
# DIGITAL CHILD PROTECTION STRATEGY OF HUNGARY

# TABLE OF CONTENTS

Greeting ..... 4

I. Situation assessment ..... 6

1. Awareness-raising and media education ..... 7

1.1 Skills required for the conscious use of the Internet ..... 7

*1.1.1 Technological skills* ..... 7

*1.1.2 Familiarity with the tools facilitating the safe use of the Internet* ..... 8

*1.1.3 General information concerning potential threats* ..... 8

*1.1.4 Identifying harmful content* ..... 10

*1.1.5 Identifying harmful behaviour* ..... 10

*1.1.6 Awareness of the harmful effects of excessive use of the Internet* ..... 10

*1.1.7 Awareness of opportunities offered by the Internet* ..... 11

1.2 The state of teaching how to consciously use the Internet ..... 11

1.3 Experiences concerning the level of consciousness of persons concerned 13

*1.3.1 Parents* ..... 14

*1.3.2 Teachers* ..... 15

*1.3.3 Peers* ..... 16

1.4 Actors involved in awareness-raising ..... 16

*1.4.1 Public education* ..... 16

*1.4.2 Government organisations* ..... 17

*1.4.3 Non-governmental organisations* ..... 17

*1.4.4 Businesses* ..... 18

*1.4.5 Other professional bodies and interest organisations* ..... 18

*1.4.6 Media* ..... 18

1.5 Best practices in awareness-raising and promoting media education ..... 19

2. Protection and safety ..... 20

2.1 Internet content posing hazard to children; experiences and consequences 20

*2.1.1 Content posing hazard to children* ..... 20

*2.1.2 Experiences and consequences concerning threats* ..... 23

*2.1.3 Possibilities for protection* ..... 24
2.2 Potential solutions for isolating children from hazardous content and users 25
*2.2.1 Examples of protective mechanisms and solutions* ..... 25
*2.2.2 The system of protective solutions in Hungary* ..... 27
2.3 Filtering software and the marking of online content ..... 34
*2.3.1 Applicable legislation* ..... 34
*2.3.2 Supporting the development of filtering software* ..... 35
*2.3.3 Experiences of the practical application of filtering software* ..... 36
*2.3.4 Recommendation by the Child Protection Internet Round Table* ..... 36
*2.3.5 Review of compliance with the recommendation* ..... 37
2.4 Protection of children's rights under the current legal system ..... 38
*2.4.1 International legislative background* ..... 38
*2.4.2 Constitutional background* ..... 38
*2.4.3 Civil law* ..... 38
*2.4.4 Criminal law and the law of petty offences* ..... 39
*2.4.5 Media Law* ..... 41
*2.4.6 Data protection* ..... 42
*2.4.7 The act on certain issues concerning e-commerce services and services related to the information society* ..... 43
*2.4.8 Act on consumer protection* ..... 43
*2.4.9 Act on gambling* ..... 44
2.5 International best practices ..... 44
2.6 Expanding the range of safe content intended for children ..... 46
2.7 Equal opportunities ..... 47
3. Applying sanctions and providing help ..... 48
3.1 The organisations concerned ..... 49
3.2 How to realise that one's rights have been breached ..... 49
3.3 Imposition of sanctions under media legislation ..... 50
*3.3.1 Procedures by co-regulatory bodies* ..... 50
*3.3.2 Proceedings by the Media Council* ..... 51
3.4 Imposing sanctions if data protection rules have been breached ..... 52

3.5 Civil law consequences ..... 52
3.6 Breaching the criminal law ..... 53
*3.6.1 Imposing sanctions under Act C of 2012 on the Criminal Code* ..... 53
*3.6.2 Legal consequences under the act on petty offences* ..... 54
3.7 Tools designed to block unlawful content ..... 54
*3.7.1 Removal of content violating the privacy of minors* ..... 54
*3.7.2 Hotlines* ..... 55
*3.7.3 Blocking of electronic data* ..... 57
*3.7.4 Self-regulation* ..... 58
3.8 Alternative dispute settlement in educational institutions ..... 59
3.9 Providing assistance and the helping of victims ..... 59
*3.9.1 Helping victims* ..... 60
*3.9.2 The activity of NGOs* ..... 60
*3.9.3 Protecting children's rights during administrative procedures (dispensing of justice)* ..... 61

II. SWOT analysis ..... 62

III. System of tools and objectives ..... 66

1. Vision ..... 66

2. The system of objectives under the strategy ..... 69
2.1 Comprehensive strategic objectives ..... 69
2.2 Objectives under each pillar ..... 71
*2.2.1 Awareness-raising and media education* ..... 71
*2.2.2 Protection and safety* ..... 73
*2.2.3 Applying sanctions and providing help* ..... 76

3. The system of tools under the strategy ..... 78
3.1 General approach ..... 78
3.2 Classification of tools by pillars ..... 78
*3.2.1 Awareness-raising and media education* ..... 78
*3.2.2 Protection and safety* ..... 87
*3.2.3 Applying sanctions and providing help* ..... 100

## Greeting

In a national consultation campaign on the Internet and digital development (InternetKon), held by the Government in 2015, a clear opinion was articulated by the Hungarian people: the World Wide Web should not pose a threat to the safety of children. In addition to the above, the drafting of the Digital Child Protection Strategy of Hungary has become indispensable due to the emergence in recent years of new hazards and concepts in connection with the use of the Internet by children, which require new types of solutions and, to a limited extent, a new system of government instruments. Children are no longer passive recipients of information. Instead, they are active communicators, thus putting themselves at risk through their own activity. It is therefore more important than ever that they should be knowledgeable and aware in terms of online communication.

On the basis of the results of the InternetKon, the Government has drawn up the Digital Success Programme in order to facilitate the digital development of Hungarian society and the Hungarian national economy. In addition to the above, the Digital Child Protection Strategy of Hungary has been drawn up as part of the programme based on the awareness that digital culture plays a decisive and ever-increasing role in influencing everyday life, society and the economy. One of the most important abilities, the conscious use of the Internet, as a channel of accessing digital culture, is an extremely complex skill. If young people with appropriate skills are able to use the opportunities offered by the digital world in a safe environment, it gives them a competitive edge while also improving the competitiveness of their communities and thus that of their country. The strategy has therefore been drawn up primarily in order to ensure that children are protected from dangerous and harmful online content and methods and to prepare children, parents and teachers for a conscious and productive use of the Internet.

In addition to supporting the conscious and productive use of the Internet, priority objectives of the Digital Child Protection Strategy of Hungary also include that regulations and measures to protect children should be enforced more than before. To that end, it is important to identify and eliminate the risks and threats to children while using the Internet and thus to prevent or minimise its harmful effects. Additional objectives of the strategy include that the protection mechanisms available should function properly and efficiently.

While the strategy focuses on children, almost all groups of society are affected. Therefore, in addition to identifying the system of government instruments, a mutual sharing of knowledge and teaching and cooperation between various stakeholders are also required in order to ensure that the strategy is successfully put into practice. To that end, the Digital Child Protection Strategy of Hungary proposes that all stakeholders, including public education, NGOs, the system of child protection institutions and law enforcement agencies should cooperate by standing up against harmful, dangerous and illegal online activities.

**Dr Tamás Deutsch**

Commissioner of the Hungarian Prime Minister

Digital Success Programme

# I. Situation assessment

## Introduction

In December 2015, the Government adopted Government Decree No 2012/2015 of 29 December 2015 on the Digital Success Programme to be implemented by the Government on the basis of the results of the national consultation campaign on the Internet and digital development (*InternetKon*).

In order to ensure that the regulations and measures to protect children and privacy should be increasingly enforced, the Government called upon the Prime Minister's Commissioner for coordinating and implementing the Government's duties related to the Digital Success Programme to prepare and submit to the Government the *Digital Child Protection Strategy* by 30 June 2016 in cooperation with the Minister for Human Resources and in consultation with professional and non-governmental organisations concerned, the President of the National Media and Infocommunications Authority (NMHH) and public and market operators (Section 4(a) of the Government Decree).

The strategy is based on three pillars and that structure is reflected in the situation assessment and the identification of objectives and tools:

- Awareness-raising and media education;
- Protection and safety;
- Applying sanctions and providing help.

# 1. Awareness-raising and media education

The objective of the Awareness-raising and media education pillar of the strategy is to achieve that the persons concerned are able to use the opportunities offered by technology in a responsible and conscious manner. Awareness-raising concerning the safe use of the Internet is required in order to avoid or at least minimise the threats and harmful effects to the healthy development of children and minors. The conscious use of the Internet thus includes both the ability to exploit the opportunities offered by the online world to the greatest extent possible and the ability to detect and identify potential threats and risks during online activities. In addition to the above, media awareness also includes familiarity with protective solutions enabling the safe use of the Internet as well as the ability to access the tools and institutions available in the event of the unexpected occurrence of a detrimental situation.

Awareness-raising, however, should not be limited to children. It is at least as important for adults children are surrounded by in their everyday life. Apart from children, it is thus of at least equal importance to raise the awareness of parents and teachers responsible for educating children as well as to provide guidance concerning external factors playing a crucial role in their lives, such as the media (or the Internet itself).
The situation assessment of the strategy collects and evaluates the information designed to raise children's awareness, focusing in particular on the threats to the persons concerned, which can be easily avoided if they have access to more information. While it is obviously impossible to accurately determine the existing level of awareness, the tools (e.g. in education) designed to raise awareness and the practical efficiency of such tools are known.

## 1.1 Skills required for the conscious use of the Internet

### *1.1.1 Technological skills*

First of all, the conscious use of the Internet means familiarity with the use, operational principles and the system of devices enabling access to the online space. Considering the rapid development of technology, the youngest generations are born into that culture and are surrounded by such tools as they grow up. It is at that point that one is confronted with the first challenge to raising awareness: given their age, children are a lot more familiar with the use of digital devices than the adults around them who ought to take an active role in raising their awareness.

### *1.1.2 Familiarity with the tools facilitating the safe use of the Internet*

The conscious use of the Internet includes that children are aware of the safety tools and solutions available that are capable of protecting them from harmful effects and consequences. While this need not include accurate information on all possible details and circumstances, such as the exact availability, application and use of the devices concerned, one must be aware at least of the existence and the basic functions of such opportunities. It is extremely important that not only children but their parents, guardians and teachers should also have at least the same or, preferably, better skills and information on relevant issues.

Familiarity with and the responsible use of certain online settings are of similar importance. The latter include the use of data protection settings, that one should at least skim through the terms of use prior to accepting them in certain situations as well as familiarity with the circumstances and the potential risks concerning online shopping.

### *1.1.3 General information concerning potential threats*

There are a number of other threats to children (and often to adults, too) in a world where the digital media, a crucial factor in the organisation of society and socialisation, tend to permeate almost all human activities. In our media-centred and convergent culture, such additional risks seriously threatening children (and adults) include the following:

- Deliberate deception, i.e. manipulation, as consumers of texts communicated by the media, particularly in societies with less plural publicity, have no opportunity to ascertain the truthfulness of information published in the media from any sources other than the same media, even if their right to obtain fair and accurate information on issues of general interest may thus be seriously impaired;
- In an online media environment, which is more difficult to regulate, there is an increased risk of hate speech or encoded speech; in such situations, stigmatisation, calls to repress any cultural difference, the strengthening of prejudices and racism constituted by representing outsiders as criminals are sources of the threat related to the use of the media;
- There is a particular risk of addiction and addiction-related ‘overuse’, a passion for online games or the non-stop use of social media sites, ‘relocating’ to the Internet, i.e. media users tend to get increasingly addicted to the online media;
- Another serious risk source is the increasing and excessive share of virtual experience in the overall human experience, i.e. the mixing of real and virtual

information to a significant extent, which may render people unprepared and vulnerable to real-life challenges;

- Other serious problems include the weakening/lapse of the knowledge of facts, the fact that ‘hard media users’ are more exposed to manipulation, particularly if certain social groups or phenomena are represented by the media to a small extent or not at all, i.e. the problem of representation;
- For the ‘click generations’ raised in that textual environment, non-linear reading and the use of texts based on the use of hyperlinks, both characteristic of the online world, make it increasingly difficult to read through and interpret traditionally structured texts and thus to access and digest more or less the entire body of knowledge/set of texts required by schools;
- The problem of the vulnerability of data security goes a long way beyond the issue of unsuspectingly disclosed personal data as it also includes the vulnerability of (digital) databases and archives, which poses a serious and actual national security risk (i.e. spying and terrorism) as well as the risk of the abuse of power and restrictions challenging fundamental democratic rights (whether with a reason or in order to protect the power of those with a political and economic supremacy);
- Similarly, the mediatization and transformation of the body are also very important, problematic (and, in its current form, a recent) phenomena related to popular culture and media (from tattoos to plastic surgery to the implantation of various cosmetic and health-improvement structures to genetic intervention), since the culture of the body is closely related to the evolution of the roles of men and women in society, the problem of sexual identities and, through the latter, the influencing of public opinion in connection with minorities;
- In a convergent culture, people are increasingly attempting to define themselves and the surrounding world on the basis of forms and patterns of expression reflected by the media, which increases the distance and reduces penetration between the experience, values and level of information of generations;
- Since, in a convergent culture, technical platforms also keep converging, i.e. tablets and smart phones serve as media players, photo and video cameras and computers communicating online, media content is increasingly difficult to be classified into distinct genres and forms of texts that are differentiated by sharp contours, which renders selection and a conscious choice of content increasingly difficult;
- Restricted access to media technologies, digital illiteracy and an exclusion from the skills required to use the media may aggravate social inequalities.

### *1.1.4 Identifying harmful content*

The skills enabling children to identify and thus to avoid harmful and dangerous content encountered during online activities constitute one of the most important parts of information. Such competence is closely related to the familiarity with the tools facilitating the safe use of the Internet; the ability to identify specific security solutions (e.g. the warning of content not recommended to persons under 18) is a priority consideration in connection with the use of the Internet. When encountering harmful content, children should also possess certain basic competences; they should really be aware of the need to avoid content not recommended for them (even despite their curiosity).

If, however, they are nevertheless confronted with harmful, dangerous or even illegal content, they should be aware of the existence and the availability of forums and services (e.g. hotline, police etc.) where such abuses may be reported. (While obviously going beyond basic awareness, it can be mentioned that, as far as children are concerned, the optimum condition would be the need to create a culture where any such content gets reported, each person taking responsibility vis-à-vis their companions with less information and thus protecting them from dangers.)

### *1.1.5 Identifying harmful behaviour*

In addition to identifying harmful content, the conscious use of the Internet includes the ability to identify and preferably avoid dangerous and, in certain cases, illegal online behaviour and take required additional action (e.g. reporting to the relevant forums and bringing legal action).

The proper recognition and management of such types of conduct involves (may involve) another skill, i.e. since they are aware of the potential effects and consequences of such behaviour, children are much less likely to commit such acts themselves.

### *1.1.6 Awareness of the harmful effects of excessive use of the Internet*

As an indirect effect rather than directly while using the Internet, a number of adverse and dangerous consequences, easy to be overlooked by the persons concerned, may arise. These may include certain types of addiction, a deteriorating ability to concentrate, due to the characteristics of online activities, deteriorating social relations etc. Such consequences obviously do not occur as a result of any long-term online activity. Searching for information required for one’s studies, browsing for reading and information purposes should be treated differently from the use of online games or browsing social media pages as a matter of routine.

### *1.1.7 Awareness of opportunities offered by the Internet*

Children should be aware of the opportunities made available by the Internet, which may empower them or facilitate their lives in a number of areas. This primarily includes facilitating one's studies and other forms of gathering information and experience. It must be noted that, in certain cases, anonymity, often exploited for abuse, may have certain advantages in this respect. In certain areas and on certain issues, children may (mostly out of fear or a sense of shame) be reluctant to open up to other people or share their experiences or psychological problems or emotional difficulties. By contrast, on online forums, it may be much easier for them to reveal their problems and may receive more efficient help from their peers.
Other important factors include the awareness of opportunities for certain forms of communication (e.g. social media sites), the conditions and circumstances of their use and the need to keep such use within 'healthy' limits and to exploit their potentials. The way there is nothing inherently 'wrong' about the Internet, there is obviously nothing wrong with these social media sites; they are shaped by the users, including children. If these skills have been acquired, such services will no longer pose a 'danger'. On the contrary, they will facilitate people's everyday life in a number of respects in various areas.

## **1.2** The state of teaching how to consciously use the Internet

In public education, a lot more emphasis should be placed on the issues of protecting children and improving their media education. Particularly important duties include:

- The review of (psychological and IT) services available at public education institutions;
- The role of organisations supporting educational work (for example, the Office of Education, including in particular the County Pedagogical Educational Centres, Pedagogical Institutes and NGOs in the counties and in the capital);
- A review of the Basic National Curriculum ('NAT') and the relevant requirements in various subjects;
- Updating the requirements of educator and teacher training;
- Reviewing the requirements established in the further training system of educators and teachers.

In that context, Report no AJB-479/2016 of the Commissioner for Fundamental Rights, published in February 2016 revealed some remarkable information, including the following:

- The NAT published in 2013 has realigned the place and the system of media education in Hungarian schools. For the first time, information regarding media education are reflected in the NAT for all age brackets within a specific subject ‘visual culture’;
- Based on Government Decree No 110/2012 of 4 June 2012 on the publication, implementation and application of the Basic National Curriculum, the school curriculum includes the shaping of critical thinking, violence appearing in the media, i.e. the interpretation of the phenomenon and making children aware of its effects and the impact of an online lifestyle on personality development, social relationships, studies, work and leisure. In 2001, it became an elective public information subject at the secondary school leaving exam;
- However, in the opinion of education experts, it has been a problem that there are considerable differences between children in terms of the level of their media education and knowledge, depending on their local and personal opportunities and possibilities at school. Moreover, as media comprehension education is related to several fields of education, it is not an independent subject, which means that most teachers having media-related knowledge did not major in that specific subject but hold a degree in various other subjects;
- In the opinion of the Commissioner for Fundamental Rights, because of the astonishing rate of growth in the amount of information and the number of information channels, there is an unprecedented need for children and young people to receive an education that enables them to safely find their way in the world of media. Children are only capable of understanding the world around them if they are able to appreciate and digest the audio and visual information they are exposed to. That purpose is served by media comprehension education;
- The Under-Secretary of State for public education emphasised that there are no consistent rules in educational institutions concerning the use of media and the Internet at school. Wherever school-level rules are applied, such rules are typically set out in the local curriculum and the school’s internal rules of procedure. Another obstacle to regulation is that the majority of students have a smartphone or tablet. The operation and use of such devices during school hours are also subject to school-level regulations. Aware of the risks involved by the use of IT devices, the Ministry responded by amending the act on public education;
- The time frame for media education is in fact set on local, i.e. school level or is in the teacher’s discretion. As no studies are available concerning the efficiency of formal school education, i.e. what actually goes on in the classrooms in Hungary, no data are available on the actual time frame of education at schools. However, the responses of the authorities contacted have suggested that the time frame scheduled for education related to media information, media comprehension and the conscious use of media is often not fully utilised. It can be concluded that, due to the low number of classes, the integrative presence and the insufficient number

of qualified teachers (a lot of whom are incompetent), media consciousness education is often insufficient and inefficient within the educational system;
- The gaining ground of the digital environment has put teachers into a difficult position as no emphasis has been placed in the training of most teachers on how to handle this area, i.e. how they should actively and safely use the media in their work. The Under-Secretary of State pointed out that, in the meantime, students should be made aware of the conscious and responsible ways of exploiting the potentials offered by the media.

According to information from the Office of the Commissioner for Fundamental Rights, relatively few complaints directly related to online child protection have been received by the Office; complainants have typically referred to or mentioned online infringements among various other complaints and grievances. Because of that, the Ombudsman's practice in this field is difficult to quantify or described in statistical terms. According to the Commissioner, the relatively low number of specific complaints and queries received on the subject may suggest that not only children but also their parents, teachers and schools are often not sufficiently aware of the actual risks and threats related to the Internet and the possible methods of handling such risks, i.e. the existence of authorities competent to take action against grievances to children in the online space. Consequently, the Commissioner called attention to the need that the teaching material of teacher training and upskilling should include information related to the handling of online abuse and harassment cases at schools.
Moreover, the Commissioner mentions that, complainants have typically complained of the terms and conditions of the most popular social media sites, sites that violate basic community principles and comments and opinions injurious to children, posted on social media sites. Other consequences of the use of social media sites parents are concerned of include the possibility that their children may be negatively viewed or discriminated against in their schools as a result of their online activity.

## 1.3 Experiences concerning the level of consciousness of persons concerned

Numerous studies and research have been conducted in the field of consciousness, while experiences obtained in other programmes are also available for the assessment of the current situation in order to get at least on outline of the situation, revealing the most important achievements, problems and deficiencies. As explained above, in order to enable children to acquire appropriate skills, the strategy of awareness-raising must be developed. and therefore, the current situation must be assessed across a much broader spectrum. The review should include not only

children but the following persons in terms of their attitudes to the use of the Internet, their existing skills, the identification of their deficiencies and the possible ways and means of eliminating such deficiencies:

- parents (close relations and families in general);
- teachers;
- representatives of the child protection system: school psychologists, social workers and educators;
- peers.

In the context of experiences, it should be noted that, in autumn 2014, the Hungarian Committee of UNICEF conducted a non-representative survey of 1,191 primary and secondary school students aged 10 to 19 concerning children's rights, including online safety. While 96 % and 88 % of respondents have a mobile phone and a social media profile respectively, half of the children do not consider the Internet as a safe place. One in three children have been exposed to online bullying. In such situations, half of these children tried to defend themselves while as few as one in ten reached out for help. According to a 2013 survey by the NMHH, three-quarters of young people aged between 14 and 17 regularly surf the Internet on a computer without an adult being present, while 10 % of Internet users living with nursery-school children also responded that children under six in the same household regularly use the Internet on a tablet or a telephone on their own, without the assistance of an adult. A small portion of Internet users responded that either they or their parents had installed a filter software on the computer (18 %), phone or tablet (11 %) used by children.

### *1.3.1 Parents*

The awareness of parents (and teachers, discussed under the next section below) is of key importance for the area. If the persons assuming a role in teaching and educating children lack the information related to the conscious use of the Internet or the intention and ability to pass on such information, it may have serious consequences. If the persons who should have a key role in the passing on of information lack the required competences, they obviously cannot be expected to pass on such information to children.

In other words, the responsibility and the role of parents (the family) have outstanding significance in terms of consciousness; as in everyday life, they are (rightly) expected to provide a similar amount of help and assistance in the online world. Unfortunately, however, experience has shown that the majority of parents are not fully aware of how to use the Internet consciously or of online threats. Apart from the lack of information on existing risks, parents often tend to be passive or to dodge problems, due mainly to fears of a potential loss of authority.

The statements concerning parents apply even more to the older generations (primarily grandparents). However, it would be wrong to conclude that, beyond a certain age, it is no longer possible to pass from an offline existence on to online 'literacy'. In Western European societies, lifelong learning has been a successful initiative and campaign supported by governments, the positive impact of which goes beyond the persons directly concerned. It would greatly facilitate the raising of awareness if grandparents were familiar with the characteristics of children's use of the Internet and their relevant attitudes and habits as the Internet also plays a substantial role in the communication of grandparents and grandchildren. As some grandparents are Skype and/or Viber users, safety is a priority issue also with regard to these communication channels.

### *1.3.2 Teachers*

In the meaning of the above, while obviously parents (and, in a broader sense, the immediate family environment) are primarily responsible for raising the awareness of children, teachers also play a role. It is because the teacher is the adult who is, for example in a cyberbullying case, in a direct relationship with the victim and often with the perpetrators and victims, too, and may thus be a key actor in detecting and resolving conflicts. The role of teachers is thus manifested in the passing on of information, while they are also responsible for possessing the skills of consciousness as an active participant of discussion and conflict management mechanisms within the framework of the educational system.
Experience has shown that, sadly, very few teachers possess the required skills. It should be noted that a number of NGOs have been organising trainings not only for children but for teachers, too (such as the MediaSmart Hungary Oktatási Közhasznú Nonprofit Kft., the Safer Internet Plus Program or the Digitális Knowledge Academy).
In that context, mention must also be made of nursery-school teachers as children often encounter smart devices and, through them, the online space, before going to school. Programmes designed to improve their skills are also available to these teachers, including, for example, a package adapted by the Televele Médiapedagógiai Műhely Egyesület or the Bibianeten website (www.bibianeten.hu), based on a Luxembourg model and operated by the International Children's Safety Service.

Achievements in terms of upskilling, specialist literature and educational resources include that, in 2015, the NMHH offered 30 hours of further training for 500 teachers on new skills facilitating media comprehension and the use of media. Topics included the culture of digital society, digital skills, digital security and public confidence, the development of conscious media consumption habits, acquiring media culture,

conscious consumer culture and a conscious and responsible civic attitude. In autumn 2015, the NMHH published a package of gap-filling technical books and educational films.

### *1.3.3 Peers*

Peers play a significant role as a number of programmes have demonstrated that children and young people may provide significant support to each other and, by passing on the relevant skills and experience, to older generations, too.
This may include the possibility of community service, under which young people help their peers get their bearings among issues of Internet security, social media pages and data protection, among others (for example, such service is operated by the International Children's Safety Service with secondary-school students).

## 1.4 Actors involved in awareness-raising

The educational system should obviously play a primary role in raising the awareness of children and other persons referred to above. However, in the light of the weight and importance of the task, a lot broader social responsibility has already been achieved in order to attain that objective; it appears that the extensive concentration of forces needs to be maintained in the future. To that end, assistance by the following stakeholders appears to be indispensable in order to ensure that genuine results are achieved:

- public education;
- other government organisations;
- NGOs;
- businesses;
- other professional and interest bodies;
- the media.

### *1.4.1 Public education*

Public education must play a key role in raising awareness among children. The experiences and information related to the state of public education and the current level of teachers' awareness are described under Sections 1.2. and 1.3.2.

### *1.4.2 Government organisations*

Government bodies, authorities and other institutions outside the public education domain also play a key role in raising awareness. These organisations rely on their human and financial resources in carrying out their duties; in particular, they may

- publish advertisements and campaigns of general interest in the media;
- operate an awareness-raising network;
- support trainings for teachers;
- carry out surveys and research.

### *1.4.3 Non-governmental organisations*

NGOs play a key role in awareness-raising as they are able to respond very quickly to the rapid changes caused by the digital world due to their operating principles and their system of objectives and tools. It must be noted that cooperation on children's Internet security has been achieved between NGOs, the industry and schools, showing that dual education plays an essential part and has a future in terms of awareness-raising.

Since 2009, the International Children's Safety Service has been a leading consortium partner of the European Union's Safer Internet programme (www.saferinternet.hu), organising expert conferences and trainings. Its trainers have held free interactive trainings throughout the country for children, young people, teachers, parents and all of those who wish to know more about the safe use of the Internet.

The Digital Knowledge Academy (www.digitalisiranytu.hu) has set up a network of volunteer trainers, organising talks for children, teachers and parents.

The UNICEF Hungarian National Committee and Telenor Hungary started their cooperation in 2013 by launching the Alarm Clock Programme. The UNICEF's now more than 100-strong team of volunteer experts holds 90-minute interactive presentations, which are free of charge to schools, on special children's rights, including in particular situations of violence against children (including the topics of cyberbullying and digital security). Familiarity with children's rights is also important from the perspective of social inclusion, which may constitute the basis for the safe and harassment-free use of the Internet for 'digital native' young people. While the two organisations originally set the goal of reaching 2,000 children a year, the need to fulfil demands from schools has meant that more than 11,000 children have attended an Alarm Clock session throughout the country over the past two years.

In possession of the required skills and experience, NGOs are capable of achieving significant results in terms of awareness-raising (among others). In the future, the government should take an active role in order to support their activities.

### *1.4.4 Businesses*

In addition to carrying out programmes in order to encourage awareness-raising, the activities of businesses are mostly manifested in complying with statutory requirements concerning the availability of a filtering software. It can be seen that most businesses (providers of access to the Internet) are attempting to be active in the field.

### *1.4.5 Other professional bodies and interest organisations*

The trade associations and interest organisations representing businesses also play a significant role in awareness-raising. By coordinating the activities of service providers, these organisations are able to influence the process of awareness-raising. Examples include self-regulating and partner regulating organisations on the media market (e.g. Association of Hungarian Television Broadcasters, Advertising Self Regulatory Board, Association of Hungarian Content Providers, Hungarian Publishers' Association), all of whom have their own code of conduct, providing guidance to businesses; further examples include the Communications Reconciliation Council or the Hungarian ICT Association, both operating in the field of communication.

### *1.4.6 Media*

Like in many other areas of life, it is beyond dispute that the media play a role and have responsibility for and an ability to influence awareness-raising with regard to the Internet. Through the content transmitted by them, they direct not only the younger generations but exert significant influence on society as a whole. That ability particularly exists with regard to children: due to the lack of experience and their vulnerability, they are even more exposed to the effects of the media (Internet).

It is of essential importance that, recognising their responsibility, the media (which, in the present case, should not be restricted to 'traditional' media providers but also including the world of the Internet) should assume a role in awareness-raising as much as possible. Similarly to NGOs, this could manifest itself in the launching of independent programmes, general circumspection regarding the content broadcast, providing appropriate space for awareness-raising campaigns and the broadcasting of programmes specifically designed to promote awareness-raising.

## 1.5 Best practices in awareness-raising and promoting media education

A number of programmes and initiatives have been set up in order to promote children's conscious use of the media and the Internet. As a result of the knowledge and experience accumulated, the 'battle' for awareness-raising has advanced a lot; the efficient use of these resources may help carry out the efforts to pass on sufficient and necessary competences.

As the various organisations, programmes and practices concerning awareness-raising have been discussed above, these need not be repeatedly listed here. However, it can be clearly concluded on the basis of the assessment of the current situation that numerous programmes are running in parallel in various areas of society, making a serious effort in order to promote the conscious use of the Internet by children. In that context, it seems to be of essential importance that the government should recognise and support the best practices of participating organisations and institutions and coordinate their activities with a view to increasing the efficiency of their efforts.

# 2. Protection and safety

The use of the Internet has become an integral part of our everyday life, which unfortunately includes that it is becoming increasingly common that one has to face its risks and dangers, too. Therefore, the legal system must find proper responses in cases where Internet users (focusing on minors or children in the present study) are faced with harmful content, or find themselves in an injurious or positively unlawful situation. As the sources, the forms and effects of the dangers encountered may vary to a great extent, the relevant responses are also rather complex.

Obviously, it is primarily the duty of the administration to use the means available to it in order to provide sufficient protection and security against the detrimental consequences of using the Internet. That objective is manifested in developing the required legal framework and the system of organisations to enforce it as well as in supporting the relevant efforts by NGOs. In terms of implementing rules, the role of NGOs is just as important as that of the public sector; the efforts by NGOs and self-regulating and partner-regulating organisations often result in more rapid and more direct responses to the problems encountered even if, at first sight, the system of tools available to them does not appear to be so efficient.

While the activities of that system of institutions is clearly not limited to or focused specifically on the protection of children, solutions and technologies specifically designed to promote the online security of the younger generations already exist.

## 2.1 Internet content posing hazard to children; experiences and consequences

### *2.1.1 Content posing hazard to children*

*A)* *Cyberbullying* has become one of greatest online dangers, which is far more successful and efficient in intimidating victims than physical violence. Common forms of its perpetration include the unauthorised publication of the victim's personal data (e.g. by registering in someone else's name on a social media or dating site and publishing false and injurious data on the site) or uploading embarrassing photos or videos of a child to the social media or video or photo sharing site without the child's knowledge or approval.

Apart from the unauthorised publication of personal data, there are numerous other forms of cyberbullying. The most common categories include:

*Flaming*: online argument using a furious and obscene language or posting

offensive, and often irrelevant, comments on a person on a public forum.

*Harassment:* online harassment occurs when a teenager falls victim to recurring and ongoing intentional injury over the Internet or by mobile phone. It may consist of recurring offensive, insulting or upsetting messages intended to humiliate, threaten, mock, exclude or discredit a person.

*Denigration*: sending, posting or distributing cruel gossip or hearsay, liable to damage a person's reputation.

*Exclusion:* shutting out a member of an online community from the group.

*Outing:* the unauthorised sharing of secrets, gossip or other personal information with others.

*Trickery:* obtaining personal data through fraud or deceit and then sharing such data with the community.

*Cyberstalking:* watching and observing the victim's online habits over a longer period and using them to attack the victim; sending threatening and intimidating messages and using them in order to arouse fear so the victim should feel that his or her safety is threatened.

*Cyberthreats:* direct threats or unsettling statements that suggest that their author is emotionally upset and is considering hurting someone or himself/herself or committing suicide.

*Sexting:* a term coined by combining the words 'sex' and 'texting'. It is used to denote a situation where the perpetrator sends sexually provocative nude or semi-nude selfies or openly sexual messages to other persons. Nude photos tend to attract the greatest attention as such images are much more likely to be further distributed to a larger group of people, putting young people to greater risks.

*B)* Online paedophilia: apart from cyberbullying, online paedophilia poses the greatest potential danger to children. Setting up a fake personality (most commonly posing as a child), persons hiding behind fake profiles attempt to take advantage of the good faith and naivety of children in order to establish an intimate relationship. Following online chats, they will often invite their victims to meet in person. The threat is even more serious if children meet online friends without telling their parents and go to the meeting unaccompanied.

*C)* Pornography: online hazards include encountering pornographic content while browsing the Internet. Some surveys suggest that about four out of ten children have visited pornographic websites. Small children may easily access pornographic content through an unsolicited advertisement or by simply clicking at the wrong place. The other main source of problems is that service providers do not or do not properly warn of pages with pornographic content.

*D)* Violence, aggression, cruelty: violent, aggressive, bloody and brutal content, often encountered without any kind of warning or the placement of a *metatag,* are also harmful to children. Such sites will often publish content related to cruelty to animals, or may encourage users to commit suicide.

*E)* Addiction: online games may be particular dangerous due to their extremely addictive nature. There are an increasing number of reports of cases when children virtually get stuck in the online space, in the virtual reality of a game while withdrawing from their real lives. The use of the Internet without any bounds or limitations also results in addiction and personality distortions.

*F)* Negative consequences of social media sites: social media have become an active part of children's everyday life. Children are often faced with false images and ideas on these sites, making them believe that they are accepted norms they will follow as an example. The images transmitted by manipulated photos result in a kind of pressure to adapt in children. Often, they are not aware that a photo shared on the Internet does not entirely reflect reality. They would like to be like the person in the photo, so the continuous sharing of content, the permanent pressure to adapt and the watching of feedback involve psychological hazards in addition to the data protection risks.

*G)* Data protection abuses: data protection abuses include the breach of any data protection legislation. For example, they include phishing, a method used to delude users so they disclose their personal and financial data through misleading email messages or websites.

Identity theft is an online crime that has gained ground in recent years and is mostly associated with phishing and social media sites. It is extremely dangerous as it may have serious subsequent consequences to the victim's life. By stealing their victims' personality (i.e. all of their personal data and often even confidential information concerning their victims), the perpetrators may, for example, take out loans in their name. Since the appearance of Wi-Fi, the situation has become worse as any data are easily accessed with the required devices.

Phishing and identity theft are common phenomena. These hazards obviously

tend to target persons who share lots of information and personal data (images and videos of themselves) and set their social media page accessible to anyone.
Risky online activities also include, for example, the thoughtless posting of personal data and registering to enticing sweepstakes which may easily result in data protection incidents.

*H)* The use of online (payment) services and online games: hazards include online payment pages (usually associated with online games) without particular control over the payment process where only a few clicks are needed to make payment and use the services or enter into a contract with (financial) consequences. That hazard is typical mostly in the realm of online games.

### *2.1.2 Experiences and consequences concerning threats*

*A)* Whatever children would prefer not to see

All over the world, children start browsing the Internet and get an insight into the opportunities it offers, at an increasingly young age. The use of the Internet plays a leading role in various fields of the lives of adults and children alike. While this opportunity obviously has many advantages, one must not be blind to the hazards children are exposed to.
Supported by the European Commission's Safe Internet Programme, the international studies EU Kids Online were based on a survey conducted in nearly 25 countries. The model the research was based on assumed that the use of the Internet by children and their time spent online may entail potential opportunities as well as risks. The series of studies primarily focused on the exploration of risk factors.
The studies have shown that, on average, Hungarian children start using the Internet on their own at the age of 9. Current trends suggest that, in the future, age is going to decrease, probably stabilising around 5 or 6 years. 60 % of the generation aged 9 to 16 use the Internet on a daily basis, i.e. they are regular users, whereas around 35 % of children browse the Internet once or twice a week. Children of that generation are active members of social media sites, two-thirds of them have their own account on some social media site. It can also be detected that, in that generation, girls are overrepresented among users of social media sites.
Of the five risky activities the research focused on, 37 % of Hungarian children aged between 9 and 16 have encountered at least one while using the Internet, whereas, on average, youngsters have had some experience with 0.74 such activities. The most common online activity is meeting other people online. 26 %

of children have done that. 16 % of children have browsed content posing potential hazard to them. Browsing pornographic content, however, is insignificant. One in ten children has had such an experience. Nearly 70 % of children included in the survey reported of having been the target of cyberbullying. 30 % of children have encountered sexually explicit images or videos, whereas 29 % of children reported of experiences related to messages and activities of a sexual nature. Only 9 % of children have been to a meeting where they first met an online friend in person, and the meeting ended badly.

The research has shown that the habits of Hungarian children in terms of using the Internet are in line with international trends. Most children have access to the required infrastructure, and using the Internet has become an integral part of their everyday lives. It must be emphasised that age is the most determining factor in terms of engaging in risky activities. The older the child, the more likely he or she will encounter risky activities of that type.

Unfortunately, it is impossible to prevent children from coming across activities involving risks. Nevertheless, it is important to reduce the frequency at which such risky activities occur, and to ensure that children are capable of managing such situations.

*B)* Latency and damage

Latency and damage associated with online hazards are difficult to quantify or estimate. There are data regarding the proportion of hazards children are most likely to encounter, and it is possible to assess which hazard has a more harmful impact. For example, cyberbullying and a personal encounter ending in violence are obviously more detrimental than watching a pornographic video. The proportions, frequency and trends can be concluded and observed on the basis of international and domestic research findings.

### *2.1.3 Possibilities for protection*

*A)* The functioning of protective mechanisms

It is not possible to develop a single protective mechanism against the hazards in question as meeting strangers online must be treated differently from online games or pornographic contents, whereas data protection-related abuses are also different. It is very important that the persons concerned (children) must be properly informed in order to enable them to better respond to each situation and to determine, on their own, which situations may be dangerous or which sites may include content that might be harmful to them. Therefore, awareness-raising

and education play a very important role. These are far more important than the institutions providing ‘follow-up’ protection or assistance.
Protection as an independent, self-standing assistance, cannot be complete; there may always be gaps. Hazards and their sources keep increasing and evolving rapidly. Therefore, a significant achievement must be attained in the first line, i.e. providing information.

*B)* Relationship between protection and awareness-raising

It follows from the above that the first and most important protection must be achieved through awareness-raising. An attitude must be developed in children, enabling them to protect themselves regardless of any other institutionalised system or solution.
While certain communication patterns or solutions may be acquired, for example in the case of meeting strangers online, where certain questions may be asked during the conversation in order to help users better identify their conversation partners, that solution works with difficulties or not at all in the case of a video sharing site.

## 2.2 Potential solutions for isolating children from hazardous content and users

The method of eliminating a hazard depends on the type of hazard. The following opportunities are available, among others, in order to identify hazardous content:

- Using filtering software and the targeted blocking of certain sites;
- Placing a warning notice on the sites concerned prior to accessing harmful content;
- The acquired self-protection mechanism of children, which helps them identify, prior to accessing the site, the factors suggesting that the site contains harmful content.

Children may access harmful content notwithstanding such protective mechanisms. Parents and teachers have a great responsibility for remaining open in such situations and for being able to discuss with children what they have seen, and the impact it may have made on them, thus reducing detrimental consequences and negative conditioning.

### *2.2.1 Examples of protective mechanisms and solutions*

*A)* Protective mechanisms

- In the case of meeting strangers online: learning communication patterns and typical questions.
- Pornographic photos and videos: a warning notice prior to downloading content, requesting the verification of age. It should be noted, however, that requesting the verification of age prior to authorising access does not provide sufficient safety to children. Whoever wants to view the content concerned will obviously specify their date of birth so it shows them to be over 18 in order to be able to access the given content. In that context, it is also important to define one's objective. Whether one only wants to inform children of the type of content to be expected or to block access to such content for certain age groups.
- Sites sharing aggressive, violent, cruel or bloody images or videos: same as for pornographic content.
- Data protection abuses: information on data protection must be disseminated in advance. Each site must display proper data protection information and handle data in accordance with the applicable legislation. The competent authorities should place a lot more emphasis on disseminating information to the persons concerned and on conducting intermittent, comprehensive reviews of data management. Through disseminating information, it is possible to achieve that everyone concerned should consider it important to check their data management settings from time to time, developing an attitude of minimising or at least keeping under control the amount of personal data shared.
- Online games, online activities, narcissism, a compulsion to share information and dependence on feedback: by showing an appropriate alternative, parents, peers and teachers should provide assistance to children exposed to the risks of the boundless use of the Internet, which may result in addiction, and thus ultimately in distorting personality. Related problems and hazards must be discussed, both at school and at home, and help must be provided for children.
- Cyberbullying: the problem requires a dual approach. An awareness must be developed in children so they do not get involved in perpetrating such acts while they should also be prepared to take action against the bully, and ask for outside help in such situations. Again, that requires awareness-raising, education and proper socialisation. The dissemination of information also plays a substantial role in informing the persons concerned of the persons they can turn to if they need help in such situations.

*B)* Protective solutions

- With regard to data protection abuses, a situation should be achieved where

service providers make available their services to users with such basic data protection settings that they are used at the strictest level of the sharing of data, disclosing the least amount of personal data possible. Service providers must be required to properly inform users of each phase of the management of their data.

- In the case of online games, online activities, narcissism, a compulsion to share information and dependence on feedback, the regular presence of a school psychologist is required in every school. The mere display of consulting hours, however, is insufficient. Psychological issues must be pro-actively discussed at schools. There should be activities related to such topics, pointing out psychological factors.
- Cyberbullying: The topic should be brought up in school psychology discussions. It is very common that children lose control and grow desperate as a result of bullying, are unable to find a solution, and distinctly harmful consequences occur. The systemic integration of school mediation may be a very important tool in managing these types of situations.
- Online payments: payment and service usage solutions requiring verification, i.e. which do not result in an immediate obligation, should be called for. As these are essentially consumer protection and civil-law issues, in such cases, guarantees must be integrated into the claims enforcement processes. Unfortunately, it is difficult to stand up against fraud, particularly if a foreign element is included in the online service provision process and thus the service provider is, for example, difficult to access.

In connection with such cases, it may again be of great assistance if children have been properly informed of the occurrence of such hazards, checking, for example, the terms and conditions of the services concerned, the service provider and its contact details. Children can be taught about the important considerations they need to care for when using an online service (including games), and that they should carefully read the information displayed in pop-up windows before clicking the Continue or OK buttons. In particular, it must be pointed out to them that debit or credit card information or other payment-related data must not be disclosed without parental control.

### *2.2.2 The system of protective solutions in Hungary*

The solutions in Hungarian legislation can essentially be divided into two groups. They are preliminary solutions providing an active protective net and solutions determining legal requirements, providing a framework to such requirements and helping to fix problems (i.e. solutions responding to existing problems).

Active solutions include the use of filter software, advertisement-specific requirements, classifications of content and legal requirements related to the provision of content. Such solutions provide protection to children while browsing the Internet. Fixing solutions, on the other hand, include civil and criminal sanctions in cases when an offence is made.

The tools for the online protection of children constitute a complex system. The relevant standards and requirements include legislative requirements in various branches of law, some of which specifically include child protection rules (e.g. media legislation, advertising provisions, e-commerce law), whereas other standards, while not specific to the protection of minors, can be applied for their protection (for example, civil law privacy protection, criminal law, data protection). In connection with the legislative environment, various mechanisms and legal institutions specifically designed for the protection of children should also be mentioned (e.g. filter software, the notification/deletion procedure applied to content violating the privacy of minors), which are not strictly enforced by the government administration.

Various public institutions have been set up primarily (or specifically) in order to promote the protection of children, including in particular online child protection. The latter include the Child Protection Internet Round Table or the children's law activities of the Commissioner for Educational Rights or the Commissioner for Fundamental Rights. Through their legally not binding statements, using the power of publicity, these organisations typically attempt to call legislators' attention to deficiencies, while guiding market operators toward abidance by the law.

Family and child welfare services represent one of the most important elements of the current child protection system, whose role has continued to expand. The persons having obtained a qualification as crime prevention coordinators under the TÁMOP-5.6.2-10 project should also be mentioned as their skills and experience may also be utilised in child protection.

The following sections include a brief summary of the child protection-related activities of these organisations.

*A)* Ministry of Human Resources

In the meaning of Government Decree No 152/2014 of 6 June 2014 on the duties and competences of members of the Government, the Minister for Human Resources is responsible for the protection of children and young people, child and youth policies and education. As part of such duties, the Minister is responsible for developing the Government's policies concerning the protection of children, monitoring the enforcement of children's rights, carrying out the Government's duties related to services concerning children and young adults and determining the system of the professional supervision of fields pertaining to child and youth policies and their operation. As part of his/her responsibility for

education, the Minister prepares the legislation concerning the phase of school education the prepares students for obtaining a qualification, public education and higher education, while he/she is also in charge of developing the Government's educational policy.
Accessible at: www.kormany.hu/hu/emberi-eroforrasok-miniszteriuma

*B)* Ministry of National Development

The Minister for National Development is responsible for audiovisual policies, electronic communications and information science. As part of such duties, in addition to his/her responsibilities for preparing the applicable legislation, in the framework of his/her responsibility for information science, the Minister supervises the implementation of infocommunication infrastructure development and service policies for budgetary bodies under his/her supervision or control and for businesses in public ownership over which he/she exercises the owner's or property manager's rights or supervises the operation and development of their system of infocommunication infrastructure assets.
The National Infocommunication Strategy (2014-2020) was drawn up by the Ministry of National Development.
http://www.kormany.hu/download/a/f7/30000/NIS_v %C3 %A9gleges.pdf
Accessible at: www.kormany.hu/hu/nemzeti-fejlesztesi-miniszterium

*C)* Ministry of the Interior

Among his/her other functions, the Minister of the Interior is responsible for preventing crime and the regulation governing offences. With the exception provided for by the law, the Minister provides centralised information and telecommunication services and ensures that users are provided with information and telecommunication tools and that such tools are operated by way of the NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
Accessible at: www.kormany.hu/hu/belugyminiszterium

The National Crime Prevention Council, set up by Government Decree No 1087/2011 of 12 June 2011, operates under the auspices of the Ministry of the Interior. It is responsible for achieving and maintaining a high level of public security, controlling crime, strengthening measures in order to consistently battle the phenomena bringing about crime, occasions to commit a crime and perpetrators, developing action plans required in order to efficiently operate the new crime prevention model and to prevent crime and coordinating the implementation of such action plans. One of the most complex priorities under the strategy is child and youth protection. In particular, the hazards of the media

and the Internet constitute a distinct strategic point, including exploring and promoting best practices, holding activities and assisting the legislative process.
Accessible at: www.bunmegelozes.info

*D)* National Cyber Safety Coordination Council

The decision to set up the National Cyber Safety Coordination Council was adopted by the Government at the end of 2013 in Government Decree No [484/2013 of 17 December 2013 laying down rules for establishing and operating the National Cyber Safety Coordination Council, the Cyber Safety Forum and sector-specific cyber safety working groups and their functions and responsibilities]. The coordination activities of the Council and the implementation of its decisions are assisted by sector-specific and functional cyber safety working groups; child protection is one of the areas specifically named under the strategy. At the suggestion of the working group, the Council may issue legally non-binding recommendations on best practices related to the handling of cyberattacks and electronic information security.

*E)* Law enforcement agencies

As part of its crime reconnaissance and prevention activities, the police exercises the powers of the general criminal investigation authority, prevents and explores criminal activities and exercises the powers of the authority dealing with administrative offences.
Accessible at: www.police.hu

*F)* The public prosecutor's department

As part of the administration of justice, the prosecution enforces the administration's claim to punishment. The public prosecutor's office persecutes crime, takes action against other unlawful acts and omissions and helps prevent unlawful acts. In order to establish the conditions of indictment, the public prosecutor orders investigations, supervises independent investigation by the criminal investigation authority or, in cases specified in the act on criminal procedure, conducts an investigation. The public prosecutor ensures that the rights of participants to the criminal procedure are enforced during an investigation.
Accessible at: www.ugyeszseg.hu

*G)* Courts of Justice

Courts are responsible for the dispensing of justice. Children may get in touch with the dispensing of justice in various 'capacities', i.e. as witnesses (in certain proceedings), offended parties or even as perpetrators. The system of child-centred administration of justice ensures that children's rights are respected and efficiently enforced at the highest possible level, while enforcing children's interests as a top priority in any case in which children are involved or affected.
Accessible at: www.birosag.hu

*H)* National Authority for Data Protection and Freedom of Information

The NAIH is responsible for overseeing the enforcement of constitutional rights concerning the protection of personal data (data protection), and the publicity of data of general interest (freedom of information) and receives citizens' complaints. Where there is a suspicion of a serious violation of data protection rights, it may start an administrative procedure, including the ordering of the blocking or destruction of data that has been managed unlawfully, ban the management of data, and impose a data protection fine up to an amount of HUF 20 million. Moreover, it is also responsible for the dissemination of information concerning information rights.
Accessible at: www.naih.hu

*I)* National Media and Infocommunications Authority

The NMHH's Magic Valley Media Comprehension Education Centre (Budapest, Hűvösvölgyi út 95.) opened on 15 May 2014. Since the opening, more than 12,000 children, about 2,000 of them disadvantaged children or children with multiple disadvantages, have taken part in thematic activities, in addition to about eight hundred teachers. The centre was set up in order to teach children how to use the media more consciously in order to avoid their hazards. Various professional activities carried out at the centre were implemented under the TÁMOP-3.1.14-12-2013-0001 project entitled 'Conscious future media consumers – propagating media education and media consciousness'. Moreover, the Authority has also operated an Internet Hotline service in order to enable unlawful online content and content harmful for minors to be reported.
Accessible at: www.nmhh.hu, www.buvosvolgy.hu

*J)* Media Council of the National Media and Infocommunications Authority

The Media Council exercises administrative control over the enforcement of the

provisions of media legislation concerning the protection of children and minors (Sections 9 to 11 of Act CLXXXV of 2010 on media services and mass communication, and Section 19 of Act CIV of 2010 on the freedom of the press and the basic rules of media content). In connection with such powers, it issues recommendations concerning the ratings provided for the protection of minors and the requirements of an efficient technical solution to ensure that certain programmes are only accessible to viewers or listeners over eighteen years of age. In addition to specific (administrative) powers, it takes a pro-active role in the development of media education and media consciousness in Hungary. As part of that activity, it coordinates the activities of other government bodies related to media education and assists the Government in drawing up a relevant periodic report to be submitted to the European Union (Section 132*(k)* of Act CLXXXV of 2010).
Accessible at: www.mediatanacs.hu

*K)* Child Protection Internet Round Table

The Round Table is consultative and review committee of the President of the NMHH, consisting of twenty-one members, the setting up of which was provided for in the relevant provisions of Act CVIII of 2001 on certain questions relating to e-commerce services and information society services (Section 4/A to D), taking effect on 1 January 2014. The Round Table is entitled to issue non-binding recommendations and statements in order to promote compliance by media content providers, e-commerce service providers and electronic communication service providers; it is also responsible for initiating measures to raise the level of media consciousness of minors and their parents. Based on the notifications received, the body is entitled to review individual cases and to issue a non-binding recommendation or statement on the basis of the generalised conclusions drawn from such cases.
Accessible at: gyermekbarat.nmhh.hu/tart/index/1624/Gyermekvedelmi_Internetkerekasztal

*L)* Office of the Commissioner for Fundamental Rights

During his activities, the Commissioner for Fundamental Rights pays particular attention to the protection of children's rights, in particular by conducting procedures ex officio. The Commissioner for Fundamental Rights may, with a view to eliminating abuses related to fundamental rights through the activity of authorities, start a procedure ex officio. An ex officio procedure may focus on the investigation of an abuse affecting a larger group of natural persons that cannot be accurately defined or the comprehensive review of the enforcement of a

fundamental right (Section 18(4) of Act CXI of 2011 on the commissioner for fundamental rights).
Accessible at: www.ajbh.hu

*M)* Office of the Commissioner for Educational Rights

Decree No 40/1999 of 8 October 1999 of the Minister for Education on the duties of the Office of the Commissioner for Educational Rights and laying down rules for its operation provides for the establishment of the Commissioner for Educational Rights. Via the office headed by him, the Commissioner is responsible for promoting the enforcement of citizens' rights related to education, which are vested in children, pupils, students, researchers, teachers, parents and their communities (Section 1(1)). The Commissioner may proceed in connection with decisions or actions in individual cases or the failure to make a decision (or to take action), breaching certain rights vested in children, pupils, parents, teachers, students, researchers or educators or directly threatening with such breach of rights. The same level of protection is granted to the statutory rights vested in communities of children, pupils, parents, teachers, students, researchers and educators (Section 3).
Accessible at: www.oktbiztos.hu

*N)* Child protection institutions

In the meaning of Act LXXIX of 2009 ('Gyvt.'), the protection of children's rights is the duty of all natural and legal persons engaged in educating or supplying children, providing their legal representation or administering their affairs (Section 11(1)). The legislation attempts to ensure that children's rights are enforced through a number of institutions, including child protection guardians and representatives of children's rights, children's residential institutions, family and child welfare centres, children's homes and correctional institutions.

*O)* NGOs (interest organisations)

A wide range of NGOs have specialised in the field of child protection, many of them specifically focusing on activities, assistance and education associated with the relationship between children and the media/Internet. Without aiming to provide an exhaustive list, these NGOs include the Nemzetközi Gyermekmentő Szolgálat (International Children's Safety Service), the Kék Vonal Gyermekkrízis Alapítvány, Eszter Alapítvány, the Hintalovon Alapítvány, the Nagycsaládosok Országos Egyesülete, the Médiaunió Alapítvány, the Gyermekmédia Egyesület, the Médiasmart Közhasznú Nonprofit Kft., the Egyszervolt Alapítvány, the

Országos Gyermekvédő Liga, the Digitális Tudás Akadémia and the UNICEF Hungarian National Committee Foundation.
Accessible at: www.gyermekmento.hu, www.kek-vonal.hu, www.eszteralapitvany.hu, www.hintalovon.hu, www.noe.hu, www.mediaunio.hu, www.gyermekmedia.eu, www.mediatudor.hu, www.egyszervolt.hu, www.ogyl.hu, http://digipedia.hu, www.unicef.hu

## 2.3 Filtering software and the marking of online content

### *2.3.1 Applicable legislation*

*A)* Requirements concerning the filtering software

Act C of 2003 on electronic communications provides that, on their websites, providers of Internet access shall make available to the public, free of charge, (an easy to install and use) filtering software (in Hungarian) enabling the protection of minors (Section 149/A). In connection with the above, the general terms and conditions of the communication service provider providing services to subscribers shall include information concerning the accessibility and use of filtering software and other services used for similar purposes (Section 131(1)*(l)*). Moreover, the service provider providing access to the Internet shall collate public information on the accessibility and use of filtering software and other services used for similar purposes, publish such information on its website and notify subscribers of its publication and accessibility on a quarterly basis (Section 144(2a)).
Public libraries and public education institutions shall provide a Hungarian-language software enabling the protection of minors, easy to install and use, on their computers with an Internet access, accessible to minors or students in order to protect the mental, physical and intellectual development of minors (Act CXL of 1997 on museum institutions, the operation of public libraries and public education, Section 55(1a); Section 9(11) of the act on public education).

*B)* Classification of online content

In addition to the above, online content other than media content under the media legislation, which may cause serious harm to the healthy development of minors, shall only be published by service providers if it is accompanied by the relevant warning. Moreover, through such obligation to rate content, the applicable statutory requirements also ensure that online content that is harmful

to the development of minors can be identified and thus filtered by the filtering software referred to above (Section 4/A(1) of Act CVIII of 2001).

The requirements set out by the law are currently only met by the software of a single company and even that is not suitable for all operating systems. In addition to that problem, it should also be noted that since the provider of the software is not required to provide the product free of charge, it may charge a fee for its use at any time, which may render compliance with the statutory requirements rather difficult. Based on individual feedback concerning filtering software, it can be concluded that the filtering software may not be used for every purpose, they do not provide complete safety, and are unable to filter all harmful content specified. Further problems include that parents may not be familiar with the way the filtering software should be properly set up or the competent persons to turn to for help. Moreover, it can be concluded that children are often more knowledgeable in using the software than their parents and are thus able to disable it so it can only achieve its actual purpose with difficulties.

Compliance with the requirements referred to above is monitored by the Child Protection Internet Round Table, set up as the consulting body of the NMHH's President, as a body promoting and supporting the efficient enforcement of legislative requirements aiming to protect minors and increase the level of media consciousness in connection with information accessible by way of e-commerce and e-communication services and media content published by media content providers. While the Round Table has no administrative powers, it may issue non-binding recommendations and statements in order to promote compliance by service providers (Section 4/D(1) of Act CVIII of 2001).

### *2.3.2 Supporting the development of filtering software*

Act C of 2003 provides that the NMHH may publish tenders in order to provide financial support to providers of Internet access so they can comply with their obligation to ensure on their websites free accessibility and usability of the filtering software, provided that:

- It complies with the requirements set out in recommendations by the Child Protection Internet Round Table;
- In addition to retail customers and private individual subscribers, the filtering software is suitable to be used by public libraries and public education institutions whose statutory duties include the provision of a filtering software for the use of the Internet by minor children using the public services provided by them;
- Providers of access to the Internet agree to provide access, directly or in cooperation with other service providers, to the filtering software for the

institutions referred to above, free of charge.

Conducting the tender procedure falls within the administrative competence of the NMHH's President. The detailed rules for the tender procedure are laid down by the President in NMHH Decree No 4/2014 of 18 June 2014 laying down rules for the tender to provide financial support to complying with the obligation related to the provision of child protection filtering software.

### *2.3.3 Experiences of the practical application of filtering software*

According to the Report No AJB-479/2016 of the Commissioner for Fundamental Rights on the situation of media comprehension education in Hungary, which refers to the report of the President of the International Children's Safety Service, problems concerning filtering software include the lack of a well-known and sufficiently transparent model or recommendation educational institutions could use; further controversial issues include the distribution and maintenance of software-related costs and the keywords the software should filter for. In most cases, schools tend to respond by drastically restricting children's access to the Internet.

### *2.3.4 Recommendation by the Child Protection Internet Round Table*

It should be noted that, based on its mandate under Section 149/A(2) of Act C of 2003, the Round Table has adopted a recommendation concerning the warning signals and filtering software applicable in the case of content and services harmful to minors. With regard to warning signals, the recommendation proposes the following solutions:

- The *metatag* in the source code should clearly indicate that the relevant content is harmful to minors (e.g. *age*=18);
- Prior to displaying the page from which the relevant content is accessible or in the relevant table of contents or in a different section (e.g. in the title bar of the URL containing the hyperlink to the content), the content provider should refer to the content that is harmful to minors by prominent optical identification;
- Prior to displaying the content, the content provider should verify the user's age and his or her authorisation to view the content (e.g. by displaying a question to verify the viewer's age: *'Are you 18 or older?* Yes – *No'*). If, based on the verification of age, the user is unauthorised to view the content, he or she should not be able to download or access the content;
- Simultaneously with the verification of age, at the same place, prominently displayed, users should be warned of the hazards to minors, for example by displaying the following notice: *'Warning! The following content contains elements that are harmful to minors. If you wish to ensure that similar content*

*should only be accessible to minors in your neighbourhood by entering an individual code, please use a content filter software. To download the filtering software and for further information, please click here.'*

In connection with the requirements concerning child protection filtering software, the recommendation sets out proposals in the following areas:

- The availability of filtering software solutions and the scope of their application;
- Installation of filtering software solutions and their settings and options;
- The method of restricting the accessibility of online content;
- Monitoring the online activities of minors; alerts.

### *2.3.5 Review of compliance with the recommendation*

Based on the results of a review of about 120 websites containing content harmful to minors, conducted at the end of 2014 and the beginning of 2015, at its meeting of 17 June 2015, the Child Protection Internet Round Table decided to call upon the content providers concerned in writing to comply with the applicable statutory provisions and the filtering software recommendation of the Round Table.

*A)* Findings concerning content providers that had applied some kind of a warning: the review covered 85 content providers that had used some kind of warning during the initial review, prior to displaying content harmful to minors. During the initial review and the verification review, the availability and suitability of the following warning elements were verified:

- The *metatag* in the source file, which enables filtering software to easily identify content that is harmful to minors;
- Notice warning of content harmful to minors and the verification of age;
- Warning of the importance of applying a filtering software and the availability of a hyperlink to the filtering software.

The review was closed with the following results:

- At the initial review, a mere 8 % of service providers used a *metatag* prior to displaying content harmful to minors. As a result of the letter, as service providers began to use metatags on a number of websites, their ratio increased to 26 %.
- With regard to the availability of warning signals on the websites, no significant change occurred. It could be concluded, however, that warning signals were acceptable on about 75 % of the websites concerned. While this does not mean that they were fully in compliance with the recommendation, at least no content harmful to minors was displayed prior to the age verification.
- At the initial review, a reference to filtering software was available on a mere

22 % of all websites. That ratio has increased slightly. Currently, there is a reference to the filtering software on 34 % of the websites.

Following the second review, it remained a problem that the warning signals employed by service providers were extremely diverse, non-consistent and ambiguous, making it difficult for parents to acknowledge hazards related to harmful content and to realise the need to use a filtering software.

*B)* Findings concerning content providers previously not employing any kind of warning signals: considering that the about 30 content providers falling into that group had previously abstained from using any kind of warning signals, they were sent the same letter in connection with compliance with the rules applicable to content harmful to minors. Unfortunately, as far as they are concerned, the results turned out to be a lot worse than in the case of service providers that had used some kind of warning before:

- It can be concluded that approximately one in seven service providers has complied with the call. Compared to zero, 16 % were now using a *metatag* or a warning notice prior to displaying content harmful to minors;
- About 13 % of the websites included a warning to the importance of using a filtering software as well as a hyperlink to such software.

## 2.4 Protection of children's rights under the current legal system

### *2.4.1 International legislative background*

According to Article 1 of the United Nations Convention on the Rights of the Child, signed in New York on 20 November 1989, for the purposes of the Convention, a child means every human being below the age of eighteen years, who is thus entitled to increased protection. Article 19 of the Convention prohibits any form of violence against children.

### *2.4.2 Constitutional background*

In the meaning of Section XVI(1) of the Fundamental Law of Hungary, every child shall have the right to the protection and care necessary for his or her proper physical, mental and moral development.

### *2.4.3 Civil law*

Addressing the protection of privacy, the Second Volume of the Civil Code sets out general provisions concerning the protection of personality rights and human dignity

(Section 2:42(1): ‘Everyone is entitled to freely practice his personality rights, including in particular the right to privacy and family life, to his home, to communication with others in any manner whatsoever and through whatever means and to having his reputation respected within the framework of the law and within the rights of others, and to not be impeded in exercising such right by others.’)
In particular, the Civil Code provides for the protection of privacy, honour, reputation, personal data, images and voice recordings (Section 2:43: ‘The following, in particular, shall be construed as violation of personality rights: any violation of life, bodily integrity or health; any violation of personal liberty or privacy, including trespassing; discrimination; any breach of integrity, defamation; any violation of the right to protection of privacy and personal data; any violation of the right to a name; and any breach of the right to facial likeness and recorded voice.’) Where such institutions are breached, the instruments of civil law may be used in order to take action against such breach, applying appropriate punitive sanctions (compensation, damages, obligation to discontinue the unlawful activity etc.) (Sections 2:51 to 2:53).
In addition to real life, personality rights may also be breached online. Children may be among the injured parties.
Online hazards may give rise to grievances, which must be construed and remedied within the framework of the privacy protection sections of civil law.
In order to enable children to protect their personality, they and their parents (guardians) must be familiar with the system of protection under the civil law, the method and the opportunities of enforcing their rights before the court and, first and foremost, their civic rights. Therefore, disseminating information concerning rights is the first step that must precede protective action. It must be incorporated into school education.
In that context, it should be noted that a special statutory option exists, which enables the simpler and more efficient removal of online content that violates the privacy of minors, thus preceding and complementing the rules of procedure under civil and criminal law (Section 13(13) to (15) of Act CVIII of 2001).

### *2.4.4 Criminal law and the law of petty offences*

A number of offences are assessed within the framework of criminal law. As far as online activities are concerned, the following facts of case under criminal law should be noted:

- child pornography
  (Section 204 of Act C of 2012 on the Criminal Code: any person who takes, offers, hands over, obtains, distributes, trades in, makes available or stores pornographic images of a person under eighteen years of age shall be guilty of a crime);

- misuse of personal data
  (Section 219 of Act C of 2012: where the personal data of a citizen (including his name, phone number, home address and photograph) are published without the consent or approval of the person concerned);
- harassment
  (Section 222 of Act C of 2012: any person who intends to regularly communicate with another person, against the will of the latter, by mobile phone, over the Internet, on social media pages or in person, thus harassing such other person);
- invasion of privacy
  (Section 223 of Act C of 2012: any person who reveals any private secret he has obtained in a professional or official capacity without due cause, thus causing a material breach of another person's interests);
- mail fraud
  (Section 224 of Act C of 2012: any person who destroys a sealed consignment addressed to another person, or opens or obtains such consignment for the purpose of gaining knowledge of the contents thereof, or conveys such to an unauthorized person for this purpose, or captures correspondence forwarded by means of electronic communication networks to another person);
- defamation
  (Section 226 of Act C of 2012: any person who engages in the written or oral publication of anything that is injurious to the good name or reputation of another person, or uses an expression directly referring to such a fact);
- producing a fake image or audio or video recording capable of damaging another person's reputation
  (Section 226/A of Act C of 2012: any person who produces a fake, forged or untruthful image or audio or video recording in order to damage the reputation of another person);
- publishing a fake image or audio or video recording liable to damage another person's reputation
  (Section 226/B of Act C of 2012: any person who publishes a fake, forged or untruthful image or audio or video recording in order to damage the reputation of another person);
- slander
  (Section 227 of Act C of 2012: any person who uses an expression liable to damage another person's reputation in connection with the performance of his duties or his public office or activities in the public interest or before the public at large or commits a similar act);
- illicit access to data
  (Section 422 of Act C of 2012: any person who, in order to gaining unauthorised access to personal data, private secrets, trade secrets or

business secrets:

- covertly searches the home or other property, or the confines attached to such, of another person,
- monitors or records the events taking place in the home or other property, or the confines attached to such, of another person, by technical means,
- opens or obtains the sealed consignment containing communication which belongs to another, and records such by technical means,
- captures correspondence forwarded by means of electronic communication networks - including information systems - to another person and records the contents of such by technical means);

- breach of an information system or data
  (Section 423 of Act C of 2012: any person who gains unauthorized entry to an information system by compromising or defrauding the integrity of the technical means designed to protect the information system, or overrides or infringes his user privileges);
- circumventing the protection of information systems
  (Section 424 of Act C of 2012: any person who creates, transfers, supplies, obtains or places on the market passwords or computer programs or offers his economic, technical or organizational skills concerning passwords or computer programs to another person).

Apart from Act C of 2012, the act on petty offences also provides for online offences committed against minors

- dangerous threat
  (Section 173 of Act II of 2012 (‘Szabs. tv.’): any person who seriously threatens another person in order to intimidate such person, threatening to disclose to the general public a fact concerning the person threatened or his or her relative, liable to damage such their reputation).

For statistical data related to the occurrence of each type of crime, see Annex 1.

### *2.4.5 Media Law*

Act CLXXXV of 2010 provides that providers of on-demand media services or broadcasters distributing the services of the former shall employ an efficient technical solution in order to ensure that programmes liable to detrimentally affect the development of persons under eighteen years of age should not be accessible to minors (moreover, they shall provide the appropriate ratings to programmes under the rating categories V and VI). As far as efficient technical solutions are concerned, exercising its mandate under Act CLXXXV of 2010, the Media Council published a recommendation and, relying on its experiences, has regularly reviewed the

proposals and guidelines set out in the recommendation (Section 11(1) to (3) of Act CLXXXV of 2010). Among other things, the recommendation addresses parental lock solutions applied in the case of on-demand media services provided under digital broadcasting services (Article IV. 4 of the recommendation) and efficient technical solutions provided by providers of mobile communications services or applied in the case of linear and on-demand media services accessible over wired and mobile Internet access (Articles V and VI of the recommendation).

Under the law, media content that is seriously harmful to minors shall not be published in on-demand media services unless it is ensured that it cannot be accessed by minors under ordinary circumstances. Similarly, the content's accessibility by minors must also be restricted in printed publications, or it may not be published unless with a warning signal including information concerning the potential hazard (Section 19(2) and (3) of Act CIV of 2010). In the meaning of Act CIV of 2010, such content includes media content liable to harmfully influence the mental, psychological, moral or physical development of minors, which includes pornography or unjustified violence.

Compliance with such statutory requirements is currently monitored by the media co-regulatory organisations having entered into an administrative contract with the Media Council.

Additional child protection provisions with a view to protecting minors (and informing parents) include that the rating of each programme shall be prominently indicated in the information published in printed publications including the media provider's programme and on the media provider's website and teletext, if any (Section 10(7) of Act CLXXXV of 2010).

### *2.4.6 Data protection*

In Hungary, the legislative framework of data protection is set out in the Information Act ('Infotv.'). Data protection sets out no special provisions or extra protection for children. An age-related distinction, different from legislation under the civil law (minors) and criminal law (juveniles), is made by setting out different provisions regarding persons under and over 16 years of age. Under Section 6(3) of Act CXII of 2011 on the right to informational self-determination and freedom of information, 'a legal statement including the consent of a minor of 16 years of age or older shall be valid without the consent or subsequent approval of his guardian' (as opposed to persons between 14 and 16 years of age, where a joint decision is required).

In other words, from a data protection perspective, the age of 16 is the watershed in the online world. No parental consent is required in order to validly approve the management of or disclose one's data, which, however, may have civil-law consequences, e.g. it may result in the conclusion of a contract, whose validity in turn

requires further action, which may easily generate further hazards.
Information on data protection is of major importance for children and young people as a number of hazards and problems may be evaded or prevented through the conscious use of tools and the conscious and safe use of the Internet, closely linked to data protection issues.
The principle of ethical and purpose-specific data management is another very important obligation service providers are responsible for.

### *2.4.7 The act on certain issues concerning e-commerce services and services related to the information society*

Act CVIII of 2001 was passed at the end of 2001 in accordance with the e-Commerce Directive and the agreements entered into by collecting bodies. The law provides for the protection of minors, setting out that any information published by a service provider, other than media content, which may cause serious harm to the intellectual, mental, moral or physical development of minors in particular through the direct and natural portrayal of violence and sexuality, shall not be published unless with a warning signal notifying on potential hazards to minors, to be published on the page containing such information, prior to displaying the information, and with identifiers referring to the relevant content category in the source code of the relevant page.
Moreover, the law provides for the liability of the service provider and the intermediary service provider and the lawfulness of information published by such service providers. The service provider shall be relieved of its liability if it was unaware of the violation or the circumstance indicating the violation, acted as reasonably expected in such situations and carries out the statutory notification and removal processes.

### *2.4.8 Act on consumer protection*

Among the special provisions intended to protect children and minors, the consumer protection law provides that, in the case of distributing software games liable to detrimentally affect the physical, intellectual, mental or moral development of persons under eighteen years of age, in particular through the direct and natural portrayal of violence and sexuality, the software game vendor shall prominently display the notice *'Suitable for persons 18+'* on the packaging of the software game. If the software game is distributed online, such obligation must be complied with as appropriate, prior to users accessing the game.
The software game vendor is required to comply with the obligation referred to above if it has not joined the Pan European Game Information (PEGI) and implemented the PEGI's rating requirements. Where the vendor fails to comply with the obligation

referred to in the previous paragraph, when putting the software on the market, distributors of software game shall display the notice defined above (Section 16/A(5) and (6) of Act CLV of 1997 on consumer protection).

### *2.4.9 Act on gambling*

Under Act XXXIV of 1991 on the organisation of games of chance, with the exception of sweepstakes organised on a non-continuous basis, no person under 18 years of age shall take part in games of chance. While providing players with the opportunity to participate in a game, the gambling organiser shall display a prominent notice on persons under 18 being banned from the game and shall, in accordance with the principle of responsible organisation of gambling, carry out the measures to enforce such ban (Section 1(5b)).
Among other information, on its online gambling website, regarding the gambling service provided by it, the organiser shall display, in Hungarian, the warning that persons under 18 are banned from the game (Section 29/I(1)*(e)*).

## 2.5 International best practices

The AVMS Directive, which serves as the basis for Hungarian media legislation, provides that 'on-demand audiovisual media services which might seriously impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see such on-demand audiovisual media services' (Article 12). That requirement is less stringent than the one applicable to 'traditional' (television and radio) media services as no such content is allowed to be published in the latter.
Member States have implemented a range of solutions for the protection of children in terms of on-demand media services. Such requirements include rating systems that are specific to on-demand services (e.g. Italy). In other countries, an attempt has been made to ensure protection by providing different programme catalogues to children and adults (e.g. in France and Spain). Technical solutions include the use of PIN codes (Italy), while common protection tools include the use of 'watersheds', making certain harmful content accessible in late nights hours (e.g. Finland, France, Germany, Sweden).
The Internet Watch Foundation (IWF) was set up in the United Kingdom in 1996. The Foundation is a non-profit organisation supported by the European Commission. Its objectives include battling unlawful online content, and minimising the availability of such content on the Internet. Special emphasis is placed on pornographic content involving children and online sexual abuses committed against children. In close cooperation with the government, the law enforcement agencies and service

providers, they are attempting to control online violations, protecting children against online hazards by developing a complex system. As a specific feature of the organisation, in addition to these activities, it operates a hotline service to enable citizens to report online violations. Such hotline service is not unknown in Hungary either: the NMHH-operated Internet Hotline service and Biztonságosinternet.hu, whose operation is supported by the Safer Internet Programme, carry out similar activities.

The model employed by the IWF could serve as an international best practice and an example for Hungary. Here, a central organisation could coordinate activities related to online child protection, take efficient action against online hazards to children.

A special solution for online child protection is used in the UK where, based on an agreement with the government, Internet access providers have voluntarily committed to restrict pornographic content as a default setting since the end of 2013 (including Wi-Fi services and all devices); no legislation has been adopted in the subject. Based on the scheme, all newcomers to the service are provided with a Safe Internet Service for Children (through network-level filtering measures). The safe settings are removed at request. Such idea goes back a long way in the UK. Since 2002, the IWF has published a blacklist on content that is potentially harmful to minors, enabling service providers to block content on a voluntary basis. The list classifies content to be banned according to the following major categories: drugs, alcohol, dating sites, pornographic content, and content that encourages suicide. The initiative has been embraced by major service providers which have also set up websites on the safe use of the Internet and awareness-raising and have provided their customers with a filtering software free of charge. Network-level filtering measures have also been introduced at schools and libraries. By the end of 2016, they expect all schools to have joined the initiative. The network-level filtering measures can only be disabled by adults.

The most common criticism concerning the functioning of the system has been that filtering has also included sites set up in order to help children who have become victims of online harassment and to educate and raise awareness of the public concerning such issues.

In the United States, the Children’s Online Privacy Protection Act (COPPA), passed in 1998 (focusing on the online protection of the personal data of minors under 13 years of age) deals specifically with data protection considerations. The legislation imposes additional obligations on the data managers of websites providing e-commercial or online services to children. Compliance with such obligations is monitored by the Federal Trade Commission in procedures instituted ex officio or based on specific complaints. The law applies to websites collecting data from minors while providing such services. In addition to websites specifically targeting children (e.g. toy webshops or the website of an animated cartoon, offering online merchandise), they include websites providing e-commercial or online services to the

general public if such services are accessible to minors, and the site operator is aware that its services are used by minors.

## 2.6 Expanding the range of safe content intended for children

In addition to protecting children from harmful content, it may be at least as important to support the production of online content specifically targeting children and corresponding to their maturity and level of intellectual development.

In addition to public institutions, NGOs have played an active role in that field. The Commission Communication on the European Strategy for a Better Internet for Children also treats encouraging the production of quality online content for children and minors as a priority, which benefits the single digital market while serving children's interests. Creative and playful content helps to develop the skills relevant to the conscious use of the Internet.

NGOs produce online content for minors relying on their own resources and by raising donations for this purpose.

In the government sector, grants are available grants are available under the Hungarian Media Sponsorship programme, a system of competitions operated by the NMHH's Media Council, for online acts available on on-demand media service platforms (NEUMANNJANOS competition). With regard to the limitations under media legislation, the system of grants is fixed to a certain extent, i.e. only 'programme items' meeting the statutory definition can be supported by the Media Council, which means that games and websites specifically designed for children are currently not eligible for full support.

The Media Council also supports the production of animated cartoons (MACSKÁSSYGYULA competition). The award procedures in recent years have had the following results:

- 2012: 16 successful applications (grants amounting to HUF 122.9 M);
- 2013: 24 successful applications (grants amounting to HUF 206.4 M);
- 2014: 23 successful applications (grants amounting to HUF 182.6 M);
- 2015: 19 successful applications (grants amounting to HUF 178.2 M).

Moreover, under a separate procedure, the Authority has also supported the production of further episodes of previously co-financed animated cartoon series geared for children, young people and families (DARGAYATTILA competition). During the two 'complete' years of the competition, first announced in 2014, the following blanket sums were awarded by the Media Council to applicants:

- 2014: 6 successful applications (grants amounting to HUF 215.2 M);
- 2015: 14 successful applications (grants amounting to HUF 244.9 M).

With regard to the two competition procedures, however, it should be noted that while the eligibility requirements under the NEUMANNJANOS competition include online

availability, the DARGAYATTILA and MACSKÁSSYGYULA competitions focus on content designed for children. However, meeting both requirements at the same time is currently not uniformly required in either case.
In addition to the above, the expansion of online content offered for children is promoted by the website of the thematic child and youth channel of public media (m2), where each act can be viewed live or at any time after they are first aired.

## 2.7 Equal opportunities

In connection with any tool or measure intended to – promote the value-generating use of the Internet or to better enforce the rules designed to protect children –, the criteria related to children with disabilities and special educational needs should also be taken into consideration. Efforts must be made in order to achieve that media education and training and the tools and efficient technical solutions promoting the use of the Internet are integrated, accessible and disabled-friendly and that the people concerned are aware of the availability of such opportunities.

## 3. Applying sanctions and providing help

Existing and future measures in order to raise awareness and create a safe online environment are intended to eliminate any risks or hazards to children. In practice, however, complete protection and safety must inevitably be achieved. Therefore, situations in which children are faced with unexpected negative and harmful effects during or after an Internet session must also be examined.

Such situations must be thoroughly examined from two points of view, i.e. the victimised child must be given help and assistance, the online violation (of rights) suffered should preferably be eliminated as fast and as efficiently as possible and, depending on the weight of the injury, appropriate punitive sanction(s) must be imposed on the perpetrators. As injuries may be of different types and nature, their consequences and thus the relevant legislation (criminal law, civil law, media legislation etc.) and the potential form of regulation (rules of law, self-regulation, codes of conduct etc.) are also rather diverse.

As with increasing media consciousness and achieving the safe use of Internet, the level of awareness of the persons concerned must be raised while remedying injurious situations. For the victims, it should mean, first and foremost, awareness of the opportunities of assistance and other appropriate forums available, whereas for potential perpetrators, awareness of the potential adverse consequences of their acts.

It must be noted that the National Information Strategy (2014-2020) specific addresses the issues of child protection, with regard to which it also provided for the existing risks to safety and the implementation of a comprehensive information programme concerning the methods intended to minimise such risks. Its avowed objectives included the creation of a proper legislative background for managing such risks, while expressing its preference that the hotline for child protection and against cybercrime should become widely familiar to the public (specifying 2016 as the target date to achieve such goals).

## 3.1 The organisations concerned

It is necessary to list the institutions and organisations potentially involved in imposing sanctions and remedying grievances if a grievance has occurred.
Following a grievance, government bodies are primarily responsible for carrying out the duties relegated into their competence by the law. In that context, the law enforcement authorities (police, the public prosecutor's office and courts of law) taking action in the case of the most serious contraventions, i.e. crimes, must be mentioned in the first place. Of institutions functioning within the organisational system of public administration with considerable differences in terms of their authorisations, investigation criteria and scope of applying sanctions, mention must be made of the NMHH, the Media Council, the Child Protection Internet Round Table, the NAIH and the AJBH.
NGOs also play an outstanding role in the field, focusing primarily on providing assistance to victims rather than the calling perpetrators to account (the Kék Vonal Gyermekkrízis Alapítvány is one of these organisations).
Finally, mention must be made of organisations assuming some of the functions of government agencies while essentially qualifying as NGOs, which receive government grants for their efforts in order to encourage compliance within their respective market segments while holding a mandate similar to government agencies (e.g. co-regulatory bodies in media administration).
As can be seen, a number of different types of organisations carry out activities in that field. However, their activities are rather fragmented as they operate in complete detachment. Detachment is an essential characteristic of their efforts as each organisation carries out its duties 'independently', acting in their respective competences. The idea of establishing a system of cooperation or a common forum would definitely be useful as it could help the parties concerned in sharing their experiences in order that problems can be resolved more easily and efficiently.
The legislator has attempted to achieve such cooperation by setting up (the Child Protection Working Group of) the National Cyber Safety Coordination Council or the Child Protection Internet Round Table. Members of these organisations include persons delegated by government agencies, child protection organisations and the interest bodies of the business sector. The JOG-OK working group has been a similar initiative, started by the Commissioner for Fundamental Rights.

## 3.2 How to realise that one's rights have been breached

It is necessary to call children's (both potential victims' and perpetrators') attention to acts that are against the law and that may thus have (serious) legal consequences

under certain conditions. Such legal awareness is the primary starting point of the situation where an aggrieved minor is able to realise that he or she has become the victim of an unlawful act (or there is a direct risk or opportunity for becoming a victim) and to take action in order to resort to tools and measures suitable for remedying the grievance.

If a grievance has occurred, it is indispensable to identify and resort to the appropriate tool to protect and restore one's rights.

Moreover, children must be made aware of specific actions that may be conducive to calling the perpetrator to account once a grievance has occurred. In that context, children should be aware of the following:

- How to make an electronic copy of the photograph, video, text message etc. that has given rise to the grievance (saving);
- Awareness of other IT solutions (notification settings in case information regarding the person concerned should appear on the Internet);
- Useful information in order to request a legal or other (e.g. removal) procedure;
- Awareness of potential action if a grievance is committed against another person (known to the observer).

## 3.3 Imposition of sanctions under media legislation

### *3.3.1 Procedures by co-regulatory bodies*

The applicable legislative environment vests the Media Council with supervisory powers with regard to specific types of online content and the power to impose sanctions if a breach of law is detected. As far as the online space is concerned, the scope of legislation applies to online publications and on-demand online media services. It must be noted, however, that, in terms of professional experience and efficiency, the applicable media legislation provides an opportunity for increasing the role of self-regulatory bodies in this respect. Consequently, self-regulatory and co-regulatory bodies are primarily responsible and empowered to enforce the rules concerning the protection of minors and to impose the potential legal consequences.

Based on contracts concluded with the Media Council, the following co-regulatory bodies are currently vested with supervisory powers over certain child protection rules, i.e. time limitations and airing restrictions and advertising rules designed to protect minors in connection with media content included in on-demand media services and online publications (Section 19 of Act CIV of 2010 and Sections 11 and 24 of Act CLXXXV of 2010):

- Association of Hungarian Content Providers;
- Association of Hungarian Newspaper Publishers;

- Association of Hungarian Electronic Broadcasters;
- Self-Regulatory Advertising Body.

In the case of a breach of law, the co-regulatory body may adopt a decision including an obligation. Its most important power is publicity (in addition to publicity, as a 'sanction', it may oblige the service provider concerned to stop the activity breaching the rules, to restore the original conditions and to give gratification, and may establish that the system of co-regulation no longer applies to the service provider, and that the latter has become subject to administrative proceedings).

According to experiences concerning the operation of the system of co-regulation in Hungary, very few citizen complaints are received by the organisations and a very small fraction of such complaints concerns child protection issues. In a system that has been operating for almost five years, merely three complaints have been received in connection with provisions concerning the protection of minors. One noteworthy decision has been made in these cases.

### *3.3.2 Proceedings by the Media Council*

The powers vested in the Media Council to conduct a wide range of administrative supervisory procedures include the right to enforce the provisions intended to provide protection to minors. Such powers, however, only concern a small part of online content.

Where the Media Council acts vis-à-vis on-demand online media services or online publications (as the service provider concerned is not subject to co-regulation), during the administrative proceedings, it enforces the provisions for the protection of minors, including the impositions of punitive sanctions.

In the case of on-demand media services, it may include a fine, an obligation to publish a communication, a suspension of eligibility and exclusion from MTVA competitions. The first two sanctions may be applied to publications. A more severe legal consequence is if the service provider fails to comply with its obligations under a binding and enforceable resolution, the Media Council may oblige intermediary service provider to suspend broadcasting the service concerned.

According to experiences to date, the Media Council has instituted very few 'direct' proceedings vis-à-vis media services or publications.

At the same time, the Authority has been monitoring the enforcement of the provisions of Section 10(7) of Act CLXXXV of 2010. So far, it has established infringements in 23 cases, according to the following annual breakdown:

- 2012: 7 cases;
- 2013: 15 cases;
- 2014: 0 cases;
- 2015: 1 case.

## 3.4 Imposing sanctions if data protection rules have been breached

If a violation of rights has occurred in connection with the management of personal data, proceedings may be requested with the NAIH: if it considers that a violation of rights has occurred or there has been an imminent threat of such violation, it will call upon the data manager to remedy the breach or to eliminate the imminent threat (Section 56(1) of Act CXII of 2011).

The NAIH may institute an administrative data protection procedure in order to enforce the right to the protection of personal data. Based on Section 61(1) of Act CXII of 2011, in its resolution adopted in the administrative data protection procedure, the NAIH may:

- declare that personal data have been unlawfully managed or processed;
- order that untrue personal data must be rectified;
- order that unlawfully managed or processed personal data be blocked, deleted or destroyed;
- ban the unlawful management or processing of personal data;
- ban the forwarding or disclosure of personal data to persons outside Hungary;
- order that the person concerned should be notified if the data manager has unlawfully failed to notify such person;
- impose a fine.

Where, during the NAIH's procedure, a well-founded suspicion of a crime should arise, it will initiate criminal proceedings with the entity authorised to start a prosecution. If a well-grounded suspicion of an infringement or a disciplinary offence should arise, it shall initiate infringement or disciplinary proceedings with the entity authorised to start such proceedings (Section 70(1) of Act CXII of 2011).

The NAIH receives few, i.e. 4 or 5 data protection-related complaints each year directly from the subjects concerned or their parents. These complaints are normally related to photos posted on social media pages. In that context, however, administrative data protection proceedings have typically been initiated ex officio. Substantially more minors are involved in these proceedings (in 2013, for example, about 8,000 minors were reported to have been unlawfully registered with online dating sites whereas hundreds of children are involved in the currently pending administrative proceedings in connection with child beauty pageants).

## 3.5 Civil law consequences

If the rights to privacy under the Civil Code are breached (such breaches typically include the right to one's image and to the protection of one's honour, reputation and personal data), the aggrieved party may turn to a civil court.

If a person's privacy is breached, on the basis of the Civil Code (Sections 2:51(1) and 2:53), he or she may demand:

- a court statement that a breach of rights has occurred;
- that the breach be terminated and the offender be prohibited from continuing the breach;
- public satisfaction;
- that the situation giving rise to the grievance be terminated, the conditions prior to the breach be restored and the object created through the breach be destroyed or divested of its unlawful nature;
- damages for non-pecuniary grievance;
- compensation for his/her losses.

## 3.6 Breaching the criminal law

### *3.6.1 Imposing sanctions under Act C of 2012 on the Criminal Code*

In the event of a crime referred to in Section 2.4.4, punishment under Act C of 2012 (Section 33(1)) and measures (Section 63(1)) may be applied. (Special legal consequences include the blocking of electronic data, which is described in detail under Section 3.7.)

In addition to the above, the Act on Criminal Proceedings provides an opportunity for mediation if certain conditions are met (Section 221/A of Act XIX of 1998 on criminal proceedings). Of the crimes referred to in Section 2.1, typically perpetrated online against (or by) children, mediation is thus allowed in cases of harassment, breaches of privacy or the privacy of correspondence or abuses of personal data (excluding child pornography). Mediation is intended to promote the reparation of the consequences of crimes and future compliance by the suspect. Mediation should attempt to reach an agreement between the suspect and the offended party, giving rise to active repentance by the suspect (Section 221/A(2) of Act XIX of 1998).

An agreement is reached when a common position is reached between the offended and the accused parties regarding compensation for the damage caused by the crime or remedying its consequences. As a result of successful mediation, criminal liability may cease and therefore the proceedings may be terminated in the case of crimes involving up to 3 years of imprisonment; whereas in the case of crimes falling into the same category but involving up to 5 years of imprisonment, the punishment may be reduced without restrictions.

(The detailed rules of the proceedings are provided for in Act CXXII of 2006 on mediation procedures in criminal cases.)

The criminal statistical data published by the Coordination and Statistical Department of the Ministry of the Interior include the number of specific types of crime in various

breakdowns (according to location, year, target, tools etc.). However, these data do not include information regarding crimes committed by or against minors/children or regarding online crimes.

### *3.6.2 Legal consequences under the act on petty offences*

A dangerous threat (Section 173 of Act II of 2012 on infringements, the infringement procedure and the infringement registration system) may involve custody or any other kind of punishment or measure imposed for petty offences.

## 3.7 Tools designed to block unlawful content

This section describes a specific form of sanctions, i.e. the opportunity of removing unlawful online content. A specific feature of that procedural option is that it is governed by different regulatory schemes depending on the specific circumstances.

### *3.7.1 Removal of content violating the privacy of minors*

Since 1 January 2014, the scope for action under the notice and take down procedure has been increased in online child protection. As a result, the applicable legislation enables minors entitled to exercise rights to privacy and their legal guardians to take effective action in order to protect the privacy of minors according to thoroughly specified rules of procedure prior to or in lieu of civil or criminal proceedings. As a result of the procedure, similarly to infringements of copyright, it is now possible to remove content (information) breaching minors' right to privacy (Section 13(13) to (15) of Act CVIII of 2001).

No administrative powers are, however, associated with the enforcement of statutory provisions. If a service provider fails to comply with its obligations to remove the deleterious information or refuses to comply with the application, the minor concerned or his guardian may apply to the Child Protection Internet Round Table as the consulting body of the NMHH President on grounds of the presumed violation of the minor's rights to privacy. By investigating such reports and using their general experiences in its activities, the Round Table may primarily rely on the power of publicity in order to achieve results.

However, in connection with the legal institution that has been effective for nearly eighteen months, it should be noted that a Round Table has not received a single complaint to take action on. Two conclusions may be drawn from this fact:

- Service providers have complied with all requests to remove content supposedly violating a person's rights to privacy, rendering involvement by the

Round Table superfluous;
- The public is unaware of the legal institution.

### *3.7.2 Hotlines*

*A)* Internet Hotline

The Internet Hotline service has been operating in Hungary since 2005 in order to enable unlawful online content and content harmful for minors to be reported. Where appropriate, the operator of the hotline service (the NMHH since 2011) will call upon the service provider concerned to remove the content reported. The service provider may then remove the content voluntarily but cannot be obliged to do so (in other words, the procedure does not replace the administrative and judicial proceedings instituted on grounds of the violation of rights).
It must be emphasised that, rather than an administrative procedure, the activity of the Internet Hotline is carried out by the NMHH in the spirit of social responsibility. In the absence of a statutory mandate, the Internet Hotline and the NMHH operating the service are unable to oblige operators to delete any unlawful content or to warn users to content harmful to minors. The Internet Hotline may only request that the reported content be removed on the grounds that it is against the law. The reported content is normally removed by website editors or hosts or a warning is inserted that it is harmful to minors.

Reporting categories of the Internet Hotline service:
- content made accessible without consent: if photographs, video or audio recordings related to the person concerned or his or her children or other personal data are posted online without the consent or authorisation of the person concerned;
- paedophile content;
- harassment or bullying: if the person concerned or his or her children fall victim to online harassment or bullying. in the case of textual content available on Internet sites or forums which include sexual comments or conversations regarding minors, and where minors are invited to take part in sexual intercourse;
- racist or xenophobic content;
- content including the portrayal of violation;
- content enticing to drug consumption;
- content inviting to commit terrorist acts or popularising or promoting terrorism;
- phishing websites, content infected by viruses, spyware and other malware;
- other content hazardous to minors.

In the practice of the Hotline, ‘unlawful’ content includes content which is presumably in conflict with the applicable laws, including in particular the provisions of the Civil Code or Act C of 2012. In the online world, the most common breaches or rights include harassment or abuses of images or other personal data of other people, e.g. the unlawful publication of such data. Content harmful or hazardous to minors include any content capable of arousing fear or dissatisfaction in minors or having a detrimental effect on their intellectual or moral development.

The Hotline staff call upon the editor of the website having published the supposedly unlawful content or the operator of the server hosting such content to remove the criticised content. The content is deleted by the server owner (intermediary service provider) on the basis of the contract it has made with the party having uploaded the content concerned. Such contracts provide that any material or website placed on the server must not include unlawful content. In the case of content hosted on a foreign server, the Hotline staff also notify the Hotline operating in the jurisdiction concerned. Where the unlawful content may constitute a crime or preparations for a crime, the Hotline staff will report it to the police.

Where the content is harmful or hazardous to minors while not constituting unlawful content, the Hotline staff will call upon the editor of the website or the server operator to clearly indicate on the website that the content on the site may be harmful to minors.

According to March 2016 data, since the start of the Internet Hotline, nearly 3,200 notifications have been received. On average, it means about 700 notifications a year. The most common notification categories include: content published without consent (accounting for 19 % of all notifications), racists or xenophobic content; (19 % of all notifications), harassment (14 % of all notifications) and paedophile content (8 % of all notifications).

Based on experience, it can be concluded that Hungarian web hosts tend to cooperate and to block unlawful content or, in the case of content harmful to minors, to publish a warning of the relevant age limit. In the case of paedophile content, the Internet Hotline cooperates with the INHOPE (International Association of Internet Hotlines). The INHOPE enables paedophile content hosted abroad but targeting Hungary to be successfully removed, or to report through the organisation if unlawful content is hosted on Hungarian servers. Where unlawful content is hosted in their jurisdiction, the reporting bodies call upon the web host to remove the content concerned and keep in touch with law enforcement authorities.

*B)* SafeInternet Hotline

The SafeInternet Hotline has been available to report unlawful content since May 2011. Part of the Hungarian Safer Internet consortium, the service was set up within the Safer Internet Plus programme, with co-financing from the European Union. The Hotline is operated by the NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

On the SafeInternet Hotline complaints page, the following types of unlawful online content as specified by the Hungarian law may be reported:

- paedophile content;
- violent content (harassment);
- racist or xenophobic content;
- content enticing to drug consumption;
- content published without consent, in breach of privacy;
- other harmful content.

### *3.7.3 Blocking of electronic data*

Since 1 July 2013, Act C of 2012 has provided for the so-called 'final blocking of electronic data' measure, which is applicable in the case of data published on an electronic communications network:

- the disclosure or publication of which constitutes a crime;
- which are used as a tool in order to commit a crime;
- which have been created by committing a crime (Section 77(1)(a) to (c) of the Act on Act C of 2012).

That sanction may also be applied if the perpetrator is not punishable or his criminal liability has lapsed. The application of the measure only requires an examination of the facts and the unlawfulness of the case, i.e. the blocking of data does not require that the perpetrator be identified.

Closely associated with the application of the measure is the form of coercion embodied in the Act on Act C of 2012, i.e. the 'temporary blocking of electronic data', which constitutes a temporary restriction of the right to dispose over the electronic data. The purpose of this measure is to render inaccessible (while leaving recoverable), until the criminal proceedings end, the data associated with a crime, in cases where such data may be made inaccessible on a final basis and temporary blocking is required in order that a crime may be prevented (Section 158/B(2) of the Act on Act C of 2012).

Two options exist for temporarily blocking electronic data: first, by requiring the web host to 'temporarily remove the electronic data' (Section 158/C(1) of the Act on Act C of 2012). Alternatively, temporary blocking may be achieved by 'temporarily blocking access to the electronic data'. This, however, may only be ordered by the court on an

exceptional basis in cases where the criminal proceedings have been instituted on the grounds of child pornography, crime against the state, an act of terrorism, drug trafficking, generating abnormal addiction, facilitating the production of drugs, misuse of drug precursors, misuse of new psychoactive substances or terrorist financing and the electronic data are related with such crime (Section 158/D(1)(a) and (b)), and the web host has failed to comply with its obligation to temporarily remove the electronic data or the request sent to a foreign authority concerning the temporary removal of electronic data remained inconclusive for a period of thirty days. In such situations, the provider of electronic communications services is the party responsible. The implementation of the forced measure is arranged and supervised by the NMHH.
The electronic data is rendered inaccessible for good by blocking access to the electronic data on a final basis (Section 596/A of Act XIX of 1998).

### *3.7.4 Self-regulation*

In addition to co-regulation under the media legislation, mention must be made of the activity of self-regulatory organisations (in addition to the four trade organisations referred to under Section 3.3.1).
Where the rules of conduct laid down in the Code of Conduct of the National Association of Hungarian Journalists (‘MÚOSZ’), applicable, among others, to the online press, are breached, the Ethical Committee may establish a breach of ethical conduct as a result of a procedure conducted according to the Committee’s rules of procedure. The Code of Conduct also sets out a requirement concerning the protection of children, which provides that ‘an ethical offence is committed by any person breaching the privacy of minors. The journalist’s ethical liability may be established despite the fact that the guardian of the minor concerned has consented to publicity. Children may only be presented with the consent of their parents or guardians or, during hours of teaching or care, with the consent of their form teacher or kindergarten teacher, as appropriate. Where such consent cannot be obtained when the video or audio recording is produced, it must be obtained prior to airing such recording ‘ (paragraph 3.1.3).
The Corrector Self-Regulation Forum (set up in December 2015 through cooperation between the Forum of Editors-in-chief, the Association of Hungarian Newspaper Publishers and the Association of Hungarian Content Providers) also provides an opportunity for lodging complaints in all branches of the press (including the online press). The result of its procedure: any condemning decision must be published and made public. Child protection rules are included in the organisation’s Code of Conduct among the provisions concerning the protection of privacy.

## 3.8 Alternative dispute settlement in educational institutions

Decree No 20/2012 of 31 August 2012 of the Ministry of Human Resources on the operation of public education institutions and their use of names provides the opportunity for conducting, prior to the disciplinary procedure against the student, a conciliation procedure with a view to discussing and assessing the events leading to the breach of duty and reaching, on that basis, an agreement between the person suspected with the breach of duty and the aggrieved party to remedy the grievance (Section 53(2)).

A similar legal institution is the procedure by an educational mediator, which may be conducted if the educational institution is unable to eliminate the threats to children or students by pedagogical means or where this is justified in order to protect the community of children or students. In such situations, the educational institution may turn to a conflict management consultant or the youth protection or family law service for assistance (Section 62(1)).

Alternatively, the educational mediation may take place in the framework of a conciliation procedure. In other words, of the various forms of alternative dispute settlement, the Decree explicitly addresses the possibility of restorative mediation. Where an educational mediator is involved in the conciliation procedure, an agreement is reached between the parties if a common position has been reached between the aggrieved party and the negligent student with regard to the compensation for the damages caused by the breach of duty or the reparation or mitigation of its harmful consequences in another manner (Section 62(9)).

It must be noted that the agreement reached during the conciliation procedure is without prejudice to the right of the aggrieved party to seek other remedies for his claims arising from the crime or offence in addition to the disciplinary procedure (Section 62(13)).

## 3.9 Providing assistance and the helping of victims

Further important factors include the treatment of children having become a victim and preventing or eliminating negative (or possibly tragic) consequences. In that context, mention must essentially be made of organisations and institutions providing assistance to children, and helping them to process their injurious condition, and to avoid such conditions in the future. In addition to the above, the importance of providing appropriate circumstances during the administrative procedures conducted on grounds of the violation of rights must also be discussed. NGOs have played an outstanding role in that field.

### *3.9.1 Helping victims*

The treatment of and providing assistance to children having become victims is one of the priorities. Foreign examples have shown that unlawful acts committed online may soon escalate to have tragic consequences in a very short time. In order to help victims, appropriate experience is required in essentially the same areas as in the protection of minors in general. In addition to parents, teachers, NGOs specialising in the relevant areas and obviously the administration itself play an important role (the important duties of the administration include, among others, establishing an appropriate environment for the aggrieved parties during the administration procedure see paragraph 3.9.3).
In that context, it is absolutely necessary to provide sufficient information to parents and teachers as to how to recognise when a child is in danger, and then how to provide assistance to the child either on their own or in cooperation with the relevant persons or organisations.

### *3.9.2 The activity of NGOs*

Of professional organisations, mention must be made of the Kék Vonal Gyermekkrízis Alapítvány. Major focus areas of the Foundation include their fight in order to increase the safety of the Internet and against harmful and unlawful content. As part of that activity, the Foundation operates a toll-free helpline service in Hungary, on the phone number 116-111. Among other things, their main activities include providing consulting to children encountering harmful and hazardous online content or online abuse or harassment.
The UNICEF Hungarian National Committee Foundation started its legal aid hotline, primarily for adults and experts, in May 2016 in cooperation with the Bibó István College, where they invite inquiries of a legal nature in connection with child abuse or other violations of children's rights; including cases related to the safe use of the Internet (http://unicef.hu/unicef-jogsegely/). On the occasion of the 'Safer Internet Day' event of 2014, the HelpAPP (http://www.unicef.hu/helpapp/), a smartphone application designed for children, called into existence by the organisation, was awarded the Best Child Protection Content of the Year special prize. The application, first of its kind in the world, provides instant assistance to children in situations of violence. If a child is being hurt or is in danger, they can ask for help or send their actual GPS coordinates at the press of a button. Using the application, they can also ask for advice on what to say or do if exposed to violence or if they want to help someone exposed to violence.

The International Children's Safety Service has also played an important role in battling unlawful content harmful to children.

### *3.9.3 Protecting children's rights during administrative procedures (dispensing of justice)*

As discussed above in paragraph 2.2.2, children may get in touch with the dispensing of justice in various 'capacities', i.e. as witnesses (in certain proceedings), offended parties or even as perpetrators. Children-centred administration of justice is a system of dispensing justice which ensures that children's rights are respected and efficiently enforced at the highest possible level, while enforcing children's interests as a top priority in any case in which children are involved or affected.

One of the means of achieving the children-friendly dispensation of justice is setting up so-called child hearing rooms in order to ensure that the investigating authority and the court can interrogate children in a room where, in accordance with the objective of the criminal proceedings, it can be ensured that the procedure is conducted with regard to children as far as possible, keeping in mind the supreme interests of children.

For witnesses of that age, the supreme interest of children essentially means that they must be protected from the damages arising from the nature of criminal proceedings as much as possible.

# II. SWOT analysis

## Awareness-raising and media education

| Strengths | Weaknesses |
|---|---|
| ➢ The background materials, NGOs and experts having the required expertise for awareness-raising are available;<br>➢ Cooperation has been started between NGOs, the industry and educational institutions about various issues related to the safe use of the Internet by children and, consequently, various programmes have been completed with a positive outcome;<br>➢ Children often have significant information and experience concerning the use of media. Such skills can be efficiently utilised in awareness-raising not only as they themselves are concerned but also for their peers as well as older generations;<br>➢ All stakeholders have expressed a strong commitment with regard to the strengthening of media education;<br>➢ Due to the level of development of Hungarian infrastructure and the high number of digital devices in their possession, most children have some experience concerning the use of the Internet. | ➢ The need for the conscious use of the Internet and the issue of media education are not properly embedded in the Hungarian society;<br>➢ In practice, a theoretically sufficient level of education is not provided fully and with adequate efficiency;<br>➢ In order to change the culture of using the Internet and to increase media education, all stakeholders should cooperate;<br>➢ According to experience, most parents (who represent the closest link for children) are still not fully aware of the tools of the conscious use of the Internet and with online hazards;<br>➢ The system of programmes and government grants to promote active cooperation by businesses has not been institutionalised, and is still not predictable in the long term. |
| **Opportunities** | **Threats** |
| ➢ A minor transformation of the public education system in order to place more emphasis on media education;<br>➢ Active cooperation by the government may ensure that the skills required for the conscious use of the Internet are acquired not only by children but for people of all ages; its consequences will have a positive effect not only on the persons directly affected;<br>➢ Teachers obtaining and developing basic digital competences (e.g. through government grants) could in itself be suitable for identifying and preventing a | ➢ A lot of stakeholders are unable or unwilling to realise the potential harmful consequences arising from the lack of the conscious use of the Internet;<br>➢ The mere fact that an effort to improve media education is included in the National Basic Curriculum will not ensure that the relevant issues are actually present in public education;<br>➢ Excessive prohibition by parents and teachers intending to protect children concerning the use of the Internet may have a consequence contrary to the |

| | |
|---|---|
| number of problems;<br>➢ As far as improving media education is concerned, the media, in particular online services, play an outstanding role. | desired result;<br>➢ The isolated and sometimes duplicated activities of government bodies, professional organisations and NGOs in order to improve the media education of children, parents and teachers may interfere with efficiency;<br>➢ Placing excessive emphasis on and exaggerating the hazards of the use of the Internet may hinder the improvement of media education while relegating the potentials of the Internet into the background. |

**Protection and safety**

| **Strengths** | **Weaknesses** |
|---|---|
| ➢ In certain groups of the society, including in particular people with a higher degree in education, the use of the Internet is around the EU average;<br>➢ Distinct organisational units specialising in cybercrime have been set up by law enforcement agencies;<br>➢ Various Hotlines/helplines exist, supporting and complementary to legislation and the administration of justice;<br>➢ Various administrative and non-governmental initiatives exist in the field of digital child protection and media education (Internet Hotline, Bűvösvölgy, Child Protection Internet Round Table, Children-Friendly Internet Programme). | ➢ Digital illiteracy well exceeds the EU average;<br>➢ A significant part of Internet users use basic services only;<br>➢ There are significant gaps in real social responsibility concerning this area;<br>➢ In public education, digital competences are not being properly addressed outside IT classes;<br>➢ No free filtering software is available in Hungarian that could be operated in any of the most popular operating systems;<br>➢ |
| **Opportunities** | **Threats** |
| ➢ Develop filtering software that comply with the statutory requirements;<br>➢ Consider the possibility of developing a children-friendly browser;<br>➢ Increase the range of children-friendly online content in order to increase the media education of children;<br>➢ Ensure that cyberbullying is managed more efficiently within the existing | ➢ A lack of proper information from parents/teachers or proper education at school, children are exposed to increased danger while online;<br>➢ Some of the youngest generation are sometimes unprotected against hazards due to the fact that the available technological solutions protecting children are still not being |

| | |
|---|---|
| legislative framework;<br>➢ Reduce digital illiteracy, launch trainings and development projects;<br>➢ Introduce requirements for efficient technical solutions enabling the safe use of the Internet. | widely used;<br>➢ The legislative background cannot be efficiently applied in all respects, i.e. infringers/perpetrators are difficult to call to account;<br>➢ Children or teachers are not provided with adequate training or education on online hazards and the options to manage such hazards. |

**Applying sanctions and providing help**

| **Strengths** | **Weaknesses** |
|---|---|
| ➢ The background materials and experts required for properly managing hazards and grievances are available;<br>➢ Government and industry stakeholders and NGOs have emphasised their commitment to digital child protection;<br>➢ In theory, the legal system may, even in its current state, be suitable for managing all kinds of behaviour and life situations;<br>➢ The hotlines for reporting content hazardous to children are functioning (Internet Hotline, Safeinternet Hotline). | ➢ The duplicated activities of stakeholders often reduce the efficiency of activities;<br>➢ Ignorance of procedures available in order to remove hazardous, harmful and unlawful contents;<br>➢ Extensive data, information and research required in order to improve the efficiency of online child protection, and to establish government action are not always available in all respects;<br>➢ Due to their ignorance of the law, children causing or suffering a grievance tend to improperly assess online acts, i.e. substantial latency exists;<br>➢ The persons and institutions involved in helping victims are not always adequately knowledgeable in order to manage the situations arising in digital child protection. |
| **Opportunities** | **Threats** |
| ➢ Encourage market and industry stakeholders to take a more active role and social responsibility;<br>➢ Increase the role and weight of alternative and restorative dispute settlement procedures and self-regulatory mechanisms;<br>➢ Involve children in the implementation of various child protection programmes | ➢ Excessive regulation may substantially reduce the efficiency of the means applicable in order to achieve the relevant objectives;<br>➢ With regard to the fast-changing nature of the digital world, new forms and methods of hazards to children will keep emerging;<br>➢ Sufficient (financial and human) |

| | |
|---|---|
| (e.g. peer mentor training);<br>➢ The competent government bodies (investigation authorities, law enforcement bodies and courts) could put more emphasis on investigating the circumstances constituting online activities hazardous to children and on sanctioning such activities;<br>➢ The efficiency of preventing and managing the most common online violations of rights (e.g. cyberbullying) may be significantly improved by various programmes. | resources are not available to all stakeholders involved in child protection in order to carry out the required activities;<br>➢ The fact that the government assumes an active role in the field may be interpreted by parents, teachers or the children themselves as interfering with their personal freedom;<br>➢ Due to the special features of the online world, the measures designed to provide digital protection to children can be easily evaded, greatly reducing the efficiency of the relevant efforts. |

# III. System of tools and objectives

## 1. Vision

The objective of the Digital Child Protection Strategy of Hungary is to promote a more efficient preparation of children, families, communities, NGOs, educational institutions and the system of government institutions for adding more value by the use of the Internet. Digital culture plays a decisive and ever-increasing role in influencing everyday life, society and the economy. One of the most important abilities, the conscious use of the Internet, as a channel of accessing digital culture, is an extremely complex skill for citizens of the information society. The conscious use of the Internet, through which added value is created, acts as a multiplier of success in terms of individual relationships, the quality of life, social networks and competitiveness on a national level.

In addition to supporting the conscious and value-creating use of the Internet, another priority objective of the strategy is to enable the identification and assessment of online risks and hazards to children, minimising or eliminating harmful impacts to the greatest extent possible. In addition to issues related to transferring and acquiring the knowledge and information required before children enter the online world, the strategy addresses issues related to facilitating the availability of conditions required in order to ensure the safe use of the Internet and mitigating potential harmful consequences.

It builds on the achievements of similar government programmes implemented in previous years, including in particular the first (2012) and second (2013) Children-Friendly Administration of Justice legal packages.

While the strategy focuses on children, almost all groups of the society are affected, including the persons in a close, everyday relationship with children (i.e. parents and teachers), the system of government institutions, industry stakeholders and the relevant NGOs. The Information society is, first and foremost, a networking society; cooperation between generations, the mutual sharing of information and teaching and the collaboration of various groups of society are indispensable success factors.

Moreover, a wider perspective is needed in order to be able to satisfactorily manage the relevant issues. Training is of primary importance also in terms of learning, with particular regard to adaptation to the fast-evolving technology/labour market conditions, and the future careers of children. If young people with the appropriate skills are able to use the opportunities offered by the digital world in a safe environment, it gives them a competitive edge while also improving the competitiveness of their communities and thus that of their country. Therefore, the

primary objective of the strategy is to ensure that children can grow up to become conscious adults familiar with the opportunities, challenges and hazards of the Internet and capable of using their skills to their best advantage.

Due to the rapid acceleration of technological development in recent decades, in a certain sense, children will often be more experienced and knowledgeable about the use of the Internet than the adults who play a leading role in their education. Therefore, the latter should inevitably be involved in the implementation of certain strategic objectives. Managing that peculiar situation is one of the key issues of the strategy in order to ensure that the information required for the conscious and safe use of the Internet should properly get across to children; training the persons passing on that information (parents, teachers etc.) media education or media consciousness is thus of outstanding importance in order to be able to achieve the strategic goals.

Providing quality training to children, as an objective, will obviously necessitate the training of teachers. As the starting point of the above, the existing conditions need to be assessed as the required tasks cannot be carried out will full efficiency if adequate data and information are unavailable. With regard to the development of media education, there are numerous initiatives (by government actors, NGOs and the industry concerned), meaning that their practical experiences may be relied upon for further activities. However, it must first be noted that the conscious use of the Internet is far from being restricted to safety alone as it includes the ability to take advantage of the opportunities offered by the Internet.

In addition to an appropriate level of knowledge, priority objectives include ensuring the conditions required for the safe use of the Internet that are beyond the control of individual Internet users. The system of conditions of the safe use of the Internet cannot be achieved without setting up and operating protective mechanisms of the required efficiency. As mentioned before, while awareness-raising consists of familiarity with the hazards of the Internet and the skills and ability to recognise the opportunities it offers, safety must be created in order to provide protection against the potentially hazardous or harmful effects of online activities. At the same time, the ability to consciously use the media (media education) is a prerequisite of the safe use of the Internet in individual users and the adults influencing them. In that regard, it is obvious that the specific objectives are closely related and mutually influence each other.

The objective set under the strategy is to ensure that the protection mechanisms available function properly and efficiently. The primary means of achieving that goal cannot be the creation of additional statutory prohibitions. In that respect, the legal system has more or less got as far as it could, i.e. extensive restrictions and prohibitions exist in order to ensure the online safety of children. The current state of the legal system needs minor corrections only rather than the enacting of new types of conduct involving punishment or new restrictive measures. The efficiency of

restrictions can be increased by the continuous monitoring and development of existing technical solutions, assigning a special role to the representatives of the telecommunications industry as well as by creating content specifically designed for children and by setting up appropriate Internet pages helping children acquire the required information and experience corresponding to their level of maturity.

While shaping the vision, one should not disregard the need to alleviate the detrimental consequences of grievances inevitably occurring in certain situations. The recognition of grievances and damages and familiarity with the organisations involved in imposing sanctions and providing assistance to the persons having suffered a grievance and the methods employed by such organisations also require the appropriate skills associated with the conscious use of the Internet. In order to manage grievances and to avoid them in the future, both the government and NGOs must be actively involved; in that context, the scope of application of best practices must be extended and followed in order to help achieve the desired results and conditions.

# 2. The system of objectives under the strategy

## 2.1 Comprehensive strategic objectives

The system of objectives of the strategy can be established on the basis of the differences between and deficiencies in the framework of online child protection outlined in the situation assessment of the strategy and the vision outlining the desired objectives. In addition to making up for deficiencies, that system of objectives also ensures the long-term sustainability and operation of the existing and functioning system. The summary assessment in the SWOT analysis provides guidance to the development of the system of objectives. It helps identify positive and negative circumstances concerning the actual conditions and the desired objectives and the system of conditions affecting the achievement of strategic goals.

When developing the objectives, in the first place, the Government had to take into consideration the relevant expectations of its National Infocommunication Strategy (2014-2020) and the achievement of goals set out under that Strategy. Moreover, the objectives identified under this strategy are also similar to the expectations set out in the Communication issued by the Commission in 2012, entitled ‘European Strategy for a Better Internet for Children’[COM(2012) 196]. The Communication from the Commission puts forth proposals to the Member States focusing on four main pillars:

- Quality online content for children and young people;
- Stepping up awareness and empowerment;
- Creating a safe environment for children online;
- Fighting against the sexual abuse and sexual exploitation of children.

The strategy must focus on children’s use of the Internet and issues closely related to that issue. The system of objectives should therefore be established in a manner to ensure that it properly addresses each question and group of problems concerning the areas covered by the various pillars. Considering that, in issues related to children’s use of the Internet, there are numerous other stakeholders in addition to the system of government institutions, various groups of the society must take an active role and assume responsibilities in the identification of objectives.

The general objective of this strategy thus consists of transferring to children the skills enabling them to use the Internet safely, consciously and for the creation of value, by training and educating both children and the persons in touch with children on a daily basis and exerting the greatest influence on their development. Additional objectives of the strategy include ensuring familiarity with and continuous access to efficient protective solutions required for the safe use of the Internet and remedying any grievances in a professional manner in order to reduce subsequent harmful effects and preventing the repetition of violations of the law.

In the light of the above, on the basis of the pillar structure outlined in the situation assessment, the objectives of the Digital Child Protection Strategy of Hungary include the following:

*Pillar I: Awareness and media education*

- Prior to commencing specific measures, a comprehensive survey must be conducted regarding the efficiency and success rate of media comprehension education at schools;
- According to the objective to be achieved essentially in connection with the media education of children, children must be prepared for the proper use of online services, for taking advantage of opportunities as well as for avoiding and appropriately managing hazards and for raising their legal awareness;
- In terms of teacher training and curriculum development, providing up-to-date, competitive and relevant skills and information to teachers participating in media education and enabling them to keep such skills up-to-date;
- In addition to the media education of children, attention should be paid to raising the awareness of and providing information to parents on the relevant issues;
- As part of providing information to parents and other stakeholders, providing media consciousness education to persons involved ex officio in proceedings related to crimes or violations against children (including in particular representatives of the investigation authorities, law enforcement bodies and courts involved in such cases) in addition to providing parents with an option to participate in such trainings;
- A web portal should be set up in order to facilitate access to information relevant to the field of online child protection for all.

*Pillar II: Protection and safety*

- Considering and continuously developing the accessibility of a filtering software and a children-friendly browser ensuring the conditions of the safe use of the Internet by children;
- Assessing the experiences of international best practices in filtering harmful content and the preliminary assessment of their potential use in Hungary;
- Participation by the industry should inevitably be encourages as it may considerably increase the efficiency of the various protective solutions;
- The government must take an active role in order to support the production of online content designed specifically for children.

*Pillar III: Applying sanctions and providing help*

- Data concerning the frequency, trends and impacts of unlawful online activities must be collected and regularly monitored in order to identify and efficiently

manage existing problems;
- The alternative (restorative) solutions of managing grievances must be given greater emphasis in remedying actions committed by or to the disadvantage of children;
- Controlling and taking efficient action against cyberbullying require the launching of adequate programmes and the provision of training to the persons involved in managing grievances;
- Information about the existing legal remedy mechanisms must be disseminated to a wider group of people.

## **2.2** Objectives under each pillar

The following section discusses the various comprehensive strategic objectives under each pillar.

### *2.2.1 Awareness-raising and media education*

**Comprehensive objective:** to provide regular training opportunities, which facilitate the acquisition of up-to-date information, for both children and teachers and, in certain cases, to make such training a compulsory part of the syllabus, in order to help them acquire competences indispensable for the safe use of the Internet and the conscious and creative use of online culture. Improving parents' media education is part of that objective.

*C1) Setting up a system of monitoring and conducting regular measurements and research*

The use of the Internet by children, the ongoing evolution of its patterns and the related damages and hazards to children – must be monitored by reliable regular, at least annual, measurements based on large samples, preferably in a breakdown by age groups, taking into consideration the characteristics of each age group –, where the results of measurements should facilitate the preparation of decisions. In addition to evaluating results separately and longitudinally, they should also be compared in an international context in order to be able to better identify relevant areas of intervention. Apart from quantitative measurements to facilitate the preparation of decision (in the spirit of cooperation between generations), there is also a need to carry out basic research based on a qualitative approach to children's experiences of various life situations.

*C2) Media education programmes for children*

Within the public education system, the media education programmes provided to children should be based on new foundations so that they should live up to the challenges of online media without substantially increasing the workload of children and teachers.

*C3) Teacher training and syllabus development*

Reforming teacher training in terms of the acquisition of competences related to media education is one of the prerequisites of providing adequate training to children within the system of public education. Producing regularly updated syllabuses, teaching aids and teachers' manuals, available both in printed form and online, based on existing material, is a task of fundamental importance. During that process, in addition to the teaching materials, the learning and teaching process itself will also be greatly conducive to the value-creating use of the Internet.

*C4) Training provided to other stakeholders*

Media education training should be provided on a continuous basis to administration of justice and law enforcement bodies faced with child protection issues in their work, while an opportunity to attend trainings should also be provided to parents. Apart from administration of justice teams, increased attention should be paid to stakeholders in the broader context of child protection, including in particular school psychologists, social workers, social services staff and policemen. These stakeholders must be provided with continuously updated guidances that clearly identify their responsibilities, roles, options and duties.
In addition to them, training opportunities should also be made available to parents and other stakeholders within the public child protection system.

*C5) Web portal and authentication*

The information available in the field of online child protection must be made easily accessible free of charge to all, while a system should also be set up where the materials including truly useful practicable information and knowledge are properly certified by a panel of experts.

On the basis of the above, the system of objectives of the pillars of awareness-raising and media education are as follows:

C1) Conducting regular and comprehensive online child protection measurements and research.

C2) Reforming children's media training.

C3) Reforming teacher training and producing the required teaching materials.

C4) Compulsory training of the stakeholders concerned within the administration of justice and the public child protection system and making training available to parents.

C5) Making information easily accessible and setting up a system of authentication.

### *2.2.2 Protection and safety*

**Comprehensive objective:** ensuring and making available the legal and technical conditions required for the safe use of the Internet and broadening the range of online content appropriate to children's level of maturity.

*C1) Continuous provision of adequate filtering software solutions*

While a filtering software solution meeting the applicable legislative requirements is available and can be downloaded on the service providers' websites, there is no guarantee that the software will remain accessible free of charge in the long run. Moreover, the software currently cannot be applied to each of the most common operating systems. Therefore, it is an essential objective that filtering software solutions widely accessible to all free of charge on the long term should, in accordance with the provisions of Section 149/A of Act C of 2003, be developed with government support; at the same time, this will help Internet access providers to comply with their statutory obligation. On the development of the filtering software, the increasing popularity of mobile devices (smartphones and tablets) should also be taken into consideration.

*C2) Alternative solutions of filtering harmful content*

In addition to the filtering software, it is desirable to take into consideration alternative solutions of keeping children safe from harmful content, for

which foreign models are also available. It appears necessary to take such foreign best practices into consideration, examine their efficiency, collect and evaluate the relevant experiences and analyse the expected consequences of their potential implementation in Hungary.

*C3) Use of efficient technical solutions*

In the meaning of media legislation, content that is particularly harmful to minors may not be published unless efficient technical solutions are employed; a recommendation was adopted by the Media Council concerning such solutions (see paragraph 2.4.5 of the situation assessment). The provisions referred to above only set out requirements concerning online content subject to the media legislation (i.e. on-demand media services and online publications); the recommendation issued by the Media Council goes beyond that, putting forth proposals for broadcasters concerning parental lock solutions. (As the recommendation was last updated by the Media Council in March 2014, its review is not becoming opportune, based on experiences obtained to date.)
Currently, no statutory requirements thus exist vis-à-vis the majority of online content (e-commerce services) concerning the application of technical solutions to restrict access by children. Efficient means of protection may include the extension of the application of technical solutions regarding content harmful to children.

*C4) Managing hazardous and recommended content (blacklists and whitelists)*

Lists must be drawn up of content that is expressly harmful to children or is potentially unlawful *(blacklist)*and cultural/educational content specifically designed for children *(whitelist)*. Such lists represent great help in filtering hazardous content and assist children in accessing content appropriate to their age, in accordance with the rules of the conscious use of media. A panel of experts is required to assist with the compilation and updating of lists. With regard to the monitoring of lists, the potentially different needs and requirements of children of different age groups and social and economic situation.

*C5) Strengthening co-regulation by the industry*

It would be practical to make increased use of the synergies offered by the activities of existing self-regulatory and co-regulatory organisations (e.g. speed and efficiency). Opportunities for cooperation must be given to

organisations on the media and communications market, which may help businesses increase the efficiency of online child protection measures.

*C6) Using criminal law as the ultima ratio*

People involved in the administration of justice must be provided an adequate level of training in order to enable them to properly identify and classify unlawful online activities, considering their diverse and special nature. Apart from the passing on of information, it is indispensable to regularly assess the effects and consequences of the application of legislation, and to use these experiences in subsequent trainings.

*C7) Expanding the range of safe and useful content for children*

In addition to protecting children from harmful and injurious content, it is also important to support efforts enabling children to find as much online content specifically intended for them as possible. The nature and subject-matter of such content may be diverse; it may also include sites displaying media content produced by children themselves.

On the basis of the above, the system of objectives of the protection and safety pillar is as follows:

C1) Making available a filtering software that meets both the statutory requirements and technological expectations.

C2) Preliminary assessment of the expected effects and consequences of the network-level filtering tools implemented by default.

C3) Considering the potential applications of efficient technological solutions with regard to online content not subject to the media legislation.

C4) Collating lists of websites with content that is harmful to children, unlawful content and content specifically recommended for children and keeping such lists updated.

C5) Establishing closer and more efficient cooperation with self-regulatory and co-regulatory organisations.

C6) Providing adequate training and further training to people involved in the administration of justice in order to ensure that unlawful activities are properly identified and rated.

C7) Increasing the volume and diversity of content designed specifically for children.

### *2.2.3 Applying sanctions and providing help*

**Comprehensive objective:** giving priority to alternative methods of managing grievances while developing a regular monitoring and assessment structure capable of evaluating the actual weight and impact of problems.

*C1) Gathering information*

No data are available based on reliable studies concerning the amount of unlawful acts committed online primarily by children or to the disadvantage of children, which substantially reduces the efficiency of preventive action. In order to enable sanctions to be imposed and genuine help to be provided, the regular collection and assessment of information is a priority objective.

*C2) Alternative methods of managing grievances*

Managing controversial situations efficiently, as considerately for the children concerned as possible is an expectation of fundamental importance. To that end, the range of existing and established alternative dispute settlement methods that give priority to the interests of children having committed an injurious act or having suffered a grievance and are capable of quickly and efficiently resolving problematic situations must be extended.

*C3) Managing cyberbullying incidents*

While exact data are not available, experience has demonstrated the frequent and damaging presence of online harassment and cyberbullying among children. The comprehensive objectives of the strategy include the resolution of that issue through extensive cooperation, which should include prevention as well as minimising or preferably fully remedying the harmful consequences of the damage done.

*C4) Activities related to disseminating information on existing legal remedy mechanisms*

It is important to disseminate information concerning the legal remedy procedures and opportunities available within the legal system to as many people as possible. The efficiency and desired impact of legislation is lost unless children having suffered a grievance or their parents and teachers are aware of the opportunities available to them. Such dissemination of information should primarily focus on the relevant provisions of the Civil Code and Act CVIII of 2001 on e-commerce.

On the basis of the above, the system of objectives of the sanctioning and assistance pillar is as follows:

C1) In order to ensure the efficiency of action, the number, nature and types of injurious activities must be collected and regularly updated in the database.

C2) Where appropriate, online harassment and cyberbullying incidents committed by or against children should be managed in the framework of alternative dispute settlement mechanisms.

C3) A framework and conditions must be provided in order to appropriately manage cyberbullying incidents and minimise their number as much as possible.

C4) In media education, the legal options of managing damages suffered and the procedures available must be prominently included.

# 3. The system of tools under the strategy

## 3.1 General approach

When identifying the system of tools, it is essential that one should consider the necessary and indispensable tools required in order to achieve both the general objectives outlined in the vision and the specific objectives discusses in the system of objectives. As a fundamental expectation, the specific points of the system of tools should cover all elements required in order to achieve the desired activities without including any tools that fail to facilitate, directly or indirectly, the achievement of any of the objectives.

## 3.2 Classification of tools by pillars

The following section discusses the tools required in order to achieve each objective, including specific measures relevant to each tool in accordance with the pillar structure of the strategy.

### *3.2.1 Awareness-raising and media education*

*E1.1) Setting up a system of monitoring and conducting regular measurements and research*

The use of the Internet by children, the ongoing evolution of its patterns, the related damages and hazards to children and problematic phenomena liable to significantly affect their lifestyle and value system – must be monitored by reliable regular, at least annual, measurements based on large samples, preferably in a breakdown by age groups, taking into consideration the characteristics of each age group –, where the results of measurements should facilitate the preparation of decisions. Quantitative measurements must be complemented by qualitative studies that are able to reveal children's own insights and ideas, plans and experiences of specific life situations. The training plans must be adjusted to the achievements.
It must be ensured that the practical application of legislation is continuously monitored, with particular regard to near-criminal deviations characteristic of young persons, such as cyberbullying. Such monitoring should cover the number of reported incidents, the type of perpetration, the characteristics of perpetrators and victims and the outcome of the criminal proceedings, including in particular the circumstances considered by the court in its ruling. Data should be collected in order

to facilitate the decision-making process and to determine the guidelines for procedures, considering the special protection needs of underage victims and juvenile perpetrators.

Preventive measures must be preceded by empirical studies. The efficiency of the development of media education at schools must be assessed. The study should focus in particular on the methods employed by teachers, the manner they are integrating media comprehension and media education into the syllabus and the tools they use in order to achieve that goal. Based on the results, recommendations may be put forth on possible ways of using the new media actively and safely in education and of developing media education and the responsible use of the media by students.

A methodology (indicators and surveying tools) required for measurements and research must be developed as these are either unavailable (e.g. concerning the effectiveness of media education at schools) or not sufficiently differentiated or suitable for identifying numerous essential aspects of the use of the Internet.

As a result of efforts by NGOs and business stakeholders, a lot of ‘best-looking practices’ appear to be available in terms of awareness-raising. Once these have been collected, the professional evaluation and impact assessment of programmes must be carried out on the basis of relevant indicators. It must be stipulated that any grants should only be awarded to programmes that also include impact assessment and follow-up activities.

Moreover, the digital shopping patterns of children as consumers should also be examined, including a survey of the types of hazards child consumers are exposed to when shopping online. In the future, the results of that survey may serve as the basis for creating opportunities to move on or to intervene in e-commerce where appropriate in the interest of consumers.

Measures (actions) related to the group of tools:

a1.1.1) Developing a methodology (indicators and surveying tools) required for measurements and research and identifying the exact focus of research.

a1.1.2) Identifying the higher-education institutions, research centres and NGOs potentially involved in measurement and research and initiating cooperation with such entities.

a1.1.3) Carrying out measurements and research on an annual basis and the evaluation and publication of results.

a1.1.4) Formulating specific recommendations and changes to support planning on a rolling basis in accordance with the applicable legislation and suiting the needs of organisations, based on the decision-preparation materials specified in paragraphs a1.1.1 to a1.1.3, and communicating such recommendations to the decision-makers.

a1.1.5) Reviewing grant opportunities in order to improve children's media education or their protection against online hazards, available to NGOs focusing on digital child protection and stakeholders on the communications and media content markets and amending the competition criteria with a view to ensuring the professional quality of applications awarded financing and ensuring that they should include impact assessment and follow-up activities.

a1.1.6) A study of the digital shopping patterns of children as consumers and the types of hazards children consumers are exposed to while shopping online and, based on the results of such research, considering opportunities to improve or intervene into e-commerce from a consumer protection perspective.

*E1.2) Improving the media education of children*

*A)* Amending media education within the public education system – 'media weeks'

Within the public education system, improving children's media education should partly be based on new foundations so that they should live up to the requirements and challenges of online media without substantially increasing the workload of children and teachers.
While it may seem that media education is an important area of the NAT, on the level of the framework curriculum, which regulates the manner media education should actually been taught at each level and in each type of school, media appears as a marginal subject, a minor character that lacks even the minimum time frame required for real improvement.
Substantially increasing the number of classes in media education would hardly be viable as it would require significant changes to the framework of compulsory classes and adding to the workload of participants of public education or would only be possible at the expense of other important subjects.
In order to achieve the desired efficiency of education by making students aware of the problems outlined in the situation assessment, a method complementary to traditional teacher training is required; to that end, intensive, project-based media

training should be introduced for the 6-7, 10, 13 and 17-year-old age groups, i.e. in the first, fourth, seventh and eleventh grades.

In these grades, so-called ‘media weeks’, i.e. an educational programme scheduled as an afternoon activity and taking place in the form of workshops designed for smaller groups and collective, plenary activities running for a week, between 2 and 5 p.m. every day, should be introduced in both school terms.

At the media weeks, certain elements of the situation assessment (e.g. the use of the media/addictions; stereotyping/hate speech; the mixing of reality and virtual reality; weakening of the knowledge or reality/representations; vulnerability of databases; contradictions between non-linear reading and traditionally structured texts/school requirements; manipulation; mediatised body culture/gender roles; weakened penetrability between generations/excessive prohibition; problems of the conscious choice of content on convergent technological platforms; social inequalities) constitute the programme of each section. These topics can be discussed using a broad range of methods (invited speakers, a public dialogue between the parties concerned, research programmes, presentations or by involving parents). Some of the activities are repeated every day with different participants so children can make a choice on which activities or sections to attend each day. On a longer term, the professional guarantee of the media weeks may consist of teachers who have received proper training, including in particular school teachers specialising in media studies (and a syllabus that is up-to-date in terms of information and methodology and supports the programme). Due to a shortage of media teachers, however, the programme cannot be immediately implemented in each school district and, therefore, it is important that freelance lecturers and other professionals should be employed during the implementation period of the new form of training. Participation at the media weeks is optional but recommended. Following the media weeks, students are given assignments and are asked to report on their results.

Media weeks are a colourful, interesting and modern form of centrally financed non-formal education at schools. Integrated with teacher training, they provide a genuine opportunity to raising awareness concerning the wide-ranging issues of media education and to acquire the required resistance.

The intellectual innovation required for teacher training and the media week activities necessitates the ongoing operation of a content and methodology improvement/research organisation (institute) based on existing organisational foundations.

Integrated with teacher training, it should also be developed and introduced as soon as possible that, within their respective subjects (and working with the problems and information of their subjects), all teachers should teach a minimum of 5 to 10 classes a year with special media focus, correlating with, reflecting on and increase consciousness concerning an element of the problem map.

*B)* Encouraging participation at the National Competition of Secondary Schools

The National Competition of Secondary Schools (OKTV) on media-related subjects is currently not functioning properly as a tool for talent development since it does not provide sufficient incentive for participation or reward the best applicants through opportunities to enter the relevant higher education institutions or otherwise. This must be changed in order to increase the weight of media education at secondary schools. Incentive may be provided by setting up a research mentor programme, with the participating university researchers and non-academic professionals assisting research through sharing research experience, specialist literature and supporting the writing of studies. The mentor programme is a natural ally and an addition to the board of expert responsible for updating the whitelist and the blacklist. By increasing basic skills and the training of mentors, the setting up of the research mentor scheme also supports the operation of the mentor network providing training and consulting as described in section D).

*C)* Avoiding the hazards of excessive prohibition

It is a well-known phenomenon that, in a moral panic situation, pleading dangers, parents may restrict the freedom of choice and action of their children by prohibiting or excessively controlling their online activities to an extent that it prohibits them from taking advantage of the opportunities of the Internet. Excessive prohibition is counter-productive and may result in an outcome contrary to the original intentions. Again, teaching media education skills at schools may provide an antidote against those risks.

*D)* Setting up a peer mentor training system

In addition to the above, a peer mentor training system should also be developed, where the advantages of the use of the Internet and the related hazards are demonstrated to the target groups by similar-age schoolchildren. (As a possible alternative, mentors a few years older may also be involved in the programme; this could be particularly effective at educational institutions where a primary and a secondary school are integrated and the latter may be interested in carrying out quality mentoring as part of their community service programme.) While the mentors may also be responsible for other (related) areas (e.g. conflict management), the programme should primarily focus on the safe use of the Internet. The point of the programme is that, following a brief training programme, mentors will provide regular assistance to the students concerned. While schools

must assume a role in mentor training or at least in teaching them new information, they should also make these activities more attractive to potential mentors.

*E)* Surveying access to digital devices

The analysis of the situation of media comprehension training in Hungary cannot be treated separately from the issues related to the available digital devices, access to such devices and digital competences. Experience has shown that, in Hungary today, the conditions and opportunities in terms of the availability of digital devices at various public education institutions vary across a very wide spectrum. The important prerequisites of the full implementation of media comprehension education would include the availability of digitally well-equipped public education institutions while the existing serous inequalities and deficiencies should be continuously remedied and improved.

Measures (actions) related to the group of tools:

a1.2.1) Drawing up the first-generation teaching and illustration materials, methodology recommendations, workbook and assessment criteria required in order to carry out the media weeks programme.

a1.2.2) Organising, carrying out and evaluating the pilot programme for the media weeks programme in the 2017/2018 academic year, based on the teaching and illustration materials and methodology recommendations referred to in paragraph a1.2.1, in at least 25 educational institutions including at least two special education institutions for each type of institution, except for kindergartens.

a1.2.3) Organising and carrying out a first-generation (instant) further training programme for teachers, which is required in order to implement the media weeks programme, in the form of an accredited training of 30 to 60 hours, primarily for practising teachers of social studies, information technology, motion picture studies and media studies.

a1.2.4) Coordinating the new NAT planned for 2018, and the related framework curricula, textbooks and other learning and teaching aids, including model syllabuses, with the measures under the Digital Child Protection Strategy of Hungary, including in particular the media weeks programme content.

a1.2.5) Media education and pedagogy: operating a content and methodology development/research workshop based on existing organisational foundations.

a1.2.6) Specifying the system of conditions of the peer mentor programme, inviting NGOs and businesses to cooperate on mentor training and preparing and implementing the introduction of the programme at schools.

a1.2.7) Surveying the digital tools of public education institutions, mapping deficiencies and submitting a proposal for the required improvements.

*E1.3) Teacher training and syllabus development*

The specialist training and further training of media teachers should also be transformed. This could take place on three levels:

- Providing a 60 to 120-hour upskilling course to teachers (outside the higher-education system);
- Starting a specialist media teacher programme as part of the media and communication programmes of higher-education institutions;
- At the same time, providing compulsory media education training to all would-be teachers as part of their training programme (in addition to the basic subjects history of pedagogy and psychology and earning a similar number of credits to those subjects).

Nursery school teachers, lower-grade and upper-grade primary-school teachers and secondary-school teachers will all need training of a different focus and different content, since they have different tasks throughout the various development phases.
Media teacher training, placed on new foundations, may then result in the breakthrough required in order to ensure that people working in the public education system are fully aware of the issues, significance and pedagogical methodology of media consciousness. That extent of innovation in teacher training is required in order that teachers should be aware of, put on the agenda and be capable of managing the socialisation challenges of the media (without taking into account or hardly taking into account the phenomena of mediatised culture and thus putting children in the same position as thirty or fifty years ago, the school of today essentially talks ‘over the heads’ of children).
Teachers should receive basic training and upskilling in terms of the use of digital tools and the safe and ethical use of the Internet. In addition to the use of tools, training should include methods to integrate the tools into the school syllabus. Teacher training must include awareness of, preventing and managing the risks of

cyberbullying as well as problematic media phenomena which have serious effects on lifestyles and children's value systems.
Schools should be prepared for preventing and managing online hazards, including in particular the problems arising as a result of cyberbullying (preventing victim blaming). To that end, appropriate knowledge and personnel resources should be available at schools. Teachers should receive supervision and psychological assistance as required, in order to help them absorb the mental burden involved with their job.
Simultaneously with reforming teacher training, the required syllabus development must also be carried out. Textbooks that are revised frequently (at least on a three-year basis) and capable of exploiting the potential of media weeks referred to above are required, along with the related websites and teachers' manuals.
In addition to developing the specialist skills and knowledge of media teachers, efforts must also be made with a view to increasing the number of qualified teachers.

Measure (action) related to the group of tools:

a1.3.1) Initiating content and curriculum development required for the integration of general media studies and media pedagogy content and methodology-related information and practices into the system of elementary and secondary teacher training.

*E1.4) Training provided to other stakeholders*

*A)* Improving parents' level of media education

Participation in media education training should also be available to parents by organising courses that provide skills relevant to the use of the Internet at a reasonable cost in order to enable parents to use the skills so acquired in raising their children. An effort must be made in order to provide cost-free training courses, too (the use of eHungary points for the purpose should also be considered).

*B)* Training people working in the administration of justice and law enforcement

People working in the administration of justice, faced with crimes and other offences against children as part of their job (i.e. people working primarily at the police or the public prosecutor's office and judges) should be trained on an ongoing basis in terms of media education, focusing on the areas relevant for their jobs. Such training should be integrated into the system of existing compulsory trainings for administrative and judicial employees (i.e. the training of

judges, public prosecutors and police employees). People dealing with to online child protection issues as part of their jobs should participate in media education training at specific intervals (at least every three years).

*C)* Supporting people working in the field of child protection

People working in child protection (social workers, social services workers, child psychologists, school psychologists and district nurses) should also be provided training, primarily by drawing up streamlined and practical guidelines and manuals including a description of the responsibilities, opportunities and challenges of the target groups concerned. This point also helps link up the Digital Child Protection Strategy with other measures of the area and other participating groups of stakeholders.

Measures (actions) related to the group of tools:

a1.4.1) Collating the curricula of media education courses available to parents, inviting NGOs and businesses willing to cooperate, announcing the courses through public education institutions and organising and conducting trainings on an ongoing basis.

a1.4.2) Integrating media education training into the system of the training of judges by developing programmes for the training and further training of judicial workers dealing with crimes and other offences against children.

a1.4.3) Integrating media education training into the system of the training of public prosecutors by developing programmes for the training and further training of public prosecutor's office employees dealing with crimes and other offences against children.

a1.4.4) Integrating media education training into the system of the training of police employees by developing programmes for the training and further training of police employees dealing with crimes and other offences against children.

a1.4.5) Integrating media education training into the system of the training of public child protection system employees.

*E1.5) Web portal and authentication*

The information available in the field of online child protection must be made easily accessible free of charge to all on a website where such content is assembled and the persons interested (parents and teachers in the first place) are able to find the answer to any relevant questions quickly and easily.
At the same time, a system must be created where materials carrying genuinely useful and practical information, which are uploaded to or linked to the website, are properly authenticated by a panel of online child protection experts. That panel of experts will take a stand on which teaching materials, teaching aids or information documents discussing online child protection issues should be published on that central website, thus guaranteeing the validity of those materials. The textbooks used in media education should be verified and approved in a procedure independent from the above, according to rules governing textbooks and teaching materials.

Measures (actions) related to the group of tools:

a1.5.1) Determining the content to be uploaded to the web portal and creating and operating the web portal.

a1.5.2) Determining the professional authentication procedure for the content to be made accessible on the web portal and carrying out such authentication on a regular basis.

### *3.2.2 Protection and safety*

*E2.1) Opportunities regarding the development of filtering software*

Experiences of the past two years have shown that while the filtering software may provide genuine protection against a significant percentage of potential hazards, various problems have also been encountered lately that need to be addressed. In the light of the applicable legislation and the Child Protection Internet Round Table (see Situation Assessment, paragraph 2.3.4), the most important conditions of the efficient use of the filtering software in order to restrict content harmful to minors can be summed up as follows:

- Availability and accessibility: all major service providers and an overwhelming majority (>80 %) of minor service providers offer filtering software meeting the criteria of the recommendation to their customers free of charge;
- Ease of use: in most cases, Internet access providers provide, on their websites, a textual and video guide to the installation of their filtering software made available free of charge;
- Compatibility with operating systems: the filtering software offered by service

providers (Norton Family) currently does not support Linux on desktop computers or the IOS, WP and Firefox operating systems on mobile devices. Similarly, it has not been guaranteed that the Norton Family filtering software will remain available free of charge in the long run;

- The situation of public institutions: the fact that the Norton Family software cannot be centrally managed makes its use at cultural institutions (about 300,000 PCs) difficult; 20 % of all workstations at schools/libraries (about 60,000 PCs) run with a Linux-based operating system for which no filtering solution is currently available on the websites of providers of communication services;
- Problems include the lack of a familiar and sufficiently transparent model or recommendation available to public education institutions. The distribution and maintenance of costs related to such software and the words and expressions to be filtered by the software are controversial. In most cases, schools tend to respond by drastically restricting children's access to the Internet (see paragraph 2.3.3 of the Situation assessment).

In order to ensure that the filtering software functions properly, lists must be collated on websites recommended for minors, including valuable content corresponding to their level of development *(whitelist)* and websites including content that is harmful and not recommended *(blacklist)*. Moreover, certain content categories must also be created, through the selection of which it can be specified whether or not a specific category should be accessible to children of a certain age as the default setting. The lists might help ensure the efficient operation of the filtering software.

In order to ensure efficient operation, the lists must be regularly updated. Considering that no filtering software meeting the requirements under Section 149/A of Act C of 2003 (i.e. it is in Hungarian and is easy to install and operate) is continuously and reliably available on the market, the government must take a role in the development of the software. Software compatible with the four most popular operating systems (Windows, IOS, Android and Linux) must be made available on a continuous basis. This may be achieved by new development, the improvement of existing software, and the purchasing of licences by the government. It is important that they should be accessible to all free of charge, and that they should be annually updated and maintained. Considering the costs (by preliminary estimate: up to HUF 100 million for each operating system; if an existing solution is upgraded, the sum may be lower), the development/upgrade/purchasing of one software a year may be expected.

Measures (actions) related to the group of tools:

a2.1.1) The technical parameters of the filtering software may be identified, the public procurement required for development may be conducted and

development may be verified for a different operating system – each year – (between 2017 and 2020).

a2.1.2) Annual updating and maintenance of software developed.

a2.1.3) Operating a helpdesk service for the software developed (in cooperation with organisations providing relevant legal aid).

a2.1.4) Consultations with providers of communication services on tools to promote awareness of and the gaining ground of the filtering software.

a2.1.5) Drawing up information materials and providing information on the filtering software on an ongoing basis at kindergartens, schools and for parents.

*E2.2) Safe Internet Service for Children*

A special solution for online child protection, described in paragraph 2.5 of the Situation Assessment, has been used in the UK where, based on an agreement with the government, Internet access providers have voluntarily committed to restrict pornographic content as a default setting since the end of 2013 (including Wi-Fi services and all devices); no legislation, however, has been adopted concerning the subject. While all newcomers to the service are provided with a Safe Internet Service for Children in the first place, through network-level filtering measures, these setting can be removed at request. Such idea, however, goes back a long way in the UK. Since 2002, the Internet Watch Foundation has published a blacklist on content that is potentially harmful to minors and, based on that list, service providers have blocked the relevant content on a voluntary basis. The list classifies content to be banned according to the following major categories: drugs, alcohol, dating sites, pornographic content and content encouraging suicide. The initiative has been embraced by major service providers which have also set up websites on the safe use of the Internet and awareness-raising and have provided their customers with a filtering software free of charge. After that, network-level measures were also introduced at libraries and schools, whereas by the end of 2016, they expect all schools to have joined the initiative. The network-level filtering measures can only be disabled by adults.
The most common criticism concerning the functioning of the system has been that filtering has also included various sites set up in order to help children who have become victims of cyberbullying and to educate and raise awareness of the public concerning such issues.

As part of the system, the UK Government maintains a dedicated website (https://www.blocked.org.uk/), where users can easily check whether a site has been blocked or, if it has been block by mistake, the release of blocking can also be requested on this website.

The table below shows the settings of various blocking categories and the blocking levels of major service providers in the UK. The extent of blocking for the various categories depends on the service provider's individual commitment, i.e. there is no single system or legislation.

| Category | TalkTalk Homesafe[100] | BT Family Protection[101] | Sky Broadband Shield[102] | Virgin Media Web Safe[103] |
|---|---|---|---|---|
| Dating | **(Default)** Dating | **(Light)** Dating | **(13)** Dating | Possibly not due to dating.virginmedia.com |
| Drugs | **(Default)** Drugs, Alcohol and Tobacco | **(Light)** Drugs | **(13)** Drugs and Criminal Skills | Drugs |
| Alcohol and Tobacco | **(Default)** Drugs, Alcohol and Tobacco | **(Light)** Alcohol & Tobacco | | |
| File sharing | File Sharing Sites | **(Strict)** File Sharing | **(13)** Anonymizers, Filesharing and Hacking | |
| Gambling | **(Default)** Gambling | **(Moderate)** Gambling | Not blocked[104] due to Sky Betting and Gaming division | Probably not blocked due to Virgin Gaming division |
| Games | Games<br>Homework Time | **(Strict)** Games<br>Homework Time | **(PG)** Online Gaming | |
| Pornography | **(Default)** Pornography | **(Light)** Pornography | **(13)** Pornography and Adult | Pornography |
| Nudity | | **(Moderate)** Nudity | | |
| Social networking and Web forums | Social Networking<br>Homework Time | **(Moderate)** Social Networking<br>Homework Time | **(PG)** Social Networking | Not blocked[105] |
| Suicide and Self-harm | **(Default)** Suicide and Self Harm | **(Light)** Hate and Self-harm | **(13)** Suicide and Self Harm | Self-harm and Suicide |
| Weapons and violence | **(Default)** Weapons and Violence | **(Moderate)** Weapons and Violence | **(13)** Weapons, Violence, Gore and Hate | Violence |
| Obscenity | | **(Light)** Obscene and Tasteless | | |
| Criminal Skills | | **(Light)** Obscene and Tasteless | **(13)** Drugs and Criminal Skills | Crime |
| Hate | | **(Light)** Hate and Self-harm | **(13)** Weapons, Violence, Gore and Hate | Hate |
| Media Streaming | | **(Strict)** Media Streaming | | |
| Fashion and Beauty | | **(Strict)** Fashion and Beauty | | |
| Gore | | **(Light)** Obscene and Tasteless | **(13)** Weapons, Violence, Gore and Hate | |
| Cyberbullying | Not blocked[106] | No[107] | **(13)** Cyber Bullying | |
| Hacking | | **(Light)** Obscene and Tasteless | **(13)** Anonymizers, Filesharing and Hacking | Hacking |
| School Cheating Sites | | **(Custom)** Homework Time | | |
| Sex education[108]<br>Gay and Lesbian Lifestyle[109] | | **(Custom)** Sex Education | | |
| Search Engines | | **(Custom)** Search Engines and Portals | | |
| (Optional) Phishing, Malware and Spyware | Virus Alerts | | **(18)** Phishing, Malware and Spyware | |
| Web-blocking circumvention tools[110] | | When any filtering enabled | **(13)** Anonymizers, Filesharing and Hacking | |

The implementation of the system established in the United Kingdom might be considered. Under the above system, as a default setting, Internet access providers only provide to their subscribers Safe Internet Service for Children, which disables access to certain unlawful content and content that may be seriously harmful to children's development. On the basis of the solution, access to such content requires an active request by the subscriber, i.e. a request that the service provider should release the ban on accessing the content concerned.

Important elements of the proposal include determining the filtering criteria; they must be restricted to content that is liable to result in serious damages to the development of minors. At the same time, the filtering should not block content serving contrary

purposes (e.g. victim helping, education and information sites). Therefore, if the proposal is accepted, the greatest emphasis must be put on developing adequate filtering criteria.
Rather than implementing that system through statutory legislative instruments, consultations should be held with Internet access providers in order to assess the potential benefits and drawbacks of filtering on the basis of a system of voluntary contracts between the competent government body and the service providers. On PCs used by children at public education institutions, it is possible to implement network-level filtering more easily and with a lot fewer concerns related to fundamental rights. The sole purpose of this strategy is to prepare a potential agreement, and lay the foundations of a final decision on the matter.

Measures (actions) related to the group of tools:

a2.2.1) Review and assessment of the practical experiences of international solutions using network-level filtering measures as a default setting.

a2.2.2) Identifying and considering the potential consequences and potential effects of implementing network-level filtering measures as the default setting in Hungary.

a2.2.3) Holding consultations with providers of communications services on issues related to using network-level filtering measures as a default setting, the potentials of implementing that system in Hungary and, if appropriate, putting forth a proposal to the Government with regard to the measures required.

a2.2.4) Regarding hotspot services provided by public education institutions and municipal governments, reviewing the possibility of finding an efficient solution to ensure that minors with an Internet access should not be able to access content that is harmful for them and that Safe Internet Service for Children should be provided on the PCs used be children at public education institutions.

*E2.3) Extending the range of application of efficient technical solutions*

In order to restrict access by children, the use of efficient technical solutions should be extended to online content not subject to the media legislation (Act CIV of 2010 and Act CLXXXV of 2010) (i.e. online content services that are e-commerce services under Act CVIII of 2001). On the basis of foreign models, the following proposals can be put forward for age verification in order to ensure a truly efficient use of technical

solutions:

- With regard to the warning on content harmful to minors, the content provider should display a standard warning (whose text is specified by the law) giving information on the content on the site that is harmful to minors, verifying the age of visitors and providing free access to the filtering software solution (see the recommendation of the Media Council on efficient technical solutions);
- Through a credit card or other payment method able to sufficiently demonstrate the card holder's age;
- By using reliable and authentic databases similar to the electoral register (although the use of government databases set up for other statutory purposes raises serious data protection concerns, which should be managed by legislation where appropriate);
- Through the demonstration of a mobile phone subscription available for holders of identification documents (e.g. an ID card or a driving licence) only;
- By the use of personal identification numbers.

The statutory use of such solutions would require an amendment to Act CVIII of 2001 which would enable administrative action against service providers offending the law (i.e. failing to use an appropriate solution). Obviously, that legislation may only apply to content services under Hungarian jurisdiction. While that alone may significantly decrease the accessibility of harmful content by children, such solutions are stipulated by a number of European countries, i.e. the tightening of rules would also be beneficial in terms of the integration of action on European level. Consequently, the justification of a potential amendment to Act CVIII of 2001 must be considered in terms of the mandatory stipulation of the use of efficient technical solutions. At the same time, the current provisions of Act CLXXXV of 2010, on the basis of which the 'efficient technical solution' applicable to on-demand video services is specified by a recommendation of the Media Council need not be amended due to their flexibility.

Measures (actions) related to the group of tools:

a2.3.1) Assessing international experiences concerning the efficient technical solutions applied with regard to online content services hazardous to the development of children and identifying the most efficient solutions.

a2.3.2) Holding consultation with providers of communications services and the trade associations of content providers with regard to various aspects of the implementation of the efficient technical solution.

a2.3.3) As far as content harmful to minors is concerned, considering the justification of a potential amendment to Act CVIII of 2001 in order to enable a standard warning.

*E2.4) Managing hazardous and recommended content (blacklist and whitelist)*

*A)* INTERPOL '*Worst of' list*

In 2009, member countries of the General Assembly of the International Criminal Police Organization (INTERPOL) unanimously voted for a resolution on combating the online sexual abuse of children (child sexual abuse images). The resolution encourages member countries to use all available technical tools to promote the blocking of websites included in the list published by the INTERPOL. The INTERPOL is responsible for compiling, updating and making available to member countries a so-called 'Worst of' blacklist.

On the basis of the above, the INTERPOL disseminates the blacklist to Internet access providers it has concluded a contract with and operating in its member countries. Based on the agreement concluded with the INTERPOL, in their networks, service providers block access to those websites containing child pornography that are included in the list.

On 1 December 2011, the Hungarian Telenor, the ORFK and the NMHH signed a memorandum of understanding with a view to creating the safe use of the Internet by children and preventing the online dissemination of content including child pornography. In the meaning of the agreement, as from 1 January 2012, Telenor Hungary blocks, on its network, the websites included in the blacklist compiled and continuously updated by the INTERPOL, which are restricted to child pornography. Telenor Hungary receives the blacklist from the INTERPOL through its parent company.

According to feedback and points of view of non-blocking service providers, in the absence of a clear statutory obligation or a relevant order by a court or other authority, it is unlawful to block any site included in the list. Therefore, such service providers have refused to block sites on a voluntary basis until the legislative criteria of blocking are specified.

If Hungarian Internet access providers blocked, on a mandatory basis, the sites included in the 'Worst of' list compiled by the INTERPOL or they were at least explicitly enabled by the applicable legislation to carry out such filtering activity, it would represent a significant step forward in terms of battling online child pornography.

On 30 June 2015, an agreement was reached between the European Council, the European Parliament and the European Commission on legislation by the TSM [Telecom Single Market – Regulation (EU) 2015/2120 of the European Parliament and of the Council]. On the basis of the new legislation, in effect since 30 April 2016, Internet access providers must not implement any traffic control

measures that go beyond the provisions of the draft legislation, i.e. they are not allowed to block to INTERPOL list. Under the new legislation, service providers are only allowed to block content in order to comply with applicable Union and national legislation.

Subject to the above provisions of the TSM Regulation, Act C of 2003 must be amended in order to enable Hungarian service providers to legally block child pornography content included in the list published by the INTERPOL, i.e. to filter for the 'Worst of' list. The amendment of legislation would authorise providers of electronic communications services providing access and search engine and cache providers to block any websites specified in the list maintained by the INTERPOL in order to enable the blocking of child pornography content.

Since each of the websites and content featured on the list published by the INTERPOL constitute a criminal case, their blocking is possible also on the basis of the current legislation under the Act on Criminal Proceedings. However, due mainly to the fact that the police and the courts are only able to handle these cases on an individual basis, the blocking procedure cannot be implemented in an efficient manner that is working properly in practice. Since the fundamental objective of criminal proceedings is to investigate and demonstrate crimes under Hungarian jurisdiction and to call perpetrators to account, the blocking of content through criminal proceedings is an inappropriate method for the mass banning of such content and URLs.

In order to enable the simple blocking of such content, Act C of 2003 must be amended appropriately.

*B)* Blacklist, whitelist and content categories related to the filtering software

Compiling and keeping updated the lists including harmful and useful websites, content categories and the lists of related keywords may be greatly conducive to the efficient operation of filtering software. Therefore, it is of key importance that they should be compiled and kept regularly updated. Such lists are required for the use of the filtering software referred to in paragraph 2.2.2 C1 of the system of tools and objectives and for determining the settings required.

Measures (actions) related to the group of tools:

a2.4.1) Compiling and regularly revising the blacklist and the whitelist.

a2.4.2) Conducting consultations required in order to implement the INTERPOL 'Worst of' list.

a2.4.3) Amending Act C of 2003 in order to enable providers of electronic communications services providing access and search engine and cache providers to legally block websites featured on the INTERPOL list, subject to the TSM Regulation.

*E2.5) Strengthening co-regulation by the industry*

*A)* Co-regulation by Internet access providers

Providers of Internet access currently engage in various activities in terms of promoting the conscious use of the Internet by children, preparing parents and making available software and applications enabling the safe use of the Internet. The government has to find a way to encourage the industry, including in particular Internet access providers, to take a more efficient and more integrated part concerning their social responsibility related to the conscious use of the Internet, through co-regulation, among other methods. Obviously, it requires that the relevant trade associations should also get involved in the standardisation of service providers' activities related to the safe use of the Internet.
In order to strengthen self-regulation and co-regulation, it would be worth considering the government recompensing efficient cooperation by service providers in the field of child protection by granting certain advantages. To that end, one of the tasks set out by the strategy is to consider the possibilities for setting up a co-regulation system and to commence discussions between the government and industry stakeholders with a view to setting up a new system of co-regulation.

*B)* Co-regulation by media content providers

In media legislation, a certain co-regulation model already exists, i.e. Act CLXXXV of 2010 enables the Media Council to relegate the supervision of compliance with certain statutory requirements applicable to on-demand media services and online publications into the competence of co-regulation bodies (see paragraph 3.3.1 of the Situation assessment). While the procedures of co-regulation bodies are provided for by codes of conduct, such rules of procedure are rather complicated and are difficult to use in practice. Therefore, the rules in question should be amended and the procedure should be streamlined to a significant extent. Hovwever, that can only be achieved by amending the agreement between the Media Council and the trade associations responsible for co-regulation.
The requirement of strengthening co-regulation mechanisms, including in particular in the field of child protection, is also encouraged by the European

Union and, therefore, it is set out in a proposal issued in May 2016 by the European Commission for amending the AVMS Directive. Since the point of the procedure by co-regulation bodies is efficiency and speed, it may be advisable to simplify and revise the rules of procedure in a manner that enables a more extensive enforcement of child protection provisions.
Moreover, it should be considered that co-regulation bodies should review, regularly and not only when a complaint is received, whether the functioning of Internet services controlled by their members complies with the applicable child protection rules (the Authority may co-finance such activity while the organisations concerned should submit a regular report on the outcome of their review). An agreement on the above issues may be concluded by amending the contracts between the Media Council and the co-regulation bodies.

Measures (actions) related to the group of tools:

a2.5.1) Conducting consultations with the trade and self-regulation associations of Internet access providers with a view to enabling the definition of the foundations for a potential new co-regulation system.

a2.5.2) Requesting the Media Council to draw up an initiate the amendment of co-regulation contracts with the trade associations of media content providers in order to simplify the rules of procedure applied in such contracts.

*E2.6) Emphasising the ultima ratio role of criminal law*

It is important to emphasise to the persons involved in preventing online hazards and managing problems (i.e. parents, head teachers, teachers, child protection experts, child psychologists and law enforcement officials) and to make them aware of the fact that criminal law should only be an ultimate solution (*ultima ratio*) in terms of assessing online deviancies among children, including in particular bullying and cyberbullying cases. One of the reasons for the above is that, very often, bullying and cyberbullying constitute a preparation for or a means of more serious acts, of which the wilfulness of only the less serious ones can normally be demonstrated. In cases occurring among schoolchildren, however, schools as the place of socialisation are responsible for resolving and preventing such cases. In Europe and in other parts of the world, there are a number of solutions that give priority to education and sanctions imposed at school level and related to education over the criminalisation of youth. According to studies in criminology, punishment involving imprisonment for juvenile crime has no preventive effect; moreover, criminalising youth can become

the antechamber of adult criminality.
The criminal and civil law provisions of Hungary ensure that sanctions are threatened against more serious acts bordering bullying (even if not bullying itself) and acts constituting a preparation for or a means of more serious acts. As an independent offence, bullying would criminalise acts prior to the situation arising as a result of acts provided for under the current definition of offences. These are abstract hazards where even a potential intention to cause harm cannot be ascertained in many cases. Moreover, since these types of behaviour are quite common with the generation concerned, it would lead to a mass criminalisation of young people, which is not justified and is even explicitly discouraged by criminal policy, pedagogy and prevention considerations.
While the current level of criminalising bullying as a preparation for or a means of more serious crimes should be maintained, legal practice should by all means be developed in order that acts committed in preparation for or used as a means of committing more serious crimes fit into existing descriptions of offences.
To that end, training and upskilling must be provided to persons working at various levels of the system of administration of justice, their skills must be continuously updated with regard to the new uses of media (i.e. how and for what purposes websites, smartphones etc. are used by young people) and to the phenomena of bullying and cyberbullying. In that respect, law enforcement personnel be essentially aware of the persons involved in and the dynamics of bullying, the intentions behind the acts and the objectives of and options for remedying and sanctioning actions. Members of the investigation authority must be trained to identify actions falling into the category of bullying when such acts are reported, to properly qualify the reported acts and properly inform (instruct) victims and to become familiar with the operation of organisations providing assistance.
Experts should assume a role in disseminating information to the public concerning non-governmental initiatives offering alternatives promoting the conscious use of the Internet in addition to precautionary measures. The new opportunities offered by start-up companies must be mapped and information on these opportunities must be disseminated to institutions, teachers and parents.

Measures (actions) related to the group of tools:

a2.6.1) Developing programmes for the training and upskilling of judicial and police employees and people working at the public prosecutor’s office, specialising in crimes or other offences against children.

a2.6.2) Conducting surveys concerning the practical application of criminal law provisions for the protection of children and adjusting the further training of law enforcement workers to the results of such surveys.

*E2.7) Supporting the production of safe and useful content for children*

*A)* Supporting children-friendly online content

Experience has shown that adults often turn a deaf ear to the online mental injuries of children. The media has a major role in identifying and managing the problem; the content released in the media should facilitate everyday awareness-raising. The issues under review point toward the conscious use of the media (information security, data management, data security and the responsible and ethical use of the media) at least as much as to the acquisition of information skills (i.e. hardware and software skills, encoding and the use of tools). Support must be given to the creation of media content focusing on the conscious use of the media; the production of regularly released programmes that speak to children and the adults (parents and teachers) responsible for the healthy development of children in a clear, easily intelligible and practical manner.

Children should be guided towards contents produced specifically for them or which may be used in the course of their typical activities. Of content produced by children, those that create value in the long term should also be supported.

This is facilitated, among others, by popularising and advertising the relevant websites on other sites, on the radio and in the printed press, which may help disseminate the information to children, the target group of such information.

Alternatively, teachers or parents may also inform children of such content. For example, a teacher hands out to students a list of websites they might find useful for their studies.

As another school assignment, children may be informed of the URLs of the recommended websites as part of general information.

Children-friendly websites must be created and children must be informed of such sites. The production of such websites must be supported centrally, in an organised manner, through a competition procedure where appropriate.

As far as their content is concerned, they may be sites containing games and entertainment, skills development content, websites providing information on children’s rights, sites providing assistance and information, educational sites that assist learning and sites supporting playful interactive learning and the acquisition of information.

Practically, the websites designed specifically for children should contain hyperlinks to similar sites in order to enable children to navigate from one content to another.

Such content may be co-financed from various sources, including in particular the MTVA’s Hungarian Media Sponsorship programme and the competition system of the National Cultural Fund. These decision-making bodies should be

requested to regularly publish tenders for the production of children-friendly online content promoting media education.

*B)* The role of public-service media

On the basis of Section 83(1)(h) of Act CLXXXV of 2010, as a public-service media provider, the Duna Médiaszolgáltató Nonprofit Zrt. is required to release programme items serving the physical, mental and moral development of minors, satisfying their interests and enriching their knowledge and educational items for the protection of children. The MTVA, supporting the operation of the former, cooperates on the above activities. The media provider currently fulfils that obligation primarily through the m2 linear audio-visual media service, and the on-demand online service of the channel.
Moreover, it should be considered in what ways public-service media organisations could possibly get involved more efficiently in raising awareness among children concerning the use of the Internet, primarily by using public media websites for the purpose. The independence of public-service media from the government must, however, be maintained. That strategy aims at the mapping of possible ways of cooperation between government bodies responsible for online child protection and the public-service media, which may be manifested as specific action in the form of agreements between the parties concerned.

Measures (actions) related to the group of tools:

a2.7.1) Drawing up support programmes for the production of online content designed specifically for children.

a2.7.2) Initiating a transformation of the Hungarian Media Sponsorship programme in order to enable the financing, from existing funds, of the production of online content designed specifically for children and increasing their level of media education.

a2.7.3) Requesting the Duna Médiaszolgáltató Nonprofit Zrt. and the system of public-service media to order and produce more content aiming to increase children’s level of media education, primarily in order to use such content on public-service media websites.

### *3.2.3 Applying sanctions and providing help*

*E3.1) Regular monitoring and database building*

It remains a substantial problem that no complete and up-to-date data and information are available on a continuous basis that would enable the drawing of inferences concerning the number, tendencies and effects of online offences (including crimes) against children. Most offences remain hidden, due in part to the victims' ignorance of their rights. Therefore, it is important that the cases and procedures reaching the administrative bodies, authorities and the police, their results and numerical ratio are accessible. That could become an efficient tool of the fight for the protection of children, which may reveal the areas where the government or even businesses or NGOs should take an increased role.
With regard to the above, regular reviews and research must be conducted concerning the presence, in our society, of online offences committed by and against children and the results of that research must be properly assessed.
Creating an opportunity for anonymous reporting would represent another possible solution for clearing up the latency.
That database should then be linked to basic longitudinal quantitative and qualitative studies by comparative analysis.

Measure (action) related to the group of tools:

a3.1.1) Reviewing the practical serviceability of data gathered in the existing system of criminal statistics concerning online crimes committed by or against children and achieving that such data should be comprehensive.

*E3.2) Restorative grievance management*

As an alternative form of dispute resolution, in addition to legal procedures (see, for example, the mediation procedure applicable in criminal proceedings), conciliation procedures may currently be conducted at educational institutions. The advantage of such procedures is that they involve very few people other than the ones directly concerned, whereas they enable the remedying of offences committed in a lot faster and more efficient manner compared to the lengthy formal procedures which often have serious harmful effects to both victims and perpetrators.
The range of application of such mechanisms, designed primarily to restore and remedy the offences committed, must be expanded and the experiences gained so far in connection with the rules of procedure must be utilised.

In terms of providing assistance to victims, cooperation is required between government bodies, NGOs, parents and teachers, while the conditions of a child-friendly administration of justice must also be ensured and its requirements must be adhered to.
A reparation procedure based on personal apologies and the recovery of damages is the most efficient method in order to dissuade people from committing further crimes. To that end, in the case of bullying-type deviancies in juvenile persons, in addition to the reparation procedure enabled by Act C of 2012 (in harassment cases, for example), the persons involved in prevention (e.g. schools) must also be able to start mediation outside the field of criminal law. Teachers and schools must be given proper information on the availability of alternative conflict management procedures and the NGOs and experts providing such services.
The various conducts qualifying as bullying or cyberbullying also need to be regulated outside criminal law, i.e. in the law of management and education. The point of such regulation is to increase the responsibility of schools and, as a long-term objective, to require schools to implement an anti-cyberbullying programme or at least a programme to promote the safe use of the Internet, to prepare, in their everyday practice, for managing online hazards in the form of internal protocols and special policies and to adopt an appropriate prevention strategy in order to ensure the peaceful co-existence of students and teachers according to predictable rules. In cases of cyberbullying, school protocols must also set out the procedure to be followed, possible administrative responses as well as civil law and criminal law consequences as the ultimate solution.

Measures (actions) related to the group of tools:

a3.2.1) An assessment of which harmful situations may be managed by rules of procedure that are more efficient and more appropriate to children in comparison with the tools of criminal law; a recommendation concerning such cases and the procedures proposed must be put forward to public-education institutions.

a3.2.2) Developing the legislative background related to the management of injurious situations primarily at educational institutions and preparing the required amendments of legislation.

a3.2.3) In order to achieve the professional coordination of restorative grievance management and to provide the required consultation, the involvement of the relevant professional associations of teachers, to assist with the development of anti-cyberbullying protocols and policies and the exchange of ideas and to promote professional dialogue.

*E3.3) Tasks related to the management of cyberbullying*

The government administration level, NGOs and the business/industry level must develop a common strategy. A common denominator must be found that will motivate all three potential stakeholders in the field of digital child protection to reach the same goal, not competing with each other but sharing competencies and tasks in order to achieve a safer use of digital devices by children.
The roles and duties of the administration of justice, educational institutions and the community, including society and parents, must be separated and clarified in the field of preventing and managing bullying. Programmes against cyberbullying have only proven successful where the school as a whole, the local community and parents have been actively involved.
The assistance provided and awareness-raising carried out by NGOs are based on grant-based projects that do not provide financing for operation. This makes it more difficult to provide high-quality assistance on an ongoing basis. Grants are only awarded to cycles and innovative new initiatives, which renders the operation of assistance services more difficult. By achieving a more structured allocation of existing grants, the government should support NGOs (working on awareness-raising and assistance) in order to enable them to cooperate. Funds must be created for the financing of operation, which will be conducive to the survival of established best practices.

Measures (actions) related to the group of tools:

a3.3.1) Creating and operating programmes to manage and prevent online harassment and cyberbullying, in line with existing programmes and drawing on their professional content and experiences.

a3.3.2) Working out a detailed action plan based on the experiences of existing anti-cyberbullying programmes in order to reduce the number of offences.

*E3.4) Activities related to disseminating information on existing legal remedy mechanisms*

It poses a problem if existing procedures and opportunities for managing grievances are not widely known. Experience has shown that the efficiency and desired impact of legislation is lost where victims of an offence are unaware of the relevant opportunities available to them. Examples to the above include the application of the relevant provisions of Act C of 2012 as well as other Internet-specific provisions of

the legal system. On the basis of Section 4/A of Act CVIII of 2001, service providers shall not release any information harmful to the development of children unless such information is accompanied by a warning on the potential hazards to children and identifiers in the source code of the page that the filtering software is able to recognise. Moreover, since 2013, it has been possible, based on Section 13(13) to (15) of Act CVIII of 2001, among others, to remove content breaching the privacy of children from the Internet in a simple and efficient manner. While that is in addition to the options offered by civil and criminal procedures, no such requests have been received by the Child Protection Internet Round Table, acting under Act CVIII of 2001. That provision was formulated in order to manage an extremely serious and, as experience has shown, frequently occurring problem. Its broader practical application would require:

- A review of the procedural rules of Act CVIII of 2001 and the amendment of such rules where appropriate, in respect of the right to self-determination;
- Concluding agreements between Internet access providers and the appointed government body, setting out the decisions and requirements concerning practical issues arising in the course of applying such provision of Act CVIII of 2001;
- Disseminating information to a broader public among children, parents and teachers, through media education and in public awareness campaigns.

Measures (actions) related to the group of tools:

a3.4.1) Producing and delivering to schools educational and information materials on the provisions of Act CVIII of 2001 designed to protect children and concerning the enforcement of consumer rights in e-commerce and making available, on the websites of each public education institution, up-to-date information concerning legislation applicable in the field of online child protection, other protective measures and the programmes to increase media education.

a3.4.2) Conducting programmes and activities in order to disseminate information to a wider public concerning the provisions of Act CVIII of 2001 and the Internet Hotline service.

# LIST OF ACRONYMS AND ABBREVIATIONS

*AJBH* – Office of the Commissioner for Fundamental Rights

*Ajbt.* – Act CXI of 2011 on the Commissioner for Fundamental Rights

*AVMS Directive* – Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive, codified version)

*Be.* – Act XIX of 1998 on criminal proceedings

*Btk.* – Act C of 2012 on the Criminal Code

*Eht.* - Act C of 2003 on electronic communication

*E-Commerce Directive* – Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

*Ekertv.* – Act CVIII of 2001 on certain issues concerning e-commerce services and services related to the information society

*ENYÜBS* – Uniform Criminal Statistics of the Investigation Authorities and Public Prosecutor's Office

*Fgy. tv.* – Act CLV of 1997 on the protection of consumers

*Gyvt.* – Act XXXI of 1997 on the protection of children and the administration of guardianship services

*Infotv.* – Act CXII of 2011 on the right of individuals to control their personal information and the freedom of information

*Köznev. tv.* – Act CXC of 2011 on national public education

*Media Council* – The Media Council of the National Media and Infocommunications Authority

*Mttv.* – Act CLXXXV of 2010 on media services and mass communication

*MTVA* – Media Support and Asset Management Fund

*NAIH* – National Authority for Data Protection and Freedom of Information

*NAT* – Basic National Curriculum

*NMHH* – National Media and Infocommunications Authority

*Ptk.* – Act V of 2013 on the Civil Code

*Smtv.* – Act CIV of 2010 laying down basic rules for the freedom of the press and media content

*Szabs. tv.* – Act II of 20102 on infringement, infringement proceedings and the system of registration of infringements

# ANNEX

## Annex 1 – Statistical data on the practice of cyberbullying[1]

Procedural data, 2015

| Act IV of 1978 | Act C of 2012 | Number of procedures | *Of which* | | | | |
|---|---|---|---|---|---|---|---|
| | | | *Denunciation dismissed* | *Investigation terminated* | *Charges raised* | *Other outcome* | *Diversion* |
| Coercion, Section 174 | Coercion, Section 195 | 539 | 149 | 283 | 68 | 33 | 6 |
| Harassment, Section 176/A | Harassment, Section 222 | 16,799 | 4,741 | 7,924 | 2,572 | 631 | 931 |
| Misuse of personal data, Section 177/A(1)(a) | | 118 | 9 | 23 | 81 | 0 | 5 |
| | Misuse of personal data, Section 219(1)(a) | 1,288 | 247 | 213 | 674 | 132 | 22 |
| Breach of the confidentiality of correspondence, Section 178(1) | Breach of the confidentiality of correspondence, Section 224(1) | 36 | 13 | 18 | 1 | 4 | 0 |
| Invasion of privacy, Section 178/A(1) and (2) | | 1 | 0 | 1 | 0 | 0 | 0 |
| | Illicit access to data, Section 422(1) | 66 | 23 | 22 | 12 | 9 | 0 |
| Libel, Section 179 | Libel, Section 226 | 336 | 84 | 139 | 59 | 36 | 18 |
| | Producing a fake image or audio or video recording liable to damage another person's reputation, Section 226/A | 1 | 0 | 1 | 0 | 0 | 0 |

[1] The data derive from the Uniform Criminal Statistics of the Investigation Authorities and Public Prosecutor's Office. It is a so-called 'follow-up statistics', which reports on the number of concluded proceedings in each case. Data are listed in the database in the order of statistical registration, not by the date on which an act is committed. The figures reflect the situation of data as at 12 July 2016.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Publishing a fake image or audio or video recording liable to damage another person's reputation, Section 226/B | 10 | 0 | 3 | 1 | 5 | 1 |
| Defamation of character, Section 180 | Defamation of character, Section 227 | 1,323 | 99 | 272 | 818 | 69 | 65 |
| Humiliation of a defenceless person, Section 180/A | Humiliation of a defenceless person, Section 225 | 9 | 5 | 3 | 1 | 0 | 0 |
| Breach of an information system or data, Section 300/C(1) | | 58 | 1 | 38 | 18 | 0 | 1 |
| | Breach of an information system or data, Section 423(1) | 622 | 64 | 179 | 64 | 280 | 35 |

Registered crimes – victims, 2015

| **Act IV of 1978** | **Act C of 2012** | **Number of registered crimes** | **Number of natural victims known** | ***Of which against persons under 18*** | ***Of which*** |
|---|---|---|---|---|---|
| | | | | | ***Committed using IT equipment*** |
| Coercion, Section 174 | Coercion, Section 195 | 120 | 120 | 35 | 1 |
| Harassment, Section 176/A | Harassment, Section 222 | 7,253 | 7,255 | 437 | 43 |
| Misuse of personal data, Section 177/A(1)(a) | | 89 | 16 | 0 | 0 |
| | Misuse of personal data, Section 219(1)(a) | 838 | 0* | 0 | 0 |
| Breach of the confidentiality of correspondence, Section 178(1) | Breach of the confidentiality of correspondence, Section 224(1) | 18 | 16 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| Invasion of privacy, Section 178/A(1) and (2) | | 1 | 1 | 0 | 0 |
| | Illicit access to data, Section 422(1) | 22 | 19 | 1 | 1 |
| Libel, Section 179 | Libel, Section 226 | 181 | 176 | 7 | 0 |
| | Producing a fake image or audio or video recording liable to damage another person's reputation, Section 226/A | 1 | 1 | 0 | 0 |
| | Publishing a fake image or audio or video recording liable to damage another person's reputation, Section 226/B | 6 | 6 | 1 | 1 |
| Defamation of character, Section 180 | Defamation of character, Section 227 | 1,078 | 1,077 | 74 | 0 |
| Humiliation of a defenceless person, Section 180/A | Humiliation of a defenceless person, Section 225 | 4 | 4 | 1 | 0 |
| Breach of an information system or data, Section 300/C(1) | | 25 | 10 | 0 | 0 |
| | breach of an information system or data 423. | 406 | 0* | 0 | 0 |

* On the entry into force, on 1.7.2013, of Act C of 2012, the ENyÜBS stopped collecting victim data.

Perpetrators, 2015

| Act IV of 1978 | Act C of 2012 | All registered perpetrators | *Of which persons under 18* | *Of which* | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | *Denunciation dismissed* | *Investigation terminated* | *Charges raised* | *Other outcome* | *Diversion* |
| Coercion, Section 174 | Coercion, Section 195 | 52 | 13 | 3 | 3 | 6 | 0 | 1 |
| Harassment, Section 176/A | Harassment, Section 222 | 2,806 | 120 | 5 | 58 | 33 | 7 | 17 |
| Misuse of personal data, Section 177/A(1)(a) | | 3 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Misuse of personal data, Section 219(1)(a) | 35 | 3 | 0 | 2 | 1 | 0 | 0 |
| Breach of the confidentiality of correspondence, Section 178(1) | Breach of the confidentiality of correspondence, Section 224(1) | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Invasion of privacy, Section 178/A(1) and (2) | | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Illicit access to data, Section 422(1) | 8 | 0 | 0 | 0 | 0 | 0 | 0 |
| Libel, Section 179 | Libel, Section 226 | 55 | 14 | 0 | 9 | 3 | 0 | 2 |
| | Producing a fake image or audio or video recording liable to damage another person’s reputation, Section 226/A | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Publishing a fake image or audio or video recording liable to damage another person’s reputation, Section 226/B | 2 | 1 | 0 | 0 | 0 | 0 | 1 |
| Defamation of character, Section 180 | Defamation of character, Section 227 | 377 | 34 | 2 | 18 | 11 | 2 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Humiliation of a defenceless person, Section 180/A | Humiliation of a defenceless person, Section 225 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Breach of an information system or data, Section 300/C(1) | | 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Breach of an information system or data, Section 423(1) | 59 | 14 | 0 | 12 | 0 | 0 | 2 |

The tables include cases corresponding to various acts qualifying as cyberbullying. They include: coercion, harassment, misuse of personal data, breach of the confidentiality of correspondence, invasion of privacy, illicit access to data, libel, producing and publishing a fake image or audio or video recording liable to damage another person's reputation, defamation of character, humiliation of a defenceless person, breach of an information system or of data and certain acts qualifying as illicit access to data.

The Uniform Criminal Statistics of the Investigation Authorities and Public Prosecutor's Office (ENyÜBS) do not provide a full picture on the widespread nature of cyberbullying, for the following reasons.

- Act C of 2012 does not provide for all acts qualifying as cyberbullying; less serious acts of cyberbullying, such as online ostracism or the posting of offensive or humiliating messages fail to reach a level of danger to society that would justify the criminalisation of such acts. At the same time, their criminalisation should also be avoided as such acts typically occur among young people or children (i.e. during the years of primary and secondary school), and criminology studies do not recommend sanctioning at such an early age, due to the danger of stigmatisation.
- The cases registered in the ENyÜBS database constitute the tip of the iceberg, i.e. most acts of cyberbullying remain hidden. This may be due to the fact that minor victims fail to mention such acts to adults or that the surrounding adults fail to report such acts to the police.
- While the system enables the sorting of acts committed using 'IT equipment', within that category, it does not enable differentiation between offences committed using a computer or mobile devices and online offences (committed by email or on social media pages). While all online acts are probably committed using IT equipment, this is not true the other way round, as

acquiring a mobile phone and deleting, modifying or tampering with the data stored on the mobile phone are not necessarily carried out online. Acts qualifying as cyberbullying are generally committed in online communication (on social media pages, websites, instant messaging applications etc.). The ENyÜBS, however, does not enable a finer breakdown in order to verify the volume of online acts.

- The ENyÜBS does not enable the establishing of a link between perpetrators and victims. While the criminal statistics include a breakdown by victims, i.e. the acts against minors (persons under 18) can be sorted, the statistics of perpetrators enable the sorting of juvenile perpetrators yet it does not enable creating a classification to determine the number of cyberbullying acts committed by juvenile perpetrators against minors.

The difference between data of self-declaration-based surveys and acts found out by the authorities would constitute an estimated figure revealing the magnitude of acts that remain hidden. In Hungary, however, neither the statistics nor self-declaratory latency surveys are suitable for estimating the magnitude of cyberbullying acts between children (persons under 18 according to the UN Convention on the Rights of the Child). The sampling, sample sizes, the weighting of samples, the ages of children included in the samples, the acts to be reviewed and the method of formulating the questions do not enable a comparison between the results of latency surveys or a comparison with ENyÜBS data. Therefore, the best method of surveying the volume of cyberbullying acts between young people would be a research of criminal proceedings files, which has never been conducted in Hungary either.

Apart from official statistics, self-declaration-based latency surveys currently provide an indication of the widespread nature of cyberbullying. Of Hungarian surveys of cyberbullying, the relevant surveys include the TABBY (*Threat Assessment of Bullying Behaviour in Youth*) and the Anti-Cyberbullying programmes.

The TABBY in Internet[2], a complex programme conducted in primary and secondary schools in Budapest and in the provinces between 2011 and 2015, surveyed cyberbullying contamination among students aged between 10 and 18. In total, 600 students were involved in the 2013 survey. More than half of the respondents (59 %) had suffered some kind of moderate online abuse, about 5 % of which had been victims to cyberbullying on a weekly basis. One of the most important findings of the research was that notorious online bullies are, at the same time, both perpetrators and victims of offline bullying at school.

[2] http://tabby-hun.weebly.com/

The survey[3] of the Anti-Cyberbullying Programme was taken at two Budapest schools in spring 2014. An anonymous questionnaire was completed by 704 students aged between 10 and 18. According to the aggregated data, 22.2 % of respondents had been victim to while 20 % had committed peer bullying at school or cyberbullying. 7 % of secondary school students had been victim to some kind of cyberbullying specified in the survey, whereas the rate of victims was somewhat lower, i.e. 6.2 % among primary school children. A substantially higher ratio (10.2 %) of secondary school students confessed of having committed a cyberbullying act compared to primary school children (2 %). The two surveys identified the following types of cyberbullying:

- The victim has been ostracised from an online community by a company of friends;
- A personal secret or a photo of the victim has been shared online without his or her permission;
- Offensive messages have been posted in the victim's name, discrediting the victim in the eyes of his or her friends;
- Offensive, cruel gossip has been spread about the victim online;
- The victim has received intimidating online messages.

[3] http://www.megfelemlites.hu/#!felmeresek/cn5y