.⁷⁷

⁷⁷ http://www.penzcentrum.hu/vasarlas/tizezreket_bukhatnak_a_gyanutlan_vasarlok_tamadnak_az_atveros_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 expression “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 Portuguese 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.⁷⁸ Among the initiatives to promote awareness of data protection and privacy issues 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”
- Office for Internet Safety - Updated Parental guides for Internet Safety (a parents’ guide to new media technologies, to social networking websites , to cyberbullying)



⁷⁸ <http://dataprotection.ie/viewdoc.asp?docID=520>

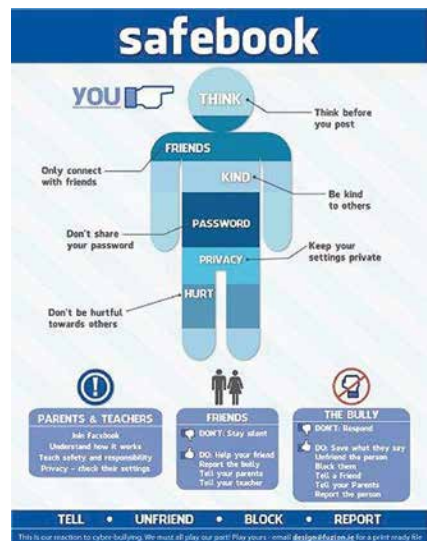


The Irish Ombudsman for Children, Mrs. Emily Logan consulted the topic of online bullying with over 300 children and young people between 10 and 17 years of age pupils with diverse socio-cultural background nationwide. The overall aim of the consultation was to hear children's and young people's views and ideas about what actions 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://www.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 including also the defence against cyberbullying. The programme was resumed by the "Cool school" project which was dedicated to upper 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/>).



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 respectme Anti-Bullying Awards to celebrate some of the amazing projects and initiatives being carried out at a local level across Scotland. (<http://www.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 cooperation between 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 consciousness 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. 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.

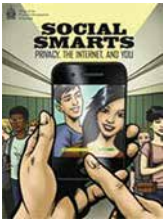
They believed that the best way forward for young people to start to think about privacy was for us to encourage people to do a presentation, for instance to school assemblies. They were also keen to see teachers or senior students using the material in class. The students discussed what aspects of privacy 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” (www.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.

f. 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://www.priv.gc.ca/youth-jeunes/index_e.asp)



The colourful graphic novel dedicated to youngs – the Hungarian version can be found in the Appendix! – illustrates how many personal information we share without will or undetected in the internet. Developed 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

g. 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 processing⁷⁹ (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

⁷⁹ 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).

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:
 - 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 parties (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.⁸⁰



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.⁸¹ 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 mar-

⁸⁰ <http://www.coppa.org/comply.htm>, 2013.04.15.

⁸¹ <http://www.ftc.gov/opa/2012/12/kidsapp.shtm>, 2013.04.22.

keting 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.ftc.gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing>)

h. EU practices

From EU projects the Safer Internet program⁸² shall be mentioned first and foremost which was launched by the European Union in 1999 and currently 30 countries are involved (Hungary joined in 2009). From 2004 on the project has been called Safer Internet 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.



⁸² <http://www.saferinternet.hu>

The EU Kids Online research (<http://www.eukidsonline.net>) summarized the results of existing reports on the one hand whereas, in fall 2011, composed a novel datasheet involving 25 countries on the other hand. Beyond the two key terms “risk” and “harm” it also analyses the inclination to harms. Major findings of the research in Hungary as follow:

“- The most widespread way of accessing the internet is the use of a shared desktop computer at home (60%), 42% have an own desktop computer whilst 8% are allowed to have an own laptop or to use it in their bedroom.

- 47% of children use mainly a single PC while 43% have access to the internet on multiple. What’s more, 12% of kids questioned have access to 4 or more gadgets. This ratio is determined primarily by the financial situation of the family (household) as well as the category of the town.

- On average Hungarian children – similar to the European figure - start using the internet at the age of nine. For 9-10 year olds this number is seven years, while for 15-16 year olds it is around ten years, indicating that as time goes by internet use occurs earlier and earlier and it will be probably stabilised at the age of around six years.

- Nearly 60% of Hungarian children between the ages of 9-16 use the internet regularly on a daily basis while an additional 35% go online once or twice a week. Generally we can conclude boys, elders and Budapest residents are the most frequent internet users.

- Top activities are using the internet for watching videos (76%), schoolwork (73%), social networking (72%), instant messaging (61%) and playing online games (60%) ...

- 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. According 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 diverse 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 diverse, 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 permission.

- 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.

- Az internetet otthonukban (is) használó gyerekek szüleinek több mint fele (52%) meg szokta nézni a gyerekek által látogatott honlapokat, közel 40% azok aránya, akik a gyerek közösségi oldalon lévő profiljára is rápillantanak, míg 35% a gyerek kapcsolatait is ellenőrzi az azonnali üzenetküldő programokban. A gyerek által kapott/küldött üzeneteibe – legyen szó email-ről vagy azonnali üzenetről – a szülők 23%-a tekint bele.

- 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.”⁸³



⁸³ BENCE SÁGVÁRI: On the EU Kids Online research in Hungary from: <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/NationalWebPages/Hungary%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:

- Caught in the Web (2012 Chen Kaige)
- The Lives of Others (2006, Florian Henckel von Donnersmarck)
- "J.Edgar" (2011, Clint Eastwood)
- The Game (1997, David Fincher)
- The Net (1995, Irwin Winkler)

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



APPENDIX

INFORMATION LEAFLET OF THE HUNGARIAN DATA PROTECTION AUTHORITY
ON CONSCIOUS INTERNET USE DEDICATED TO CHILDREN



LISTEN, THIS IS IMPORTANT!

It is only up to you to decide whether you put the net for good or wrong use!

A good decision, however, is subject to information therefore if you are interested learn the examples from real life and consult the relating information!



DID YOU KNOW?

PERSONAL DATA: any information relating to a person (data subject) that shall be protected!

DATA PROCESSING: any operation performed on personal data e.g. collection, disclosure, modification or deletion.

LIABILITY and RESPONSIBILITY: in the virtual world personal data may be disclosed by a single press of button and nobody can ever remove the information afterwards. The data controller shall bear responsibility for his actions concerning other persons' personal data!

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 of internet advertising (“Button” = advertisement in more little pixel size than that of banner).

bookmark:

Possibility offered by the browser programme to mark the internet site visited in order to facilitate the return thereto.

botnet:

“robot network”, network of zombie computers that, by virtue of various viruses and Trojan softwares, get under control of a cracker. Following 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 in the net, 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:

Bug: error or malfunction 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 infocommunication (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 online 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 exchange 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 the reactions 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”

unfriend:

rejection of a person

URL:

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

viber:

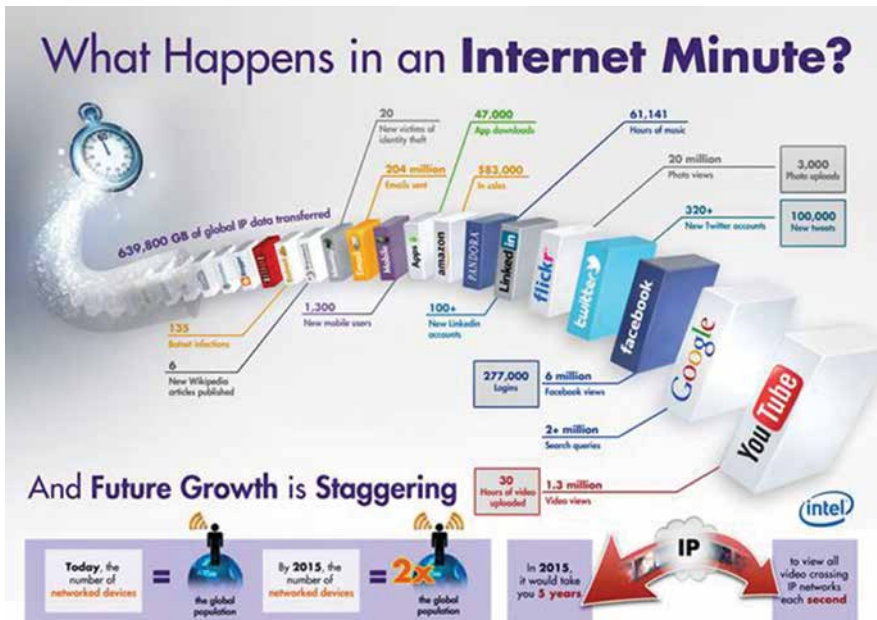
an installable programme similar to Skype that enables free (or very cheap) internet telephoning and sending of messages to friends who have also installed the programme.

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.



Source: <https://www.google.hu/search?q=what+happens+in+a+minute+on+the+internet&source=lnms&tbm=isch&sa=X&ei=tZ8NU6fxAYbUsgbEyYcDQ&ved=0CAcQAUoAQ&biw=1024&bih=585>

ARE THERE CHILDREN'S RIGHTS EXISTING?

Of course, yes, e.g. it is prohibited to degrade a child or take revenge against him based on his parents, family, own features including his religion, language, financial situation, origin or his beliefs. He shall have the right to acquire a nationality, to have his own name, family relationship and to express his views freely in all matters affecting him during official procedures.

It is also prohibited to observe a child via the internet arbitrary and to abuse his personal data relating to him!

He may get informed freely, can express his views without insulting others.

What does a "child" mean from legal point of view? A child is a human being below the age of 18 unless majority is attained earlier by a special legal provision (e.g. through marriage).

Is a parental consent needed to data processing?

Below 14: yes.

Between 14 and 16: the minor and the parent agree together

Above 16: the minor decides alone.



EXAMPLE

- **the student ID card of 1st grade pupils are signed by the parent**
- **in the 8th grade the application form for the secondary school is signed both by the minor and by the parents.**
- **the application for admission to the university is signed solely by the student**

You may already have heard about it; however, you might not have payed attention that unluckily the internet may also be used for vicious or harmful purposes:



For instance:

- **internet bullying (cyberbullying)**
- **memes**
- **trolls**
- **sending erotic images (sexting)**
- **internet paedophilia**
- **other abuses with personal data (e.g. phishing, identity theft)**

INTERNET BULLYING (CYBERBULLYING)



Cyberbullying always begins for personal reasons and the offender “tortures” his victim for a longer period recurringly aiming at intimidating or arbitrarily insult him (e.g. someone sends threatening or degrading emails night and day, sends messages on a social site, posts offensive comments or insults his fellow in his blog diary).

Bullying is a crime and it’s punishable with imprisonment even up to one year!

EXAMPLES

Unfortunately the case happened to a 13 year-old American girl isn’t single; a girlfriend of her made her believe that she was dating with a boy, 16, in the course of 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 in 2006. As a consequence a law was enacted in Missouri that penalize online insulters or vexatious persons with fine and imprisonment.

A girl from 6th class wanted to help her classmate and turned to Blue Line. The dicky and shy classmate has recently changed her school due to having been exposed to “fatal” bullying remarks and insults in her previous school though the caller thinks she will be targeted in the new school as well. At school nobody bullies her but on Facebook unpleasant photos are being circulated on her and in evening chats feature the “clumsiness” of the new girl makes permanent headlines. The calling girl does not want to join the insulting classmates but she fears that by supporting the new girl she will also be targeted.



INTERNET MEMES (SENDING OUT MEMES)

Internet memes consist mainly of circulating unlimited faked news embarrassing videos or images. 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.



EXAMPLE

A fresh graduate Hungarian man expressed his special thanks to his senior colleagues (including also the Prime Minister) for granting him an office job on his Facebook site in May 2013 – soon he became featured in numerous insulting memes as a result of unveiling his name and photo. Due to his personal message originally directed to his friends a fresh graduate has become a victim of a public degrading campaign...

TROLL (PROVOKING COMMENTER)



The troll 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. Trolls evidently unleash passions: both the abuses and the backlashes are made in a brutal style; even death threats are very frequent. Don't feed the trolls!, i.e., it is advisable to ignore these comments.

EXAMPLE

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 the ratings #keyboardwarrior and #jimmybrownpants converted into the most popular hashtags due to this issue.



SENDING EROTIC PHOTOS (SEXTING)



More and more teenager girls are tending to send sexy (bikini, monokini or naked) images or videos of them. Moreover surprisingly numerous kids received an erotic image which had not been supposed to be shared with them initially. The major problem is that later such recordings come to an independent life and serious abuses may occur! Be aware that the fired boy- or girlfriend may be capable to do anything out of revenge...

Additionally there are trash websites that urge sending in such images:

“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 bugging us around the more certain you are going to succeed!”

EXAMPLE

A girl submitted an application for a beauty competition called Miss MyVip and uploaded photos to her application form. Later a friend of her called her attention that she had been found on a pornographic site. The request sent to the editor of the site for deletion remained unnoticed.

In another case the photos of the complainant’s daughter of 16 had been removed from a social site and uploaded to a porn 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.

In 2013 a girl of 17 made a complaint to the police claiming that a new Facebook profile has been created using a nude photo which had previously been sent only to two friends.



INTERNET PEDOPHILIA, GROOMING

The abnormal paedophile adult has sexual desire for children and the internet is unluckily an ideal terrain to gratify his sick passions: to make acquaintances, contacting, obtaining and sharing pornographic images of children. Moreover paedophiles and other "internet groomers" do not put their cards on the table: they masquerade as someone else so could a dangerous and malicious stranger become "familiar" shortly. Most perpetrators hunt for their young victims (boys and girls equally) on social sites with a well-founded strategy for months.

EXAMPLE

A male in his forties registers on a social networking or dating site as being 18 years old, uploads "of him" an attractive photo, begins to date with teenager girls, they become friends quickly, the girl will take "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.

A worried mother called Blue Line from a small town. Her son, 17, met a girl pretending to be 19 on the internet and now he wants to go to her to Budapest in order to spend the weekend together. The mother visited the girl's Facebook profile and, as a result, felt uneasy due to the low number of friends and the artificiality of photos (a full set of "fashion images").

INTERNET GAMES



Playing is certainly a pleasant activity though some aspects should be considered. During the registration a username, a mailing and an e-mail address as well as a date of birth shall be given – however we should avoid disclosing the address or school and we always shall use strong passwords!

“Free” games aren’t all the time free of charge, we shall be cautious principally with regard to buying “accessories” in order to avoid a huge cash outflows due to calling high-toll numbers or sending such SMSs.

EXAMPLE

At certain games players who “quit” prematurely may be excluded from the game for a while, for hours/days/weeks with the heavy financial consequence of losing the money invested so far.

The online games can cause serious problems in the development of addiction. The Blue Line has been approached by the father of a 15 year-old boy because the child neglects the school and his family as well as gave up attending physical courses. He plays all the time with online games and who knows what else he does in the internet... Parents may feel they cannot do anything to stop this process and they are desperate as it is clear the boy is in a hopeless situation.



TIPS

In general:

- The style is the man himself – do not degrade yourself by vulgar or rough speech.
- Use complicated passwords and change them frequently.
- You should rather delete the suspicious messages or opinions instead of opening them.
- Think before you click.

Social networking site:

- Get to know and use security settings!
- Think before posting information online.
- Your online reputation is valuable, do not destroy it heedlessly.
- The truly personal information should be confidential.
- A smaller and more reliable circle of friends the better.
- The direct path is always shorter: you should be honest to your friends, discuss the grievances; it might only be a stupid misunderstanding between yourselves!
- If somebody threatens or insults you on the net, report it instantly to the administrator, print out or save the evidences and erase the perpetrator from among your acquaintances.

Mobile web devices:

- Be aware that on the net you are never alone!
- Beware of thieves; if someone were to steal your device also your personal data stored therein may get to unauthorised persons!
- Even on the phone you should use password and other security settings.
- Do not give your phone number or email address to anybody.
- Before buying an app, examine previously what services it will have access to (e.g. social site or positioning programme).
- Switching on and off the positioning system is enabled.
- Public networks (Wi-Fi hotspots) are insecure; they may pose risk to your personal data.
- In the event of online purchase check out the money transfer separately.
- You should keep away from answering suspicious calls (voice calls, sms etc.) you had better not react; block the doubtful sources!
- Always ask for permission from the data subject before taking a photo or video recording.
- Avoid posting of images/videos of others without prior consent.




AND THE MOST IMPORTANT:




Do not do anything to anybody you also wish to evade, however, if you were to get in trouble be sure you are not the only one coping with this setback and ask for help without delay!




Where to call for help in Hungary?

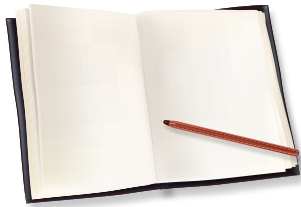


Where?	Contact	In what cases?
<p>National Authority for Data Protection and Freedom of Information</p> <p>www.naih.hu</p> 	<p>1125 Budapest, Szilágyi Erzsébet fasor 22/C.</p> <p>Tel: +36 -1-391-1400</p> <p>e-mail: ugyfelszolgalat@naih.hu</p>	<p>If I have questions concerning my constitutional rights 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.</p>
<p>Commissioner for Fundamental Rights</p> <p>www.ajbh.hu</p> 	<p>1051 Budapest, Nádor utca 22.</p> <p>Tel: (06-1-) 475-7100</p> <p>e-mail panasz@ajbh.hu</p> <p>or specially for children: kerdesemvan@obh.hu</p>	<p>If the activity or negligence of a public authority violates or may directly violate my fundamental rights.</p>
<p>National Media and Infocommunications Authority</p> <p>www.nmhh.hu</p> 	<p>1133 Budapest, Visegrádi u. 106.</p> <p>Tel: (06-1) 468 0673</p> <p>e-mail: info@nmhh.hu</p>	<p>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).</p>

Where?	Contact	In what cases?
<p>National Media and Infocommunications Authority</p> <p>Internet Hotline</p> 	<p>www.internethotline.hu</p> <p>1015 Budapest, Ostrom u. 23-25.</p> <p>e-mail: internethotline@internethotline.hu</p>	<p>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).</p>
<p>Blue Line Child Crisis Foundation</p> <p>www.kek-vonal.hu</p> 	<p>Tel.: 116-111</p> <p>e-mail: gyerekjogasz@kek-vonal.hu</p> <p>chat: http://chat.kek-vonal.hu</p>	<p>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.</p>
<p>International Child Welfare Service</p> <p>www.gyermekmento.hu</p> <p>www.saferinternet.hu</p> 	<p>H-1066 Budapest Teréz krt. 24.</p> <p>Tel: +36 1 475 7000</p> <p>Fax: +36 1 302 4136</p> <p>ngysz@gyermekmento.hu</p>	<p>If I 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 I want to be involved in such courses.</p>

Where?	Contact	In what cases?
<p>Government Incidence Response Centre</p> <p>www.biztonsagosinternet.hu</p> 	<p>bejelentes@biztonsagosinternet.hu</p> <p>https://www.facebook.com/biztonsagosinternet</p>	<p>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.</p>

My **privacy diary: what happened to my online data in the past week/fortnight/month?**



In what scope have I disclosed my personal data? Possibly what has another- familiar or unknown - person said or written about me? Have I disclosed my name, phone number or email address to anybody? Have I logged into websites? Have been files down- or uploaded to my PC? Have I used a mobile application on my mobile phone? etc.

Creating a portrait and a profile of a third party

1. By using the diaries collect all available or disclosed data and information on you and/or on a well-known person then create a profile based on it. Evaluate individually whether the online profile provides a true picture of the real person?

2. The second task is to choose a close acquaintance (family member, classmate or a teacher) and create a profile on the respective person by utilizing all online sources (e.g. images uploaded to the internet, marked favourite activities, shared websites, clubs, free time activity etc.). Show this to the person concerned and observe his reactions whether there are information that the person is unwilling to hear or see on himself though previously he shared this information with everywhere.



QUIZ

1. You meet a boy/girl on the internet who is very attractive. You have been chatting for a while when s/he ask you to send him/her an image::

- a) Now then, my profile image looks so good finally we could meet up.
- b) At worst, s/he won't like me.
- c) Surely not, after all s/he can see on my profile image how I look like. For what additional pictures to him/her.

2. A person adds you to his friends' list on Facebook with whom you haven't ever met:

- a) I accept him to have more acquaintances.
- b) I will think where I may know him from.
- c) I do not accept him. I haven't met him before therefore I can't see why he added me.

3. You read in a newspaper: the newest internet trend is posting memes:

- a) What the hell it is?
- b) Something was told at school, it's going on some awkward images.
- c) You mean circulating digital files (mostly pictures) on the internet for the purpose of entertaining a wide scope of users on an embarrassing situation or faked news/manipulated picture?

4. At the age of 15 you wish to visit a website that, prior to entering, offers the following alternatives: "I'm already above 18, I'm entering the site" or "I'm still below 18, I'm leaving the site".

- a) I don't see the ground for the distinction.
- b) Though I'm already above 15, I'm capable of assessing whether or not I may visit a website.
- c) Might I save myself from something unpleasant if I neglect the site?

5. You need to specify a bank account number to be admitted to an online game:

- a) I don't care; the point is that I can play.
- b) Don't know, I should consult with someone more experienced.
- c) No way, ultimately I would be redirected to a commercial site.

6. You realize that your girlfriend has uploaded some bikini photos on herself:

- a) I also take this chance and upload some photos in bathing costume.
- b) Bikini is out of the question; however, I'm going to upload some better photos of myself.
- c) Finally lots of users will download them to their PCs to have fun of me. I surely don't want to see myself on other people's PCs.

7. You receive an email message stating that you have won an exotic holiday trip. You merely should specify the following personal data and you can take over the prize immediately: name, place of residence, phone number, bank account number, ID card number, tax number:

- a) What a piece of luck, I'm sending my personal information straight away, shortly get into holiday!
- b) Why have I been selected for such a prize? It's worth a try anyway.
- c) Ah yes, they draw weekly. This is a pure hoax; I don't send them any information.

- 8.** Your friend tells you that somebody is sending emails on his behalf to your classmates:
- Ah yes! How the hell could someone log into his mailbox?
 - I suppose he might have given his password to someone else who is now playing a trick on him.
 - Unluckily nowadays is an easy task to compromise somebody's mailbox.
- 9.** At school you were told that the photo qualifies as a personal data:
- No. Personal data include the name, place of residence, ID card number etc. It's common knowledge.
 - Only if it bears the name of the person of whom it was taken.
 - Obviously, as anyone can be clearly identified from a photo.
- 10.** Personal data of a friend of yours have been abused. He told you he approached the NAIH for help:
- Even then I didn't understand what he meant.
 - Yeah, surely some international body dealing with data.
 - If I am right it is about the Hungarian data protection authority.
- 11.** In a disco your phone number is required:
- I will give it. I like meeting other people.
 - It's okay, unless I won't answer it if it will be bothering me.
 - I have already heard of several harassment stories. Rather not...
- 12.** Your sister, 14, is admitted to the internet only upon parental supervision:
- It's too bad that she is not free on the net.
 - Why to sit there, the visited pages can be checked out subsequently.
 - It is surely an unpleasant situation, but at least she won't see anything that is not for her.
- 13.** A friend uploaded a sticky photo of you onto the internet:
- I became a bit angry though I will ask him to delete the picture and it will be all right.
 - I'm going to upload a photo of him as well.
 - Fine...I will remove it never in a thousand years.
- 14.** I registered into Facebook in order to:
- meet more and more people, upload photos of me, share videos, post my everyday activities.
 - not to fall behind from others. Almost everyone is present on Facebook where you can collect more and more friends.
 - look for my friends and long lost friends.
- 15.** If I'm asked whether I take care of the protection of my personal data my response would be affirmative since:
- I disclose my personal information only to nice people.
 - I unveil information only if it is requested, not automatically.
 - I don't release personal information to anyone without well-founded reason.

EVALUATION

In case of most a) replies:

Based on your answers you should watch out more for the protection of your personal data. You cannot assess what detrimental consequences may arise if you share your phone number heedlessly or post photos of yourself to social sites. We strongly recommend you to examine the instructive cases and useful tips contained in this project leaflet!

In case of most b) replies:

Your replies show that you have previously heard of data protection or you have good sense of avoiding the reckless disclosure of your personal information. There are situations when you suspect when enquiring about your personal information – and it's all right – but finally you generally open up. Since your knowledge should be still refined we strongly encourage you to study this project booklet with a view to enhance your understanding!

In case of most c) replies:

Congratulations! You have successfully passed the data protection quiz! Your responses evidently show that you are aware of major data protection issues. Even in real life, in everyday situations you can properly estimate when the disclosure is useful and when it may lead to difficulties. Keep it up; you should study this project booklet in order to deepen your knowledge!



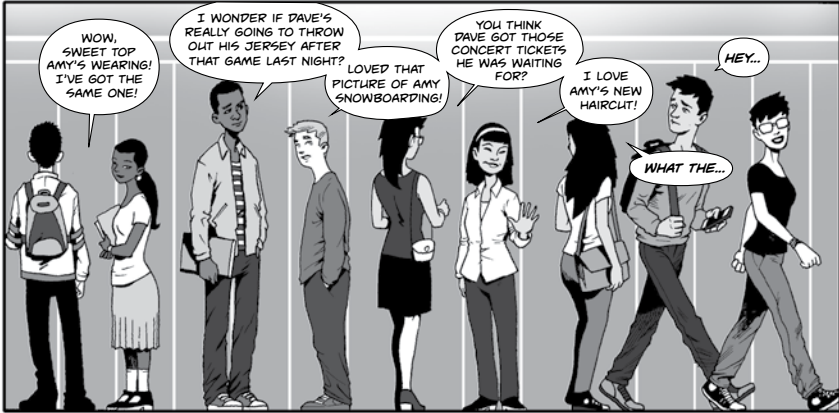
Office of the
Privacy Commissioner
of Canada

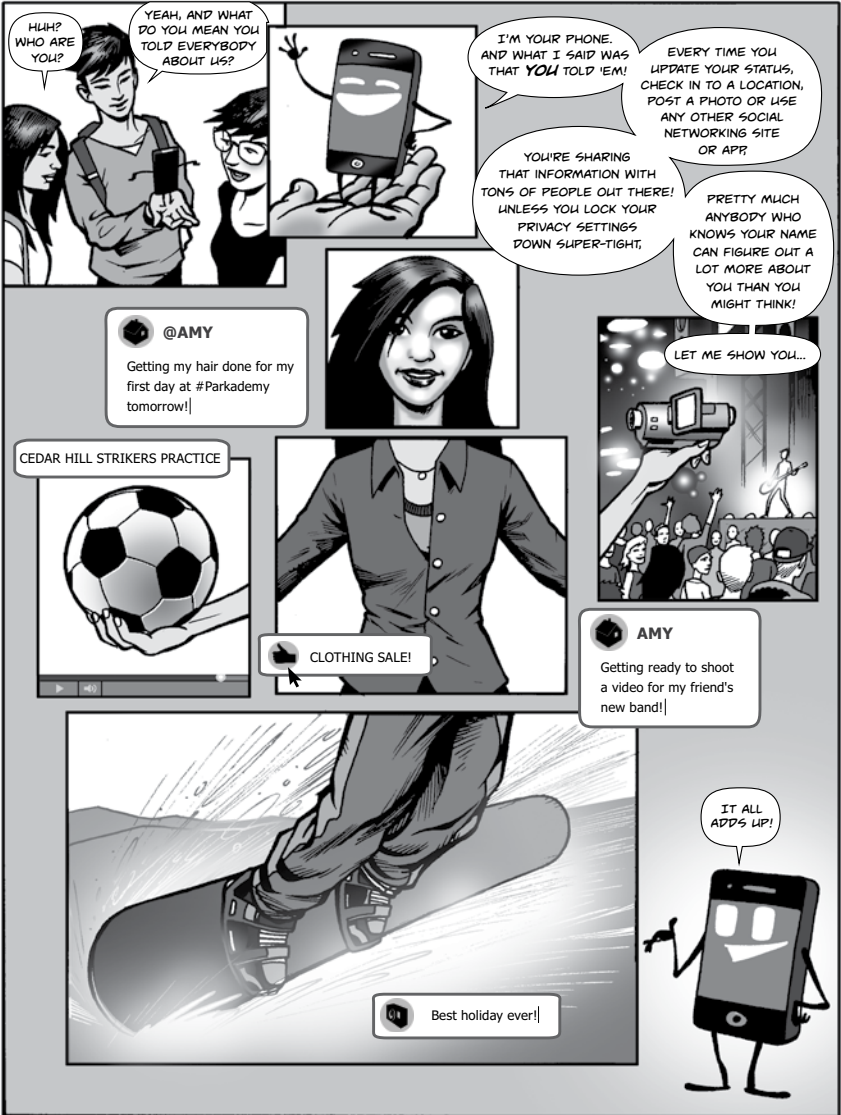
SOCIAL SMARTS

PRIVACY, THE INTERNET, AND YOU



Special thanks to the Canadian Privacy Commissioner
for his authorisation to let us use the original cartoon.
http://www.priv.gc.ca/youth-jeunes/fs-fi/res/gn_index_e.asp





HLH? WHO ARE YOU?

YEAH, AND WHAT DO YOU MEAN YOU TOLD EVERYBODY ABOUT US?



I'M YOUR PHONE, AND WHAT I SAID WAS THAT YOU TOLD 'EM!

YOU'RE SHARING THAT INFORMATION WITH TONS OF PEOPLE OUT THERE! UNLESS YOU LOCK YOUR PRIVACY SETTINGS DOWN SUPER-TIGHT,

EVERY TIME YOU UPDATE YOUR STATUS, CHECK IN TO A LOCATION, POST A PHOTO OR USE ANY OTHER SOCIAL NETWORKING SITE OR APP,

PRETTY MUCH ANYBODY WHO KNOWS YOUR NAME CAN FIGURE OUT A LOT MORE ABOUT YOU THAN YOU MIGHT THINK!

@AMY
Getting my hair done for my first day at #Parkademy tomorrow!



CEDAR HILL STRIKERS PRACTICE



CLOTHING SALE!



LET ME SHOW YOU...

AMY
Getting ready to shoot a video for my friend's new band!



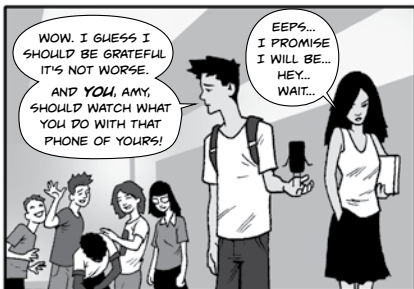
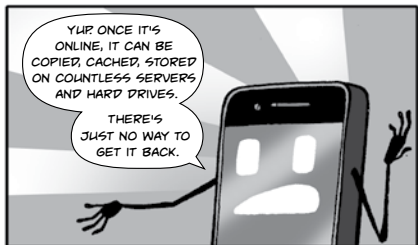
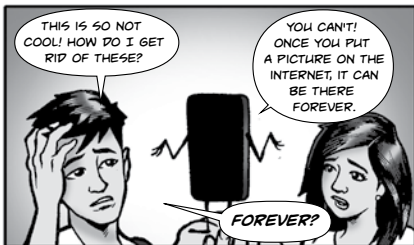
Best holiday ever!

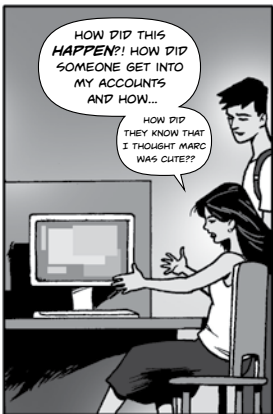
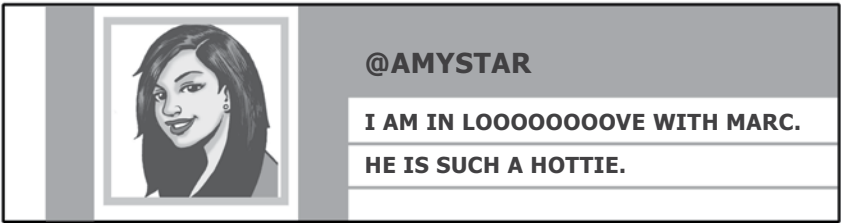
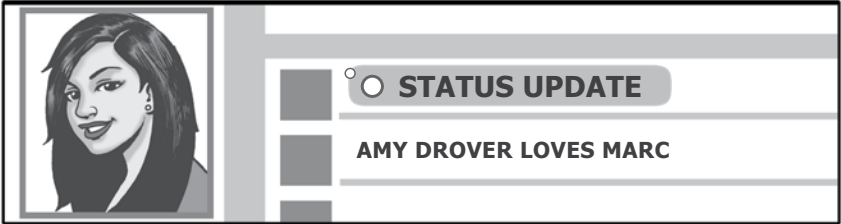


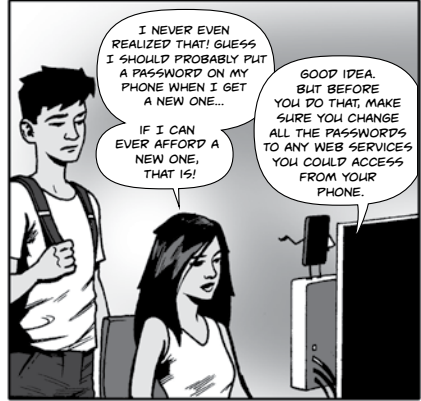
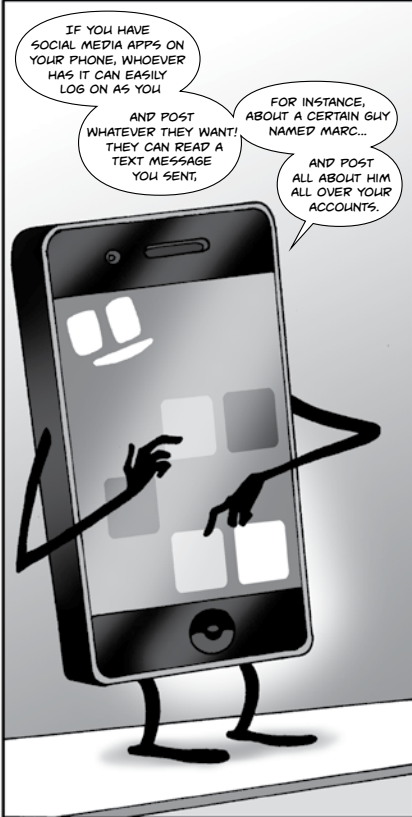
IT ALL ADDS UP!

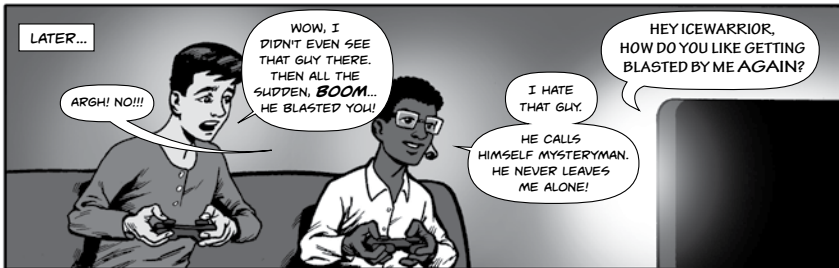
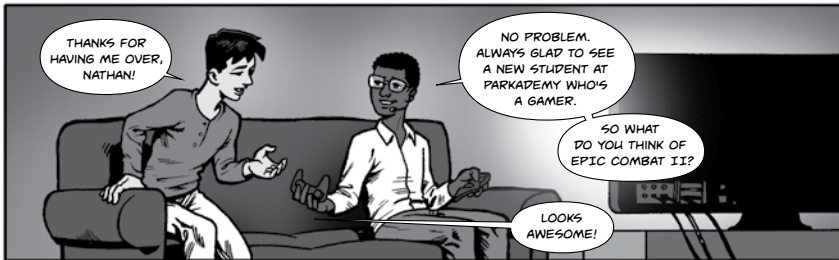
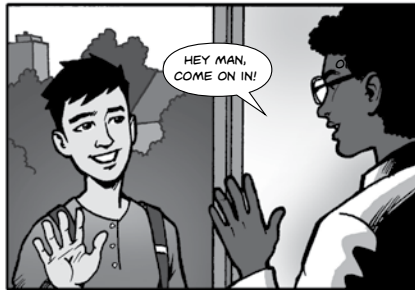


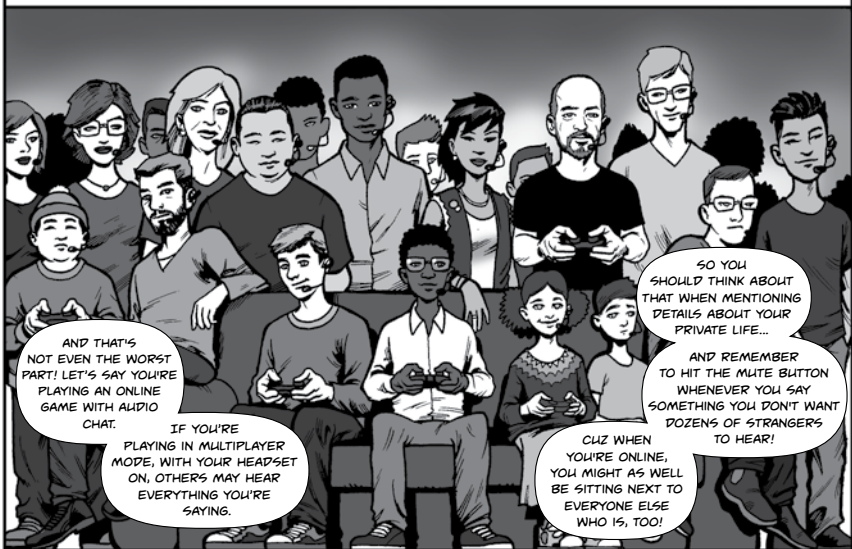
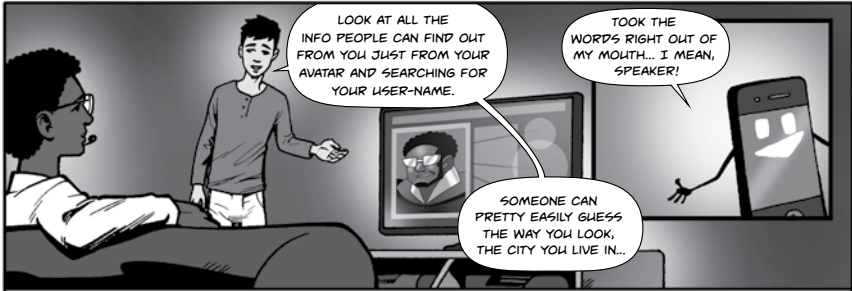












LATER THAT NIGHT...

DAVE

Thanks for having me over tonight! Let's get together and beat MYSTERYMAN again soon!

MAKE SURE YOU SET THE PRIVACY SETTINGS FOR THAT UPDATE SO ONLY YOUR BUDDIES CAN SEE IT!

OH YEAH, GOOD CALL!

THAT'S NOT EXACTLY RIGHT...

HLAH?

Geeks & Heroes

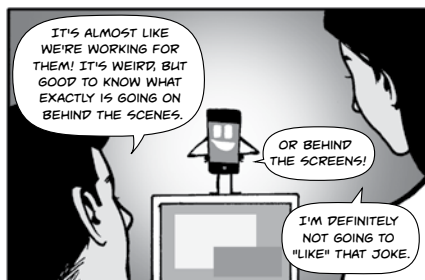
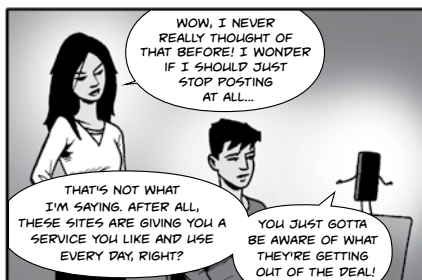
DAVE
Can't wait to go windsurfing tomorrow!

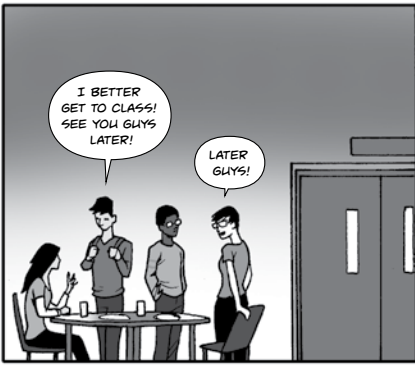
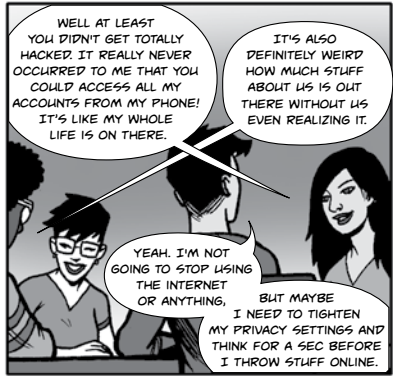
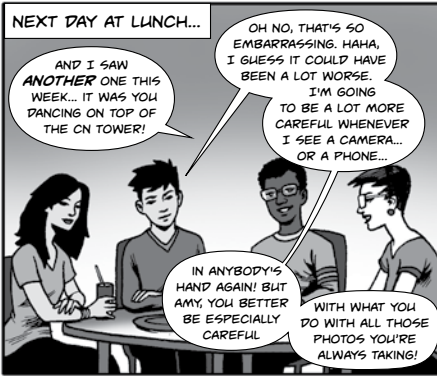
WINDSURFING LESSONS
Click now to find out more.

BURGER JOINT

EVER WONDER HOW SOCIAL NETWORKING SITES CAN AFFORD TO PROVIDE ALL THESE SERVICES TO HUNDREDS OF MILLIONS OF USERS FOR FREE?

THEY DO IT WITH YOUR HELP—BY USING ALL THE DATA YOU HAPPILY GIVE THEM.





Tips to help you stay safe on Facebook and online

Take control

1 Take some time to make friend lists or create groups

Consider the amount of information you want to share with different people. Do you want to share the same things with your workmates as your best friends? On Facebook, you can create custom lists to limit your sharing. Learn more in our Help Centre: www.facebook.com/help/friendlists



2 Get familiar with your privacy settings

Facebook's privacy settings help you control who can see your stuff on Facebook and how you connect with other people. Check your privacy settings at: www.facebook.com/privacy



3 Check what your profile looks like to other people

On Facebook you can see exactly what your profile looks like to the public or a specific person by using the 'View As' tool in your privacy shortcuts. To find out more about privacy shortcuts visit: www.facebook.com/help/privacysortcuts

4 Check your activity log

Facebook has an activity log that is only visible to you. This is where you can see and control the privacy of things you've posted on Facebook. Learn more about your activity log at: www.facebook.com/help/activitylog



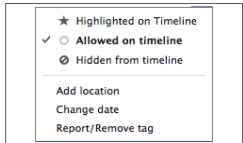
5 Check your audience before you post

Check your audience before you post. Facebook has in-line privacy controls so that you can set your audience – Private, Friends, Friends of Friends, Public – before you post a status update. Learn more in our Help Centre: www.facebook.com/help/audienceselector



6 Think before you tag and check what you are tagged in

Through activity log, you can untag yourself from photos you're tagged in or use Facebook's social reporting tool to ask someone to remove photos entirely.



7 Don't share your password

Passwords are not social. Don't share your password with anyone. For additional security tips go to: facebook.com/help/securitytips

Tips to help you stay safe on Facebook and online

Learn about reporting and blocking

8 Learn how to block people

If someone is bothering you on Facebook then you can block them by choosing the 'block' option on the front of their profile or by entering their name in the 'How do I stop someone from bothering me?' box on the left hand side of your profile. Blocking someone means they will no longer be able to contact you on Facebook.

9 Learn how to use Facebook's reporting tools

If someone is bothering you on Facebook or breaking our rules report them to us via the reporting links near each piece on content or via our help center. More information about how to report things on Facebook can be found at www.facebook.com/report

10 Ask people to take stuff down

If a friend posts something like an embarrassing photo, which you find upsetting but may not break Facebook's rules use our social reporting tools to ask them to take it down. To learn more about social reporting go to www.facebook.com/report



Stay informed

11 Talk about internet safety

If you are a parent then have conversations about safety early and often with your children. One of the best ways to begin a conversation is to ask your teens why services like Facebook are important to them. You might also ask them to show you how to set up your own Facebook account, so you can see what it's all about. Discuss what's appropriate to share online—and what isn't. Check out the Family Safety Centre for more advice: www.facebook.com/safety

12 Stay up to date on the Facebook Safety Page

On Facebook, safety is a conversation and everyone has a role. Stay up to date on safety by visiting our page at www.facebook.com/fbsafety



13 Check Out the Family Safety Centre, the Facebook Help Center and Anti-Bullying Hub

If you are a parent, teen or teacher and want safety advice then visit our Family Safety Centre: www.facebook.com/safety There's also lots of information in the Facebook Help Centre: www.facebook.com/help

For specific advice about how to deal with online bullying then visit the Facebook Anti-Bullying Hub: www.facebook.com/safety/bullying



THINK BEFORE YOU SHARE

Tips from Facebook and MediaSmarts



We always hear that sharing is a good thing. And thanks to technology, we can share our ideas, opinions, pictures and videos with our friends and other people.

Most of the time, sharing *is* good. But if we aren't thoughtful about how we share, we run the risk of hurting ourselves or someone else. Also, remember that the things you share with your friends can end up being shared with others. That's why it's important to think before you share.

YOUR OWN STUFF

Whenever you're sharing things about you – whether it's a picture, video or personal things like your phone number – keep in mind that it could easily end up being seen by people you didn't want it sent to.

Also, it's not a good idea to share things when you're feeling really emotional – whether you're angry, sad, or excited. Calm down first and then decide if it's really a good idea.

Next, ask yourself:

- ✔ Is this how I want people to see me?
- ✔ Could somebody use this to hurt me? Would I be upset if they shared it with others?
- ✔ What's the worst thing that could happen if I shared this?

Passwords are not social: There's some things you need to be really careful about sharing. Sometimes friends share passwords with each other when all is good, but unfortunately this can turn into a nightmare later.

An image lasts forever: Some people think sharing a nude or sexy photo with a girlfriend or boyfriend – or someone they hope will be their girlfriend or boyfriend – shows they love or trust them. Be extra careful in this situation and think – an image can outlast a relationship.



Remember that if somebody asks you to share something you are not comfortable with you have the right to say no. Nobody who loves or respects you will pressure or threaten you.

Gone in seconds, but maybe not gone forever: Some apps or social networking sites promise to auto-delete images or videos after a few seconds of viewing. But there's ways around this – the viewer could take a screenshot – so you still have to make smart decisions about sharing.



FacebookTIPS:

1

Passwords are not social. Don't share your password with anyone. For additional security tips go to: facebook.com/help/securitytips

2

Check your privacy settings at facebook.com/privacy to see who can view your posts.

3

Check the audience selector each time you post on Facebook in order to make sure you are sharing it with your desired audience.



OTHER PEOPLE'S STUFF

Most of the time when people send things to you, they're okay with you sharing them with other people. If you don't know for sure, think twice before doing this. Even better, ask the person who sent it if they mind if you share. The same is true if you're sharing photos or videos that have other people in them: ask before you tag, re-post or pass them on.

If someone shares something with you with somebody else in it, ask yourself:

- ✓ Did the person who sent this to me mean for it to be shared?
- ✓ Did they have permission from the person who's in it?
- ✓ How would I feel if somebody shared something like this with me in it?



If what you received makes that person look bad, would embarrass them, or could hurt them if it got around, **don't pass it on**. The person who sent it to you may have meant it as a joke, but jokes can be a lot less funny when something is seen by the wrong person.

A lot of people – boys especially – get pressured by their friends to share nude photos of their girlfriends or boyfriends. It can be hard to stand up to this pressure, but you have to think about how much giving in could hurt you and your girlfriend/boyfriend.



FIXING THINGS IF THEY GO WRONG

Everyone makes bad choices sometimes. That doesn't mean that you shouldn't do everything you can to fix things.

If you shared something you shouldn't have, the first step is to ask the people you sent it to not to pass it on.



If someone else posted something you sent them, start by asking them to take it down. It's actually pretty effective most of the time. **Remember not to do anything while you're mad**: give yourself time to cool down and, if you can, talk to the person offline.

If they refuse to take it down, don't try to get back at them by sharing private things they sent you, harassing them or getting your friends to gang up on them. For one thing, this almost always makes things worse. For another, the more you get back at them, the more it might look like it's just as much your fault as theirs.


If you're tagged in a photo that you don't like, remember that a lot of photo-sharing and social networking sites may let you take your name off any pictures you've been tagged in. On Facebook, you can also select to review posts you are tagged in before they post to your timeline under your privacy settings: [facebook.com/privacy](https://www.facebook.com/privacy).



take note!

If you're on Facebook and don't feel comfortable confronting someone yourself, or don't quite know what to say, Facebook has a **Social Reporting tool** with some messages you can use and ways to get a parent, teacher or trusted friend to help you out.

For more serious things, for instance if it's a partly or fully nude picture or video, if it's defamatory (it's not true and hurts your reputation) or if it's being used to harass or bully you, you can ask the site or service that was used to share it to take it down. In those cases you can report it to the police too.

 **If you are in a situation where a person is threatening to share a nude photo of you unless you provide more nude photos – you should involve a trusted adult and contact the police right away. This is unacceptable behaviour and in many countries it is illegal.**



How to use the Social Reporting Tool

To learn more about social reporting or reporting abusive content on Facebook, go to facebook.com/report.

Remember that you are not alone – you can always talk to your parents, a teacher or counsellor, another adult you trust, or a help-line to get advice and support.



BROUGHT TO YOU BY:



FOR ADDITIONAL INFORMATION PLEASE CHECK OUT THE LINKS BELOW:

MediaSmarts

mediasmarts.org

Facebook Family Safety Center

facebook.com/safety

Bullying Prevention Tips

facebook.com/safety/bullying

Facebook Help Center

facebook.com/help



Hungarian National Authority for
Data Protection and Freedom of
Information



National Authority for Data Protection and Freedom of Information
(NAIH)

1125 Budapest, Szilágyi Erzsébet fasor 22/c
Mail: 1530 Budapest, Pf.: 5

Tel: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Internet: <http://www.naih.hu>

E-mail: ugyfelszolgalat@naih.hu, privacy@naih.hu