



Nemzeti Adatvédelmi és
Információszabadság Hatóság

KULCS A NET VILÁGÁHOZ!



A NAIH tanulmánya
a gyermekek biztonságos és jogtudatos internethasználatáról

3. kiadás

2025

KULCS A NET VILÁGÁHOZ!

A NAIH tanulmánya
a gyermekek biztonságos és jogtudatos internethasználatáról

(a gyermekek (jog)tudatos internethasználatának elősegítése
az alapjogi jogvédelem eszközeivel)

2025

A tanulmány célja:

A gyermekek internethasználatához kötődő veszélyekre való figyelemfelhívás, a jövő kihívásainak azonosítása, a tudatos internethasználat és joggyakorlás elősegítése az elméleti és gyakorlati kutatások eredményeinek felhasználásával

A tanulmánykötet létrehozásában közreműködtek:

Árvay Viktor
Bácskai Krisztina Mária
Belső Nóra
Eszteri Dániel
Kozma Laura
Lux Ágnes
Márkus Petra
Mátyásfalvi Attila
Ránki Sára
Reményiné Csekeő Borbála
Ságvári Bence
Sárközi Gabriella
Somfalvi Dániel
Somogyvári Katalin
Sziklay Júlia
Tordai Zsófia

Szerkesztette:

Sziklay Júlia

Harmadik kiadás, 2025
ISBN 978-615-82797-0-3

TARTALOMJEGYZÉK

1. Bevezető.....	5
2. A NAIH bemutatása	9
3. Magyar jogesetek	10
A. ADATVÉDELMI HATÓSÁGI GYAKORLAT	10
B. OMBUDSMANI GYAKORLAT	15
C. RENDŐRSÉGI GYAKORLAT.....	21
4. A magyar gyermekek internethasználati szokásairól.....	26
A. ÁLTALÁNOS TRENDEK	26
B. ISMERŐSÖK SZÁMA	34
C. AKTIVITÁS	35
5. A gyermekek jogai online környezetben	38
6. Kiemelt kérdések	45
A. ÉLETKOR ÉS ÉRETTSÉG	45
B. ANONIMITÁS – MASZKKAL KÖNNYEBB?.....	48
C. SZEMÉLYISÉGTORZULÁS	49
D. KÖZÖSSÉGI TEREK – ISMERETLEN ISMERŐSÖK	55
E. KÁROS TARTALMAK.....	60
F. KERESŐMOTOROK – INTERNETES „KAPUŐRÖK”.....	63
G. NYELVI PROFILOZÁS AZ INTERNETEN.....	63
H. A JÖVŐ FEJLŐDÉSI IRÁNYAI	68
7. Problématérkép – online devianciák.....	72
A. ONLINE ZAKLATÁS	73
B. INTERNETES KIBESZÉLÉS (MÉM KÜLDÉS).....	75
C. TROLLKODÁS	76
D. EROTIKUS KÉPEK KÜLDÖZGETÉSE (SEXTING)	76
E. AZ INTERNETES PEDOFÍLIA	78
F. ONLINE BEHÁLÓZÁS (GROOMING) ÉS AZ ONLINE RAGADOZÓK (PREDATORS)	79
G. „ÉGETÉS” (<i>FLAMING</i>)	81

H. ONLINE (SZEREP)JÁTÉKOK GYERMEKEKNEK	81
I. SZEMÉLYES ADATTAL VALÓ EGYÉB VISSZAÉLÉSEK ..	87
8. Jó gyakorlatok – külföldi példák	90
A. PORTUGÁLIA, DADUS PROJEKT.....	90
B. ÍRORSZÁG, „PRIVATE I, PUBLIC EYE” VIDEÓKLIP- VERSENY	91
C. SKÓCIA, „TISZTELJ ENGEM!” PROGRAM.....	92
D. NORVÉGIA, „TE DÖNTESZ!” KAMPÁNY.....	92
E. LENGYELORSZÁG: YOUR DATA – YOUR CONCERN PROGRAM.....	93
F. FRANCIAORSZÁG, „MORE RIGHTS FOR YOUR PERSONAL DATA”	93
G. SPANYOLORSZÁG, „PANDI PROJEKT”	94
H. ÚJ-ZÉLAND, GYERMEKJOGI PROJEKT.....	94
I. KANADA, KÉPREGÉNY ÉS TIPPEK.....	95
J. USA	96
K. UNIÓS PROGRAMOK	99
9. Baj esetén kihez fordulhatok?.....	104
10. „Magyar recept”	107
11. Online szótár – internetes kifejezések magyarázata.....	110

BEVEZETŐ

„Az internet nem jó és nem rossz – csupán jellemző. Tükör. Úgy tűnik, ami ennek révén keletkezik, nem radikálisan új. A hálólét öröklí a társadalmi lét megannyi nyugót és nyavalyáját.”

(Dr. Ropolyi László)¹

A számítástechnika, az internet, a telekommunikáció gyors fejlődése az elmúlt évtizedekben az élet szinte minden területén gyökeres változásokat indított el a világban. Az információs társadalom jelenségeinek alapja az információ szinte korlátlan bősége és terjedése. *„A jelenlegi technológiai forradalmat nem a tudás és az információ központi szerepe jellemzi, hanem a tudás és az információ alkalmazása további tudás és újabb információ feldolgozó és kommunikációs készülékek létrehozására².”* – írja Manuel Castells a hálózati társadalomról, amibe gyermekeink már beleszülettek, és ami a természetes kommunikációs közeget jelenti számukra.

A rendelkezésre álló kutatási adatok³ túlbecsülése nélkül is megállapítható, hogy a világhálón kommunikáló és szocializálódó ember – már csak az információk mennyisége okán is – általában érdeklődőbb, „kíváncsibb”, az újdonságok iránt nyitottabb, ugyanakkor kevésbé óvatos, mint az internetet nem használó embertársai.

A főleg gyermekekre koncentráló nemzetközi kutatások eredményei⁴ arra is felhívják a figyelmet, hogy az internetezőknél nagy az ún. kettős morál kialakulásának veszélye – a gyakori internetezők online normái megengedőbbek, kevésbé szigorúak, mint az offline világban ugyanazon személy által elismert szabályok – ez megnyilvánul a rendszeres, jogellenes szoftverletöltésekben, a durva chat-stílusban, a mások becsületébe gázoló kommentekben, vagy akár az online zaklatásokban, a közösségi „hálótársak” személyes adataival való visszaélésekben.⁵

1 Ropolyi László: Internethasználat és hálólét-konstrukció, in.: Információs Társadalom, VI(4), 39-46, 2006

2 Castells, Manuel: A hálózati társadalom kialakulása, Gondolat-Infonia, 2005, 68.o.

3 lásd: Csepeli György-Praszák Gergő: Internetezők az értékek vonzásában in.: Mit értékelnek a magyarok? Az Európai Értérend Vizsgálata 2008. évi magyar eredményei, szerk.: Rosta Gergely-Tomka Miklós, OCIPE Magyarország-Faludi Ferenc Akadémia, Bp., 2010, 187-204.o.

4 Például Isabelle Michelet: Our Children at Risk Online: The Example of Thailand., ECPAT International Bangkok, 2003

5 „a gyakran, hosszú ideig internetező gyerekekből hiányzik az empátia és az arcról olvasás képessége, nem tudják érzékelni az olyan finom jelzéseket, amilyeneket az ember nem verbálisan vagy írásban közöl és ez sok konfliktus alapja az offline kommunikáció során.” in.: Parti Katalin-Virág György: A szájbergerek és a bicikli. A kelet-európai gyerekek nethasználatának specifikumai, Kriminológiai tanulmányok 48., OKRIO Bp., 2011, 43.o.

Az új kultúra új viselkedésformákat alakít ki, amiket nekünk, felnőtteknek meg kell ismernünk, értenünk és az ebből fakadó esetleges veszélyekre fel kell tudnunk készíteni a következő generációt⁶ is. A gyermekekre leselkedő online veszélyekkel szerencsére nagyon sok program, kampány és szervezet foglalkozik Magyarországon is. Nem szabad azonban elfelejteni, hogy a „hálózatok hálózata” rengeteg előnyt is kínál a gyermekek számára. A 2013-as magyar nyelvi középiskolai felvételi feladatsor internethasználatra vonatkozó esszé feladatában 14 éves tanulók olyan válaszokat adtak, mint „Az internet nagyon fontos és hasznos az emberiség számára, mert manapság már mindent meg lehet rajta találni. Nagyon könnyen információkhoz, fontos dokumentumokhoz juthatunk segítségével. Az emberek nagy része – főként a tizenévesek – viszont tanulás helyett inkább a közösségi oldalakon való böngészéssel tölti az idejét”. A válaszok között szerepelt továbbá, hogy „Sokkal könnyebben szerezhetünk információkat és sokkal könnyebben tarthatjuk a kapcsolatot azokkal, akik messzebb élnek, de valószínűleg több haszontalan információt szerzünk, mint hasznosat, ha felmegyünk az internetre.”⁷

Az USA-ban már 2010-ben az internet vált a legfőbb információforrássá a fiatal felnőttek számára⁸, a magyar 14-19 éves gyermekek esetében ez az arány 48 %.⁹ Itt nincsenek terjedelmi vagy időkorlátok, sokszorosítási és egyéb külön költségek, bármilyen formátumú és minőségű információ tárolása és keresése „gyerekjáték”. Az építő jellegű szórakozáshoz, készségfejlesztéshez vagy barátkozáshoz is kiváló terep lehet a világháló, ha a felhasználás kulturált és biztonságos keretek között zajlik.

6 Y generáció: az 1976 és 1995 között születettekből álló új nemzedék, melyre a technológia száguldó fejlődése hatott, a Z nemzedék a világ első globális generációja, a mai tinédzserek, akik 1995-2009 között születtek.

7 Forrás: saját gyűjtés

8 a megkérdezettek 65 %-a internetes forrásokat idézett hírforrásként, ez az arány majdnem kétszerese a 2007-es adatoknak. Forrás: Pew Research Center study, 01-04-2011 in: <http://mashable.com/2011/01/04/internet-surpasses-television-as-main-news-source-for-young-adults-study/>

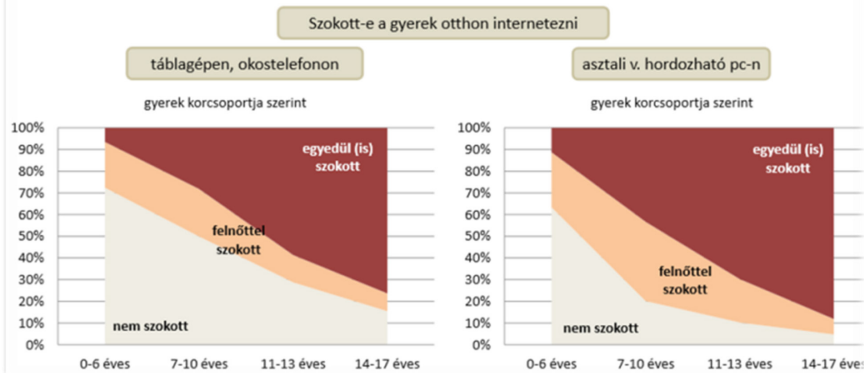
9 NMHH által megrendelt online piaci felmérés a lakossági internethasználatról, 2014 http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf 2016. február 12.

GYEREKEK INTERNETEZÉSE

Az internetezők 39%-a él olyan háztartásban, amelyben van 18 évesnél fiatalabb háztartástag.* E háztartások 85%-ában él olyan gyerek, aki internetezik otthon.

A 18 évesnél fiatalabb háztartástaggal élő vagy 14-17 éves internetezők (együtt az összes internetező 39%-a) körében:

- | | |
|---|-----|
| - van bármely eszközön internetező gyerek | 85% |
| - van táblagépen, okostelefon internetező gyerek | 68% |
| - van asztali v. hordozható pc-n internetező gyerek | 81% |



1.ábra: Az NMHH által megrendelt online piaci felmérés a lakossági internethasználatról, 2014¹⁰

Egy 2010-es, 10-18 éves gyermekek szokásait összehasonlító magyar tanulmány¹¹ következtetése szerint a minden nap „gépező” gyermekek célja fiú-lány megoszlásban leginkább a közösségi kapcsolattartás (47-53%), a szórakozás (46-37%), a játék (29-6%) és csak legvégül a tanulás (5-4%). Ugyanakkor azoknál, akik legalább hetente kapcsolódnak rá a netre, már a cél főleg a tanulás (40-50%), a szórakozás (37-45%), a közösségi tevékenység (32-35%) és a játék (43-26%).

Egy 2021-es felmérés adataiból megállapították, hogy a 15–50 éves korosztály tagjainak 97,1 százaléka rendszeresen használja az internetet. A 15 év alattiak körében még nem teljes körű az internethasználat, bár a rázkodás egyre fiatalabb korban kezdődik. A vizsgálatban részt vevő családok szerint a 2 éves gyermekek 4 százaléka már internetezik, míg a 3 évesek közül 9 százalék használja – viszonylag rendszeresen – az internetet.¹²

10 http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf 2016. február 12

11 Székely Levente: Internetszima az iskolapadon in.: új ifjúsági szemle 2010/tél, 79-87.o.

12 https://nmhh.hu/cikk/229984/Kiderultek_az_internetezesi_szokasok_a_2_eves_gyerek_es_a_85_eves_idos_ember_is_hasznalja_a_netet

A tanuláshoz kapcsolódóan keresőoldalakat szinte mindenki használ, elterjedtek az elektronikus szótárak és általános a Wikipédia használata is. Ritkán, de látogatottak a tematikus linkgyűjtemények és az oktatási segédanyagokat vagy dolgozatokat gyűjtő oldalak, illetve a különböző nyelvi és egyéb teszteket (pl. érettségi, felvételi tételsorokat) kínáló oldalak.

A netes kultúra hatással van a gyermekek, fiatalok szokásaira az élet szinte minden területén. Új szavak születnek (például *trollkodás, deleb, lájkolok*), új kommunikációs formákat használnak (levélírás helyett elektronikus üzenet, napló helyett blog, képeslap helyett MMS stb.), a világban történő események (legyen az kulturális – például egy fiataloknak szóló regény vagy dal megszületése, illetve egy kifejezett divatcikk) egyidejűleg hatnak rájuk – mindez alakítja gondolkodásmódjukat, viselkedésüket. Hangsúlyozzuk, hogy ez a változás szükségszerű és egyáltalán nem elítélendő. Ugyanakkor a tudatosság és óvatosság, a kritikai, jelenségek hátterét elemző hozzáállás mindenképpen előnyt jelent ezen a terepen.

Jelen tanulmány célja, hogy alapjogi – elsősorban adatvédelmi – szempontokkal járuljon hozzá a téma megfelelő és korszerű feldolgozásához és szándékaink szerint az elemzéseken túl gyakorlati eszközökkel is segítse a gyermekek online kultúrájának minőségi javítását. A megközelítés alapja, bázisa az adatvédelem anyajoga, az emberi méltóság, ami a magyar alapjogi értelmezés szerint sérthetetlen és korlátozhatatlan. Ha az internetet használó gyermek gondolkodásába beépül ez a stabil értékrend, akkor nem tesz olyat, amivel más méltóságát bánthatja, sőt, tudatosan fellép az őt érintő vagy a környezetében előforduló bántó jelenségek ellen és ezzel kiszolgáltatottsága is jelentősen csökken.

A pedagógusképzésben ma már mindenképpen szükség lenne az adatvédelem elkönyvelt oktatására, a naprakész és gyakorlati ismeretek szakszerű átadására annak érdekében, hogy a gyermekek felkészülten és tudatosan használják a modern IT technológia eszközeit és kiszolgáltatottság nélkül mozogjanak a digitális térben. 2016 márciusában a köznevelésért felelős minisztériumnál és a tanárképzés felsőoktatási központjainál kezdeményeztük, hogy a tanárképzés tematikájában kapjon helyet az adatvédelmi ismeretek oktatása is, ehhez a NAIH örömmel ajánlja fel tapasztalatait, szellemi termékeit és nemzetközi kapcsolatrendszerét is. Sajnos egyelőre a kezdeményezés és felajánlás nem hozta meg a várt eredményt.

A Kulcs a net világához! című NAIH kiadvány 2013-as első kiadásának sikere azt mutatja, hogy a gyermekekkel foglalkozó magyar szakemberek – pedagógusok, gyermekvédelmi szakemberek, segítő szervezetek – körében nagy az igény a tapasztalatok kicserélésére, a jó gyakorlatok megismerésére. Ezért született meg 2016-ban a második, bővített és frissített kiadás, majd 2025-ben az uniós adatvédelmi rendelet, a GDPR alkalmazásának tapasztalataira is reflektáló harmadik kiadás.

Dr. Péterfalvi Attila, a NAIH elnöke és Dr. Sziklay Júlia, a kötet szerkesztője

A NAIH BEMUTATÁSA

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) 2012. január 1-jén kezdte meg működését, de speciális jogvédő tevékenységét tekintve az 1995-2011 között működő adatvédelmi biztos munkáját folytatja. A GDPR¹³ független adatvédelmi felügyeleti hatóságokra vonatkozó rendelkezéseinek megfelelően, a magyar Alaptörvény értelmében és a vonatkozó törvény (Infotv.) rendelkezései szerint¹⁴ felelős állami szervként felügyeli a személyes adatok védelméhez (adatvédelem) és a közérdekű adatok nyilvánosságához (információszabadság) való alkotmányos jogok érvényesülését, fogadja az állampolgári panaszokat. Súlyos adatvédelmi jogsértések gyanúja esetén hatósági eljárást indíthat, melynek során határozatban elrendelheti a jogellenesen kezelt adatok zárolását, megsemmisítését, megtilthatja az adatok kezelését vagy akár húszmillió euróig terjedő adatvédelmi bírságot is kiszabhat¹⁵.

Az internet a személyes és közérdekű adatok kezelésének rendkívüli terepe, tekintettel az információk, az adatkezelések és az érintettek hihetetlenül magas számára és a korlátlan nyilvánosság erejére. A gyermekek adatainak védelme pedig kiemelt terület az adatvédők számára, hiszen itt koruknál és az ebből fakadó élettapasztalat hiányánál fogva az érintettek eleve kiszolgáltatottak, sebezhetőek és a jogsértések következményei személyiségfejlődésükre súlyosan kihathatnak. Az internettel összefüggő és gyermekeket érintő adatkezelésekre tehát az adatvédelmi hatóságnak egyértelműen sok gondot kell fordítania. A már megtörtént jogsértések orvoslása és az érintettek, valamint a közvélemény figyelmének felhívása mellett a megelőzésnek, felvilágosításnak óriási a szerepe. Jelen kiadványunk mellett egy nemzetközi projekt keretében így született meg 2015-ben több oktatási segédanyag is pedagógusok részére (Európai Kézikönyv a Magánszféra- és a Személyes Adatok Védelméről Iskolák Számára, valamint Adatvédelmi Kézikönyv Pedagógusoknak címmel). Kiadványaink szabadon letölthetők a www.naih.hu honlapról.

13 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

14 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

15 GDPR 83. cikk (5) bekezdés: Legsúlyosabb esetben a szankció legfeljebb 20 000 000 EUR összegű közigazgatási bírság, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg, azzal, hogy a kettő közül a magasabb összeget kell kiszabni.

A. Adatvédelmi hatósági gyakorlat

Korábban az adatvédelmi biztoshoz, majd 2012. január 1-től a NAIH-hoz mindig is sok panasz érkezett internetes visszaélésekkel kapcsolatban. A sértett személy életkorának ismerete hiányában is leszögezhető, hogy a személyhez fűződő jogok sérelme – a becsület és az emberi méltóság megsértése, jó hírnév rontása, képmással, hangfelvétellel való visszaélés, levéltitok, magántitok megsértése, adatkezelés és adatfeldolgozás során sérült személyhez fűződő jogok kapcsán keletkező viták – esetén a sérelmet szenvedett fél polgári peres eljárást kezdeményezhet a jogsértő személlyel szemben. Követelhető a jogsértés megtörténtének bírósági megállapítása, elégtétel adása, a jogsértés abbahagyása és a jogsértő eltiltása a további ilyen cselekménytől, valamint kártérítési igény is érvényesíthető. Rágalmazás, becsületsértés, visszaélés személyes adattal bűncselekmények esetén az eljárás a nyomozó hatóságnál tett feljelentéssel indul. Ezen kívül a sértettnek jogában áll a portál üzemeltetőjénél a rá vonatkozó és személyiségi jogait sértő hozzászólások, tartalmak eltávolítását kérni.

A legtöbb panasz tárgya, hogy a közösségi portálokon publikált személyes adatokat, fényképeket harmadik személyek más célokra használják fel. A személyes adatok jogellenes felhasználását jelenti, ha a honlapon egy másik személy nevében, annak tudta, és beleegyezése nélkül történik a regisztráció. Ugyanez a helyzet a gyalázkodó profilok esetében.

A NAIH álláspontja szerint a nyilvánosság a közösségi portál logikái felépítése szerint zárt körben értelmezhető. A regisztrált tagokon kívül álló személyek vagy szervek csak egy regisztrált tag közreműködésével ismerhetik meg a rendszerben közzétett személyes adatokat. Ez a fajta nyilvánosság azonban nem jelenti az adatok korlátlan felhasználhatóságát, mert a portálon közzétett adatok gyűjtése, rendszerezése, kezelése minden esetben adatkezelésnek minősül. A regisztrált felhasználó a közzétett adatokat meghatározott célból kezelheti, de csak az érintett hozzájárulásával vagy törvény felhatalmazásával továbbíthatja azokat harmadik fél számára.

Néhány konkrét ügy az adatvédelmi biztos gyakorlatából:

- A beadványozó barátja iWiW-en található arcképét felhasználták tudta és beleegyezése nélkül egy ezoterikus kötet borítójához. Mivel az érintettnek nincs kapcsolata a könyv témájával, másrészt egyetemi tudományos fokozatának védeke elött állva sem szívesen adná arcát a kiadványhoz, mindenképpen sérelmes volt számára a megjelenítés. (2534/P/2009)

- Egy édesanya azért fordult az adatvédelmi biztoshoz, mert gyermekéről felkerült egy fénykép a Facebook közösségi oldalra, amelynél egy becsmérő kifejezést tartalmazó címke volt látható. A szülő azt a kérdést tette fel, milyen módon távolíttathatja el ezt a képet a közösségi oldalról, illetve milyen módon vonhatóak felelősségre a fényképet nyilvánosságra hozó személyek? Az adatvédelmi biztos tájékoztatta a beadványozót arról, hogy a közösségi oldalt kiszolgáló szerverek nem Magyarország területén találhatók, ugyanakkor a Facebook rendelkezik központtal az Európai Unió területén (Írország-Dublin), ezért aláveti magát az európai közösségi jog joghatóságának és vonatkoznak rá azok az Európai Unió által elfogadott adatvédelmi rendelkezések, amelyek a magyarországi adatvédelmi szabályozás alapját is képezik. A gyermekről készült fénykép személyes adatnak minősül, annak közzététele tehát csak a gyermek, illetve törvényes képviselője hozzájárulásával jogszerű. A fénykép eltávolítását az érintett (illetőleg törvényes képviselője) kérheti a Facebook ügyfélszolgálatától (a fénykép alatt található „fénykép jelentése” menüpontra kattintva) és a körülményektől függően polgári, illetve büntetőper is indítható. (ABI-7949/2012/P).
- Egy másik szülő a középiskolás lánya néhány képét feltöltötte egy közösségi oldalra, de valaki a képeket névvel ellátva átmásolta egy nyilvános internetes portálra, ahol becsületsértő megjegyzések jelentek meg a képek mellett. Az édesanya írásban többször kérte a portál szerkesztőjét, hogy lánya összes adatát töröljék a honlapról. Az oldal üzemeltetője ezeket a leveleket is névvel-címmel megjelentette, cinikus, sértő, alpári hangnemben nyilvánosan válaszolt, továbbá több olyan olvasói levelet, kommentet közölt, amelyek szintén súlyosan sértették a bejelentő egész családjának jó hírnevét. (ABI-7041/P/2010).
- A panaszos egy szépségversenyre nevezett a MyVip közösségi portálon, az adatlapja mellé fényképeket is töltött fel. Egy ismerőse jelezte, hogy a www.puruttya.hu oldalon megtalálta őt pornográf képek mellett, amely rajta kívül további kilenc lányt is igen rossz hírbe hozott. Az oldal főszerkesztőjéhez címzett törlési kérelemre nem érkezett válasz. (ABI-4900/2010/P)
- Egy másik panaszos 16 éves leányának fényképeit leszedték a www.myvip.com oldalról, és feltették a www.pedomaci.hu oldalra teljes nevével, lakhelyével, életkorával, telefonszámával. Fenyegető leveleket kapott és telefonon zaklatták, valamint trágár kommentárokat fűztek a képeihez. Törlési kérelmére csak annyit válaszoltak, hogy „innen soha a büdös életbe nem fogsz lekerülni”. (ABI-4865/2012/P)
- Egy hasonló ügyben a szülő 15 éves lánya képviseletében írt az adatvédelmi biztosnak. Lánya közösségi oldalon szereplő személyes adatait és fényképeit feltöltötték a www.pedomaci.hu weboldalra, teljes nevével, lakóhelyével, életkorával együtt, és ízléstelen hozzászólásokat írtak hozzá. A beadványozó azért nem írt a honlap üzemel-

tetőjének törlési kérelmet, mert az maga buzdítja a felhasználókat törvénysértésre az alábbi módon: „Küldj be az interneten magukat kellettő 16 éves vagy annál fiatalabb csajokat (myvip vagy iwiw adatlap címet feltétlen írd)! Ha felkerültél az oldalra, és emiatt szomorú vagy, írd nekünk, és talán levesszük a képeidet az oldalról. Mivel bunkók vagyunk, és a szép szóból nem értünk, minél inkább mocskolódsz, annál biztosabb, hogy sikerrel jársz!” (ABI-4841/2012/P)

- Egy másik beadványozónak az iwiw-re küldött ismeretlen személy levelet az oda feltöltött képeit tartalmazó xxx.puruttya.hu linkkel, amelyen az ő képei szerepeltek nevével, valamint obszcén megjegyzésekkel együtt. A beadványozó számos üzenetet kapott iwiw postaládájába az oldal látogatóitól. (ABI-1243/2010/P)

Az ismételt panaszokra tekintettel az adatvédelmi biztos 2011. február 15-én ismeretlen tettes ellen feljelentést tett a Büntető Törvénykönyvről szóló 1978. évi IV. törvény 177/A. § (1) bekezdésébe ütköző visszaélés személyes adattal vétségének elkövetése miatt. A panaszolt oldalak a következők voltak: www.tundermacko.info, www.pedomaci.net, www.puruttya.hu, www.sunaszemle.hu, www.agyiszint.hu, www.napiszar.com (a nevek egyébként a szankciók miatt állandóan variálódnak). Ezen a portálokon más, általában közösségi oldalokról átvett fényképeket jelentettek meg, mely a legtöbb esetben számos, a beazonosíthatóságot elősegítő adat (név, telefonszám, lakcím, közösségi portálon való fellelhetőség) nyilvánosságra hozatalával párosult.

A célhoz kötött adatkezelés az adatvédelmi törvény egyik legfontosabb alapelve, így a képmás, illetve egyéb személyes adatok engedély nélkül történő felhasználása jogellenes adatkezelésnek minősül. A nyilvános adatbázisok felhasználása esetében meghatározó, hogy az adatok közzétételének eredetileg mi volt a célja. Valamely adatállomány törvényben, vagy az érintettek rendelkezése nyomán meghatározott céltól történő nyilvánosságra hozatala tehát nem járhat azzal a következménnyel, hogy az információkat bármely adatkezelő az eredeti céltól eltérően felhasználhatja. (A bírói gyakorlat is ezt az értelmezést követi. A Fővárosi Ítéltábla a 2.Pf.21.792/2009/4. számú ügyben született ítéletében kifejtette, hogy egy fénykép zárt rendszerben – közösségi oldalon – való elhelyezése nem ad jogosultságot más helyen, más feltételekkel történő engedély nélküli felhasználásra, nyilvánosságra hozatalra.) Az adatvédelmi biztos az oldalakat regisztráló cégeket az általuk regisztrált honlapokon elkövetett jogsértések miatt megkereste, de az ügyvezetők nem tudták megnevezni a jogsértő tartalmak feltöltőjét. Mivel a *domain* valós használója nem azonos a *whois* nyilvántartásban feltüntetett céggel, a személyes adatokkal visszaélő személy vagy társaság felderítése nyomozást igényel. Sajnálatos módon a Budapesti XIII. kerületi Rendőrkapitányság 2011. július 28-án kelt határozatában a nyomozás megszüntetéséről rendelkezett. Indokolásában kifejtette, hogy a képek, adatok gyűjtése, rendszerezése adatkezelésnek minősül, így a sérelmezett

magatartás formailag tényállásszerű, jelentős érdeksérelem azonban nem állapítható meg. A Rendőrkapitányság nyomozást megszüntető határozatát az V. és XIII. kerületi Ügyészség hatályon kívül helyezte, hiszen a Rendőrkapitányság határozatának indokolása maga is rámutat, hogy a vizsgált magatartás alkalmas lehet más bűncselekmény – becsületsértés – megállapítására (azonban ez a bűncselekmény már nem közvérdra, hanem magánvérdra üldözendő).

Az adatvédelmi biztos a fenti eseteket a rendelkezésére álló ún. vizsgálati eljárásban vizsgálta.

Néhány konkrét ügy a NAIH gyakorlatából:

2012. január 1-től a NAIH a kötetlenebb vizsgálati eljáráson felül a jóval kötöttebb, a közigazgatási hatósági eljárás általános szabályairól szóló 2004. évi CXL. törvény rendelkezéseit követő hatósági eljárást is indíthatott, amelynek keretében a jogsértés megállapítása esetén határozatban akár százazertől húszmillió forintig terjedő bírságot is kiszabhat. 2018-tól pedig a GDPR adatvédelmi bírságra vonatkozó rendelkezései értelmében akár 20 millió eurós pénzbüntetésről is dönthet.

A Generál Média Publishing Kft. adatkezelésének vizsgálata már hatósági eljárásban történt. Ennek egyik oka, hogy a próbaregisztrációk megerősítették: a www.love.hu, a www.szeretlek.hu és a www.talalka.hu társskereső weboldalakon mintegy 3500 olyan adatlap található, melyeknél a regisztrált felhasználók életkora 10-15 év közötti (és „természetesen” hiányzott a szükséges törvényes képviselői előzetes engedély, illetőleg utólagos jóváhagyás). A NAIH 2013. március 7-én kelt határozatában a társskereső honlapok üzemeltetőjét 3.000.000,- Ft adatvédelmi bírság megfizetésére kötelezte, elrendelte a jogellenesen kezelt személyes adatok törlését, (vagy a szükséges törvényes képviselői nyilatkozatok utólagos beszerzését), valamint az adatkezelési gyakorlat jogszabályoknak megfelelő átalakítását a regisztrációnál. A NAIH álláspontja szerint a közösségi hálózatepítő oldalak közül különösen a társskereső oldalak hordoznak magukban igazi kockázatokat, ahogyan www.naih.hu azt a próbaregisztrációk során tapasztaltuk is: a regisztrációt követő napokban több olyan zaklató, burkoltan, illetve kevésbé burkoltan szexuális irányultságú levél érkezett a létrehozott profil postaládájába, melyek minden kétséget kizáróan illegális, káros és életkorhoz nem illő tartalomnak minősíthetők. (NAIH-5951/2012-H)

Egy másik ügyben a bejelentő előadta, hogy az egyik legnépszerűbb közösségi oldalra férje – aki annak nem tagja – fényképét egy számukra ismeretlen felhasználó feltöltötte, azt profilképként is beállította, ezt követően a panaszost ismerősnek jelölte és azóta is zaklatja őket. (NAIH-1001/2013-V)

Sajtótermékekben – mely lehet internetes újság vagy hírportál is – a születési rovatban időszakosan megjelentetett adatközlés gyermekek nevére, születési idejére és anyja nevére vonatkozóan adatvédelmi szempontból aggályos. (NAIH/2015/503/V)

A gyermekszépségversenyek világához kötődik az az ügy, amelyben a panaszosok a modellügynökség internetes oldalán keresztül szervezett fotózások, modellkedések és egyéb rendezvények miatt fordultak a NAIH-hoz. A honlap tartalma alapján nem beazonosítható a rendezvényeket lebonyolító és a honlapot üzemeltető cég kiléte, a szervező céggel nincs lehetőség a kapcsolatfelvételre, továbbá, a honlapon nem található adatkezelési tájékoztató. (NAIH/2016/330/V)

A kiskorú törvényes képviselője telefonon megkereste a magán egészségügyi szolgáltatót annak érdekében, hogy 15 éves gyermekének vérértelre időpontot kérjen. A szolgáltatás igénybevétele után a törvényes képviselő a Google Maps alkalmazás értékelés rovatában leírta az egészségügyi szolgáltatással kapcsolatos negatív tapasztalatait teljes nevének, fényképének megadásával. Az értékelésre adott válaszban szerepel, hogy a kiskorúak STD (sexually transmitted diseases, vagyis szexuális úton terjedő betegségek) vizsgálatát csak szülői hozzájárulással végezhetik el, így a válaszreakció egyértelműen azt a látszatot keltette, hogy a gyermek vizsgálatát szexuális úton terjedő betegség miatt kérték, holott nem erről volt szó. Valótlan egészségügyi adat került a hozzászólásban nyilvánosságra oly módon, hogy a szülő az internetoldalon egyértelműen beazonosítható volt. A gyermek megnyugtatása és érdekei védelme érdekében törölte véleményét, így az arra tett válaszreakció is elérhetetlenné vált, de az egészségügyi szolgáltató védekezése, miszerint válaszában általános jellegű tájékoztatást adott, így az „semmilyen módon nem volt összefüggésben konkrét személlyel, így a panaszos gyermekével sem” – nem helytálló. Az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerint az egészségügyi adatok és a szexuális életre vonatkozó adatok kezelése tilos. A 9. cikk (2) bekezdés e) pontja alapján az (1) bekezdés nem alkalmazandó abban az esetben, ha az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott. A szülő azonban nem, kizárólag a szolgáltató hozta nyilvánosságra a gyermekkel összefüggésben az STD-vizsgálatra vonatkozó adatot. A Hatóság az eljárásban megállapította, hogy: a Kérelmezett adatkezelésével megsértette az általános adatvédelmi rendelet a 6. cikk (1) bekezdését, valamint a 9. cikk (1) bekezdését, amikor a kiskorú gyermekre vonatkozó egészségügyi adatot hozott nyilvánosságra. A Hatóság külön súlyosító körülményként értékelte azt, hogy a Kérelmező törvényes képviselőjének el kellett távolítania a Kérelmezett által nyújtott egészségügyi szolgáltatásról kialakított véleményét annak érdekében, hogy a Kérelmezett által a kiskorú Kérelmező vonatkozásában közzétett adatok is törlésre kerüljenek. (NAIH-3888/2023.)

Egy utolsó példa 2023-ból: a bejelentő házaspár babaváró kölcsönszerződést kötött egy hitelintézettel, majd gyermeket fogadtak örökbe titkos örökbefogadás keretében, melynek

tényét a hitelintézetnek bejelentették és kérték a törlesztés szüneteltetését. A bejelentő azt kifogásolta, hogy az örökbefogadást engedélyező végleges határozatot teljes egészében kellett benyújtaniuk a hitelintézethez, amelyben olyan személyes adatok és információk is szerepelnek, amelyek a törlesztés szüneteltetése iránti kérelem elbíráláshoz nem szükségesek, így különösen a gyermek örökbefogadás előtti neve, valamint a kötelező gondozási időszak során tapasztaltak leírása. A Hatóság álláspontja szerint a babaváró támogatásról szóló kormányrendelet vonatkozó rendelkezései, valamint az ezen felhatalmazás alapján az örökbefogadást engedélyező végleges határozatok teljes egészében történő, hitelintézetek általi kezelése sérti az adattakarékosság elvét. A babaváró támogatásról szóló kormányrendelet módosítása érdekében a Hatóság javasolta, hogy a jövőben az örökbefogadás tényét az illetékes gyámhatóság által kiállított hatósági bizonyítvánnyal kelljen igazolni, amely a támogatottak és az örökbefogadott gyermek természetes személyazonosító adatain – az örökbefogadott gyermek esetében az örökbefogadás előtti nevet ide nem értve – kívül, pusztán az örökbefogadás tényét, annak megtörténtét, illetve az örökbefogadást engedélyező határozat számát és annak véglegessé válásának napját tartalmazza. A Hatóság javasolta, hogy ezen hatósági bizonyítvány alkalmazását az örökbefogadás megtörténtének igazolására a jogalkotó tegye kötelezővé. Ennek oka, hogy az örökbefogadást engedélyező határozatok indokolásában érzékeny, a család életének, életkörülményeinek részleteit bemutató személyes adatnak minősülő információk kerülnek rögzítésre. Ezen személyes adatoknak a hitelintézetek általi kezelése nem indokolt, és messzemenően meghaladja az adatkezelés célja – a törlesztés szüneteltetési és támogatási jogosultság fennálltának ellenőrzése – elérése érdekében szükséges adatkört, azt eredményezve, hogy a hitelintézetek a jogi kötelezettségük teljesítése során megsértik az adattakarékosság elvét. (NAIH-6491/2023)

B. Ombudsmani gyakorlat

Magyarországon 1995 óta létezik ombudsmani intézmény, országgyűlési biztos, akit 2012. január 1-től az alapvető jogok biztosának neveznek. Az ombudsman legfőbb feladata, hogy az alapjogokkal kapcsolatos viisszasságokat panaszok alapján, avagy hivatalból indított eljárással vizsgálja, és orvoslásuk érdekében ajánlásokat tegyen, intézkedéseket kezdeményezzen hatóságokkal szemben.

Önálló gyermekjogi ombudsman híján, Magyarországon az alapvető jogok biztosa látja el a gyermekjogok védelmének feladatát¹⁶. 2008 óta működtet önálló gyermekjogi honlapot (www.gyermejjogok.ajbh.hu), 2011 óta pedig Facebook oldalt (www.facebook.com/Gyermejjogok) is. Az egyedi internetes gyermekjogi panaszok – mivel azok többnyire a sze-

16 Az alapvető jogok biztosáról szóló 2011. évi CXI. törvény

mélyes adatok védelmével kapcsolatosak – nem tartoznak ombudsmani hatáskörbe, de arra joga és lehetősége van a biztosnak, hogy speciális gyermekjogi projekt keretében hivatalból, átfogó jellegű tematikus vizsgálat sorozatot végezzen, így 2015-ben a médiaértés-oktatás hazai helyzetének feltárásával foglalkozott.

Az Európai Unió Bizottságának 2009-es, médiaműveltségről szóló ajánlása¹⁷ szorgalmazza, hogy a médiaoktatás és a médiaműveltség váljék az oktatási rendszer szerves részévé, és az egyes tagállamokon belül minél több lehetséges szereplő vegyen részt ebben a munkában. A médiaértés-oktatás célja és lényege tehát, hogy a gyermekeket felkészítse a kritikus médiafogyasztásra, a tudatos fogyasztóvá válásra, arra, hogy különbséget tudjanak tenni a hírek, vélemények között. Oktatási szakértők szerint azonban problémát okoz, hogy meglehetősen nagy különbségek tapasztalhatóak a gyermekek tudása között attól függően, hogy milyenek a helyi, személyes és iskolai lehetőségeik.

A 2013-ban megjelent Nemzeti Alaptanterv (a továbbiakban: NAT) alapján a médiaműveltségre vonatkozó ismeretek külön nevesítve beépülnek a vizuális kultúra elnevezésű tantárgyba¹⁸, ahol szerepet kap a kritikai gondolkodás kialakítása, a médiában megjelenő erőszak, a jelenség értelmezése és hatásának tudatosítása, az online életforma hatása a személyiség fejlődésére és a társas kapcsolatokra, a tanulásra, a munkavégzésre, valamint a szabadidő eltöltésére.

Az ombudsmani átfogó vizsgálat azonban megállapította, hogy a valós képet csak a helyi tantervek mutathatják, hiszen az az élő gyakorlat. Helyi szinten dől el, hogy önálló tantárgyként vagy egy másik tantárggyal összekapcsolva tanítja az adott ismeretet az iskola. A tantestület dönthet arról, hogy például a „Mozgókép- és médiaismeret” stúdium oktatására önálló tantárgyként vagy az irodalom, az informatika, esetleg a rajz vagy a vizuális kultúra tantárgy keretein belül kerül sor. Mivel ez többnyire integrált formában, más tantárgyak keretein belül történik, azon tantárgy óraszámá megemelkedik azzal az időkerettel, amelyet a kerettanterv a médiaismeret oktatására előír. A gyakorlatban pedig az ismeretek átadására szánt idő elenyészik, az időkeretet nem is használják fel célzottan.

A tanárképzés rendszerében Magyarországon Mozgóképkultúra és médiaismeret alapszak (BA), Mozgóképkultúra és médiaismeret-tanár (tanári MA), Média-, mozgókép- és kommunikáció tanár (osztatlan tanárképzés) szakon sajátíthatóak el a médiaértés-oktatással kapcsolatos speciális ismeretek, mellyel az általános és középiskolákban bevezetett mozgóképkultúra és médiaismeret tantárgy tanítható. A szakok képzési és kimeneti követelményei között az internet veszélyeire, az online bántalmazás jelenségére, kezelésének módjára vonatkozó ismeretek azonban nem szerepelnek.

17 „Egy versenyképesebb audiovizuális és tartalomipar, továbbá egy befogadó tudásalapú társadalom érdekében a digitális környezethez igazodó médiaműveltségről” című ajánlás

18 2001-től már választható közismereti érettségi vizsgatárgy is

A vizsgálat következtetése szerint hazánkban a médiatanárok igen kevés százaléka rendelkezik szakképesítéssel, éppen eléri a 20-30 %-ot. A médiatanárok szakképesítésére vonatkozó kötelező előírások azonban nincsenek, ebből következően a formális oktatásban a médiaismereteket az a tanár oktatja, akit az érdekel, vagy akit megbíznak vele, függetlenül attól, hogy rendelkezik-e szakképesítéssel vagy sem, ugyanis a hazai jogszabályi környezet lehetővé teszi olyan pedagógusok alkalmazását is e területen, akik nem rendelkeznek megfelelő szakképesítéssel.

Az alacsony óraszám, az integratív jelenlét, valamint a kevés számú szakképzettséggel és hiányos kompetenciával rendelkező pedagógus iskolai jelenléte miatt a médiatudatosságra nevelés sok esetben nem valósul meg maradéktalanul és hatékonyan az oktatási rendszerben.

A viszonylag kevés óraszám és a megfelelő szakképzettséggel rendelkező tanárok hiánya pedig különösen azért sérelmes, mivel a vizsgálat megállapításai szerint a gyermekek sok esetben nincsenek tisztában a közösségi média használatának veszélyeivel, nem mindenki ismeri az adatvédelmi beállításokat, zaklatás esetén pedig nem tudják, kihez forduljanak segítségért.

Az UNICEF Magyar Bizottsága „Ébresztő-óra” gyermekjogi iskolai programja külön érinti az online biztonság kérdéskörét. Az UNICEF tapasztalatai szerint a gyerekek nagyon érdeklődőek a téma iránt, és már vannak előzetes ismereteik az online média veszélyeiről és tudatos használatáról. Az UNICEF 2014-ben kiadott „Jogod van a jogaidhoz” gyermekjogi felmérés eredménye szerint a gyermekek fele találkozott már olyan tartalmakkal, amiket nem értett és minden 3. gyermeket ért már „piszkálódás” a neten. Ezekben az esetekben a gyerekek fele (53%) megpróbálta megvédeni magát, míg negyede (26%) gyorsan bezárta az oldalt, de segítséget csak minden tizedik gyerek kért (11%). A gyerekek fele szerint (47%) nem biztonságos az internet. Egyértelműen biztonságosnak tehát csak a gyerekek 21%-a (minden ötödik gyerek) érzi a netet. A gyermekek 11%-a teljesen biztonságosnak, 10%-a inkább biztonságosnak, míg 32% is-is, 22%-a pedig inkább nem, 25%-a pedig egyáltalán nem biztonságosnak minősítette az internetet.¹⁹ A 10-18 éves gyermekek 96%-a rendelkezik mobiltelefonnal, 88%-ának van profilja közösségi oldalon. *Különösen érdekes adat, hogy a 10-12 éves korosztályban a gyerekek 78%-a rendelkezik profillal, holott hivatalosan erre csak 13 éves kor felett lenne lehetőségük.* 10-ből 8 gyerek tudja, hogy vannak olyanok, akik arra használják az internetet, hogy gyerekeket zaklassanak. 10-ből 8 gyerekkel már beszélgettek az internetes biztonságról. A gyerekek fele találkozott olyan internetes tartalmakkal, amelyeket nem értett. Ilyenkor a gyermekek kétharmada bezárta az oldalt, de 18%-uk ott maradv

19 Az UNICEF kutatás teljes szövege: <http://unicef.hu/a-gyerekek-kozel-fele-szerint-egy-pofon-belefer/cimen>

kattintgatni kezdett rajta, és csak 14%-uk kért segítséget másoktól a látott információk értelmezéséhez.

A médiaértés-oktatás hazai helyzetének elemzését természetesen nem lehet függetleníteni a rendelkezésre álló *digitális eszközpark*, a *digitális eszközök hozzáféréseinek kérdésétől*, valamint a digitális kompetenciától, amely az információs és kommunikációs technológiák használatával kapcsolatos kompetenciákat jelöli.

Bár ez utóbbiak gyakorlati megvalósulása nem képezte az ombudsmani vizsgálat tárgyát, érdemes kiemelni, hogy *ma Magyarországon az egyes köznevelési intézményekben rendkívül eltérőek a digitális eszközök tekintetében az adottságok és lehetőségek*.

2011-ben 27 országban – köztük Magyarországon is – az ESSIE elnevezésű projekt keretében több mint 190 ezer kérdőív alapján monitorozták a digitális oktatást. A kutatási eredmények szerint 2006 óta megduplázódott a számítógépek száma az európai oktatásban, de az informatikai eszközök használata és a digitális kompetencia terén nagy egyenlőtlenségek tapasztalhatók. A magyar országjelentés szerint a számítógépekhez való hozzáférés közel áll az európai átlaghoz, a tanárok eszközhasználati magabiztossága azonban minden felmért évfolyamon alacsonyabb az európai átlagnál. Összességében a magyar iskolák jellemzően a *digitálisan részben felszerelt iskolák* közé tartoznak, ezt a típust az alacsonyabb eszközszint és a lassú internet vagy a szélessávú kapcsolat hiánya jellemzi.

A kutatások alapján a diákok közel felének van iskolán belüli mobilinternet elérhetősége, ezért még inkább szükség lenne az iskolák digitális eszközparkjának fejlesztésére, mivel így legalább ellenőrzött, adott esetben szűrt tartalmakkal találkozhatnak az oktatás alatt a gyermekek. Ezért az alapvető jogok biztosának álláspontja szerint a médiaértés-oktatás teljes körű megvalósításának egyik fontos előfeltétele a digitálisan jól felszerelt köznevelési intézmények léte, a meglévő egyenlőtlenségek, hiányosságok pedig feltétlen folyamatos orvosolásra, fejlesztésre szorulnak.

Az alapvető jogok biztosának vizsgálata arra is rámutatott, hogy szorosan összefügg a médiaértés-oktatás és az ezzel kapcsolatos jogtudatosítás szintjével az utóbbi években egyre inkább elharapózó jelenség, az *online megfélemlítés vagy bántalmazás (cyber-bullying) jelensége*, melynek kezelésében a gyermekeknek, fiataloknak feltétlen szükségük lenne egyértelmű iránymutatásokra, melynek a szakértők egyöntetű véleménye szerint a médiaértés-oktatás lehetne ennek az igazi terepe. Az *online bántalmazás* kezelésében a gyermekek nagyon kevés ismerettel bírnak, sok esetben nem tudják, melyik szervhez fordulhatnak segítségért. Ugyanakkor célként sem a NAT, sem a tanárszakok képzési és kimeneti követelményei nem tartalmaznak az online bántalmazás jelenségével, kezelésével kapcsolatos kompetenciákat.

A pedagógusképzésben jelenleg még nem jelent meg hangsúlyosan az, hogy hogyan kezeljék, hogyan adják át a médiaműveltséggel kapcsolatos tartalmakat, hogyan tudják az oktatás során aktív és biztonságos módon alkalmazni a médiát. Holott az internethasználat

és a különböző digitális eszközök használatának megkezdése szabadidős tevékenység (játék és kapcsolatépítés) céljából egyre korábbi életkorra tehető. Gyakori és a gyerekre nézve nagyon veszélyes jelenségek a cyberbullying, a kritikátlan posztolás és képhasználat, valamint az internetfüggőség, az adatok felelőtlen kezelése. Ezekben a helyzetekben a gyerekek az életkori sajátosságukból fakadóan viselkednek, ám a felnőttek által adott védelem, iránymutatás, a keretek kiépítése nem megfelelő. A cyberbullying jelenség egyik jellegzetessége, hogy a bántalmazó és az áldozati szerepek váltakozhatnak, így a feldolgozás során a felelősség tudatosítása és a segítség nyújtása egyaránt fontos. A téma feldolgozása lehetőséget ad arra is, hogy a konfliktusok megoldásában fejlődhessenek a gyerekek és arra is, hogy közösségi értéké váljon a segítség és a figyelem. A vizsgálat fontos következtetése az is, hogy a valódi közösségi teret nem szabad elkülöníteni a kibertér közösségetől és amennyiben erőszak tapasztalható valamelyik közösségi térben, annak orvoslása során szükséges a kettőt egymással szoros összefüggésben kezelni.

Az interneteléréssel rendelkező okostelefonok újabb problémákat vetnek fel e témakörben, hiszen a szülő sokkal kevésbé tudja kontrollálni, szűrni, blokkolni a különböző alkalmazások használatát a gyermeke számára.

A vizsgálat feltárta, hogy a közoktatási intézmények jelentős részében vannak szűrőszoftverek a káros, illetve jogellenes tartalmak szűrésére, így a tanulók többnyire tanári ellenőrzés mellett interneteznek. Problémát jelent azonban a szűrőszoftverek kapcsán, hogy nincsen olyan megfelelő ajánlás, amely felhasználható lenne a köznevelési intézményekben, továbbá e szoftverekkel kapcsolatos költségek megoszlása, karbantartása vitatott. Az iskolák ezért inkább legtöbbször az iskolai internet-hozzáférés drasztikus korlátozását választják. Egy megfelelő tanári iránymutatás mellett azonban nem feltétlenül van szükség szűrőszoftverre, a probléma a tanítási időn túl kezdődik, amikor otthon, közösségi helyeken folyik az internetezés, a mobilinternet használata rejtja a legnagyobb veszélyt magában, mivel gyakorlatilag ellenőrizhetetlen a tanár és a szülő számára is.

A fentiek miatt különösen nagy szükség lenne azokra az információkra, és szituációs leírásokra, amelyek alapján azonosíthatják a fiatalok a problémát, továbbá azokra az eljárásokra, módszerekre, amelyeket a gyermekek online biztonságát támogatnák. Ugyanakkor szakértők egyetértenek abban, hogy a legerősebb védelem, ha a szülő is használja az internetet és nyíltan beszélget a tapasztalatairól a gyermekével. Másrészt fontos lenne a hangsúlyokat áthelyezni a közösségi, interaktív megközelítésre, a jogorvoslati lehetőségekről való tájékoztatásra a káros, illegális, bántó tartalmak, vagy a zaklatás terén. Ehhez azonban elengedhetetlen a pedagógusok személetének formálása, eszköztáruk bővítése, és olyan élmények meg tapasztalása, amelyek nem a didaktikus oktatás, hanem a tapasztalati és a nem formális tanulásra épülnek. Ezekben a fejlesztési célokban ideális partnerek lehetnek a civil szervezetek, alternatív iskolák, élménypedagógiai szervezetek, ifjúságfejlesztő műhelyek.

A NAT a következőképpen fogalmazza meg a médiatudatosságra való nevelést: „Cél, hogy a tanulók a mediatizált, globális nyilvánosság felelős résztvevőivé váljanak: értsek az új és a hagyományos médiumok nyelvét. A médiatudatosságra nevelés az értelmező, kritikai beállítódás kialakítása és tevékenység-központúsága révén felkészít a demokrácia részvételi kultúrájára és a médiumoktól is befolyásolt mindennapi élet értelmes és értékelvű megszervezésére, tudatos alakítására. A tanulók megismerkednek a média működésével és hatásmechanizmusával, a média és a társadalom közötti kölcsönös kapcsolatokkal, a valóságos és a virtuális, a nyilvános és a bizalmas érintkezés megkülönböztetésének módjával, valamint e különbségek és az említett médiajellemzők jogi és etikai jelentőségével. A digitális kompetencia felöleli az információs társadalom technológiáinak és a technológiák által hozzáférhetővé tett közvetített tartalmak magabiztos, kritikus és etikus használatát a társas kapcsolatok, a munka, a kommunikáció és a szabadidő terén. Ez a következő készségeken, tevékenységeken alapul: az információ felismerése (azonosítása), visszakeresése, értékelése, tárolása, előállítása, bemutatása és cseréje; digitális tartalomalkotás és megosztás, továbbá kommunikációs együttműködés az interneten keresztül.”

Összefoglalva a NAT előírásaiban megjelenő szakmai követelmény pusztán egy külső formális elvárást takar, de összességében jelenleg a köznevelés rendszerében leginkább a médiaoktatás szándéka látszódik, annak eredményei már sokkal kevésbé. Mindezek alapján az alapvető jogok biztosa megállapította, hogy a megfelelő kompetenciával rendelkező szakképzett pedagógusok hiánya, a médiaértés-oktatásra vonatkozó ismeretek főként elvi szinten létező, a gyakorlatban ellentmondásos, hiányos átadása, a médiaértés-oktatás hatékonyságát felmérő, átfogó, illetve reprezentatív állami kutatás, a célokat meghatározó helyzetelemzés hiánya együttesen a gyermekek védelemhez és gondoskodáshoz való jogával, ennek kapcsán a művelődéshez való jogával összefüggő visszásságot okoz. A jelenlegi helyzet ugyanis alkalmas arra, hogy a jogsérelem közvetlen veszélyét idézze elő.

A fenti problémák orvoslása érdekében az alapvető jogok biztosa felkérte az illetékes minisztert, hogy kezdeményezze a médiaértés-oktatás hazai helyzetének átfogó állapotfelmérését, a pedagógusok szakirányú ismereteinek, készségeinek fejlesztését és tegyen lépéseket a szakképesítéssel rendelkező pedagógusok létszámának növelése érdekében. Továbbá kezdeményezte a NAT jelenlegi célrendszere és a pedagógusképzés felülvizsgálatát, hogy a képzési és kimeneti követelmények között az online bántalmazás jelenségével kapcsolatos ismeretek is helyet kapjanak.

C. Rendőrségi gyakorlat²⁰

„Gyermekepornográfia büntette miatt négy ember ellen emelt vádat a Budapesti I. és XII. Kerületi Ügyészség – tájékoztatta a Magyar Nemzetet a Fővárosi Főügyészség. 2013-ban egy XVII. kerületi házibuliban vettek részt, és felvételt készítettek arról, hogy két társuk közösen egy ittas 15 éves lánnyal. A fiatalok a videót e-mailben több ismerősüknek is elküldték. A vádlottak közül hárman még maguk is fiatalok, azaz 18 éven aluliak voltak. A büntető törvénykönyv szerint az, aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt szerez meg vagy tart, három évig terjedő szabadságvesztéssel büntethető. Aki viszont ilyen felvételt készít, kínál, átad, vagy hozzáférhetővé tesz, egytől öt évig terjedő szabadságvesztést kaphat.”²¹

A magyar rendőrség látóterébe került, gyermekeket érintő, internettel kapcsolatban álló súlyos bűncselekmények jelentős része eszközcselekmény: tehát a súlyosabb cél eléréséhez szükséges egy enyhébb bűncselekmény elkövetése is.

Az első lépcső a személyes adatok megszerzése, amely tekintetében a közösségi oldalak fontos „vadászterületet” jelentenek. Veszélyforrás egyrészt az, hogy a gyerekek általában egyszerű jelszavakat adnak meg, hiszen szándékuk szerint ők csak kapcsolatot szeretnének tartani és játszani kortársaikkal. Másrészt naivitásukból kifolyólag, ha felnőttekkel érintkeznek, könnyelműen kiadhatnak fontos információkat magukról, környezetükről. Még „egyszerűbb” a helyzet, ha az elkövetők magukat gyerekeknek álcázva becsapják őket.

Problémát okoz a közösségi oldalakon elterjedt játékok egy része is, amelyeket a gyermekkorú felhasználókról történő adatgyűjtés céljából készítenek. A fiatalok osztálytársaik tanácsára játszanak játékokkal, néznek meg videó felvételeket, böngésznek bizonyos oldalakat; ugyanakkor nem rendelkeznek ehhez kellő szintű nyelvtudással, továbbá nem készültek fel a támadó kódok elleni védekezésre sem. Általában a kíváncsiság győz, így letöltik az adott tartalom megnyitásához szükséges programot, nem gondolva arra, hogy egy adatgyűjtő trójai alkalmazást „szabadítottak” a számítógépükre vagy mobil telefonjukra. Ezen szoftverek külön gyűjtik a gyerekekkel kapcsolatos adatokat, aminek már fekete piaca is létezik a szexuális bűncselekmények elkövetésében érdekelt számára. Egy új játék közösségen belüli elterjedését követően gyakran érkeznek olyan panaszok, amelyek szerint a gyerek oldalát feltörték, megváltoztatták. Ráadásul ez sokszor nem is derül ki, hiszen a gyerek az esetet általában eltitkolja, nem tudva, hogy veszélyes vagy tömeges jelenség érintette.

A második lépcső a megszerzett adatok fel- és/vagy kihasználása. Gyakori bűncse-

20 Köszönet az ORFK-nak (Dr. Gömbös Sándor r.ezredes, Dr. Szabó Henrik r. alezredes és Szabolcsi Zsolt r.százados) a tájékoztatásért.

21 http://index.hu/belfold/2016/03/10/hazibulin_eroszakoltak_meg_a_15_eves_lanyt/, 2016.03.10.

lekmény a zsarolás anyagi indíttatásból vagy gyermekpornográfiára való rákényszerítésből. A közösségi oldalak az elkövetők számára rendkívül jó platformot biztosítanak, hiszen ott minden korosztály megtalálható egy helyen, ráadásul a potenciális áldozatról előre lehet tájékozódni.

Az adatok egy részének megszerzése történhet szándékos kapcsolatfelvétel útján, de általában trükkös módon is, ahol egy linket küldenek „véletlenül”, vagy spam formájában az illetőnek. Ez a link egy olyan oldalra mutat, amely valamely közösségi oldal vagy azonnali üzenetküldő szolgáltatás (pl. *Messenger*) belépési oldalát másolja le és engedi tovább a beírt jelszó után a felhasználót a valódi oldalra. Az így megszerzett jelszó birtokában egy ideig adatgyűjtésre kerül sor, majd a céltól függően egy videó- vagy képfelvétel feltöltésének kilátásba helyezésével jön létre a zsarolás.

Ez a felvétel létrejöhet egy közkedvelt módszer, azaz egy trójai alkalmazás útján, amely a webkamerát a felhasználó tudtán kívül távolról bekapcsolja, és az elkövető rögzíti az adott helyiségben történt eseményeket. Jellegzetesen fürdés utáni meztelenségről vagy öltözésről, esetleg önkielégítésről készülnek felvételek. A zsaroló a zsarolás megkezdésekor természetesen első lépésként megváltoztatja a tényleges felhasználó jelszavát, majd ezt követően megmutatja, bebizonyítja az áldozatnak, hogy hatalma van felette, irányíthatja őt, például a nevében a neten ír egy ártatlan megjegyzést, bejegyzést. Ezt követően kilátásba helyezi, hogy a kényes felvételt megosztja a közösségi oldalon, ahol a szülők, osztálytársak, barátok láthatják az áldozatot. Ez egy mára már kialakult, előre összeállított forgatókönyv alapján történik, amely során természetesen figyelmeztetik az áldozatot, hogy amennyiben segítséget kér másától, úgy szintén közzétételre kerülnek a felvételek. A következmény nemzetközi tapasztalatok alapján mindenhol ugyanaz. A fiatalok ilyenkor hónapokon keresztül maradnak egy-egy zsaroló áldozatai anélkül, hogy bárki tudna helyzetükről. A szülők csak az általános rosszkedv és a hosszan tartó folyamatos depresszió tünetei miatt figyelnek fel arra, hogy valami baj lehet. Azonban az eltelt idő és a megszégyenültség érzete miatt ilyenkor sem „táruznak fel” az okok, sajnálatos módon gyakori a hazugságokba menekülés és számos esetben a kilátástalanság miatti öngyilkosság.

Fontos lenne, hogy a regisztráció alkalmával az ahhoz szükséges adatokon kívül ne töltsenek fel magukról egyéb személyes információt (lakcím, születési dátum, mobiltelefonszám, a kedvenc zenei stílus, vagy érdeklődési kör), az intim képek pedig egyértelműen visszauíthatnak például továbbtanulás, álláskeresés során. A kihívó képek súlyosabb bűncselekmények (nemi erkölcs elleni bűncselekmények, lopás, rablás, betörés) elkövetését is eredményezhetik.

Óvatosnak kell lenni a családi felvételek nyilvánosságra hozatalával is, mivel a szülők ezáltal akár áldozattá is tehetik gyerekeiket (és fordítva, a gyerek által közzétett információk is felkelthetik, mondjuk a betörők figyelmét).



2. ábra A német rendőrség nyilvános felhívása szülőknek 2015. októberében

Rendőrségi tapasztalatok alapján egyes elkövetők e célból látogatják a közösségi oldalakat és a fent lévő adatok alapján tudatosan választják ki leendő áldozatukat: szerelmet színelnek, hostess- vagy művészi modell munkát vagy nyugat-európai iskolákat ajánlanak, amely ígéreteknél a fiatalok könnyen bedőlnek.

Akár egész életre kiható sérelmet okozhat a személyiséglopás. Ez akkor következhet be, ha az elkövető egy álprofiloldalt hoz létre valakinek az eltulajdonított adataival egy közösségi oldalon, és az ő személye mögé bújva tesz közzé dehonesztáló képeket, szövegeket, esetleg sérteget másokat, netán bűncselekményeket követ el. Erre akkor van lehetősége az elkövetőnek, ha a személyiséglopáshoz megfelelő adatokkal rendelkezik, képekkel, egyéb személyes adatokkal, amit legkönnyebben egy minden adattal ellátott profiloldaltól szerezhet meg.

Problémát jelent az is, hogy a közösségi oldalakon a tinik visszaigazolnak számukra ismeretlen személyeket csak azért, hogy ismerősi körük minél nagyobb legyen. Az internetes adatgyűjtés, a felhasználók „digitális lábnymainak” összegyűjtése a fiatalokat érintve sokkal kiterjedtebb lehet, mint gondolnánk. Mivel a közösségi háló, a megosztások és a *kommentélések* a fiatalok mindennapjainak részét képezi, így ha elég kitartó az elkövető, úgy részletes keresések során több olyan információt is be tud szerezni, amit az áldozata nem akart nyilvánosan megosztani. Ilyenek lehetnek a rég nem használt e-mail címmel regisztrált és írt hozzászólások különböző fórumokban, barátok által készített csoportképek szórakozóhelyeken (annak ellenére, hogy azon az áldozat nincs „betagelve”). Hasonló információforrást jelenthet egy-egy idősebb rokon, kevésbé hozzáértő nagymama internetes jelenléte is, akik sok esetben nincsenek tisztában azzal, hogy a megosztott tartalmaikat ki láthatja.

A csevegő programok magukban hordozzák az anonimitás lehetőségét, ebből kifolyólag a gyerekek jóhiszeműsége, hiszékenysége könnyen kihasználható: az elkövetők ennek következtében érzékeny adatokat szednek ki belőlük, találkozókat beszélnek meg velük, képeket szereznek meg róluk, vagy számukra zaklató tartalom megtekintésére kényszerítik őket. A „szemérem sértés” törvényi tényállása ez esetben jogi értelemben gyakran nem valósul meg, hiszen a képek megszerzése vagy megtekintése az érintett hozzájárulásával történik; a bűncselekményeket pedig a naplózás bekapcsolt állapotának hiánya miatt nem lehet bizonyítani.

„A gyerekek számára számos információ még ismeretlen, ráadásul sok esetben nem képesek reálisan felmérni tetteik jelentőségét, súlyát. Az internetezés során emiatt akaratlanul is olykor könnyen jogsértések vagy akár bűncselekmények elkövetőjévé is válhatnak. A gyerekek sokszor nem gondolnak bele, hogy egy szűk baráti közösségnek szánt, jó „hecc”, amit az interneten elhelyeznek (írnak, feltöltenek), valójában mindenki számára elérhető információ, így egyúttal nagy nyilvánosságot jelent. Ennek átgondolatlansága miatt könnyen fordulhat elő, hogy szándékuktól eltérően „nagy nyilvánosság előtt elkövetett becsületsértés, rágalmazás” bűncselekményét valósítják meg, ugyanis az internet, mint felület – a chatoldalak, közösségi oldalak, fórumok, blogok vagy egyéb megosztó oldalak, mint társalgási terület – megfelel a „nagy nyilvánosság” törvényi feltételének.”

Idegen levelezések megtekintése a jogban egyenértékű a „levéltitok megsértése” bűncselekmény elkövetésével. Ennek tipikus esete, mikor az iskolában vagy internetcávézóban a felhasználó megjegyzteti a jelszavát a géppel, avagy nem lép ki elektronikus postafiókjából, így elkövetővé válhat az, aki utána a géphez ülve szándékosan beleolvas a megnyitva felejtett levelezésbe. A telefonon folyamatosan szinkronizált alkalmazások (Facebook, Gmail, Viber stb.) is lehetőséget adhatnak arra, hogy illetéktelenek (iskolatársak, barátok) egymás profiljait megnézzék, mások nevében posztoljanak. A technika folyamatos fejlődésével és egyre bonyolultabbá válásával még a fiataloknak sem könnyű adott esetben lépést tartani, ami sok esetben védtelenné teszi a felhasználókat. Erre az egyik példa a mobiltelefont áruló boltok tesztkészülékei, amelyek közül nem ritka az olyan készülék, melyben bejelentkezve maradnak a Facebook alkalmazásban a többségében fiatal nézelődők. Az okostévék és a hozzá kapcsolódó mobiltelefonos szinkronizálási lehetőségek elterjedésével ugyanez a helyzet.

Mivel a Google ugyanazon profil alatt kezeli a felhasználók YouTube fiókját, mint a Gmail, drive és más egyéb alkalmazásait, így ez is könnyen védtelenné teheti a fiatalok adatait. Ha adott esetben egy házibuli alkalmával a barát, barátnő telefonjáról bejelentkezve játszanak le YouTube zenét, nem feltétlenül tudatosul, hogy amennyiben nem jelentkezik ki, csak bezárják az ablakot, úgy a mobiltelefonról minden más személyes adatuk, levelezésük később bármikor máshol is elérhető lesz.

Az iskolai eseményeken készült felvételek, iskolatársaktól kapott képek interneten történő megosztása személyes adatok védelméhez való jogot sérthet. „Súlyosabb lehet a verekedések, zsarolások telefonnal, kamerával történő rögzítése, feltöltése és megosztása, mert ilyenkor az erőszakos bűncselekmény mellett súlyosbító körülményként jelenik meg a személyes adattal való visszaélés.”

A fiatalok szexualitással összefüggésben is felhasználják az IT eszközöket kapcsolat-tartásra, érdeklődésük bővítésére. Azonban bűncselekményt követ el, ha valaki az igényét úgy igyekszik kielégíteni, hogy 18 év alatti szereplőről készített képeket tölt le korra, nemre

és érdeklődésre való tekintet nélkül. „Előfordulnak azonban olyan esetek is, amikor a párok (a felnőttekhez hasonlóan) felvételt készítenek az intim együttlétről, amely szintén bűncselekmény, még akkor is, ha önmagukról, egymás beleegyezésével készítik el. Megtörtént, hogy egy 16 éves lány a párjának szándékozott kedveskedni, vágját fokozni, ezért a laptopjába épített webkamera segítségével az MSN-n a fiú részére „műsort” adott, amelyen önmagát elégítette ki meztelenül. Ezzel bűncselekményt követett el. A lány esetében a készítéssel és közzétételével 2-8 évig terjedő, a fiú esetében 3 évig terjedő szabadságvesztéssel büntethető bűncselekményről van szó. Természetesen az ilyen esetek egyedi mérlegelést igényelnek. Teljesen más megítélés alá esik, amikor bulikon és/vagy buliból készülnek felvétel(ek) és azok kerülnek továbbításra, megosztásra. Jelenleg a jogi szabályozás nem kielégítő. Ami viszont ennél is súlyosabb, hogy a fiatalok sem képesek ezeket megfelelően kezelni, hiszen egyrészt buli, másrészt „ciki” ha nem vesz részt benne, harmadrészt bizonyos felvételek igen komoly pénzkereseti lehetőséget jelentenek.

A gyermekpornográfiával kapcsolatban megjegyzendő, hogy a specifikus oldalakon használt „teen” kifejezés és a magyar „tini” szó alkalmazása kapcsán hazánkban gyakran adódik félreértelmezés. A szexuális tartalmú oldalak és a kialakult ipar tekintetében a „teen” arra utal, hogy a 18-20 év közötti, azaz pontosabban a 20. életévét még nem betöltött személyekről vagy más néven fiatal felnőttekről szexuális tartalmú képeket, filmeket tesznek közzé, amely azonban nem büntetendő. Ez egy kialakult igényre adott jellegzetessé vált válasz. A gyermekpornográfiával kapcsolatos felderítés bizonyos esetekben jogi akadályokba ütközik. Alapvetően a weboldalak ellenőrzésével, illetőleg a peer-to-peer hálózatokon a felhasználó által megosztott tartalom letöltésével és mellette a kapcsolat forgalmának ellenőrzésével lehetséges eredményes felderítést végezni.” Ennek kivitelezése azonban sokszor azért nehéz, mert az ilyen fórumhoz vagy tartalomhoz való hozzáférés előzetes feltétele éppen a hasonló képek vagy videók feltöltése, de létezik olyan oldal is, ahol személyes kapcsolatfelvétellel próbálják „kiszűrni” a nyomozókat, akik még fedett státuszban sem követhetnek el ilyen cselekményeket.

Sajnos az agresszív oldalreklámok miatt nem ritka a vétlen oldallátogatás sem. Ráadásul a szexipar kiszolgálói sajátos kulcsszavakat is használnak, így egy tájékozatlan netező számára megtévesztő például a „PTHC Inc.” megjelölés, ami nem egy cégnévre utal, hanem a „pre-teen hard core included”, azaz „tinikor előtti kemény szexet tartalmaz” megjelölésre.

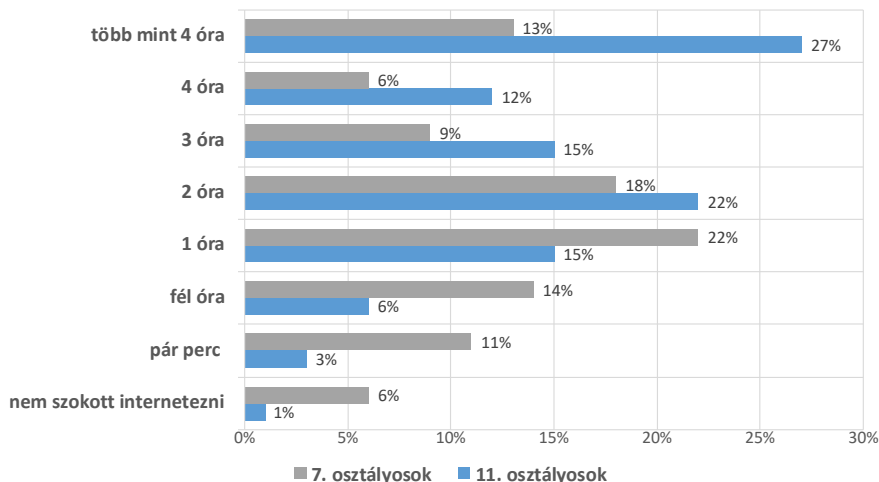
A MAGYAR GYERMEKEK INTERNETHASZNÁLATI SZOKÁSAIRÓL²²

A. Általános trendek

Az elmúlt évek kutatásai alapján a magyar gyerekek egyre fiatalabb korban kezdik el használni önállóan az internetet. A többség esetében ez jelenleg valahol 8-10 év között van, ami elsősorban az életkortól és a háztartásban elérhető „géppark” (pl. hagyományos számítógépek, mobil eszközök, stb.) mennyiségétől és minőségétől függ. 2015 őszén a 7. osztályba járók átlagosan 8, míg a 11. osztályosok 10 évesen kezdtek el önállóan internetezni, ami természetesen nem jelenti azt, hogy ne lennének olyanok, akik ennél az életkornál 1-2 évvel korábban, illetve később kezdik el ezt a tevékenységet.

A vizsgált korosztályban az internetezéssel töltött idő átlagos mennyisége még hétköznapiakon is inkább órákban, mint percekben mérhető. A konkrét mennyiség azonban ekkor erősen életkorfüggő. A 11. osztályosok körében még hétköznapi is azok vannak a legnagyobb arányban (27%), akik 4 óránál többet interneteznek, míg a fiatalabbak körében a legtöbben napi 1 órát töltenek a világhálón, és csaknem egyharmad azoknak az aránya, akik ennél kevesebbet, vagy semennyit sem interneteznek tanítási napokon (31%). Ugyanez már csak minden tizedik 11. osztályosra igaz, tehát a két korcsoport közötti néhány év különbség egyben eltérő intenzitású internethasználatot is jelent. Jelentősebb növekedés az általános iskola befejezésekor, illetve a középiskolába való átmenet kezdetén figyelhető meg.

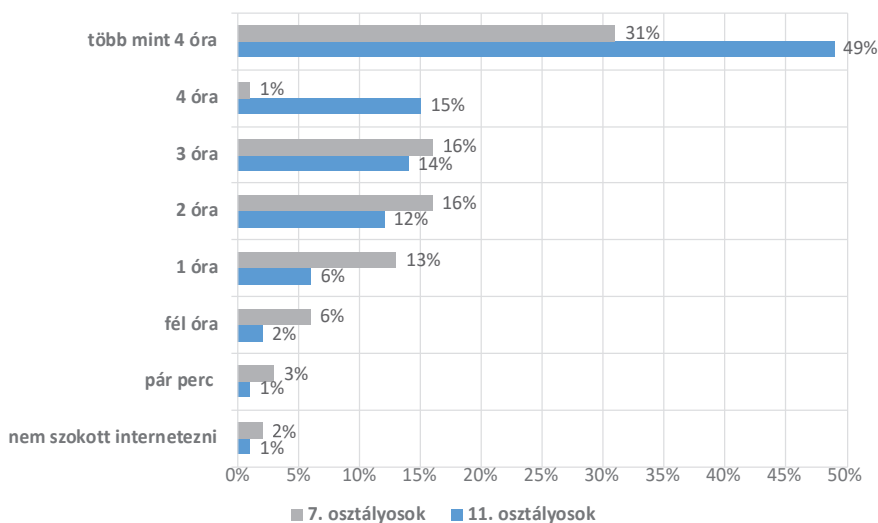
22 Ez a fejezet – szerzője Dr. Ságvári Bence – a Nemzetközi Gyermekmentő Szolgálat (NGYSZ) megbízásából az ITHAKA Nonprofit Kft. által 2015 őszén készített, a magyarországi alap- és középfokú oktatási intézmények mintájára reprezentatív kutatás eredményein alapul. A kutatásban 7. és 11. osztályos diákok vettek részt (2x1200 fő), akik iskolai keretek között töltötték ki kérdőíveket. Az eredmények tehát szigorú statisztikai értelemben erre a két korcsoportra vonatkoznak, nem pedig a fiatalokra „általában”. A némileg megengedőbb, ám jobban használható interpretáció szerint azonban az eredmények a 13 és 18 év közötti fiatalokra többé-kevésbé általánosíthatók.



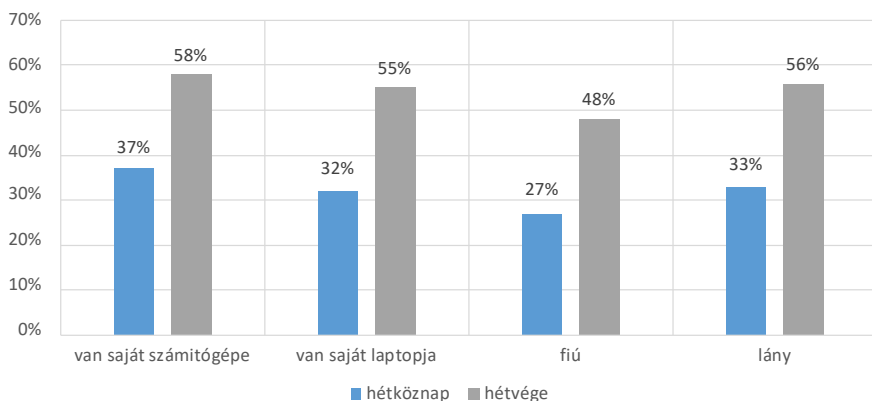
3. ábra: Internetezéssel töltött idő egy átlagos tanítási napon (a két vizsgált korcsoport szerinti bontásban)

Nem meglepő, hogy hétvégén mindkét korosztály képviselői sokkal többet neteznek. Ekkor már a fiatalabbak körében is a napi 4 óránál többet internetezők aránya a legmagasabb. Ugyanakkor a két korosztály közti különbség még ezeken a tanítás nélküli napokon is kimutatható. Hétvégén a 15 évesnél idősebbeknek majdnem a fele 4 óránál többet netezik, míg ugyanez a 13-15 éveseknek csak 31%-áról mondható el.

Az internetezéssel töltött idő mennyisége az életkor mellett még leginkább két tényezőtől függ: az adatok azt mutatják, hogy a lányok, és a valamilyen saját eszközzel rendelkezők töltenek az átlagnál több időt online.



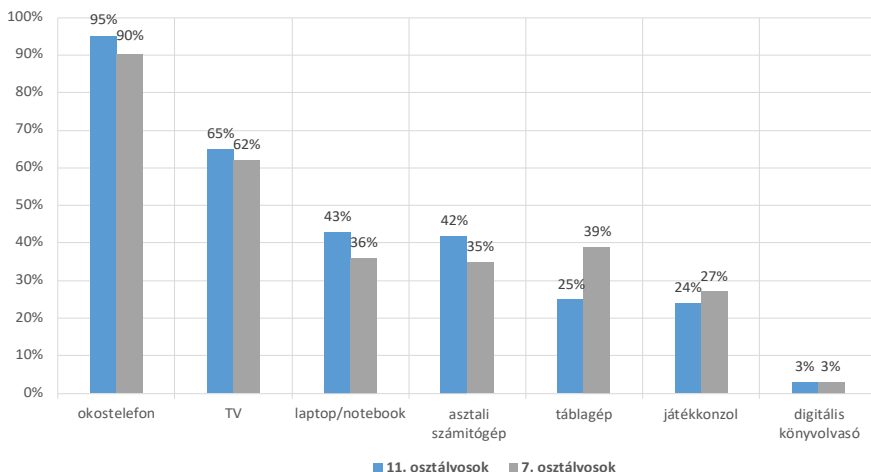
4. ábra: Internetezéssel töltött idő egy átlagos tanítás nélküli napon (a két vizsgált korcsoport szerinti bontásban)



5. ábra: A hétköznapi és hétvégén napi három óránál többet internetezők aránya (a saját számítógéppel rendelkező, illetve nem rendelkező kérdezettek körében, illetve nemek szerinti bontásban)

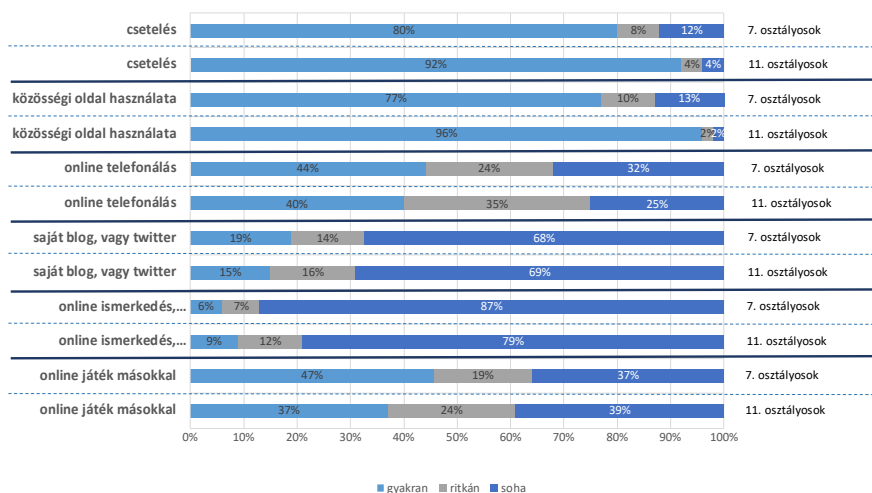
A fiatalok internethasználatának elsődleges helyszíne az otthon, illetve az iskola, de ma már azok aránya sem elhanyagolható, akik utazás közben használják. Saját bevallásuk szerint a 7. osztályosok 30%-a, míg a 11. osztályosok 61%-a gyakran internetezik menet közben. A kizárólag saját használatban, illetve a saját szobájában megtalálható eszközök nyil-

vánvalóan jelentős mértékben növelhetik az internetezéssel eltöltött időt. Míg az okostelefonok tekintetében nincsen érezhetőbb különbség a két korosztály között, addig a fiatalok szobájában inkább vannak mobil eszközök, mint hagyományos asztali gépek. A 7. osztályosok körében minden harmadik, míg az idősebb korosztályban minden negyedik gyerek rendelkezik táblagéppel. Érdekesség azonban, hogy nekik viszont nagyobb arányban van saját laptopjuk (43%), mint fiatalabb társaiknak (36%). Azaz már ez a néhány évnyi korbéli különbség is mutat trendszerű különbségeket abban, hogy a fiatalok milyen „digitális ökoszisztémához” férnek hozzá.



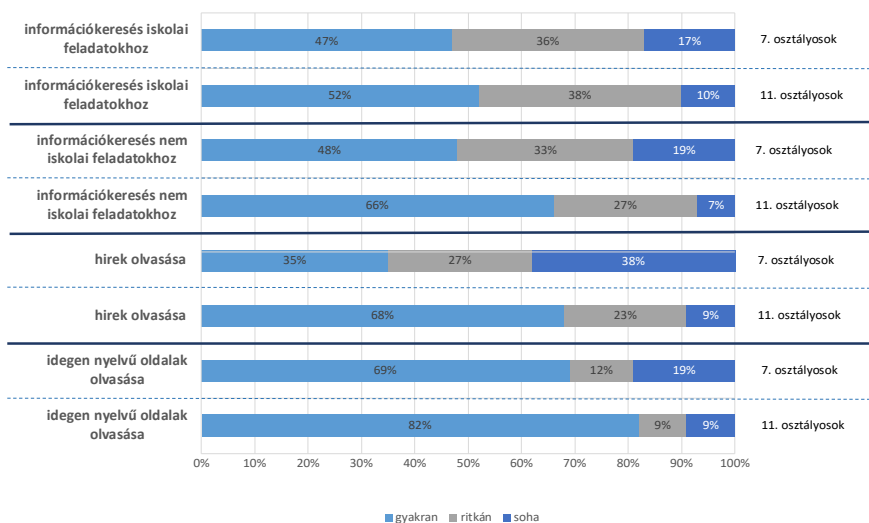
6. ábra: Eszközök saját tulajdonban, vagy saját szobájában (azok aránya, akiknek saját tulajdonában, vagy szobájában van az adott eszköz, a két vizsgált korcsoport szerinti bontásban)

Az elmúlt néhány év során ebben a korosztályban a mobiltelefon (okostelefon) vált az egyik legfontosabb platformmá. A legnépszerűbb tevékenységek ennek megfelelően a zenehallgatás/letöltés, illetve a csetelés és a közösségi oldalak használata. A 13-15 évesek 78%-a, a 16-18 évesek 90%-a gyakran hallgat zenét online, és csupán 9%, ill. 2% azok aránya, akik sosem tesznek ilyet. Továbbá a fiatalabbak 80%-a, az idősebbek 92%-a gyakran csetel a mobilján. Gyakorlatilag alig van olyan 15 év feletti, aki ne állította volna, hogy gyakran szokta a közösségi oldalakat használni (96%), de a fiatalabbak 77%-a is ebbe a csoportba sorolható. Bár ez utóbbi is igen nagy arány, a közösségi oldalak használatát illetően mutatkozik az egyik legnagyobb különbség a két korosztály között: míg az idősebbek (11. osztályosok) körében szinte mérhetetlen azok aránya, akik nem használnak valamilyen közösségi oldalt, addig a 7. osztályosok körében az arányuk (még) 13%.

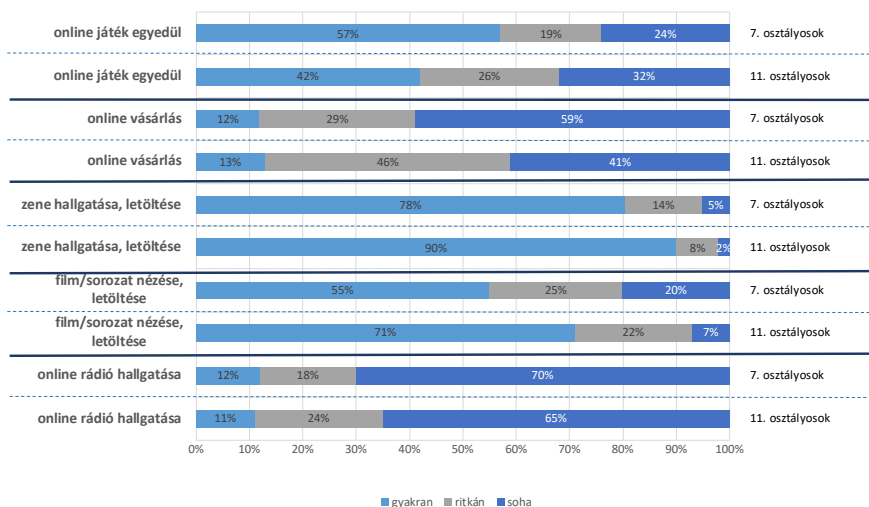


7. ábra: Internethasználat: kommunikációs és kapcsolattartási felhasználási módok (a két vizsgált korcsoport szerinti bontásban)

A csetelés szintén valamivel gyakoribb az idősebbek körében, csakúgy, mint a hírek olvasása, vagy a különböző információkereséssel kapcsolatos böngészések. Viszonylag elhanyagolható a különbség az iskolai feladatokat illetően: mindkét korosztálynak nagyjából a fele szokott a tanuláshoz szükséges dolgokat gyakran keresni a neten. Ezzel szemben a nem tanulási célzatú információkeresés sokkal elterjedtebb a 15 évesnél idősebbek körében, akiknek kétharmada gyakran böngész ilyesmit, szemben a fiatalabbak 48%-ával. Az online játékok viszont, akár egyedül, akár másokkal játsszák őket, népszerűbbek a fiatalabbak között: utóbbival csaknem felük, előbbivel több, mint felük (49%, ill. 57%) gyakran tölti idejét. Mindkét játékfajta esetében tíz idősebb gyerek közül nagyjából négy tartozik a gyakori játékosok csoportjába. Az online telefonálás, illetve a saját blog, vagy mikroblog írás szintén népszerűbb a fiatalabbak körében, bár ebben az esetben a különbségek már egyáltalán nem jelentősek. Összességében a mintába került fiatalok nagyjából 40%-a szokott gyakran online telefonálni, míg valamilyen blog írására egyharmaduk vállalkozik. A gyakran a szülők rémképeinek legfőbb forrásaként szóba kerülő online ismerkedés a jelek szerint viszont korántsem annyira elterjedt, mint azt sokan gondolják: a fiatalabbaknak 13%-a, az idősebbeknek 21%-a szokott online ismerkedni, tehát a döntő többségük sosem tesz ilyet.

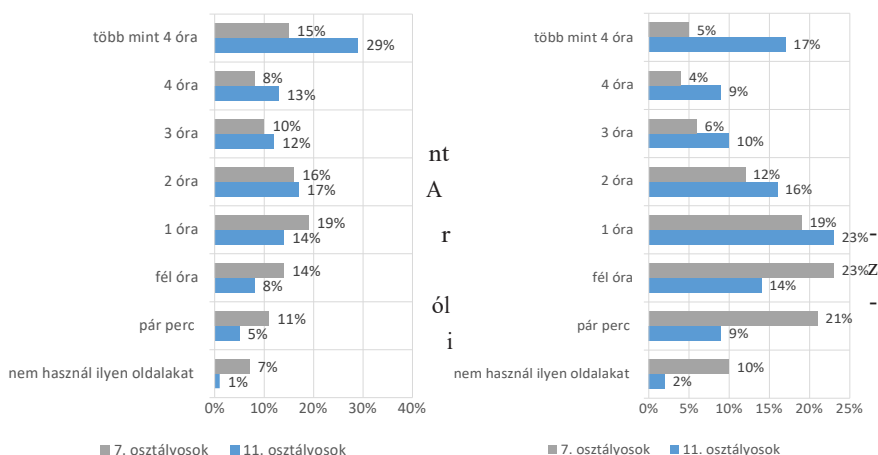


8. ábra: Internethasználat: információ- és ismeretszerzési felhasználási módok (a két vizsgált korcsoport szerinti bontásban)



9. ábra: Internethasználat: szórakozási célú és tranzakciós felhasználási módok (a két vizsgált korcsoport szerinti bontásban)

A filmek, sorozatok nézése/letöltése a zenehallgatást követően a legnépszerűbb online szórakozási forma: az idősebbek 71%-a, a fiatalabbak 55%-a gyakran tölti ezzel idejét. Az internetes vásárlás ezzel szemben nem nevezhető elterjedtnek, igaz ugyan, hogy ezzel kapcsolatban a gyakori előfordulás nem feltétlenül jelent napi megrendeléseket. Ebből a szempontból az, hogy a 13-15 évesek 12%-a, az idősebbek 13%-a szokott gyakran online vásárolni nem tekinthető alacsony aránynak, különösen azzal kiegészítve, hogy az idősebbeknek ezen felül csaknem fele ritkán, de szokott az interneten rendelni termékeket. Ugyanakkor a 13-15 évesek 59, a 15 évesnél idősebbek 41%-a sosem tesz ilyet. A legnépszerűtlenebb szórakozási célzatú internethasználati-forma a felsoroltak közül (és egyben a második legnépszerűtlenebb az online ismerkedés után) egyértelműen az online rádióhallgatás, amivel a fiatalok több mint kétharmada sosem tölti idejét.

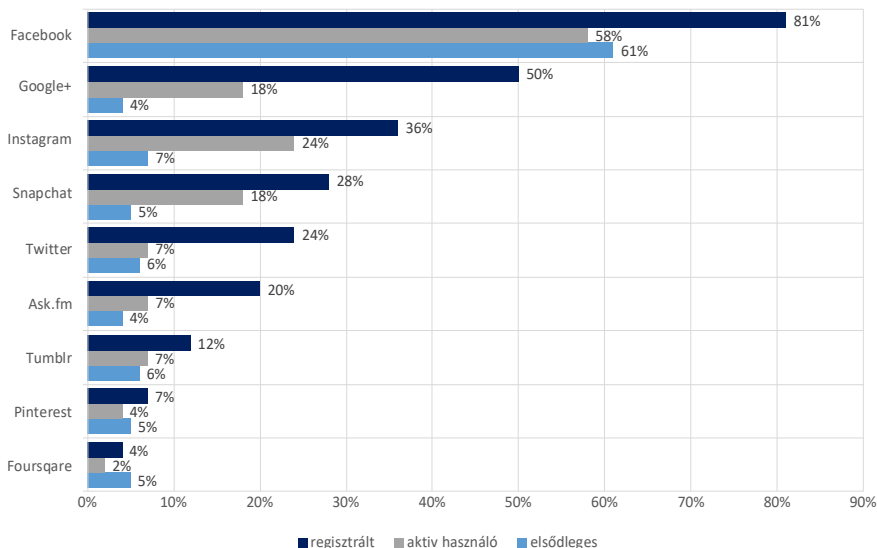


10. ábra: Egy átlagos tanítási napon és tanítás nélküli napon a közösségi oldalak használatával töltött idő

Látható, hogy a két vizsgált korosztály közötti pár évnnyi életkorbeli különbség a közösségi oldalak használatát is nagyobb mértékben meghatározza. A 13-15 évesek körében a használat még jóval kevésbé intenzív, sőt ebben a korcsoportban minden tizedik megkérdezett hétköznap nem is látogat ilyen oldalakat, sokan pedig csak fél percet, vagy nem több mint fél órát töltenek a közösségi oldalakon. A tanítás nélküli napokon természetesen más a helyzet, de 4 óránál többet még így is csupán 15%-uk van a közösségi oldalakon.

Akár még néhány évvel ezelőtt is, a közösségi oldal egyet jelentett pár nagy szolgáltatóval: a felhasználók jellemzően az iWiW – MySpace és a Facebook hármasa közül választottak. Az online közösségi hálózatoknak ez a „tájképe” mára nagymértékben átalakult.

kult. A Facebook kitüntetett szerepéhez nyilvánvalóan nem férhet kétség, ugyanakkor megjelentek és egyre népszerűbbek a némileg mást és máshogyan kínáló szolgáltatások. Nem véletlen tehát, hogy alig akad olyan fiatal a két korcsoportban, akinek ne lenne regisztrációja valamelyik közösségi oldalon. Vagy az érem másik oldalát tekintve, mindössze 8% azok aránya, akiknek saját bevallásuk szerint nincsen regisztrációjuk egyetlen szolgáltatónál sem.



11. ábra: A különböző közösségi oldalak népszerűsége (a 7. és 11. osztályosok körében)

Bár a fiatalok 81%-ának van Facebook regisztrációja, elsődleges közösségi oldalának már csak 61% tartja. De még ennél is kisebb, 58% azoknak az aránya, akik aktív Facebook-használónak tartják magukat. Ami magát a regisztrációt illeti, a második legnépszerűbb közösségi oldal a Google+, amire azonban valószínűleg sokan a Gmail szolgáltatáshoz kapcsolódóan, vagy az Android rendszerű telefonjuk miatt regisztrálnak, hiszen az aktív használók aránya jóval alacsonyabb, és alig mérhető azok aránya, akiknek ez lenne az elsődleges szolgáltatás. Nem így az Instagram, ami amellet, hogy a kérdezettek 36%-ának van rajta regisztrációja, 24% életében aktívan jelen is van. A Snapchattal kapcsolatban hasonlóak az arányok, bár valamivel kevésbé népszerű. A Twitteren szintén sokan vannak elvileg jelen, de az aktív használók aránya még alacsonyabb, csakúgy mint az Ask.fm esetében.

A fiatalok átlagban majdnem három (2.8) oldalon vannak regisztrálva, 18% pedig igazi „mindenevő”, hiszen nekik öt, vagy annál több oldalon is van regisztrációjuk. Az adatok alapján a lányok szinte mindegyik oldalra nagyobb arányban regisztrálnak. Viszonylag

nagy a különbség az Instagram (lányok 43, fiúk 30%-ának van regisztrációja) és a Tumblr (lányok 17, fiúk 9%-a regisztrált használó) esetében. A Google+ viszont érdekes módon a fiúk közt népszerűbb. A másik meghatározó tényező a kor: érthető módon az idősebbeknek szinte mindegyik közösségi oldalon nagyobb arányban van regisztrációjuk. A Facebook esetében a különbség 8 százalékpontos (77 és 85%), a Snapchat esetében ennél jóval nagyobb (21 és 34%), és viszonylag számottevő a Tumblr esetében is (9 és 16%).

B. Ismerősök száma

A közösségi oldalon lévő kapcsolatok számáról nem könnyű pontos adatokat kapni. A kutatás során az elsődlegesen használt közösségi oldallal kapcsolatban kérdeztük meg, hogy ott a válaszadónak hány ismerőse van. Átlagosan 521 ismerőssel rendelkeznek elsődleges közösségi oldalukon, ezer, vagy annál több ismerőse pedig 15%-uknak van. A 7. osztályosoknak átlagosan sokkal kevesebb ismerősük van (326), mint az idősebbeknek (668). Emellett – hasonlóan az eddigi trendekhez – a lányok átlagosan több kapcsolatot tartanak a közösségi oldalakon, mint a fiúk (536 és 509).

	7. osztályos	11. osztályos
fiú	310	638
lány	341	706

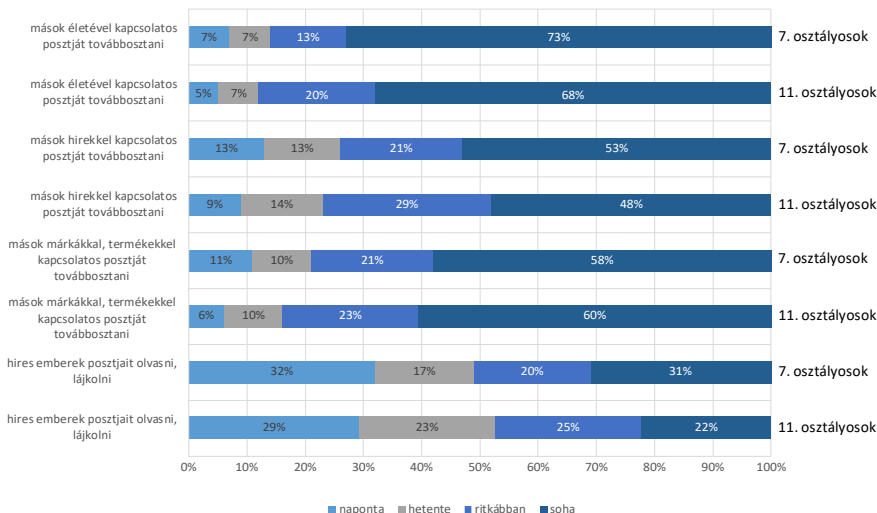
12. ábra: Ismerősök átlagos száma a két nem körében (a két vizsgált korcsoport szerinti bontásban)

Amint az a fenti táblázatból kiolvasható, a fiúk és a lányok közti különbség a korcsoportos bontásban is jelentkezik, ennek megfelelően a 11. osztályos lányok rendelkeznek átlagosan a legtöbb ismerőssel.

A rengeteg ismerős kezelésének egyik legfontosabb módja, és egyben a biztonságos használat, megosztás elősegítője is, ha a felhasználók csoportokba rendezik ismerőseiket (eszerint lehet pl. egyszerűbben kezelni az ismerősök jogosultságait). Ezzel a lehetőséggel azonban csak kevesen élnek: a fiatalok fele (52%) egyáltalán nem szokta ismerőseit ilyen módon rendezni, 43%-uk ismerőseinek egy részét rendezi csoportokba, és csupán 4% azok aránya, akik minden ismerős esetén élnek ezzel a lehetőséggel. Minél több kapcsolattal rendelkezik valaki, annál valószínűbb, hogy azokat csoportba rendezi. Ugyanakkor jelentős különbség csak a legkevesebb ismerőssel (50-nél kevesebb) rendelkezők és az összes többi csoport között fedezhető fel.

C. Aktivitás

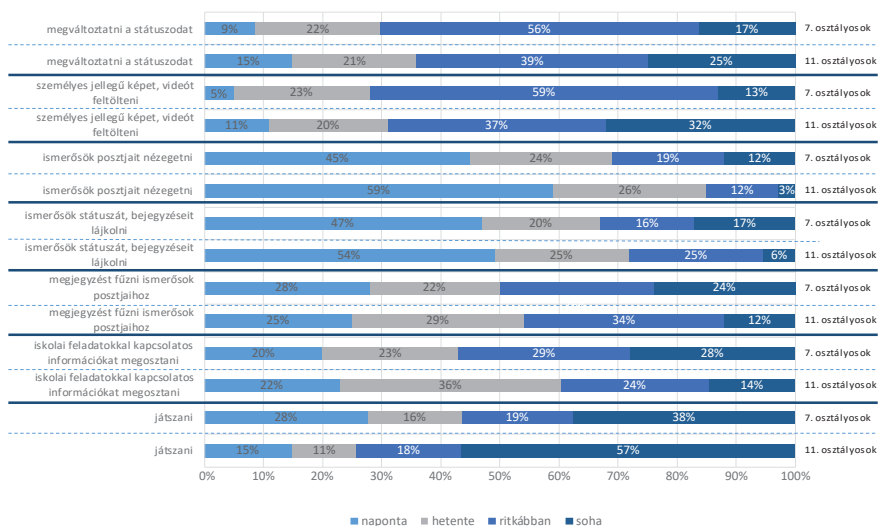
Mint láttuk a „mai fiatalok” nagy része mindennap órákat tölt a közösségi oldalak használatával, a hétvégi programok közül pedig még inkább előkelő helyet foglal el a szabadidő eltöltésének ez a módja. De vajon mit is takar a közösségi oldalak használata? Az adatok szerint egyrészt a használati mintázatokat tekintve nincs jelentősebb különbség az idősebb és a fiatalabb korosztály között, másrészt pedig a passzív felhasználási módok vezetnek a népszerűségben. Itt is igaz az a korábban már a mobiltelefon és az internet használatánál megfigyelt jelenség, hogy az idősebbek gyakorlatilag minden használati formában aktívabbak, kivéve a játékokat. Ugyanakkor mindkét korosztályban a legnagyobb arányban azok vannak, akik gyakran nézegetik, illetve lájkolják ismerőseik posztjait. A fiatalok (és persze a felnőttek) legnagyobb része a közösségi oldalakon a mások által létrehozott tartalmak (cikkek, képek, videók) fogyasztói, esetleg továbbterjesztői. Jóval kevesebben vannak azok, akik saját maguk hoznak létre valamilyen kreatív vagy kevésbé kreatív tartalmat.



13. ábra: Aktivitás a közösségi oldalon I. (a két vizsgált korcsoport szerinti bontásban)

Nagyjából a kérdezettek egyharmada „híres emberek” posztjait is gyakran olvasgatja. A saját profil „ápolása” már korántsem olyan elterjedt: sem a státusz frissítését, sem a saját képek, videók feltöltését nem végzik különösen nagy arányban gyakran a fiatalok. Mindkét esetben nagyjából egyharmadukról mondható el, hogy heti rendszerességgel, vagy ennél gyakoribban foglalkoznának saját profiljukkal. Az iskolai feladatokkal kapcsolatos aktivitás

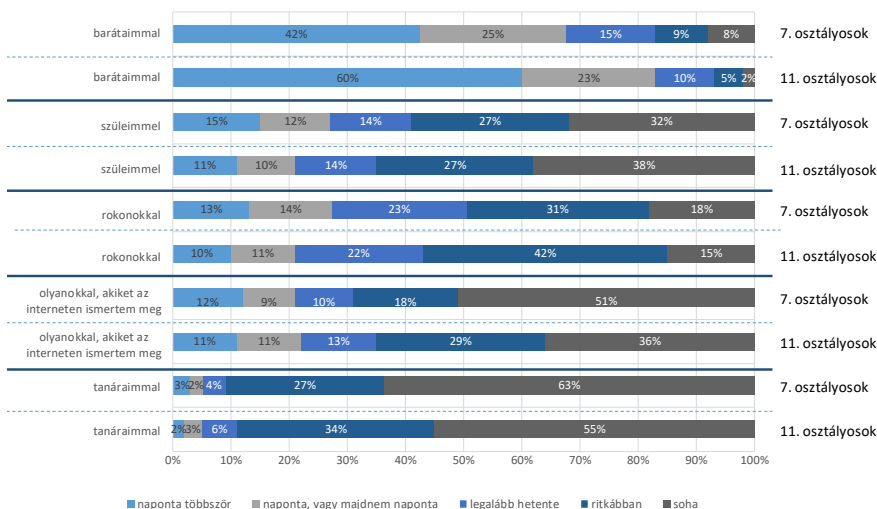
valamivel gyakoribb, sőt az idősebbek körében már 58% azoknak az aránya, akik minimum heti rendszerességgel használják erre (is) a közösségi oldalakat.



14. ábra: Aktivitás a közösségi oldalon II. (a két vizsgált korcsoport szerinti bontásban)

A mások posztjainak megosztása egyáltalán nem népszerű, legyen szó akár magán-jellegű beírásokról, hírekről, vagy márkákkal kapcsolatos információkról.

A közösségi oldalak egyben a barátokkal való beszélgetésnek, kapcsolattartásnak is fontos helyszínét jelentik: a 11. osztályosok 60%-a naponta többször is érintkezik így a barátaival, és csak 2% az aránya körükben azoknak, aki sosem használja erre a közösségi oldalt. A fiatalabbak ugyan ritkábban használják ezt a kommunikációs csatornát, de még körükben is 42% azoknak az aránya, akik naponta többször is beszélgetnek barátaikkal ebben a formában.



15. ábra: Milyen gyakran vagy kapcsolatban az alábbiakkal a közösségi oldalon? (a két vizsgált korcsoport szerinti bontásban)

Más csoportokkal nem ilyen élénk a közösségi oldalon folyó kommunikáció, de azért szerepe nem elhanyagolható. A fiatalok többsége a szüleivel is fenntart bizonyos mértékű kommunikációt ebben a formában. Sőt, 15% és 11%-uk (korosztálytól) függően lényegében folyamatos, napi kapcsolatban van a szülőkkel a közösségi oldalakon keresztül. Ennél jóval kevesebben vannak azok, akik a tanáraikkal is fenntartanak kapcsolatot, de azért minden tizedik fiatal legalább hetente él ezzel a lehetőséggel.

A GYERMEKEK JOGAI ONLINE KÖRNYEZETBEN

A gyermekek jogait 54 cikkelyben rögzítő, a Gyermek jogairól szóló, New York-ban, 1989. november 20-án kelt ENSZ Egyezmény és a magyarországi kihirdetéséről szóló 1991. évi LXIV. törvény katalógusa szerint haladva az alábbi jogok vagy szabályok érvényesíthetők közvetlenül online környezetben (kivonat):

1. cikk: Az Egyezmény vonatkozásában gyermek az a személy, aki tizennyolcadik életévét nem töltötte be, kivéve, ha a reá alkalmazandó jogszabályok értelmében nagykorúságát már korábban eléri.
2. cikk: a gyermeki jogokat a gyermeknek, szüleinek vagy törvényes képviselőjének faja, színe, neme, nyelve, vallása, politikai vagy más véleménye, nemzeti, nemzetiségi vagy társadalmi származása, vagyoni helyzete, cselekvőképтелensége, születési vagy egyéb helyzete szerinti különbségtétel nélkül kell biztosítani. Az Egyezményben részes államok megteszik a megfelelő intézkedéseket arra, hogy a gyermeket hatékonyan megvédjék minden, bármely formában jelentkező megkülönböztetéstől és megtorlástól, amely szülei, törvényes képviselői vagy családtagjai jogi helyzete, tevékenysége, véleménynyilvánítása vagy meggyőződése miatt érhetné őt.
3. cikk: a hatóságok minden, a gyermeket érintő döntésükben a gyermek mindenek felett álló érdekét veszik figyelembe elsősorban.
4. cikk: Az Egyezményben részes államok meghoznak minden olyan törvényhozási, közigazgatási vagy egyéb intézkedést, amelyek az Egyezményben elismert jogok érvényesüléséhez szükségesek. Amennyiben gazdasági, szociális és kulturális jogokról van szó, ezeket az intézkedéseket a rendelkezésükre álló erőforrások határai között és szükség esetén, a nemzetközi együttműködés keretében hozzák meg.
5. cikk: Az Egyezményben részes államok tiszteletben tartják a szülőknek vagy, adott esetben a helyi szokás szerint, a nagycsaládnak vagy a közösségnek, a gyámoknak vagy más, a gyermekért törvényesen felelős személyeknek azt a felelősségét, jogát és köteletségét, hogy a gyermeknek az Egyezményben elismert jogai gyakorlásához, képességei fejlettségének megfelelően, iránymutatást és tanácsokat adjanak.
6. cikk: Az Egyezményben részes államok a lehetséges legnagyobb mértékben biztosítják a gyermek fejlődését.
8. cikk: Az Egyezményben részes államok kötelezik magukat arra, hogy törvénysértő beavatkozás nélkül tiszteletben tartják a gyermeknek saját személyazonossága – ideértve állampolgársága, neve, családi kapcsolatai – megtartásához fűződő, a törvényben elismert jogát. Ha a gyermeket törvénytelen módon megfosztják személyazonossága alkotó elemeitől vagy azoknak egy részétől, az Egyezményben részes államok megfelelő segítséget és védelmet nyújtanak ahhoz, hogy személyazonosságát a lehető legrövidebb időn belül helyreállítsák.

12. cikk: Az Egyezményben részes államok az ítélőképessége birtokában lévő gyermek számára biztosítják azt a jogot, hogy minden őt érdeklő kérdésben szabadon kinyilváníthassa véleményét. A gyermek véleményét, figyelemmel korára és érettségi fokára, kellően tekintetbe kell venni.

13. cikk: A gyermeknek joga van a véleménynyilvánítás szabadságára. Ez a jog magában foglalja mindenfajta tájékoztatás és eszme határookra tekintet nélküli kérésének, megismerésének és terjesztésének szabadságát, nyilvánuljon meg az szóban, írásban, nyomtatásban, művészi vagy bármilyen más, a gyermek választásának megfelelő formában. Ennek a jognak a gyakorlása csak a törvényben kifejezetten megállapított korlátozásoknak vethető alá, amelyek

a) mások jogainak és jó hírnevének tiszteletben tartása, illetőleg

b) az állam biztonsága, a közrend, a közegészségügy, vagy a közkerölcs védelme érdekében szükségesek.

14. cikk: Az Egyezményben részes államok tiszteletben tartják a gyermek jogát a gondolat-, a lelkiismeret- és a vallásszabadságra. Az Egyezményben részes államok tiszteletben tartják a szülőknek vagy, adott esetben, a gyermek törvényes képviselőinek azt a jogát és kötelességét, hogy a gyermeket e jogának gyakorlásában képességei fejlettségének megfelelően irányítsák. A vallás vagy meggyőződés kinyilvánításának szabadságát csak a törvényben megállapított olyan korlátozásoknak lehet alávetni, amelyek a közbiztonság, a közrend, a közegészségügy, a közkerölcs, vagy mások alapvető jogai és szabadságai védelmének érdekében szükségesek.

15. cikk: Az Egyezményben részes államok elismerik a gyermek egyesülési jogát.

16. cikk: 1. A gyermeket nem szabad alávetni magánéletével, családjával, lakásával vagy levelezésével kapcsolatban önkényes vagy törvénytelen beavatkozásnak, sem pedig becsülete vagy jó hírneve elleni jogtalan támadásnak. 2. Ilyen beavatkozás vagy támadás ellen a gyermeket megilleti a törvény védelme.²³

17. cikk: Az Egyezményben részes államok elismerik a tömegtájékoztatási eszközök feladatának fontosságát, és gondoskodnak arról, hogy a gyermek hozzájusson a különböző hazai és nemzetközi forrásokból származó tájékoztatáshoz és anyagokhoz, nevezetesen azokhoz, amelyek szociális, szellemi és erkölcsi jóléte előmozdítását, valamint fizikai és szellemi egészségét

23 A francia ombudsman 2012-es tanulmányának (Children and screens: Growing up in a digital world) kiindulópontja, hogy az internet – és különösen a hordozható, egyre olcsóbbá és kisebbé váló eszközök – elterjedése megállíthatatlan, a gyerekekre váró veszélyek ismertek, ugyanakkor nincs egységes stratégiája sem a jogalkotóknak, sem a jogalkalmazóknak, sem a szakembereknek. Míg a kisgyermek túlzott tévézésének negatív hatását nem vitatja senki, addig a modern és divatos neveléshez hozzátartozik, hogy maga a szülő adjon egyre kisebb – szinte csecsemő – gyermeke kezébe iPad-et, iPod-ot, okostelefont. Mivel a gyerekek beleszületnek a digitális világba, és ez az ő esetükbe alig-alig elválasztható a való világtól, meg kell határozni a „digitális magánélet” fogalmát a New York-i Gyermekjogi Egyezmény 16. cikkelyének vonatkozásában. In.: <http://crin.org/enoc/resources/infoDetail.asp?id=30126>, 2013-03-14

szolgálják. Ebből a célból a részes államok: a) előmozdítják azt, hogy a tömegtájékoztatási eszközök – a 29. cikk szellemének megfelelően – a gyermek számára szociális és kulturális szempontból hasznos tájékoztatást és anyagokat terjesszenek; b) előmozdítják a nemzetközi együttműködést a különféle hazai és nemzetközi, kulturális forrásokból származó ilyenfajta tájékoztatás és anyagok előállítására, cseréje és terjesztése érdekében; c) előmozdítják a gyermek-könyvek előállítását és terjesztését; d) előmozdítják, hogy a tömegtájékoztatási eszközök különösen vegyék figyelembe az őslakossághoz, illetőleg a kisebbségi csoportokhoz tartozó gyermek nyelvi szükségleteit; e) elősegítik a gyermek jólétére ártalmas információk és anyagok elleni védelmét megfelelően szolgáló irányelvek kidolgozását a 13. és a 18. cikk rendelkezéseinek figyelembevételével.

19. cikk: 1. Az Egyezményben részes államok megtesznek minden arra alkalmas, törvényhozási, közigazgatási, szociális és nevelési intézkedést, hogy megvédjék a gyermeket az erőszak, a támadás, a fizikai és lelki durvaság, az elhagyás vagy az elhanyagolás, a rossz bánásmód vagy a kizsákmányolás – ideértve a nemi erőszakot is – bármilyen formájától mindaddig, amíg szüleinek vagy valamelyik szülőjének, illetőleg törvényes képviselőjének vagy képviselőinek, vagy bármely más olyan személynek, akinél elhelyezték, felügyelete alatt áll. 2. Ezek a védelmi intézkedések szükség szerint olyan hatékony eljárásokat foglalnak magukban, amelyek a gyermek és gondviselői számára szükségesek szociális programok létrehozását teszik lehetővé, továbbá a fentebb leírt rossz bánásmód eseteiben hozzájárulnak a cselekmény felismeréséhez, bejelentéséhez, a jelentés illetékes helyre juttatásához, vizsgálatához, kezeléséhez és az esetek figyelemmel kíséréséhez; szükség szerint magukban foglalják a bírói beavatkozással kapcsolatos eljárást is.

23. cikk: Az Egyezményben részes államok elismerik, hogy a szellemileg vagy testileg fogyatékos gyermeknek emberi méltóságát biztosító, önfenntartását előmozdító, a közösségi életben való tevékeny részvételét lehetővé tevő, teljes és tisztességes életet kell élnie.

28. cikk: Az Egyezményben részes államok elősegítik és előmozdítják a nemzetközi együttműködést az oktatásügy területén, különösen annak érdekében, hogy megszüntessék a tudatlanságot az egész világon, és megkönnyítsék a tudományos és technikai ismeretek megszerzését, valamint a korszerű oktatási módszerek megismerését.

29. cikk: 1. Az Egyezményben részes államok megegyeznek abban, hogy a gyermek oktatásának a következő célokra kell irányulnia:

- a) elő kell segíteni a gyermek személyiségének kibontakozását, valamint szellemi és fizikai tehetségének és képességeinek a lehetőségek legtágabb határáig való kifejlesztését;
- b) a gyermek tudatába kell vésni az emberi jogok és az alapvető szabadságok, valamint az Egyesült Nemzetek Alapokmányában elfogadott elvek tiszteletben tartását;
- c) a gyermek tudatába kell vésni a szülei, személyazonossága, nyelve és kulturális értékei iránti tiszteletet, valamint annak az országnak, amelyben él, továbbá esetleges származási országának a nemzeti értékei iránti és a sajátjától különböző kultúrák iránti tiszteletet;

d) fel kell készíteni a gyermeket arra, hogy a megértés, a béke, a türelem, a nemek közti egyenlőség, valamennyi nép, nemzetiségi, nemzeti és vallási csoport és az öslakosok közötti barátság szellemében tudja vállalni a szabad társadalomban az élettel járó mindenfajta felelősséget;

e) a gyermek tudatába kell vésni a természeti környezet iránti tiszteletet.

31. cikk: Az Egyezményben részes államok elismerik a gyermeknek a pihenéshez és a szabadidő eltöltéséhez, a korának megfelelő játékhöz és szórakoztató tevékenységekhez való jogát, azt, hogy szabadon részt vehessen a kulturális és művészeti életben.

34. cikk: Az Egyezményben részes államok kötelezik magukat arra, hogy megvédik a gyermeket a nemi kizsákmányolás és a nemi erőszak minden formájától. Ebből a célból az államok hazai, kétoldalú és többoldalú síkon különösen az alábbiak megakadályozására tesznek intézkedéseket:

a) a gyermek ösztönzése vagy kényszerítése törvénytelen nemi tevékenységre;

b) a gyermekek kizsákmányolása prostitúció vagy más törvénytelen nemi tevékenység céljára;

c) a gyermekek kizsákmányolása pornográf jellegű műsorok vagy anyagok elkészítése céljára.

36. cikk: Az Egyezményben részes államok megvédik a gyermeket a jólétére bármilyen szempontból káros kizsákmányolás bármely más formája ellen is.

41. cikk: Az Egyezmény egyetlen rendelkezése sem érinti a) az Egyezményben részes valamely állam hazai jogszabályainak; vagy b) az ebben az államban hatályban lévő nemzetközi jognak a gyermek jogai megvalósulása szempontjából kedvezőbb rendelkezéseit.

42. cikk: A részes államok kötelezik magukat, hogy az Egyezmény elveit és rendelkezéseit hatékony és arra alkalmas eszközökkel a felnőttek és a gyermekek széles körében ismertetik.

Az általános gyermekjogok mellett szó kell, hogy essen a kifejezetten az adatkezeléshez kötődő jogosítványokról is. Az uniós adatvédelmi rendelet közvetlenül alkalmazandó főszabályként minden magáncélú adatkezelésre, míg a bünygyi, nemzetbiztonsági és honvédelmi célú adatkezelések szabályai az **információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (Infotv.) kerültek beépítésre**

A jogszabályok . értelmében személyes adat minden olyan információ, mely egy élő emberhez (érintett) közvetlenül vagy közvetve kapcsolható. Személyes adatokat kezelni csak megfelelő joggalappal, például az érintett beleegyezésével vagy jogi kötelezettség teljesítése érdekében, esetleg közveszély elhárítása érdekében szabad. A személyes adatok speciális kategóriája a különleges adatok köre, ide tartoznak a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviselési szervezeti tagságra, a szexuális életre, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adatok, valamint a bünygyi személyes adat. A különleges adatok kezeléséhez nagyon szigorú törvényi feltételek járulnak Magyarországon 14 év alatti gyermek esetében az adatkezelési nyilatkozatokat törvényes képviselője adja, ugyanakkor

az internetes szolgáltatások igénybevételéhez szükséges hozzájárulást a 16. életévet betöltött fiatal már önállóan megteheti.

A klasszikus adatvédelmi elvek értelmében:

- Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.
- Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
- A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
- Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

Az érintettnek joga van a tájékoztatáshoz, a hozzáféréshez, a helyesbítéshez, bizonyos esetekben az adatok másik szolgáltatóhoz való átviteléhez, a törléshez, a tiltakozáshoz és ahhoz, hogy jogorvoslatért a NAIH-hoz vagy bírósághoz forduljon. A bíróság adatvédelmi jogainak sérelme miatt akár kártérítést is megítélhet a sértett részére. (A Polgári Törvénykönyv „sérelemdíj”²⁴ megnevezésű jogintézménye alapján a károsult szintén nem vagyoni kártérítést kérhet személyiségi jogainak megsértése esetén – például, ha jogellenesen kezelték személyes adatait vagy engedély nélkül hozták nyilvánosságra fényképét. Újdonság, hogy már nem kell bizonyítani az elszenvedett lelki sérelem költségoldalát, ezt a bíróság mérlegeléssel állapítja meg.)

24 A Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:52. § (1) Akit személyiségi jogában megsértenek, sérelemdíjat követelhet az őt ért nem vagyoni sérelemtől. (2) A sérelemdíj fizetésére kötelezés feltételeire – különösen a sérelemdíjra köteles személy meghatározására és a kimentés módjára – a kártérítési felelősség szabályait kell alkalmazni, azzal, hogy a sérelemdíjra való jogosultsághoz a jogsértés tényén kívül további hátrány bekövetkeztének bizonyítása nem szükséges. (3) A sérelemdíj mértékét a bíróság az eset körülményeire – különösen a jogsértés súlyára, ismétlődő jellegére, a felróhatóság mértékére, a jogsértésnek a sértettre és környezetére gyakorolt hatására – tekintettel, egy összegben határozza meg.

Gyermekek esetében az általános elv – a gyermek mindenk felett álló érdeke – elméletileg összeütközésbe kerülhet a gyermek magánéletének sérthetlenségéhez fűződő jogával. Ez különösen a gyermekvédelmi eljárások során következhet be, mikor a törvényben előírt kötelező adatkezelések felhatalmazást adnak a kezelőorvosnak, a tanárnak vagy a gyermekvédelmi jelzőrendszer többi szereplőjének, hogy a veszélyeztetett gyermek legintimebb adatait is a hatósági eljárás során átadják, továbbítsák (például családon belüli erőszak vagy gyermekkorú anya terhessége esetében).

Az adatkezelési általános elvek is különös színezetet nyernek gyermek-érintett esetében: a tisztességes adatkezelés vagy az adatok naprakészségének számonkérésénél bizony figyelemmel kell lenni az érintett korára és arra, hogy ami kisebb korban még legitim célú adatkezelés volt, az egy nagyobb gyermeknél vagy fiatal felnőttél egész más dimenziót jelent²⁵ (például orvosi kutatás céljára készült fényképek esetén).

Az interneten történő kommentezésekkel, a személyes adatok visszaélészerű felhasználásával polgári jogi jogsértések és bűncselekmények is megvalósulhatnak – ám ezek tipikusan olyan esetek, ahol a hagyományos jogérvényesítési utak nem feltétlenül járhatók. Ha a közösségi oldalt kiszolgáló szerver nem Magyarország területén található, joghatósági, illetékességi problémák merülhetnek fel. Könnyen előfordulhat, hogy nem tudni, ki az elkövető, vagy gyermekkor miatt nem büntethető.

Az internethasználat során megvalósult jogsértések (például zaklatás, becsületesítés) közül a személyhez fűződő jogok megsértése esetén segíthet leginkább valamilyen konfliktuskezelési eljárás, melyet az érintett felek már zajló jogi eljárások közben, illetve azok megindulását megelőzően is igénybe vehetnek.

A **mediáció** egy speciális konfliktuskezelési módszer, amelynek lényege, hogy a két fél vitájában felkérésükre egy semleges harmadik fél (mediátor) jár közben. A mediátor a problémamegoldó folyamat keretében segít tisztázni a konfliktus természetét és olyan megoldást találni, amely mind a két fél számára kielégítő. A mediáció arra is kiváló fórum lehet, hogy a kárt okozóval a sértett átbeszélje a sérelmeit, számba vegyék, hogy milyen anyagi és nem anyagi kár keletkezett.

Alapvetően két típusú mediáció létezik az iskolákban: az egyik a klasszikus, amikor két fél leül egy külső harmadik fél vezetésével nézeteltérésük, problémájuk megbeszélésére, a másik a resztoratív (helyreállító) típusú jóvátételi egyeztetés, ahol valamilyen normasértés történt, és az elkövető vállalja a felelősséget azért, hogy ezt jóvá teszi. A klasszikus iskolai mediáció jelenleg nincsen szabályozva, de ahhoz, hogy a pedagógusok és intézményvezetők beépítsék mindennapi munkájukba az erőszakmentes kommunikációs technikákat és a békés vitarendezés módszereit, nem is szükséges külön szabályozási háttér. A resztoratív

jóvátételi egyeztetés intézményét viszont a fegyelmi eljárás keretei közé beemelte a jogalkotó. A nevelési-oktatási intézmények működéséről szóló 11/1994. (VI. 8.) MKM rendelet 32. §-a alapján 2008-tól már van lehetőség arra, hogy normasértés esetén az általános vagy középiskolában, illetve a kollégiumban megszervezzék azt az egyeztető eljárást, amely keretei között fel lehet tární a kötelességszegéshez elvezető eseményeket, és megoldást lehet keresni az érdeksérelem orvoslására is. Az eljárás során az érintettek megismerhetik a kötelességszegéshez vezető okokat és indokokat, az okozott kárt, a sértett érdekeit, lehetőség nyílik a jóvátételre és a reintegrációra, valamint hozzásegítheti a feleket a problémáik megoldására. Az egyeztető eljárás folyamán az érintettek tulajdonképpen közös tervet készítenek a probléma megoldására. Ha az elkövető tettét beismeri, vagyis felelősséget vállal az általa okozott kárért, segíthet annak helyreállításában. Az elkövető a kár helyreállításnak módját a sértettel együtt beszéli meg, és egy megállapodás keretében rögzítik.

Végül a büntetőeljárás keretében is van lehetőség mediációra. A hatályos büntető-kódex szerint, ha a fiatalkorú terhelt tevékeny megbánást mutat és a meghatározott, a nem igazán súlyos bűncselekmény elkövetését a vádemelésig beismerte, valamint közvetítői (mediációs) eljárás keretében a sértett által elfogadott módon és mértékben a bűncselekménnyel okozott sérelmet jóvátette, akkor a büntetés kiszabása vagy végrehajtása felfüggeszthető.

Kutatások alapján a jóvátételi technikák alkalmazása hatékonyan segíthet megelőzni későbbi konfliktusok kialakulását és az emberi kapcsolatok helyreállítását – például egy iskolai osztályban. Sajnos a tapasztalatok alapján nem ritka, hogy a kiszemelt áldozat ellen az online bullying „elkövetője” nem egy gyerek, hanem az osztályból nagyon sokan egyszerre vagy párhuzamosan ugyan, de egymást erősítve.

A. Életkor és érettség

Gyermek az a személy, aki 18. életévét még nem töltötte be, kivéve, ha a reá alkalmazandó jogszabályok értelmében nagykorúságát már korábban eléri.²⁶ A magyar polgári jogi szabályozás²⁷ ezt megismétli és hozzáteszi, korlátozottan cselekvőképes az a kiskorú, aki a 14. életévét betöltötte és nem cselekvőképtelen.

A gyermek helyzete statikus és dinamikus nézőpontból egyaránt megközelíthető: gyermek az a személy, aki még sem fizikailag, sem lelkiileg nem teljesen érett, ugyanakkor testileg és lelkiileg is folyamatosan halad a felnőtté válás útján²⁸. A valóságban azonban nem biztos, hogy egy 19 éves fiatal felnőtt és egy 16 éves gyermek más érettségi szinten áll. Azt, hogy valaki a korához képest érett vagy éretlen, rengeteg tényező befolyásolhatja, például társadalmi-, vallási-, etnikai hovatartozás, neveltetés, családi háttér, addig szerzett életbeli tapasztalatok (külső hatások), egyéni adottságai, valamint a tanulás, az olvasottság, vagy az ismeretek bővítésére irányuló akarat. Az érettség-éretlenség relativitását is feltételez, hiszen mindig a kortársakhoz viszonyítunk.

A magyar büntetőjogban a büntetőjogi vétőképeség 12 éves kortól kezdődik, a polgári jogi nagykorúsághoz kötött cselekvőképeség (az adott személy szerződéses viszonyt létesíthet, vagy más jognyilatkozatot tehet) ugyanakkor a betöltött 18. életévhez kötött. Ekkor a szülők felügyeleti joga megszűnik, lehetségessé válik a külön engedély nélküli házasodás, munkavállalás, a szavazás, a felügyelet nélküli külföldre utazás, autó- vagy lakásvásárlás, hitelfelvétel, alkoholfogyasztás és dohányzás stb. Ezt megelőzően (kiskorúság) a legtöbb hasonló tevékenység vagy tiltott, vagy a szülő/gyám engedélyéhez kötött. A világ legtöbb országában az ember 18 év után válik nagykorúvá, elérve az önálló döntések meghozatalának lehetőségét (kivételek például Skócia, Japán, Indonézia vagy néhány észak-amerikai tagállam).

Mivel a gyermekek még fejlődésben lévő személyek, jogaik gyakorlásának – így az adatvédelemmel kapcsolatos joguk gyakorlásának is – testi és lelki fejlettségi fokukhoz kell igazodnia. Ezért az egyes jogrendszerek különbséget tesznek a 12 éves kor előtti, a 14-18, a 12-16, valamint a 16-18 éves kor közötti időszakok között.²⁹

26 A gyermekek jogairól szóló, 1989. november 20-i ENSZ-egyezmény 1. cikk

27 2013. évi V. törvény a Polgári Törvénykönyvről, 2:10

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

29 A95/46/ EK irányelv 29. alapján létrehozott munkacsoport 2009/2. sz. véleménye a gyermekek személyes adatainak védelméről (elfogadás időpontja: 2009. 02. 11.)

Gyermekek esetén mindig tekintettel kell lenni arra, hogy a személyes adatokhoz fűződő alapjog a gyermeket illeti, nem törvényes képviselőit, akik csupán nevükben és érdekében járnak el. A jogok érvényesítésének egyik vizsgálandó tényezője az adatkezeléshez való hozzájárulás lehetősége. A magyar jog előírja a kisebb gyermek véleményének kikérését (14 év alatt), ezt követően a gyermek és törvényes képviselőjének párhuzamos hozzájárulása szükséges (14-16 év között), nagyobb gyermek esetében pedig a gyermek kizárólagos hozzájárulása is elegendő (16 év felett). Kivételes esetben egy kisebb gyermek is tehet érvényes nyilatkozatot szülői hozzájárulás nélkül (például ha szexuális visszaélés áldozatává válik és a segítségvonalat szeretné hívni).

A hozzájárulás mellett másik fontos tényező a részvételhez való jog, tehát egy eljárás során a gyermek egyéni véleményét figyelembe kell venni.³⁰ Amikor azonban a gyermek képessé válik a részvételi jog gyakorlására, annak eredménye lehet egy közös, vagy akár önálló döntéshozatal is, például a róluk készült képek felhasználásának kérdésében: a szülő vajon felteheti-e a közösségi oldalra gyermeke képét, ha az tiltakozik és kínosnak tartja a megjelenést? (Divattá vált csecsemőkről és kisgyerekekről képek és videók tömegeit feltölteni, így a fejlett nyugati országokban élő, kétévesnél fiatalabb gyerekek több mint negyötödének már van digitális lábnyoma.³¹).

További érdekes téma a személyes adatokhoz való hozzáférés joga, amit a gyermek törvényes képviselője vagy a két szereplő közösen, de a gyermek akár törvényes képviselője ellenében is gyakorolhat (például kérheti kezelőorvosát, hogy a rá vonatkozó egészségügyi információkat ne adja át, azonban ebben az esetben az orvosnak lehet mérlegelési joga). Magyarországon a „16 éves szabály” az egészségügyben azt jelenti, hogy az egészségügyről szóló 1997. évi CLIV. tv. 16 § (6) bekezdése alapján már nem kell a törvényes képviselőt tájékoztatni az egészségügyi kezelésről, ha a gyermek erről így dönt és a gyermek saját jogán iratbetekintési joggal rendelkezik. Az Egyesült Királyságban a tizenévesek 12. életévük betöltését követően önállóan gyakorolhatják hozzáférési jogukat, több országban a törvényes képviselők tizenéves leánygyermekük adataihoz való hozzáférési joga abortusz esetén korlátozott.³²

Az életkor vizsgálata szempontjából lényeges azon internetes oldalak bemutatása, amelyek a regisztráció korhatárához kötött. A gyakorlatban köztudott, hogy a gyermekek a regisztráció során csak akkor adnak meg valós adatokat, ha ez nem akadályozza őket a további használatban. A televíziós műsorszolgáltatás során a korhatárjelölések és a szülői

30 Európa Tanács Miniszteri Bizottságának az egészségügyi adatok védelméről szóló ajánlása. 1998. február 13-i R(97)5. sz. ajánlás, 5.5. és 6.3. pont.

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

32 95/46/ EK irányelv 29. alapján létrehozott munkacsoport 2009/2. sz. véleménye a gyermekek személyes adatainak védelméről (elfogadás időpontja: 2009. 02. 11.)

felügyelet együttesen alkalmasak lehetnek a gyermekek megfelelő tévézési szokásainak kialakítására, de az internet világában sajnos nem lehet ilyen egyszerűen megoldani a gyermekekre káros tartalmak kiszűrését, mivel a világhálón lévő tartalmak nincsenek úgy kategorizálva, mint a televíziós műsorok. A neten egyetlen korlátozással találkozhatunk: a 18 év felettieknek szóló oldalakkal, melyek általában pornográf jellegűek. Az erőszakot sugárzó videók, képek, filmek általában nincsenek levédve. Ráadásul a pornográf oldalakra való bejutás sem okoz különösebb nehézséget egy gyermeknek, hiszen a legtöbb esetben az oldal felajánl két lehetőséget: elmúltam 18 éves; még nem múltam el 18 éves. A gyerek rákattint az elmúltam 18 éves földre, és már nézheti is a képeket, videókat, filmeket. Más oldalak látogatása korhatárral összefüggő regisztrációhoz kötött. Ebben az esetben a továbbjutás feltétele – és erre a fiatalok is hamar rájönnek –, hogy olyan születési dátum legyen megjelölve, ami alapján a regisztráló személy 18 év felettinek minősül. A gyermek ítélőképessége többek között azért is minősíthető éretlennek, mert állítólagos előnyökért cserébe hajlamos helytelen módon információkat kiadni magáról és nem méri fel annak veszélyét, hogy ezzel saját maga teremti meg a lehetőséget a visszaélésekre, tisztességtelen adatkezelésekre³³.

Egyszerűen szereti kipróbálni azokat a szolgáltatásokat, amelyekről hall az iskolában vagy a baráti körben. Hiába van például a Facebookon 13 éves korhatár, a regisztráltak közül sok millió tíz év alatti.³⁴

Végül komolyan felvetődhet a felelősség kérdése is, például a gyermek által okozott kár megtérítése során. A német Szövetségi Legfelsőbb Bíróság 2012 novemberi döntése értelmében például a szülő nem felelős a 13 éves gyermek illegális letöltéseiért (és az interneten elkövetett egyéb jogsértésért), amennyiben korábban kielégítő módon felvilágosította a gyermeket az internethasználat szabályairól és az alapvető tudnivalókról.³⁵

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

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

35 A szülő nem felelős a gyerek torrentezéséért in.: http://index.hu/tech/2012/11/23/a_szulo_nem_felelos_a_gyerek_torrentezeseert/, 2013-03-08

B. ANONIMITÁS – maszkkal könnyebb?

Az identitás, én-azonosság szerepeken, magatartásformákon, értékrendszereken keresztül a „teljes én” érzésével társul. A személyiségfejlődés a szocializáció eredménye, az emberi kölcsönhatások során jön létre. Az anonimitás kérdése az interneten számos dilemmát vet fel: egyrészt az interneten sokan álarc mögé bújnak, valódi nevüket és identitásukat nem vállalva nick- és álneveket használnak, egyszer használatos e-mail címek mögött blogolnak, fórumoznak, kommentelnek, és közben rettegnek attól, hogy valaki „felismeri” őket és megszerzi a személyes adataikat. Miközben ugyanezeket az adatokat a közösségi oldalakon önként adják meg boldog-boldogtalannak.³⁶ Másrészt azonban az anonimitás feladása és a személyes adatok kötelező kiszolgáltatása a szabadságjogok csorbulásához és a magánélet sérelméhez is vezethet.

Az online identitás, internetes identitás, avagy online személyiség olyan, internet felhasználók által létrehozott közösségi (csoport)identitás, amelyet hálózati közösségekben és weboldalakon használnak. Sokan eredeti nevüket eltitkolva álneveket használnak, így valós énjükről csupán annyi és olyan információt osztanak meg másokkal, amennyit és amilyen képet önmagukról festeni szeretnének. Az online identitás, amely legtöbb esetben egyébként anonimitást is jelent, több kérdést is felvet arról, hogy az interneten megjelenített személyiség hogyan és milyen kapcsolatokat képes létrehozni és fenntartani a virtuális világban. Amikor az online anonim egyén interakcióba lép egy szociális szférában, akkor egy maszkot tart a személyisége elé, hiszen meg kell adnia olyan specifikus információkat magáról, mint életkor, nem, cím, felhasználónév és így tovább. Anonim módon bárki bármit közölhet a világ felé, ami közel sem valószínű, hogy fedi a valóságot. Ebben az esetben egy hamis maszk mögé rejtőzik az illető, ami félelemtől és az önbecsülés hiányáról árulkodik.

Az internetes visszaélések, és a bűncselekmények megelőzése érdekében egyre inkább tendencia az anonimitás eltörlése. Dél-Korea példáját követve az interneten való regisztráció során kötelező személyes azonosítókat használni Kínában,³⁷ de az ötlet felmerült már Franciaországban³⁸, Brazíliában³⁹ és több amerikai államban⁴⁰ is.

Az anonimitás eltörlése melletti legfőbb érv az, hogy ha az ember a nevével vállalja minden kommentjét és minden kattintását, és felelősségre is vonható azért, amit írt, „trollból” átváltozik civilizált emberré. Azonban ennél sokkal „nyomósabb” üzleti érv, hogy így sokkal könnyebb információkat gyűjteni a felhasználókról, és a netezési szokásai alapján

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

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

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

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

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

célzott hirdetésekkel bombázni.

A kötelezően használandó valódi nevek hátrányai nyilvánvalóak: a végét jelentené a személyes anonim blogoknak és rosszul járna mindenki, akinek jó oka van ragaszkodni a névtelenséghez, mondjuk, mert olyan hobbija, érdeklődési köre van, vagy olyan kisebbséghez tartozik, aminek nyilvánosságra kerülése hátrányos lehet számára. Az anonimitás biztonságot is nyújthat például identitáslopás vagy más visszaélés ellen. Ráadásul vannak jelei annak, hogy a névtelenség eltörléséhez sokkal inkább politikai és üzleti érdekek fűződnek, mint a jobbító szándék.⁴¹

Mindezekre is tekintettel az Európa Tanács 2012-15-re szóló Internet stratégiájában tartja magát a Miniszterek Bizottsága által 2003-ban kinyilvánított elvhez, miszerint az online megfigyelés ellen és a véleménynyilvánítás szabadságának érdekében az egyes internet-használónak joga van eldönteni, hogy identitását fel kívánja-e fedni vagy sem.⁴²

C. Személyiségtorzulás⁴³

– „A kérdésem az, hogy mivel érhettem el nála, hogy ennyire nem érdekli a tanulás, a család mindennapjai, hogy nem restelli, hogy bukott: hogy csak az internet, s valamilyen stratégiai játéka, s azok szereplői, a virtuális barátai, azok léteznek a számára. Ha kérdezem, mi a baj, mit és hogyan segítek, a válasz: semmi, semmit. Kétségbe vagyok esve...

– Az a gyanúm, hogy kislánya az évek során internetfüggővé vált. Levele alapján nehéz megmondanom, mi ennek az oka, de a szülők válása, anyu egyetemi tanulmányai, befelé forduló természete együttesen kiválthatták azt a magányosság érzést, ami a virtuális kapcsolatok felé terelte őt. Azt gondolom, rendezni kellene a gyerek viszonyát a számítógéppel – és nemcsak úgy, hogy korlátozzák a gép előtt töltött időt!”

(Ranschburg Jenő: A serdülés gyötrelmei, kérdések és válaszok)⁴⁴

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

42 Principle 7 of Anonymity of the Declaration of the Committee of Ministers on freedom of communication on the Internet: „In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and cooperating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.” in.: <https://wcd.coe.int/ViewDoc.jsp?id=3703>, 2013-04-23

43 A fejezet szerzője: Dr. Belső Nóra pszichiáter szakorvos

44 Saxum Könyvkiadó 2011, 107.o.

A pszichológiai és pszichiátriai szakirodalomban⁴⁵ egy viszonylag új, az 1990-es évek óta megnevezett és tárgyalt kérdéskör a viselkedési addikciók és az elfogadható határokat átlépő számítógép használat, a kóros internetfüggőség és legújabbban a kóros szociális média használat, illetve függőség.

A számítástechnika és a webes jelenlét fejlődésével párhuzamosan egyre több ilyen irányú pszichés probléma és kóros viselkedésforma került a szakemberek látóterébe. A jelenség az egész populációt – de különösen a gyerekeket – érinti, így az ezzel kapcsolatos szakirodalom fellelhető a pediátriai szaklapoktól, a családi-közösségi-szociológiai lapokon át, egészen a pszichiátriai, illetve neurológiai agyi képalkotó vizsgálatokat elemző tanulmányokig.

A nethasználattal kapcsolatos változások egy része természetesen pozitívan értékelendő, hiszen számos, korábbi nehézkesebb, lassabb folyamatot (információhoz jutás, kutatás, adatgyűjtés, szervezés, stb.) meggyorsít, ezáltal időt takarít meg a felhasználó számára. Ugyanakkor a magatartás és viselkedés kóros változásai, a nem megfelelő használat esetén jelentkező káros hatások számos pszichés probléma forrásai lehetnek.

A legújabb pszichológiai szakirodalomban leggyakrabban a Facebook-jelenség emberi kapcsolatokra gyakorolt hatását, a közösségek megváltozott működését és szerkezetét, valamint az egyén személyiségére gyakorolt hatását elemzik. A modern funkcionális agyi képalkotó vizsgálatokkal már azt is vizsgálják a kutatók, hogy mely agyi területeket, milyen tartalmak, illetve netes viselkedés, miképpen aktivál. Ez utóbbi típusú pszicho-neuro-kognitív vizsgálatok bizonyítékaul szolgálnak a már korábbi gyakorlati megfigyeléseknek, azaz, hogy a net, de még inkább a szociális média használat az arra hajlamos egyéneknél orvosi értelemben véve is okozhat függőséget, tehát valódi addiktológiai kórképet. Figyelemre méltóak azok a vizsgálatok, amelyek az internetet használó agy fejlődésével, neuronhálózatának kialakulásával foglalkoznak és felteszik a kérdést: vajon a netező fiatalok agyában más lesz a neuronhálózat anatómiája és/vagy funkcionálitása, mint az előző nemzedékekében? Egy biztos: egyre fiatalabban kezdik a net használatát a gyerekek és a napjainkban rohamosan terjedő táblagépek és okostelefonok használata kezdi kiszorítani az elavult PC-ket és félokos mobilokat, ezzel együtt a mozgás, beszéd és kommunikáció fejlődése háttérbe szorulhat,

45 Dr. Belső Nóra által felhasznált források:

– Cecilie Schou Andreassen (2013). The relationships between behavioral addictions and the five-factor model of personality. *Journal of behavioral addictions*, 2013 ápr.12. 2062-5871

– DEVELOPMENT OF A FACEBOOK ADDICTION SCALE1, 2 CECILIE SCHOU ANDREASSEN *Psychological Reports*, 2012, 110, 2, 501-517. © Psychological Reports 2012 Department of Psychosocial Science University of Bergen, The Bergen Clinics Foundation, Norway

– Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C. & Egloff, B. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science*, 21, 372-374

mindez pedig valós egészségi veszélyeket is rejthet magában. Számos orvosi szakterület vizsgálja az internettel töltött idő és más betegségek kialakulásának, lefolyásának és gyógyulási folyamatának összefüggéseit (kóros elhízás, mozgásszegénység, táplálkozás változásai, szabadlevegő hiánya, szemészeti vonatkozások, dohányzás, epilepszia stb.), ami mutatja a kérdéskör egészségi, egészségügyi vonatkozásainak jelentőségét.

Pszichológiai, pszichiátriai szempontból több tényező hatását is érdemes számba venni:

1. Az internettel, közösségi médiával töltött idő (szörfözés, böngészés, 1-1 tartalom folyamatos keresése, olvasása, posztolás, chat stb.)
2. Internetes játékok (kóros játékszenvedély, szerencsejátékok, stb.)
3. Az internet által elérhető szociális média használatával kapcsolatos pszichés hatások (visszahatások)

Az 1. és a 2. pontban leírtak valójában az addiktológiai vonatkozásokat jelentik, míg a 3. csoport a közösségi média egyénre gyakorolt (pszichológiai, pszichiátriai) hatásait foglalja össze. Mindhárom tényezőre igaz ugyanakkor, hogy az egyén és a környezet viszonyára erősen hatnak, és a kialakult interaktív folyamatok keretében az egyén kapcsolata önmagával és a világgal teljesen átminősül. Amennyiben ez a folyamat patológiássá válik, szociális károsodás, pszichológiai és pszichés zavarok alakulhatnak ki. Ezek legfőbb formái a következők.

- Személyiségtorzulás (különös tekintettel az anonimitás álarca mögé bújásra)
- Kóros illetve addiktív viselkedések, online devianciák kialakulása
- Addiktológiai vagy kóros viselkedési forma kialakulása (viselkedési addikció)
- Egyéb pszichológiai, pszichiátriai problémával való interakció, komorbiditás (betegségtársulás).

A személyiség minőségének és működésének alakulása egy életen át tartó interaktív folyamat, amelynek alapja genetikai meghatározottságú, de a környezeti tényezők (minták, hatások, tanulás, életesemények, stb.) is meghatározóak lehetnek. Számos vizsgálat kutatta a nethasználat személyiségtorzító hatását, továbbá azt, hogy mely személyiségvonások azok, amelyek hajlamosítanak a kóros és káros viselkedésformák kialakítására. A kutatók egyetértenek abban, hogy valószínűbb a net használatával kapcsolatos problémák megjelenése olyan egyéneknél, akik vagy még éretlen személyiségűek (gyermekek) vagy személyiségzavaros, kóros személyiségjegyekkel rendelkeznek. Ebből következik, hogy a gyermekek minden életkorban és helyzetben veszélyeztetettek, hiszen személyiségfejlődésük kóros irányt vehet, ha nem megfelelő módon tanulják meg vagy használják az internetet. A tanulási

folyamat több összetevőből áll: a szülő és/vagy a testvér, a kortársak viselkedései (minta követés) és az aktív tanulás (szülőtől, tanártól). Éppen ezért a szülők és a környezet netezési szokásai meghatározóak. Gyermekkorban, amikor a személyiség még kialakulóban van, nem beszélhetünk személyiségtorzulásról, hanem a személyiség kóros irányú fejlődéséről, amelynek közbülső negatív eredményei a tanulás és a teljesítmény zavarai, az interperszonális kapcsolatok sérülése és zavarai, ennek végeredménye vagy egy személyiségzavar, vagy egy rosszul működő személyiség lesz (ez utóbbi kóros személyiségvonásokat jelent). Felnőttként ezzel a személyiséggel már eleve rosszul „működik” az egyén, így további torzulások várhatók mind a szociális integrációban és működésben, mind pedig az egyénnek önmagával való kapcsolatában.

A netezés közvetlen személyiségtorzító tényezői:

- a gép előtt töltött idő (időbeosztás, fontossági sorrendek elhanyagolása, más teljesítmények visszaszorulása),
- baráti kapcsolatok megváltozása (húsvér kapcsolatok helyett netes ismerősök), „igazi” barátok elvesztése,
- virtuális tér és idő (távolodás a valós élet léptékeitől, élményeitől, kihívásaitól, a realitásoktól),
- bizonyos tartalmak feldolgozási képtelensége (durvaságok, szex) – a következmények lehetnek kóros feldolgozás, hibás rögzülés, későbbi patológiás reakciók, kapcsolati zavarok,
- kommunikáció megváltozása (szegényedése): beszédképesség romlása, metakommunikáció megváltozása, nonverbális gesztusok felismerésének beszűkülése, érzelmi kifejezőképesség és érzelmek felismerésének a romlása,
- mindezek következtében bizonytalanság, szorongás és félelmek megjelenése a valós környezetben, amelynek következménye a szociális visszahúzódás, majd az izoláció lehet (ugyanakkor torzan megnyilvánuló „erősödés” a virtuális vagy anonim környezetben például durva hangvétellel, agresszivitással).

Mit tudunk tanácsolni a személyiségtorzító hatások kivédésére?

- Oda kell figyelni a szülők és a környezet netezési szokásaira is,
- időbeni korlátokat kell szabni az egyes felhasználási felületekhez,
- el kell magyarázni a gyermek korának és értelmi képességeinek megfelelően a szabályokat és a lehetőségeket,
- figyelmeztetni kell őt az esetleges veszélyekre,

- pozitív impulzusokkal, alternatív programok (a net nem bécicsősz!) ajánlásával el kell „csábítani” a gép mellől (kirándulás, sport, különórák),
- súlyos esetben család- vagy egyéni pszichoterápia.

A kóros, vagy addiktív viselkedések a tárgyalt online devianciákkal és az egyes kiemelt kérdésekkel állnak szoros összefüggésben. Ezek azok a pszichológiai hatások, amelyek a netező gyermeket érik, érhetik és hatásukra pszichológiai reakciók (félelem, szorongás, bűntudat, vágyak stb.) jelennek meg benne. Ugyanakkor az sem elhanyagolható, hogy a netet használó gyermek maga is válhat zaklatóvá, deviáns magatartásúvá. Kétirányú „lehetőségről” van tehát szó. Az internetes beszólás, kibeszélés, zaklatás, behálózás komoly lelki sérüléseket okozhat az áldozatnak. Mindezek hatására erősödhet a visszahúzódás, a valódi közösségektől, kapcsolatoktól való vélt vagy valós félelem, kialakulhat az izolálódás, amely erősíti a szorongást és az internetes pozitív kapcsolatok, barátok felé irányítja a gyermeket. Annál nagyobb a gyermeket érő negatív hatás, minél hiányosabb (érzelem, biztonság, bizalom) a valós élete. Nagy gondot kell ezért fordítani a kétirányú bizalommal teli szülő – gyermek kapcsolat folyamatos alakítására, hiszen csak így várható el, hogy a gyermek megossza szüleiével az őt ért súlyos hatásokat (az enyhébbekről ugyanakkor még egy baráti viszonyban sem feltétlenül számol be). Fel kell világosítani a gyermeket ezekről a veszélyekről, hangsúlyozva, hogy ezek sajnos nem egyedi esetek, és ha ilyesmi történne vele, akkor ez nem az ő hibája („*Nem veled van a baj!*”).

A nettel összefüggő addiktológiai kórkép (viselkedési addikció) kialakulásának veszélye elsősorban azoknál várható, akik erre hajlamosak. A hajlamosságot a családi anamnézis (elsőfokú rokonok közötti kóros játékszenvedély, függőségek, szerfüggőség, tágabban egyéb pszichiátriai probléma), a család szerkezete és működése (elvált szülők, családon belüli zaklatás, kóros minták, érzelmi elhanyagolás, impulzushiány) valamint az egyéni érzékenység (temperamentum és személyiség alapjai, érdeklődés) alakítják ki. Függőség alatt a kóros szenvedély, a vágyakozás, az elvonáskor megjelenő pszichés és testi tünetek, valamint a magatartás és a viselkedés tartós változásait értjük. A függőségeket vagy szenvedélyeket tárgyak szerint csoportosíthatjuk. Ezek szerint valaki lehet netfüggő, de ezen belül a neten még tartalom szerint is függhet valamitől, ugyanakkor, lehet, hogy csak „kütyü”-függő (mobil-függőség, tablet-függőség, stb.).

A közösségi médiához is hozzá lehet szokni. A kutatások alátámasztják, hogy a Facebook-függőség (és minden más közösségi oldal, ahol az illető információt oszt meg saját magáról másokkal) egy igen jól definiálható, az agyi jutalmazó rendszert aktiváló állapot, ennek is köszönheti gyors terjedését. Egy norvég kutatócsoport 2012-ben publikálta a saját maguk által létrehozott egyszerű és önkéntöltős ún. Bergeni Facebook Addikció Skála (BFAS)

használatával szerzett tapasztalatait⁴⁶. A skála bevezetésével Magyarországon is elérhető lehetne ez az egyszerű önmegfigyelési eszköz.

Feltételezhető, hogy az ilyen problémával küzdő gyermekeknél felnőtt korban más szenvedélybetegség, vagy kóros magatartásforma is kialakulhat, továbbá megnőhet az életet veszélyeztető szorongás és depresszió előfordulásának az esélye.

Ezekben az esetekben is nagyon fontos a felvilágosítás és a szakemberhez fordulás (pszichológus, addiktológus), illetve önszegítő egyesületek működtetése, a hasonló problémákkal küzdőkkel való személyes tapasztalatcsere.

Interakciók és komorbiditás szinte bármilyen pszichiátriai kórképpel előfordulhat. A kóros nethasználat mellett gyakrabban fordul elő szorongás, amely kellően hosszú idő után szorongásos betegséghez (generalizált szorongás, szociális fóbia, pánik betegség, kevert szorongásos és depressziós zavar), hangulatingadozáshoz és hangulatzavarhoz is vezethet. A komorbid depresszió előfordulási gyakoriságáról még nincsenek valós adatok, de az valószínű, hogy az együttes előfordulási arány igen magas. Bizonyos rejtett zavarokkal való együttes előfordulás is magas arányokat mutathat, hiszen ezekben az állapotokban sokkal könnyebb az anonimitás maszkja mögé bújva „érvényesülni” (személyiségzavarok, szociopátiák, anorexia, nemi és identitászavarok, stb.). Ilyen esetekben elengedhetetlen az ismert kórtörténet vagy családi anamnézis esetén a pszichiátriai konzultáció.

A pszichológiai-pszichiátriai elemzést összefoglalva megállapítható tehát, hogy az internet tudatos és célirányos használata számos pszichés és szociális károsodást megelőzhet. A kóros nethasználat súlyos lelki zavarokat okozhat, de a már meglévő pszichés zavarok is előidézhetik, fenntarthatják a problémás felhasználói magatartást. A hatások többsége a félelem és a szorongás kialakulásának irányába hat, mely számos pszichés probléma alapját képezi. A kóros és káros működések interaktívan hatnak különösen a gyermekek esetében a személyiség fejlődésére, a folyamatban lényegesek a minták és a tanulás folyamata és minősége. Mindezt kiemelt fontosságú a téma többirányú feldolgozása, a jogi és egyéb védelmet is biztosító hatóságok, szervezetek, valamint a hasonló problémákkal küzdő önszegítő csoportok ajánlásainak és elérhetőségeinek megismertetése a nyilvánossággal. Fontos felhívni a figyelmet arra is, hogy súlyos pszichés zavarok (függőség, szociális izoláció, veszélyeztető magatartás) esetén a szakember segítsége elkerülhetetlen!

46 DEVELOPMENT OF A FACEBOOK ADDICTION SCALE1, 2 CECILIE SCHOU ANDREASSEN Psychological Reports, 2012, 110, 2, 501-517. © Psychological Reports 2012 Department of Psychosocial Science University of Bergen, The Bergen Clinics Foundation, Norway

D. Közösségi terek – ismeretlen ismerősök

Az internetes jelenségek közül – viharos gyorsaságú elterjedése és a magánéletre gyakorolt hatása miatt – kiemelendő a virtuális közösségeként formálódó közösségi hálók szerepe. Az internetalapú közösségi hálók (*Social Networks*) lényege, hogy valamilyen közös csoportismérv (iskola, foglalkozás, hit, hobby stb.) alapján ismeretlenek vagy ismerősök online kapcsolatba kerüljenek egymással kapcsolatépítés vagy szolgáltatásnyújtás céljából.

Az internetalapú közösségi hálózat alapvető kritériumai⁴⁷:

- a felhasználók publikus vagy fél-publikus profiloldalát hozhatnak maguknak létre,
- a felhasználók között biztosított az összeköttetés,
- a felhasználók saját és mások kapcsolati hálóját is megismerhetik.

Az első ilyen közösségi oldal 1995-től az USA-ban üzemel *classmates.com* néven és célja osztálytársak, munkatársak, katonatársak felkutatása volt. Az első olyan oldal, ahol a felhasználók profiloldalakat is létre tudtak hozni és kapcsolataikat áttekinthették, a *SixDegrees* volt 1997-ben⁴⁸ (az oldal egyébként 2000-ben bezárt, mert üzileg nem hozott sikert). 2003-tól a világon mindenhol megjelennek ilyen közösségi oldalak, jelenleg azonban a világon a legnépszerűbb közösségi háló egyértelműen a Facebook. 2021. október 28. óta a cég neve Meta, nevében is tükrözve a „világbirodalmi” törekvéseket⁴⁹, mely 2012. október 4-én elérte az 1 milliárd, 2017 júniusában a 2 milliárd regisztrált felhasználót. A Facebook használata ingyenes, egy egyszerű regisztrálással lehet meghívás nélkül csatlakozni. A felhasználók létrehozhatnak egy személyes profilt, kapcsolódhatnak ismerőseikhez, csoportokhoz és rajongói oldalakhoz egyaránt, valamint üzeneteket válthatnak és eseményeket szervezhetnek, az üzenőfalon keresztül híreket, információkat, weboldalakat és videókat is megoszthatnak egymással. A saját hálózaton belül mások adatlapja részleteiben is látható, míg más közösséghez tartozó felhasználó adatlapja nem, de ez függ a felhasználók egyedi

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

48 a név utal a „hat lépés távolság – Six degrees of separation” elméletre, mely szerint a földön bárkivel kapcsolatba hozhatók vagyunk úgy, hogy közöttünk összekötőként maximálisan öt személy van

49 <https://web.archive.org/web/20211020021631/https://www.theverge.com/2021/10/19/22735612/facebook-change-company-name-metaverse>

beállításaitól is. 2011 augusztusában a Facebook megújította adatvédelmi rendszerét, jelentős részben a honlapot ért kritikák és a Google hasonló fejlesztésének hatására. Ugyanakkor emellett folyamatosan újabb fejlesztéseket vezetnek be, amelyek online életünk számos mozzanatát naplózzák, a felkeresett tartalmakat automatikusan lájkolják.

2015. január 30-án újból megváltoztatták a felhasználási feltételeket, amiért több adatvédelmi hatóság is eljárást indított. A belga hatóság eljárásában a Facebookot elmarasztaló bírósági ítélet is született, mert a közösségi oldal üzemeltetője jogellenesen követte az internetezők böngészési szokásait. Ha valaki (akár a közösségi oldalon nem regisztrált internetező) egy olyan honlapra tévedt, ahol a Facebookhoz kötődő kiegészítő (pl.: *like* vagy *share* gomb) került elhelyezésre, akkor a Facebook minden értesítés nélkül egy apró azonosító alkalmazást (ún. *DATR cookie*) helyez el a felhasználó gépén, amellyel követni tudja böngészési szokásait, lényegében megfigyeli viselkedését. Németországban pedig a Düsseldorf-i Kerületi Bíróság 250 000 Euróra (mintegy 80 millió forint, továbbá alternatív büntetési tételleként még szerepel 6 havi börtönbüntetés a cég vezetőjének) bírságot 2016-ban egy nagy divatcéget, mert egy velük kapcsolatba álló kis ruházati bolt honlapján vásárolók személyes adatait előzetes figyelmeztetés nélkül a Facebookos „like” gomb megnyomásával automatikusan továbbították hozzájuk.⁵⁰

Az Európai Adatvédelmi Testület (EDPB) 2022-ben nagy horderejű döntést hozott az ún. Instagram-ügyben. Az Instagram-profilát üzemeltető Meta 2016-ban bevezetett a felhasználók számára egy újfajta Instagram-fiókot, az üzleti fiókot („business account”). Azoknak az Instagram-felhasználóknak, akik a személyes fiókról („personal account”) üzleti fiókra váltottak, további információkat kellett megadniuk, amelyek nyilvánossá váltak az Instagram-felhasználók, továbbá a követők számára. 2019-ig az üzleti fiókra váltó felhasználók, ideértve a gyermekkorú felhasználókat is, kötelesek voltak megjelentetni a profiljukon olyan további, a nem üzleti célú felhasználók esetében nem kötelező, kapcsolattartásra szolgáló adatokat, mint az e-mail-cím és/vagy telefonszám (2019. szeptember 4-én a Meta egyébként eltörölte ezt a kötelezettséget). Az illetékes ír hatóság bizonyos pontokon nem túl szigorú döntéstervezetével szemben a német, a francia, az olasz, a holland és a norvég felügyeleti hatóságok nyújtottak be kifogást. Az EDPB azt állapította meg, hogy az Instagram üzleti fiókot használó gyermekek nevezett kontaktadatainak kezelése nem szükséges az Instagram mint szolgáltatás nyújtásának teljesítéséhez és az adatkezelés így jogellenes volt, ennek hatására végül az illetékes ír felügyeleti hatóság 405 millió euró összegű közigazgatási bírságot szabott ki a Meta IE-re.

A közösségi hálók profiloldalának nyilvánossága szolgáltató függő, van, ahol teljes a nyilvánosság, előfordul, hogy csak a regisztrált tagok nézhetik meg az adatokat, és van, ahol

50 <http://www.reuters.com/article/us-facebook-like-germany-idUSKCN0WB1OI>, 2016-03-11.

a korlátozások külön-külön is beállíthatók. A hálózatban a „felhasználói lét” a személyes adatok megadásával kezdődik: minimális adatszolgáltatási követelmény az érintett neve, életkora, lakhelye, érdeklődési köre, egy kis kötetlen bemutatkozás, és bármi, amit az érintett még magáról fontosnak tart, általában elvárás a fénykép feltöltése is. A milliós nagyságrendben nyilvánosságra hozott személyes adatok tömege egyrészt igen sérülékeny magánszférát eredményez globális mértékben meghatározott teljes – elsősorban fiatal – generációk vonatkozásában.

A közösségi terek mellett megfelelő terepet biztosít online visszaéléseknek is. Egy amerikai felvilágosító kisfilm – <https://www.youtube.com/watch?v=6jMhMVEjEQg> – reálsan megmutatja, hogy tini lányok mennyire könnyen, szüleiket kijátszva és magukat veszélyes helyzetekbe sodorva beszélnek meg randevúkat „ismeretlen ismerősökkel” annak ellenére, hogy a családban korábban már beszélgettek arról, hogy súlyos következményei lehetnek az óvatlan ismerkedésnek.

Európai kutatások eredményei⁵¹ egyértelműen megerősítik, hogy a hálózati kapcsolatépítés mennyire népszerű a fiatalok körében: már 2011-ben is a 9-12 éves gyerekek 38%-a, míg a 13-16 évesek 76 %-a tagja volt valamilyen hálózati közösségnek (a 9-16 évesek harmada Facebook kötődéssel – ebből is látható, hogy a 13 éves korlátozás mennyire komolytalan) és a fiatalabbak egyben óvatlanabbak is: egyértelműen nagyobb százalékban engednek személyes adataikhoz (akár lakcímükhöz, telefonszámukhoz is) hozzáférést idegeneknek.

2014-ben tovább emelkedett az interneten csetelők – gyerekek és felnőttek egyaránt – aránya, ami elsősorban az okostelefon terjedésével hozható összefüggésbe. A 14-19 éves korosztály 95%-a használ szöveges, 74%-a hangos csetet. 96%-uk látogatja a Facebook-ot, 93%-uk YouTube-ot legalább hetente (ez az adat a szülői – 40-49 éves korosztálynál 71% és 59%).⁵² A 9-16 éves magyar gyerekek kétharmada legalább egy közösségi oldalon saját profillal rendelkezik, inkább a lányok és az idősebbek azok, akik használják ezeket az oldalakat. A gyerekek egynegyedének van 50-100 közötti, egyharmadának pedig 100-300 közötti ismerőse, míg 13%-uknak ennél is több. Az összes megkérdezett gyerek 55%-ának volt nyilvános, azaz mindenki által látható profilja közösségi oldalon. 22% azok aránya, akik azt részlegesen publikussá tették, míg csupán 16% volt azok aránya, akik olyan beállításokat alkalmaztak, hogy azt csak barátaik láthassák.⁵³

A virtuális térben kontroll nélkül keringő személyes adatokat az adatalany eredeti szándékától vagy mindenkori akarától független célokra is könnyen fel lehet használni. Az

51 EU Kids Online – Social Networking, Age and Privacy Sonia Livingstone, Kjartan Ólafsson and Elisabeth Staksrud kutatásai in.: <http://eprints.lse.ac.uk/35849/> 2013-06-13

52 http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf 2016-02-12.

53 Ságvári Bence: Az EU Kids Online magyarországi kutatásáról in.: www2.lse.ac.uk/.../EUKidsOnline/.../Hungary%20webpage.pdf, 2013-03-07

érintettől tudomása nélkül bármikor digitális dossziék (*digital dossiers aggression*)⁵⁴ készíthetők, listázva például a hobbijait vagy a barátnői nevét. (Például New Yorkban a rendőrség szerint részben azért csökkent a gyilkosságok száma, mert 2012 októberében indult egy közösségimédia-figyeléssel foglalkozó rendőrségi projekt, ahol nyomon követték a tinédzser bandatagok megnyilvánulásait azért, hogy időben rajtuk üthessenek⁵⁵). A profilokból összegyűjtött adatok sorsára az adatalanynak már nincs további rálátása, az információ önálló életet kezd élni. Ha ehhez hozzáadjuk, hogy a különböző közösségi oldalak adattartalma is könnyen összekapcsolható, könnyen érthetővé válik milyen mértékű potenciális veszélyeket (leendő munkáltató általi ellenőrzés, zsarolás stb.) rejtene magukban a közösségi oldalak biztonsági beállítások nélküli állapotukban. A 2013 júniusában kirobbant ún. Prism-botrány pontosan arról szól, hogy az amerikai titkosszolgálat az óriási internetszolgáltatók és cégek által egyébként jogszerűen tárolt milliós személyes adatokhoz (képek, videók, mailek, egyéb dokumentumok) minden kontroll nélkül, állampolgárságra tekintet nélkül közvetlenül hozzáfér.⁵⁶

A felhasználók által megadott adatok között egyre növekvő szerephez jutnak a képek (nemcsak az ún. profil-, hanem az albumokba feltöltött és megosztott képek), ami azért lehet veszélyes, mert azokból további következtetéseket lehet levonni (másodlagos adatokhoz lehet jutni) a felhasználó személyiségére, társas kapcsolataira, vagyoni helyzetére vonatkozóan, így az eredeti környezetéből kikerülve egy ártalmatlan képből is kellemetlen ségei keletkezhetnek. A legnagyobb veszélyt azonban az jelenti, hogy a képek és a hozzájuk kapcsolt felhasználók által megadott másodlagos információk könnyen összekapcsolhatóvá teszik a különböző szolgáltatók rendszereiben tárolt profilokat, adatokat (mondjuk egy nevesített közösségi oldali profilt egy elvileg anonim vagy álneves társskereső oldal adataival).

A legtöbb közösségi oldalon lehetőség van arra is, hogy a felhasználók a feltöltött képekhez további adatokat csatoljanak, pl. a rajta szereplők megnevezésére, profiljukhoz való direkt hozzáférést biztosító link megadására, e-mail címek hozzáadására stb. (ún. tagging). Ez szintén elősegíti a profilok összekapcsolhatóságát. Különösen kényes kérdés ez abban az esetben, ha az így érintett személy nem felhasználója a közösségi oldalnak (tipikus megoldás ilyenkor a szolgáltató részéről, hogy ilyenkor „értésítést” küld a nem felhasználónak a felhasználó általi tagról és egyben felhívja a csatlakozásra is – minthogy a megjelölt személy többnyire a kép megtekintésén túl többet regisztráció nélkül nem tehet. Ez a NAIH véleménye szerint a jelen jogi környezetben spamelés a szolgáltató részéről, illetve hozzájárulás hiányában személyes adattal való visszaélés a felhasználó részéről). A problémát az jelenti tehát, hogy míg a felhasználóknak saját adataik tekintetében lehetőségük van megválasztani

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

55 http://index.hu/tech/2013/02/26/cskosten_a_bunozes_a_Facebook_miatt/, 2013-02-26

56 http://index.hu/tech/2013/06/07/az_amerikai_titkosszolgalat_mindent_lat/, 2013-06-24

mit tesznek közzé és mit nem, addig ez a tagging esetében a más által rólunk közölt adatok esetében nem, vagy csak nagyon korlátozottan lehetséges (a legtöbb szolgáltató adatvédelmi szabályzata erre vonatkozóan nem tartalmaz rendelkezéseket), így gyakorlatilag kiüresedik az önrendelkezés lehetősége.

Nem elhanyagolható az (adat)biztonság kérdése sem: számos visszaélés fordul elő azzal kapcsolatban, hogy valaki más nevében „kreál” profiloldalakat, tölt fel (akár kompromittáló, kellemetlen) fényképeket vagy egyéb információkat. A Lindqvist-ügyben hozott európai bírósági ítélet⁵⁷ lényege pontosan az volt, hogy még teljesen jóhiszemű célból, egyházi karitatív munkában részt vevő személyek adatait sem lehet bejegyzésük nélkül egy weboldalon nyilvánosságra hozni. Az emberek emellett gyakran elfeledkeznek arról, hogy minden adat, ami egyszer a világhálóra kerül, onnan többé tökéletesen már soha nem távolítható el. Különösen igaz ez a már említett, másodlagos adatgyűjtések miatt. A komplett profilok teljes törlése nehéz, gyakran gyakorlatilag lehetetlen, hisz míg maga a felhasználói profil elvileg könnyen törölhető, addig a másodlagos adatokat, tartalmakat a felhasználó nem vagy nem teljesen tudja törölni (mások profiljában szereplő képek, kommentek, üzenetek stb.). Vannak már olyan automatikus programok, melyek lehetővé tennék a teljes törlést, az ún. virtuális öngyilkosságot, ám ezek használatát a szolgáltatók többsége tiltja, korlátozza. Illetve gyakran nem egyértelmű a helyzet abból a szempontból sem, hogy a törlés mit jelent: tényleges és azonnali törlést, vagy csak hozzáférhetetlenné tételt és bizonyos ideig történő további megőrzést (pl. Facebook profil esetén a deaktiválás után a felhasználó még reaktiválhatja profilját bizonyos ideig, azaz a profil tényleges törlése egy ideig a valóságban nem történik meg, ugyanakkor nincs magyar nyelvű tájékoztatás a követendő lépésekről). Mindezek a problémák valójában azt a félelmet erősítik meg, illetve igazolják, hogy az internet nem felejt, az egyszer megosztott adatokat már nem lehet törölni – azaz végső soron a felhasználó elveszti rendelkezési jogát adatai felett.

Szintén ésszerűen kell tartani, hogy minden adat, ami rólunk az internetre kikerül, az adatahalászkok számára is megszerezhetővé válik. A legkönnyebb számukra az e-mail címek begyűjtése, melynek kellemetlen következménye postaládánk kérésre küldeményekkel való elárasztása. A felhasználók ismerősei a kapcsolati hálón keresztül könnyen lenyomozhatóak, így bárkiről megszerezhetőek személyes adatok. Az ezzel kapcsolatos adatvédelmi aggályokat úgy tűnik, a magyar felhasználók nem veszik komolyan, aminek jele a felhasználók számának napi emelkedése, illetve a fiatal korosztályok Facebook-hoz kötődő, már-már függőségbe hajló viszonya (magyar tizenévesek beszélgetéseinek állandó témája a *„mennyi időt voltam fent a Facebook-on”* és *„ott milyen izgalmas információkat fedeztem fel ismerőseimről”*).

E. KÁROS TARTALMAK

Az interneten közzétett, nem kifejezetten jogellenes, ugyanakkor a közvélekedés és/vagy a szakértők (pedagógusok, pszichológusok stb.) által a gyermekek testi-lelki fejlődésére károsnak tartott tartalmakkal való megismerkedés – történjen az akár a gyermek, akár a gondozását felügyelő felnőtt által⁵⁸ – rendkívül veszélyes lehet. Tipikusan ilyenek az erőszakos, pornográf, öngyilkosságra, drogfogyasztásra vagy kóros táplálkozásra⁵⁹ biztató oldalak.

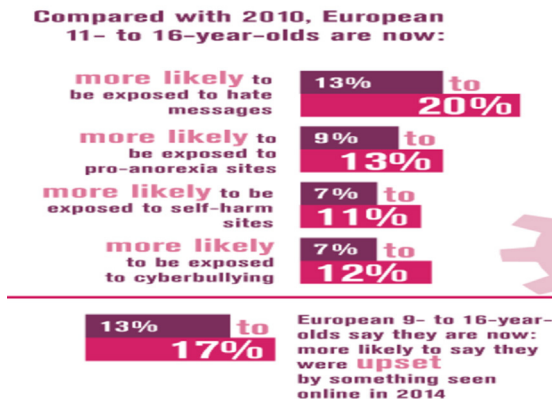
A Magyar Védőnők Egyesületének elnöke azért fordult beadvánnyal az ombudsmanhoz, mert egy fiatalok szexuális felvilágosításával foglalkozó rádió műsorában derült fény arra, hogy a Google kereső '*szexuális felvilágosítás*' szóra adott első találat egy „viccesnek szánt”, tartalmilag azonban vérfertőző, homo- és heteroszexuális animáció bemutató linkje. Az ombudsman hatásköri korlát híján csupán tájékoztatást tudott adni az illegális/káros tartalmak bejelentésének lehetőségéről⁶⁰.

A legfőbb probléma, hogy a káros tartalmakkal való megismerkedéshez nem feltétlenül szükséges a szándék, vagyis a felhasználó véletlenül, vagy akár akarata ellenére is kinyithat ilyen oldalakat (beír egy ártalmatlannak tűnő keresőszót például „lányok” és válogatás nélkül jönnek fel a találatok, illetve még egy megbízhatónak ítélt netes könyvtárház kínálatában is találkozhatunk olcsó pornografikus tartalmú e-könyvekkel). Böngészéssel hasonló módon navigálhatjuk magunkat káros tartalmú oldalakra. A 2014-es EU Kids Online felmérés összehasonlító adatai szerint a 11-16 éves internetező európai gyerekek 20%-a találkozhat gyűlöletre, 13% anorexiára, 11% önpusztításra buzdító oldalakkal, 12%-uk kitett internetes zaklatásnak (a 2010-es felmérés adataihoz képest a negatív változás szignifikáns).

58 A halálra éheztetett agárdi csecsemő halála ügyében történő nyomozásnál a „nyomozók a házban talált számítógép memóriájának elemzésével arra keresnek választ, kikkel tartották a kapcsolatot a gyermek szándékos éheztetésével gyanúsított szülők, milyen oldalakat nézegettek a neten. Szintén vizsgálják, hogy tartottak-e kapcsolatot olyan személlyel, aki útmutatást adhatott volna nekik a gyermek éheztetésével kapcsolatban.” In.: http://index.hu/belfold/2013/04/22/vizsgaljak_az_agardi_szulok_beszamithatosagat/, 2013-04-22

59 Egy 800 diák bevonásával elvégzett felmérés szerint a táplálkozással kapcsolatos kérdéseknek a gyerekek főleg az interneten néznek utána – családtagjaikhoz azok fordulnak inkább, akiknél fontos az egészséges táplálkozás in.: Böröndi-Fülöp Nikolett: A fiatalok táplálkozási szokásainak vizsgálata a Dél-Dunántúlon, 2012 PhD Értekezés, phd.ke.hu/fajlok/1348561429-borondi-fulop_n_tezisek.pdf, 2013-03-01

60 Erre az NMHH Internet Hotline bejelentő felületén (<http://internethotline.hu/tart/index/31/Bejelentes>) és az internethotline@internethotline.hu e-mail címen van lehetőség!



16. ábra: <https://lisedesignunit.com/EUKidsOnline/> 2016.02.17.

Mit tehetünk? A gyermeket egyrészt fel kell készíteni arra, hogy ilyen oldalak léteznek. Egy véletlen találkozás során elmélyült tanulmányozás helyett az ilyen oldalt inkább hadléktalanul el kell hagynia, illetve a tartalmát felül kell tudnia bírálni (például táplálkozásról, testi-lelki egészségről számtalan tudománytalan vagy megtévesztő, szélhámos hír kering a neten is). Legjobb, ha a gyermek negatív élményeiről később önként be is számol szüleinek vagy egy megbízható felnőttnek (ennek előfeltétele azonban a bizalom, illetve hogy a gyerek ne féljen az esetleges büntetéstől).

A másik megoldás technikai: tartalomszűrő szoftverekkel el lehet kerülni a nem kívánt találkozást. Többféle szűrés jöhet szóba a gyermek- és a felnőtt tartalom szétválasztására:

- a valós idejű szűrés a megtekinteni kívánt oldalt elemzi szöveg-, esetleg képfelismerő algoritmusokkal, és nem enged hozzáférést azokhoz, amelyekben a szűrőbe betáplált ismertetőjegyek megtalálhatók;
- a listák elvén működő szűrők letiltják a „feketelistára” tett weboldalakot/ szervereket vagy csak a „fehérlistán” engedélyezett honlapok böngészését engedik meg, így egyfajta biztonságos gyerekjátésozteret alakítanak ki a veszélyes internetből;
- a címkézésre alapozott szűrőszoftverek azokat a jelzéseket, címkéket veszik figyelembe, amelyeket vagy a szolgáltatók, vagy a felhasználók, vagy az erre szerveződött vállalkozások helyeznek el a weboldalakon – hasonlóan a filmek korhatárjelzéseéhez.

Az indokolatlan szűrés, a túlblokkolás ugyanakkor több hátránnyal, mint előnnyel jár. Mindenképpen tiltani kellene azonban az internet „lehívásos” (pull) természetével ellentétes „tolakodó” (push) típusú felbukkanó ablakokat, az elektronikus levelezést tönkretevő spamhez hasonlóan. Bár a kéretlen böngészőablakok között is vannak ártalmatlanok (pl. reklámok), de ez az agresszív technológia lehetővé teszi, hogy olyan káros tartalmú weboldalakra irányítsák a gyanútlan felhasználót, amelyeket az nem akart megnézni, és az oldal bezárására tett kísérletek sokszor csak újabb és újabb ablakokat nyitnak meg. A másik fontos teendő a gyermekeknek szóló hasznos tartalmak bővítése, és a gyerekek megtanítása ezek használatára. Minél több kedvére való tartalmat és feladatot talál a gyerek az interneten, annál kevésbé fog a felnőtteknek szóló oldalakkal foglalkozni.⁶¹

Egyes országokban központi internetcenzúra működik, így például Kínában, Szaúd-Arábiában vagy Vietnámban a központi szűrés kiterjed a vallási, politikai okokból nem kívánatos, vagy egyébként pornográf tartalmú oldalakra. Bizonyos illegális témák esetében európai országok is alkalmaznak blokkolást (Németország: holokausztagadás, Norvégia: gyermekpornográfia, USA: közösségi internet-hozzáférési pontok).

Magyarországon a gondolat- és véleménynyilvánítás szabadságjogainak tisztelete okán 2012-ig kizárólag az önkéntes alapon történő szűrés volt elfogadott, ezen ütött rést a Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) 77. §-a egy új bírói intézkedési forma – az elektronikus adat végleges hozzáférhetetlenné tétele – bevezetésével:

77. § (1) Véglegesen hozzáférhetetlenné kell tenni azt az elektronikus hírközlő hálózaton közzétett adatot,

- a) amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg,*
- b) amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy*
- c) amely bűncselekmény elkövetése útján jött létre.*

(2) Az elektronikus adat végleges hozzáférhetetlenné tételét akkor is el kell rendelni, ha az elkövető gyermekkor, kóros elmeállapot, vagy törvényben meghatározott büntethetőséget megszüntető ok miatt nem büntethető, illetve ha az elkövetőt megrovásban részesítették.

Az új intézkedést a törvény indokolása szerint tipikusan a gyermek pornográf felvételeket tartalmazó weboldalak eltávolítására használják majd fel, eleget téve a 2011/93/ EU iránylevél⁶² 25. cikke szerinti előírásnak.

61 Drótos László: Referátum Bayer Judit: A háló szabadsága : az internet tartalmának szabályozási problémái a véleménynyilvánítás szabadsága tükrében c. könyvről in.: http://tmt.omikk.bme.hu/show_news.html?id=4633&issue_id=479, 2013-04-02

62 AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2011. december 13-i 2011/93/EU IRÁNYELVE a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/ IB tanácsi kerethatározat felváltásáról

F. KERESŐMOTOROK – internetes „kapuőrök”

Az internetes forgalomirányító szolgáltatásokban a megjelenített információk személyre szabott találasáról van szó. A magyar internetezők gyakorlatilag kivétel nélkül használják a Google keresőjét (93-96%) – 2014-ben a keresőmotorral végzett keresések aránya 99% volt⁶³ –, miközben általában nem is gondolnak bele abba, hogy a készen kapott találatlista nem biztos, hogy kizárólag az ő információéhségüket hivatott csillapítani, esetleg lehetnek más szempontjai is az összeállításnak. A Google a felhasználó ún. „szubjektív relevancia” fogalmával dolgozik a találatok megjelenítésekor, mikor a korábbi keresési szokások alapján egy hat kategóriás fontossági sorrendet állít fel (vital – useful – relevant – slightly relevant – off topic és useless), de természetesen a sorrendre hatnak a reklámozók által kifizetett óriási összegek is. A gazdasági verseny szempontjából nagy jelentősége van a sorrendnek – különösen a domináns platformok esetében –, mivel a fogyasztó jellemzően arra a hirdetésre kattint, amelyet az első öt találat ad (gondoljunk csak a szállodafoglalásokra).

Az internetező gyerekeket tehát meg kell tanítani a keresés technikája mellett (melyek a jó keresőszavak, ezeket hogyan írjuk be stb.) a szolgáltatás helyes használatára, valamint a kapott információforrások minőségének helyes értékelésére is. Így elkerülhető lesz az az amerikai iskolai életből már ismert jelenség, hogy a tanár az osztálynak feladott, gyűjtőmunkán alapuló elemzést a lényegében megegyező, ugyanazt a silány forrást kimásoló húszt házi feladatban legyen kénytelen újra és újra végigolvasni.

G. NYELVI PROFILOZÁS AZ INTERNETEN⁶⁴

A kommunikációs technológia vívmányai a bűnözés újabb formáinak megjelenését tették lehetővé. Nem csak nemzetközi, de hazai szintén is nehéz feladatnak számít az internetes bűnözők felderítése. A nyelvészszakértő többek között a nyelvi profilalkotás módszerével segíti a rendvédelmi szervek munkáját.

A bűnügyi nyelvészet egyik ága a nyelvi profilozás, amely a hiedelmekkel ellentétben nem grafológiát jelent, hanem szövegelemzést. Úgy alkotunk⁶⁵ valakiről profilt (ezt szociodemográfiai jellemzőnek nevezzük), hogy az általa közölt szövegből próbáljuk meg megállapítani a korát, nemét, iskolai végzettségét, anyanyelvét, hányan szerezhették a szöveget. Ezen kívül a nyelvi profilozás része lehet a tartalomelemzés is: a szakértő kap egy levelet, amely nincs aláírva (anonim) vagy álnévvel van ellátva (pseudonim), akkor ahhoz, hogy tudjuk,

63 http://nmhh.hu/dokumentum/166308/internet_2014_webre.pdf, 2016-02-12

64 A fejezetértész szerzője: Ránki Sára nyelvész, eseti nyelvészszakértő

65 A tanulmány a kutatói gyakorlatnak megfelelően Többes szám Első személyben íródott.

kit kell keresni, nyelvi profilozást kell végezni. Az is előfordulhat, hogy tudjuk, hogy kit kell keresni, és akkor összehasonlító vizsgálat (komparatív) miatt készül a profilozás, hogy megállapítsuk, hogy ugyanaz-e a szerzője a szövegeknek.

A bűnügyi nyelvészet, más néven kriminalisztikai nyelvészet nem egy újkeletű tudományág a nemzetközi irodalom szerint. Hazai téren viszont igen. Bár, az első tanulmányok az 1960-as években jelentek meg, igazi gyakorlattá vagy hivatássá csak mára kezd válni. Ez egy alkalmazott nyelvészeti tudományág, a nyelvészet megállapításait használja fel a gyakorlatban, jelen esetben például bűnügyek megoldásának segítésére.

Az igazságügyi nyelvészet témaköréből⁶⁶ Szilák Jolán r. alezredes már 1979-ben leírta, mennyire fontos a valóságelemek vizsgálata névtelen vagy álnévvel ellátott levelekben. A névtelen levelek vizsgálata során a valóságtartalmat a szövegrendszerben kell keresni: a nyomozó feladata, hogy a szövegben leírt adatokat, tényeket ellenőrizze, a további vizsgálat célja ugyanakkor a szöveg mögöttes tartalmának a feltárása. Ilyenkor a szakértő ütközteti egyrészt a szavakban megnyilatkozó tartalmat a szöveg mögöttes tartalmával, másrészt a saját ismereteivel, és ezek eredményeiből következtet a szerző személyére. Egy másik tanulmányban Szilák egy olyan kutatásáról számolt be, amelyben száz ismertté vált névtelen szerző levelét vizsgálta abból a szempontból, hogy magukban a nevekben és helynevekben mennyi a valóságos elem. Fontos megjegyezni, hogy azok a levelek, amelyek kitalált, hamis névvel vannak ellátva, a névtelen levelekkel egy kategóriába tartoznak, azonos elbírálás alá esnek. Ennek a vizsgálatnak az eredményei a következők: a kitalált nevek egy része tömegnév pl. *Tóth* vagy *Nagy*, ugyanígy a kitalált utcanevéké is: *Fő tér* vagy *Kossuth utca* stb. A névkitalálásnak különböző fajtái vannak: van, aki valódi nevének egyes elemeit kombinálja kitalált elemekkel. Mások a fonetikai hasonlóságra vagy eltérésre építenek például úgy, hogy valódi nevük első szótagja vagy magánhangzósora megmarad pl. *Szalay-Szabó* vagy *Gábor-János*. Beszélő nevekkal is találkozunk, ezekben általában kifejeződik a fogalmazónak a témával kapcsolatos véleménye. Előfordul, hogy valaki a másik nem neve mögé rejtőzik. (Szilák szerint a férfiak ritkábban vesznek fel női nevet, mint ahogyan a nők férfinévet.) Akad olyan is, aki saját neve helyett egy közismert, de legalább a saját környezetében ismert ember nevét kölcsönzi. Az anonim vagy kitalált nevű szerzők címadása (helység- és utcanevék) is tanulságos. Sok esetben következtetni lehet ezekből az adatokból a levélíró műveltségére, esetleg foglalkozására, lakóhelyére. A névtelen levelezők között akad olyan, aki a saját szociodemográfiai tulajdonságaival ellenkező tulajdonságokkal rendelkezők képviselésében ír, például az idősebbek a fiatalok, az értelmiségiek a munkások nevében. Nagy Ferenc Kriminalisztikai szövegnyelvészet című könyvében (1980) leírta, hogy a szöveg szándékos megváltoztatása egyirányú folyamat, tehát a művelt ember fel tudja tüntetni magát műveletlennek, de fordít-

66 Erről lásd Ránki 2011: <http://e-nyelvmagazin.hu/2011/08/31/a-kriminalisztikai-szovegnyelvessel-hazai-kutatas-tortenete-1960-tol-1990-ig/>

va ez már elképzelhetetlen. A tanulmány végkövetkeztetése szerint minden kitalált névben, címben és persze a szövegben is vannak olyan valóságelemek, amelyek a fogalmazó akaratán túl információkat adnak. Éppen ezért a félrevezető kísérletek nem zárják ki a szövegező vagy levélíró csoporthovatartozásának megállapítását, személyének megközelítését.

A digitális világban kezdetben a mobiltelefonos üzenetek dekódolása jelentett gondot. Azzal, hogy korlátozták az üzenetek karakterhosszát, kikényszerítették a nyelvnek azt a tulajdonságát, ami a rövidség mellett az érthetőségre törekszik. Így alakult ki, hogy már az sms-ek szövegei is rövidítésekből állnak, azért, hogy minél több információt juttassunk el a kommunikációs partnerhez. A rövidítések nagy része angol szavak vagy kifejezések főnémaít vagy számokat tartalmaznak. Például a 'lol' (*laugh out loud*) a „hangosan felnevet” rövidítése. A 'b4' (*before*) az „előtt” jele. A 'btw' (*by the way*) a „mellékesen” rövidítése.

Ma már az online játékoknak is megvan a saját nyelvük. A kommunikáció legfontosabb jellemzője itt is a gyorsaság és a rövidség. Kommunikálni a csapattársakkal kell gyorsan, mert aki sokat ír, az nem játszik. Az online játékok nagy része viszont csapatjáték: ha részese akar lenni valaki, ismernie kell a közeg nyelvhasználatát.

A digitális világ nem csak a bűnözőknek teremt lehetőséget a rejtőzködésre, de a bűnüldözők munkáját is megkönnyíti. Igazi adatmátrixszal jellemezhető már egy ember, a távollátó műholdak segítségével például ki tudják elemezni egy ember árnyékát, mozgáslenyomatot adva ezzel.⁶⁷ Az internetes nyelvhasználatnak, az internetes nyelvi viselkedésnek vizsgálatáson azonban még sok szempontból várta magát.

Az interneten elkövetett bűncselekményekhez kapcsolódó szövegek vizsgálatát jelenti a csetoldalak elemzése, tartalomelemzés, Facebook-on meglévő különböző profilok összehasonlító elemzése, gyűlölet-bűncselekmények vizsgálata. Különbséget kell tenni az interneten keletkezett szövegek és az internetre feltett szövegek között. Az interneten keletkezett szövegek magukon viselik az internetes szövegjellemzőket, ezeket netnyelvészeti eljárással kell vizsgálni. Azok a szövegek pedig, amelyek internetes csatornán jelennek meg, de egyébként hétköznapi szövegek, közelebb állnak az úgynevezett nyelvi normához és ezeket inkább hagyományos szövegnyelvészeti eljárással érdemes elemezni. Ilyenek lehetnek az e-mailek, blogok, hirdetések, egyes honlapok.

Az internetes nyelvhasználatunk, amelyet nevezhetnénk digitális nyelvi identitásnak, sokban eltér a saját hétköznapi nyelvhasználatunktól. Mégis, ez a fajta nyelvhasználat is lehet egyedi, csak ránk jellemző. Az, ami egyedivé teszi, nem kifejezetten a szóhasználat, hiszen pont ez az, ami általános az internet világában, hanem a nyelv más egységei. Gondoljunk csak a toldalékokra vagy a mondat szerkezetre. Találkoztunk olyan esettel, amikor összehasonlító profilozásnál onnan lehetett a szövegeket elkülöníteni, hogy egyfajta tolda-

67 Erről részletesebben lásd a Titkos kódok című könyv 148. oldalát (Titkos kódok, 2009. Budapest, Kossuth Kiadó.)

léktípust csak az egyik szerző használt, ráadásul mindig rosszul. Ez olyan szövegsajátosság volt, amely alapján azt lehetett mondani, hogy harminc levél közül azt a tizennégyet biztosan egy szerző írta.

Miért áruklodó a nyelvi tevékenységünk? Azért, mert senki nem annyira tudatos nyelvhasználó, hogy az általa rutinszerűen használt nyelvi jellemzőket megváltoztassa. Az átlag nyelvhasználó például, ha butábbnak akarja magát mutatni, akkor a pontos „j”-és szavakat „ly”-nal fogja írni. Ez jellemző szövegtorzítási technika, hiszen az ember a nyelvről úgy is gondolkodik, hogy, ha nem írom helyesen, akkor már más vagyok, másnak adhatom ki magam. Emellett saját, nem reprezentatív megfigyeléseink szerint iskolai végzettségtől, kortól, nemtől függetlenül valószínű, hogy ugyanazt az álnevet adnánk egy „bűnöző társunknak”. Ez is bizonyíték arra, hogy a nyelvhasználatnak, a nyelvről való gondolkodásnak nem feltétele az iskolai végzettség, vagy például ebben az esetben a kor. A névadásvizsgálatnak azért lenne jelentősége a gyermekek ellen irányuló internetes bűncselekményeknél, mert a *nicknevek* széleskörű elemzése közelebb vihetne minket a különböző pornográf oldalak felhasználóinak profilozásához. Az internetes álnevek dekódolásánál figyelembe kell venni, hogy az ember nem tud elvonatkoztatni magától, mindig van valami csak ránk jellemző az álnevünkben. Például a születési évszámunk vagy a gyerekünk neve, esetleg az utca nevének kezdőbetűje, ahol élünk. Megfigyelhető az a jelenség, hogy a különböző oldalakon a felhasználók tudják egymást azonosítani a *nickneveik* alapján. Nem csak a szexuális bűncselekményekkel kapcsolatos szlenget lehetne vizsgálni tematikusan, hanem az egyéb bűnözői csoportok nyelvezetét is (fegyverkereskedők, kábítószerrel visszaélők). Eddigi tapasztalataink alapján mérhető a különböző bűnözői csoportok titkos nyelve. A „titkos nyelv” bevezetésének célja kettős: egyrészt a többségi társadalomtól való nyelvi elkülönülés (mi ne értsük őket), illetve a csoporton belül egymás azonosítása (ők viszont értsék egymást). Az egyes bűnözői csoportok tehát tevékenységüknek megfelelő titkos nyelvet hoznak létre. Feltételezzük, hogy az interneten használt bűnözői nyelv valamennyire eltér a nem internetestől, de vizsgálatuk mindenképp célszerű lenne.

Az internet biztonságos terep azok számára, akik nem akarják felfedni magukat. Lehetővé teszi az anonimitást, a személytelenséget. Az, aki az interneten követ el bűncselekményt, azt gondolja, hogy nem lehet őt beazonosítani. De senki nem olyan ügyes, hogy a nyelvi tevékenysége alapján ne bukna le, legalább abból a szempontból, hogy tudjuk, mennyi idős valójában, férfi-e vagy nő, és mik a szándékai. Egy negyvenöt éves férfi nem tud úgy „beszélni”, mint egy tizenöt éves fiú vagy lány. Annál sokkal rutinszerűbben használjuk a nyelvet, mintsem előállítsunk egy, nem a korosztályunkra jellemző nyelvhasználatot.

A különböző profilozások során segítségünkre lehet a genderszociolingvisztika. A társadalmi nemek nyelvhasználatának vizsgálata nagy jelentőséget kap nem csak a nyelvészetben, hanem az egyéb társadalomtudományokban is. Igazak a sztereotípiák is: a nők sokkal érzel-

mesebben fogalmaznak, mint a férfiak. A férfiak viszont lényegre törőbbek, ezért rövidebben írnak, mint a nők.

Mutatunk egy példát az álnévdekódolásra. A nyomozó hatóság részéről az volt a kérdés, hogy a két álnév (Sebinoka Hai és Solomon Cedar) alatt megjelenő szövegek származhatnak-e ugyanattól a személytől, illetve, hogy a két álnév alatt szereplő személy paranoid skizofrén-e. A nyelvészszakértő nem válaszolhat arra a kérdésre, hogy egy személy paranoid skizofrén-e, mert az nem nyelvészeti szakkérdés. Arra viszont adhat választ, hogy a szövegeknek, illetve az álneveknek van-e referenciájuk a valóságban. Ha nem, akkor lehet mondani, hogy a szöveg szerzője eltérő nyelvi viselkedést mutat az átlagoshoz képest. A két álnév alatt szereplő feltételezett személy nőket üldözött, életveszélyes fenyegetéseket küldözve nekik.

Sebinoka Hai: a „hai” szót meg lehet találni szótárban, cápát jelent. A „Sebinoka” okozott fejtörést. Egy szótárban, egy nyelven sem találkoztam ezzel a szóval. Egy olasz nyelvű oldalon szerepel a „sebino” kifejezés, ez egy különleges babafélének az elnevezése. (Ember formájú élethű babák emberi szörzettel.) A „ka” végződésről feltételezhető, hogy magyar kicsinyítő képző (babácska). Az előfordul a magyar nyelvben, hogy idegen szóhoz magyar toldalék kerül, pl. cset + ”I”, csetel.

A „*Sebinoka Hai*” dekódolása „babaevő cápának” és ismerve az ügyet, ez bele is fért a képbe.

A „*Solomon Cedar*” is nehéz falat volt. Ezt a szókapcsolatot nem lehet megtalálni csak az angol nyelvű Bibliában: „So Hiram gave Solomon cedar-trees and cypress-trees [according to] all his desire.” Salamon király cédrusfából építtetett templomot. Az isten felé való törekvés, az égiekkel való kapcsolat is megjelenik eltérő nyelvi viselkedést mutató személyeknél. Mindez azt igazolhatja, hogy a két álnevet takaró személy lehet olyan, akinek nyelvi tevékenysége eltér a hétköznapiétól. Az elemzésre került szövegek is ezt támasztották alá.

Feltételezzük, hogy az interneten megvalósuló online zaklatásnak megvan a külön nyelve. Sokszor anonim vagy álprofil a bejelentkezés, így a bántalmazást elkövető azonosítása nehéz. Az internetes nyelvhasználatra jellemző a rövidsége való törekvés, az egyszerűbb fogalmazás, az internetes szleng használata. Nincsenek meg azok a nyelvhasználatot kísérő jelenségek viszont (szupraszegmentális eszközök, mint hangszín, hanglejtés, hangmagasság), amelyek egy interakciót árnyalhatnak. Egyéb, a beszédet kísérő jelennel sem találkozunk közvetlen az internetes kommunikációban: hiányzik a mimika, a gesztikulálás. Ezeket helyettesíti viszont az emotikon. Az emotikon, azaz az érzelmeket kifejező ikon állandó kísérője az internetes beszélgetéseknek. Jelenlétük megerősíti egy üzenet tartalmának jelentését, azt nyomtatékosítja vagy magát a szöveget helyettesíti.

Az online behálózás (*grooming*) során az internetes anonim ismerkedés utáni találkozások sokszor tragikus következményekkel járnak, holott a magát fiatal fiúnak kiadó, a va-

lóságban felnőtt korú bűnöző internetes kommunikációjából rá lehetne jönni, hogy igazából kivel beszél meg randevút a gyanútlan áldozat.

A világháló lehetővé teszi a rejtőzködést, de a saját „nyelve” előtt senki nem bújhat el.

H. A JÖVŐ FEJLŐDÉSI IRÁNYAI

Az online világ fejlődését elképesztő dinamikája teszi félelmetessé – a sokirányú fejlesztés révén az internetes világ valamennyi meghatározó összetevője (pl.: hardver, szoftver, hálózat, társadalmi elvárások) pillanatról pillanatra változik.

Az online világ megjelenítéséhez és a vele való hatékony interakcióhoz tartozó hardver környezet mellett a design is rengeteget fejlődött az elmúlt tíz évben és a divat meghatározó eleme a minél összetettebb és vagányabb megjelenésű szerkezet, „kütyü”. A fiatalok körében az elismertség és a presztízs egyik szimbóluma a minél okosabb (és drágább) telefon. Míg az internet hőskorában egy asztali számítógép képernyője mögött szöveges weboldalakat nézegettünk, ma már egy kicsi telefon képernyőjén bármely közösségi oldalon azonnal megoszthatjuk az utcán készített fényképünket földrajzi helyzetünkkel együtt. A fejlődés pedig töretlen, újabb és újabb egyszerű eszközöket próbál okossá varázsolni és az internetre kapcsolni. Nemsokára olyan szemüvegben sétálunk az utcán, mellyel a szemünk által észlelt kép szimultán az interneten is látható; lesz karóránk, amely két percenként méri a pulzusunkat és online adatbázisokkal összehasonlítva nem csak előrejelzi betegségünk, hanem még az orvost is riasztja; lesz játékkonzolunk, amely a szobába való belépésünket érzékelve újabbnál újabb játékokat ajánl nekünk. Az okos eszközöket a jövőben az állandó internetes kapcsolat mellett már rengeteg olyan szenzorral szerelik fel, amellyel az eszköz a környezetét is megfigyelheti (pl.: gyorsulásmérő, kamera arcfelismeréssel, mélységmérő, lézeres letapogató, GPS szenzor, zajszint mérő és elemző)

Az „Internet of Things” (‘IoT’, vagyis a **Dolgok Internete**) kifejezés azt jelenti, hogy a személyes környezetünk valamennyi eszköze online és önállóan kommunikál, így már a hűtőgép is tudni fogja, hogy elfogyott a friss tej, szóval érdemes a tableten leadni a rendelést. (Ilyen okoshűtő már létezik, mellyel a HomeChat alkalmazáson keresztül bármikor kapcsolatba léphetünk. Mivel az intelligens hűtő fotózni is tud egy beépített kamera segítségével, így akár okostelefonról vagy tabletről végigkövethetjük a hűtő aktuális tartalmát anélkül, hogy kinyitottuk volna az ajtaját. Egy szoftver figyelemmel követi a tárolt ételek frissességét is, és azonnal jelzi, ha egy termék szavatossága lejárt. A reklám szerint az okos hűtő az egészségünkre is ügyel: az „egészséges étrend ajánló” alkalmazás egészséges napi és heti étrendet is össze tud állítani a felhasználók személyes adatai (súly, nem, magasság, BMI index) alapján. Dél-Koreában már működik az a sütő is, amely recepteket tud ajánlani, majd

magától beállítja az adott ételhez szükséges sütési hőfokot és időt. A chat programon keresztül pedig megkérdezhetjük, hogy milyen ételt javasol az általunk megadott alapanyagokból, majd a receptkereső ablakon keresztül már küldi is a lehetséges variációkat.⁶⁸⁾

A fenti adattenger mind egy-két multinacionális vállalatnál fut majd össze, amelyek óriás adathalmazai (*big data*) és bonyolult algoritmusai segítségével a fogyasztókat kategorizálják és nagy valószínűséggel meg tudják jósolni viselkedésünket is – ha úgy tetszik, majd helyettünk gondolkodnak és hoznak döntéseket. Először csak apró-cseprő dolgokban, majd később egyre önállóbban.

A másik valós veszély, hogy ezek az okoseszközök adatbiztonsági értelemben rendkívül sebezhetőek, igen könnyen meghackelhetőek.

A gyermekeket közvetlenül érinti, hogy a legtöbb eszközből most már tudatosan fejlesztenek a legkisebb korosztály számára is. A jövő nagy kérdése, hogyan tudja a szülő a gyermeke legelső hónapjaiból, éveiből számúzni az állandó digitális és internetes jelenlétet, ami az ember természetes fejlődésétől mindenképpen életidegen.

De nem csak a hardver fejlődik dinamikusan, a megosztási csatorna és felület is egyre bővül. A mobilinternet gyorsulása révén a videók megosztásához már le sem kell szállnunk a villamosról. A tartalmak közzétételének a lehetősége is egyre szélesebb, az internet hőskorában még csak kör e-mailben küldözgettük személyes adatainkat, ma már egy közösségi oldalon százmilliók csoportosulnak, és két kattintással közvetíthetjük videóinkat milliók számára. A fejlődés itt sem áll meg, egyre több tematikus közösségi oldal alakul, a tematikus honlapok pedig egyre gyakrabban célozzák meg a fiatalkorúakat, sőt az egyre felhasználó-barátabb rendszerekben saját tematikus mikroközösséget is alkothatunk.⁶⁹⁾ Az igazi kihívást a kiskorúak szempontjából azonban a közösségi oldalak alapját képező marketing tevékenység rejti, amely az egyik legjövődélmezőbb szegmensnek ezt a korcsoportot látja. A közösségi oldalak egyre erősebben koncentrálnak a viselkedésalapú reklámokra, a kiskorúak megosztásait, alkalmazásait figyelve próbálják egyre személyre szabottabb reklámokkal becserkészni őket.

A magánszféránk közzétételére alkalmas közösségi alkalmazások közül is a legtölkodóbbak kerülnek előtérbe, terjednek a folyamatos aktivitást igénylő megoldások, illetve a kép és videó megosztásra építő szolgáltatások.

A szoftver fejlesztések oldaláról nézve a mobil platformok alkalmazás boltjaiban egyre több az egyéni fejlesztők által kifejlesztett program, amelyek a személyes szférára tekintet nélkül próbálják a kiskorúak személyes adatait megszerezni. Az alapvetően a felnőtt élet kényelmi szempontjait kiszolgáló fejlesztések – mindenhol elérhetőek legyünk, sorban

68 <http://impressmagazin.hu/szia-huto-van-otthon-tej-okos-technologia-a-konyhaban/#!prettyPhoto>, 2016-02-12

69 Hollandiában egy kiskorú által kiskorúaknak kifejlesztett közösségi oldalt is vizsgálat alá vont a holland adatvédelmi hatóság.

állítás nélkül elintézhessük dolgainak – ma már a reklám szempontjából sokkal jövedelmezőbb korosztályt, a kiskorúakat célozzák meg. Egyre kiemelkedőbb divat lett a különböző online szolgáltatásoknak a gyermekekre optimalizálása. Ha ma végigtekintünk egy online applikációkat kínáló alkalmazásboltban, hemzsegnek benne a gyermekeknek szóló programok. A kicsik kifestőzhetnek a tableten, beszélgethetik a virtuális macskát az okostelefonon, vagy simogathatnak virtuális oroszlánt a játékkonzolon. Az applikáció gyártók azonban nem csak ilyen kreatív ötletekkel csalogatják be a gyermekeket a virtuális környezet határtalan világába – a legnagyobb veszélyt a gyermekeknek gyártott játékok végeláthatatlan sora képezi, az ingyenes játékoké, amelyek azonban a környezetnek megfelelően csak virtuálisan ingyenesek. A gyermek alapesetben személyes adataival fizet értük, rosszabb esetben azonban a szülő pénztárcája is kinyílik. Rengeteg az olyan játék, ahol kisebb-nagyobb előnyökért, újabb pályákért kell apró fizetéseket produkálni. A becsalogató mikrofizetések olyan pszichológiai módszert használnak, hogy egy komoly élettapasztalattal rendelkező felnőtt is könnyen csábításba esik, nemhogy egy gyermek.

Az online közösségi élmény elvárás minden alkalmazástól, egy kiskorú ma már az összes játékot ismerős vagy idegen játékosok ellen játssza az interneten és az alkalmazás legfejlettebb opciója, hogy ismerősei személyes adatainak kiszolgáltatásával játéktársakat hívjon meg. A legtöbb játékban megoszthatjuk, merre jutottunk, mit csináltunk, de ezen is túlmenően élő telefonos kapcsolatban szapulhatjuk egymást a neten, vagy adhatunk meg személyes adatokat idegeneknek.

További veszélyt jelent, hogy a mobil alkalmazások egyre több személyes adatot kérnek vagy osztanak meg. A legtöbb alkalmazás hozzáférést követel a mobilon tárolt valamilyeni tartalmunkhoz, kapcsolatainkhoz, közösségi oldalon létrehozott profilunkhoz, földrajzi helyzetünkhöz. Az óriási adathalmazból, így még jobban fel tudják térképezni életünket.

A hardveres és szoftveres környezet mellett természetesen a társadalmi nyomás is személyes adataik kiadása felé kényszeríti az érintetteket. Egyre erősebb a hajtóerő a kiskorúakban, hogy az online környezetben is meglepő és mulatságos látványosságokkal rukkoljanak elő. Ez olyan meghökkentő és vicces közzétételeket kíván, amely a saját vagy társunk magánszférájának teljes kitárulkozásával jár.

Az online világ fent említett dinamikus fejlődéséből adódóan a szülők, akik nem ebben a digitális világban nőttek fel (ún. X és Y generáció), nem képesek követni és megismerni annak veszélyeit, így nem tudják kontroll alatt tartani és segítséggel ellátni a gyermekeiket (ún. Z generáció). Természetesen az iparág is tehetne annak érdekében, hogy az új technikák már figyelembe vegyék az adatvédelmi szempontokat, de ezek a szempontok gyakran szemben állnak a gazdasági megfontolásokkal. Az állami szerepvállalás növelése világszinten tendencia, de a hatékony megoldások többnyire elvesznek a hasztalan stratégiaalkotás és a gyors iparági fejlesztések között. A veszélyekre ezért azoknak a felnőtteknek kell

felhívni a kiskorúak figyelmét, akik felelősek a fiatalabb generációk neveléséért. Ne felejtjük el, hogy ők azok, akik már az online közösségben szocializálódtak, a mindennapi életük része, hogy státuszüzenetben vagy fényképpel megosszák a világgal a fontosabb vagy kevésbé fontosabb történeteiket.

Végül, de nem utolsósorban szót kell ejteni a napjainkban legnagyobb térhódítást végző technológiájáról, a mesterséges intelligenciáról. A mesterséges intelligencia (MI) egy számítástechnikai tudományág, amely arra törekszik, hogy olyan rendszereket hozzon létre, amelyek képesek az emberi intelligenciához hasonló gondolkodásra, tanulásra és problémamegoldásra. Fő jellemzői:

- tanulás: Képes adatokat elemezni és tapasztalatokból tanulni (lásd gépi tanulás).
- következtetés: Döntéseket hoz meglévő információk alapján.
- nyelvi képességek: Feldolgozza, értelmezi, vagy akár előállítja az emberi nyelvet (lásd beszédfelismerés, szövegalkotás).
- kép- és hangfelismerés (lásd arcfelismerő programok)
- Autonóm működés: Önállóan is képes bizonyos feladatok elvégzésére (lásd önvezető autók).

Az MI jelentős hatása lehet a gyermekek életében, a személyre szabott tanulás (például otthoni nyelvtanulás) nagyon hasznos eredményeket hozhat, ugyanakkor ez a technológia a gyermekek magánszférájára, adatvédelmére nézve kifejezetten kockázatos, hiszen akár a „tanulási”, akár a „döntési” fázisban olyan mennyiségű és minőségű információt használ, ami szinte kontrollálhatatlannak tűnik.

Adatvédelmi kockázatok gyermekek esetében:

1. Túlzott adatgyűjtés: sok alkalmazás és játék olyan adatokat is gyűjt, amelyek nem szükségesek a működéshez, például pontos földrajzi hely, keresési szokások, arcfelismerés, ami különösen veszélyes gyerekeknél, mert ők nem mindig értik meg, milyen adatokat osztanak meg.

2. Profilalkotás és célzott reklám: az MI képes a gyerekek viselkedéséből következtetni érdeklődési körökre, szokásokra – ezek alapján reklámokat, videókat ajánl, ami manipulatív hatása lehet, különösen, ha a gyerek nem is érti, hogy őt „megfigyelik”.

3. Hosszú távú adatmegőrzés: a gyerekekről gyűjtött adatok hosszú ideig tárolódhatnak, ami később hátrányos is lehet számukra (például később kizáródhatnak egy adott szolgáltatás igénybevételéből).

4. Biometrikus adatok kezelése: egyes MI-eszközök hang-, arckép- vagy ujjlenyomat-alapú működést használnak, ezek az adatok nem visszavonhatók, nem lehet őket „újra cserélni”, mint egy jelszót, aminek egy esetleges adatszivárgásnál rendkívül súlyos következményei lehetnek az egyén életében.

PROBLÉMATERKÉP – ONLINE DEVIANCIÁK

„Ha nem posztolod, meg sem történt!” jelmondat irányítja a fiatalok mindennapiját. Természetességgel élük életüket különböző online platformokon, virtuális ismeretleneket vagy „félismerőseket” is barátnak vélnék, ebből következően túlzottan kitarulkozóak a saját és mások magánéletével összefüggésben, és mindaddig nem is érzékelik tetteik súlyát, míg a veszélyek következményei el nem érik őket.

Az információs társadalom új devianciáinak körében jelentkező jelenségek a „furcsa”, rossz érzést maga után hagyó benyomásoktól a bűncselekményt megvalósító magatartásokig terjedhetnek.⁷⁰ Az egyik lehetséges ok az új életviszonyok okozta anómia. Az anómia a szó szoros értelmében normahiányos helyzetet jelent, tágabban olyan állapotot, amikor általában új, ismeretlen élethelyzetekre nincs régi, eligazító norma vagy a kialakult társadalmi gyakorlat eltér a társadalom által vallott normáktól.⁷¹ Katelyn McKenna szerint az infokommunikációs eszközök segítségével folytatott interakciókban négy olyan fő rizikófaktor van jelen, amelyek nagymértékben meghatározzák a környezet pszichológiai hátterét: ezek az anonimitás, a fizikai jelenlét szükségességének csökkenése, az interakciók ideje és menete feletti erősebb kontroll, és a hasonló gondolkodásúak könnyebb találkozása.

A látszólagos anonimitás mellett egy másik rizikófaktor az enyhének tűnő közösségi szankció, mivel a deviáns viselkedésnek a virtuális térben legtöbbször csupán annyi következménye lehet, hogy a másoknak nem tetszőn viselkedőt kizárják a csoportból, ellentétben a közvetlen élethelyzetekkel, ahol sokkal súlyosabb következményei is lehetnek egy normaszegésnek. A kibertéri közösségek enyhe szankciói mellett a valóvilágbeli társadalom szintén enyhe értékelése is erősíti ezeket a devianciákat. Az anonim online élet egyfajta kettős morál kialakulásához vezet, ami az offline társadalmi normák lazább értelmezését jelenti, azaz a felhasználók nagy része hagyományosan normakövető marad, de az internetes kommunikációja során már eltérő szabályok szerint él.⁷²

Az online világ egy olyan tér, ahol „felszakadnak” a gátlások, ahol mindenki sokkal könnyebben tud kapcsolatot kialakítani ismeretlenekkel is, ahol bátrabban közöl véleményt vagy ad ki információt, akár önmagát felvállalva, akár anonim módon. A fiatalok többsége pedig vakon tárulkozik ki a világ számára. A lányok jobb esetben bikinis képeket töltenek fel magukról, közlik a világgal, hogy éppen hol tartózkodnak, hova mennek hétvégén bulizni, vagy éppen azt, hogy egyedül lesznek otthon egy teljes hétvégre.

70 Adler F., Mueller, G.O.W. & Laufer, W.S., Kriminológia, Osiris Kiadó Budapest, 2002. pp. 34-35.

71 Gönczöl K., Kerezi K., Korenik L. & Lévy M. (ed.) Kriminológia-Szakkriminológia Complex Kiadó Budapest, 2006. p. 104.

72 Szathmáry Zoltán: Bűnözés az információs társadalomban, Alkotmányos büntetőjogi dilemmák az információs társadalomban, Doktori értekezés, Budapest 2012. pp. 64-65.

Dr. Peszleg Tibor rendőr őrnagy tapasztalatai szerint a gyermekekben a veszélyérzet a netezés során a szükségesnél általában alacsonyabb: *„A gyermekben lebontják azokat a gátakat, melyek ösztönösen, vagy a családi neveltetése folytán benne vannak. Az internetes beszélgetések után jön a személyes találkozó, mely során a fiatalok már valamely bűncselekmény sértettjévé válhat. Ilyen veszélyes ismerkedési lehetőségek az internetes chat szobák, levelező fórumok, IRC csatornák. Munkám során találkoztam olyan gyermekkorúval, aki egy chat szobában ismerkedett meg felnőtt korú személlyel, a személyes találkozás során nemi kapcsolatot létesített vele, és közösen fogyasztottak kábítószer. Több napig is távol volt a családjától, és hazatérte után sem érezte cselekedete és a vele történtek veszélyét. Meghallgatása során elmondta, hogy nem ez volt az első ilyen, úgynevezett „chat-es kapcsolata”.*⁷³

Az úgynevezett „esernyő fogalomként” használt **kiber-megfélemlítés (cyberbullying)** célja, hogy a megfélemlítő az áldozat felett egyfajta negatív „hatalomra” tegyen szert. A bántást elektronikus eszközök igénybevételével, online felületeken (email, sms, chat, mobil alkalmazások, blogok, közösségi oldalon történő posztolás) valósítja meg.

A cyberbullying egyik formája – a becsületsértés, rágalmazás, gyűlöletbeszéd, szervezett kiközösítés, személyes adatokkal való visszaélés, zsarolás, magántitok megsértése, az emberi méltóság és egyéb személyiségi jogok megsértése mellett – a zaklatás. Emellett ide sorolhatók olyan rosszindulatú cselekedetek is, melyek bár nem jogszabály ellenesek, mindazonáltal az áldozat tekintélyét, önbizalmát, erőpozícióját és/vagy társadalmi státuszát rombolják, károsítják.

A büntető törvénykönyv viszonylag új tényállása a kiszolgáltatott személy megalázása, melynek minősített esete alapján ha valaki mást annak kiszolgáltatott élethelyzetét kihasználva arra bír rá, hogy magát megalázó magatartást tanúsítson és a magát megalázó személyről felvételt készít, vagy ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz, akár két év szabadságvesztés büntetést is kaphat (üzletszerű elkövetés esetén 3 évet).

A. Online zaklatás

A modern technikai eszközöknek, és az internet egyre szélesebb körben való elterjedésének következtében egyre gyakrabban lehet hallani a felvilágosítás hiánya miatt leginkább a 10-16 év közötti korosztályt érintő online zaklatásról. Ez mindig személyes indítékkal indul és az elkövető hosszabb ideig, visszatérően „kínozza” áldozatát.

73 Dr. Peszleg Tibor: Internet és pedofília in.: Belügyi Szemle 2004. december in.: http://www.remet.hu/cms/index.php?option=com_content&task=view&id=16&Itemid=4, 2013-02-12

A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) a magánszférát sértő, abba durván beavatkozó zaklatás tényállását a következőképpen szabályozza a 222. §-ban:

- (1) *Aki abból a célból, hogy más megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen vagy tartósan háborgatja, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.*
- (2) *Aki félelemkeltés céljából*
- a) más vagy rá tekintettel hozzátartozóját személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével megfenyeget, vagy*
 - b) azt a látszatot kelti, hogy más életét, testi épségét vagy egészségét sértő vagy közvetlenül veszélyeztető esemény következik be,*
- vétség miatt két évig terjedő szabadságvesztéssel büntetendő.*

A kulcsszó a rendszeres háborgatás megfélemlítési céllal (ezek mind tényállási elemek), a háborgató cselekmények azonban eltérőek lehetnek: például valaki éjjel-nappal fenyegető vagy megalázó tartalmú elektronikus leveleket küld, közösségi oldalakon üzenget, bántó tartalmú kommenteket ír vagy blogos naplójában sértegeti társát. Kamerával felszerelt mobiltelefon birtokában egy bárhol megtörtént kellemetlen jelenetet már aznap tömegek nézhetnek valamelyik közkedvelt közösségi oldalon. Az infokommunikációs eszközök segítségével elkövetett támadó jellegű cselekmény egy kortárs személytől kiindulva ismétlődő jelleggel irányul egy kiszemelt áldozat ellen, amelytől az nem tudja önmagát megvédeni. Durva tréfa, ugratás, amely során jellemzően a 13-17 éves fiatal korosztályok tagjai különböző platformokon lejáratják egymást.⁷⁴

2010-es adatokkal összehasonlítva 2014-ben a 11-16 éves európai gyerekek 12 %-ánál valószínűsíthető, hogy találkozik online zaklatással (a korábbi 7%-hoz képest az elmozdulás szignifikáns)⁷⁵.

A zaklatás következményei pedig igen súlyosak is lehetnek: egy uniós felmérés szerint a zaklatás áldozatául esett gyermekek 55%-a depresszióról számolt be, 35%-a tett kárt magában és 38%-uk gondolt az öngyilkosságra, mint megoldásra.⁷⁶ Ráadásul az internet használata és az online lét egyre fiatalabb – 8-10 éves – korban kezdődik, ebből fakadóan a gyerekek valószínűleg találkoznak ártó, életkoruknak nem megfelelő tartalommal vagy viselkedéssel.

74 Szathmáry Zoltán: Bűnözés az információs társadalomban, Alkotmányos büntetőjogi dilemmák az információs társadalomban, Doktori értekezés, Budapest 2012. pp. 68-69.

75 <https://lisedesignunit.com/EUKidsOnline/index.html?r=64> (2016.02.22.)

76 http://europa.eu/epic/news/2014/20140805-cyberbullying-harm-european-children_en.htm (2016.01.14.)

Az online és offline térben előforduló zaklatás gyakran jár kéz a kézben, ugyanis az online térben elkezdődött zaklatás folytatódhat az osztályteremben vagy az utcán is, így az áldozat nem menekülhet az őt ért támadás elől.

B. Internetes kibeszélés (mém küldés)

A digitális fájlok vagy hivatkozások eredetileg reklámcélú kiküldése manapság gyakran hamis hírek, kínos videók vagy képek terjesztéséből áll, ami jelenthet akár művészi kifejezést, mosolyra fakasztó kedveskedést is, de sokszor kifejezetten durva lejárató kampányba torkollik. A *mémelés* a *cyberbullyingtől* abban különbözik, hogy a kárvallott alany általában idegen személy, akit az internetes közösség „kipécéz” magának valamilyen tulajdonsága vagy megnyilvánulása alapján. Ismert emberekről van szó, például XVI. Benedek lemondása után igazi „mém sztár” lett, sokszor kifejezetten ízléstelen módon megjelenítve a pápát, de előfordul, hogy hétköznapi emberek – ritkán gyerekek – is a hálóba akadnak. Ez történt egy 11 éves kaliforniai kislánnyal is 2010-ben, aki YouTube videókat osztott meg magáról és zenei preferenciáiról a neten. Megnyilatkozásai ellenszenvet váltottak ki egy internetes közösségből, ezért elhatározták, hogy „megbüntetik”: hamis híreket raktak fel a kislány és egy ismert énekes állítólagos szexuális kapcsolatáról, amit a gyerek anyja elhitt és botrányt csapott, a kislány ezért elkeseredésében fenyegető hangú képüzenetet küldött a közösségnek.

Erre valahogy megszerezték a család telefonszámát, e-mail címeit és elindult a zaklató áradat, beleértve a halálos fenyegetéseket is. A kislány sírva kérte újabb videó üzenetében, hogy hagyják őket végre békén, de a felvétel közben bejött a haragos apa és keresetlen szavakkal fejezte ki véleményét. Bosszúból az apát a neten nyilvánosan megvádolták lánya megrontásával és bár a vád alól a bíróság felmentette, az apa hamarosan szívrohamban meghalt, míg a kislány azóta is pszichiátriai kezelésre szorul. A megszólaltatott amerikai szakértők tanácsa ilyen esetekre világos: nem szabad felvenni a kesztyűt, a mocskolódásokra nem kell a neten reagálni, mert az a közösség tagjaiból csak hisztérikus bosszút vált ki.⁷⁷

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

C. Trollkodás

A troll internetes szlengben olyan személy, aki provokatív, ingerlő módon, tárgyhoz nem tartozó üzenetekkel bombáz egy online közösséget (például internetes fórumon, chaten, blogon, levelező listán), vagy személyes véleményét erőszakosan súlykolja azzal a szándékkal, hogy más felhasználókból heves reakciókat váltson ki, vagy egyébként egyéb módon zavarja, ellehetetlenítse a témába vágó eszmecsere. Az angol „*Do not feed the trolls*”, azaz „*ne etesd a trollokat*” kifejezés (rövidítése: DNFTT) azt jelenti, hogy az ilyen hozzászólókat ignorálni kell.

A trollok között „divat” híres sportolókat nyilvánosan gyalázní.⁷⁸ Egy fiatal angol boxolóra „szállt rá” egy twitteres zaklatója, aki Jimmibob88 néven bejelentkezve változatos sértéseket vágott a sportoló fejéhez és gúnyolódott eredményein. A heves vérmérsékletű sértett a Twitteren 1000 font „vérdíjat” ajánlott annak, aki elárulja a troll nevét és címét. Nem sokára rá is talált ellenfelére, még egy fotót is kipoztolt a házáról bizonyítva, hogy bármikor elkaphatja. A troll könyörgésre fogta a dolgot és bocsánatot kért. A Twitteren az eset miatt a legnépszerűbb hashtagek közé emelkedett a #keyboardwarrior (billentyűzetharcos) és a #jimmybrownpants (kb. beszari Jimmy) minősítés.⁷⁹

A trollok ténykedése egyértelműen elszabadítja az indulatokat: mind a gyalázkodás, mind az ellenreakciók brutális stílusban zajlanak, gyakori a halálos fenyegetés is. Egy rosszul sikerült meccs után a sportolót akár ilyen üzenetek is várhatják: „*I hope you, your wife, kids and family die, you deserve it*” – Remélem te, a feleséged, a gyerekeid és családod is meghal, megérdemlitek.”⁸⁰ A szélsőséges véleményüket csak álnév mögött vállaló trollok biztosan nem segítik elő a kulturált internetes stílust, és általában is rossz hatással vannak a többi felhasználóra.

D. Erotikus képek küldözgetése (sexting)

„Gyakran futok bele abba, hogy a tizenéves lányok azzal szórakoznak, hogy kiteszik az üzenőfalukra: ötven lájkért fölteszek a netre magamról egy félmeztelen képet vagy elárulok egy intim titkot az életemből, aztán megmutatja a képet, és egyáltalán nem érzi problémának.”⁸¹

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

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

80 <http://bleacherreport.com/articles/1034961-san-francisco-receiver-kyle-williams-receivers-death-threats-on-twitter>, (2013.06.18.)

81 Kalapos Éva Veronika, író

A sexting erotikus képek vagy videók infokommunikációs eszközökkel történő küldözgetése, mely az utóbbi években vált a fiatalok körében divatos jelenséggé.

2014-es kutatási adatok alapján a tini lányok 22%-a, míg a kamasz fiúk 18%-a küldött már magáról erotikus képet. Ráadásul 15 %-uk olyan személynek is küldött ilyen képet, akivel sohasem találkozott. A fiúk fő motivációja egyértelműen a vágykeltés, a lányoknál már megjelenik a kényszer, de sok esetben csak viccnek fogják fel mind a küldést, mind a fogadást.⁸²

A legtöbb „felderített” sexting esetről megállapítható, hogy az erotikus jellegű felvételeket az érintettek önmagukról vagy közös megegyezéssel másról készítették, de a felvételek sorsa a későbbiekben már tőlük függetlenül alakul. A nyilvánvaló körülmény, amely visszaélésekre adhat lehetőséget az, hogy a többszörözött képek minden további engedély és egyéb korlát nélkül továbbíthatók. A felelőtlenség („jó vicc”) mellett a másik motivációt a bosszúvágy jelenti, amikor egy párkapcsolat megszakadása után az egyik fél – legtöbbször a fiú, férfi – a párjáról készített felvételek megosztásával „bünteti”, zsarolja vagy megszegényíti a másikat.

Egyes vélemények szerint a mai tinédzserek szexuálisan koraérettnek és csak szórákozásból küldözgetik az erotikus üzeneteket. Mások azt vallják, hogy a fiatalok kísérletező magatartása miatt hoznak rossz döntéseket. Azonban a témakörrel foglalkozók abban egyetértenek, hogy az erotikus felvételek haragból vagy bosszúból történő terjesztése további létező, emocionális visszaélésekkel és erőszakkal jellemezhető fiatalkori párkapcsolati magatartásminták része is lehet. Hiba volna azt feltételezni, hogy csak a fiatal generációkra jellemző ez az attitűd, azonban technikai lehetőségek birtokában a tizenévesek emocionális élete, alapvetően impulzív viselkedése az oka annak, hogy ők biztosan nem mérlegelik a hosszú távú következményeket.⁸³

ANAIH látkörébe került eset jól szemlélteti a fent elmondottakat: egy 14 éves kamasz lány és egy 16 éves kamasz fiú erotikus fényképeket készítettek egymásról. A fiú a képeket dicsekvésből megosztotta egy közösségi oldal zárt csoportjában, melynek majdnem a teljes osztály tagja volt. A lány édesapja tudomást szerzett az esetről és feljelentést tett a rendőrségen. A nyomozás során az osztály fiú tagjait gyanúsítottként kihallgatták, hiszen a lány a felvételek kezeléséhez soha nem adta kifejezett hozzájárulását és a képeket valakinek megismerték. Eldöntendő jogkérdés, hogy a megismerésen túl a gyanúsítottak továbbították-e a képeket másnak, mert ebben az esetben megvalósul a személyes adattal való visszaélés tényállása (az adat megismerése önmagában nem minősül adatkezelésnek). A szembesített fiatalok az eljárás során is közömbösen, éretlenül viselkedtek, egyedül a szülő volt valóban feldúlva a történet miatt.

82 <http://nobullying.com/sexting-statistics/> (2016. 02.04.)

83 Szathmáry Zoltán: Bűnözés az információs társadalomban, Alkotmányos büntetőjogi dilemmák az információs társadalomban, Doktori értekezés, Budapest 2012. p. 70.

Ezek az új trendek érzékletesen jellemzik nemcsak a morál változásait, de az érintett szereplők – gyerekek – egyes védett társadalmi értékekhez való viszonyát is.

E. AZ INTERNETES PEDOFÍLIA

Pedofil az a felnőtt személy, aki személyiségzavara okán gyermekkorúak iránt érez szexuális vágyat. A pedofília társadalmi megítélése rendkívül negatív és különféle megnyilvánulásait a büntetőjog is több tényállásban bünteti:

- szexuális visszaélés: az a tizennyolcadik életévét betöltött személy, aki tizennegyedik életévét be nem töltött személlyel szexuális cselekményt végez, vagy ilyen személyt arra bír rá, hogy mással szexuális cselekményt végezzen; vagy
- gyermekpornográfia: aki tizennyolcadik életévét be nem töltött személyről vagy személyekről (ideértve a virtuális, nem létező személyeket is!) pornográf felvételt készít, tart, hozzáférhetővé tesz vagy pornográf műsorban szerepeltet, szereplésre hív.

Az elkövetők ezért tevékenységüket természetesen titkolják. Az internet kiváló fórum az anonimitás megőrzésével megvalósuló pedofil vágyak kielésére. Nem csak az egyéni, hanem a szervezett bűnözés megvalósulására is, hiszen a gyermek pornográf képek megszerzése és egymásnak való átadása a hálózaton keresztül sokkal gyorsabb, egyszerűbb. Egy nem szokatlan példa: negyvenes éveiben járó férfi 18 évesként regisztrál egy közösségi portálon vagy egy társkereső oldalon, feltölt „magáról” egy vonzó képet, elkezd tini lányokkal ismerkedni, egyre közelebb kerülnek egymáshoz, a kislány bizalmába fogadja a „fiút”, akinek kérésére esetleg további képeket küld magáról, rosszabb esetben meztelen vagy félmeztelen felvételeket.

Az internetes pedofília megvalósulása során tulajdonképpen az elkövetők az internetet eszközként használják a szexuális visszaélés (korábban megrontás) véghezviteléhez ismerkedésre, kapcsolatépítésre, vagy a sértettek valós szándékát, illetve érdekeiket súlyosan sértve szereznek be róluk pornográf felvételeket.

Adatvédelmi szempontból problémát jelenthet, hogy sok esetben a pornográf képek begyűjtését maga a sértett akarva-akaratlanul megkönnyíti azáltal, hogy önként tölti fel magáról a felvételt, illetve külön szakértő bevonását igényli és még így is nehéz a bizonyítása, hogy egy pornográf felvételen valóban az adott gyermek található-e. Sok esetben ugyanis megváltoztatják a képeket, például egy meztelen testhez egy idegen fejet szerkesztenek hozzá egy egyszerű képszerkesztő szoftver segítségével.

Végül szólni kell a gyermekek kizsákmányolásának új formájaként jelentkező webkamerás, virtuális pedofilizmusról, mely az elkövetőknek sokkal biztonságosabb és olcsóbb is. 2013-ban tíz hét alatt ezer pedofilt azonosított a Terre des Hommes nevű holland gyermekjogi szervezet, az akcióhoz egy 3D modellt használtak, aki egy tízéves filippínó kislányra hasonlított. A Sweetie névre keresztelt virtuális kislány csetszobákban várta a férfiakat, a kísérlet két és fél hónapja alatt több mint húszezren elegyedtek vele online beszélgetésbe úgy, hogy valamilyen szexuális szolgáltatást kértek tőle, sokan közülük fizetni is hajlandóak lettek volna ezért. Ezer pedofil személyazonosságát sikerült megállapítani, általában a közösségi médiában publikusan fellelhető információk alapján, az adatbázist a szervezet átadta az Interpolnak. A jogvédő csoport dokumentumfilmet is forgatott az akcióról, a programban részt vevők ebben azt mondják, a gyermekprostitúció elleni küzdelemben ledolgozott évek után is sokkoló közvetlen közlelől meg tapasztalni, miket kérnek a pedofilok egy tízéves kislánytól. A nyomozás szerint a legtöbb beazonosított szexuális ragadozó amerikai volt, utánuk a britek, majd az indiaiak következtek, összesen 71 országból akadt horogra pedofil. Általában teljesen hétköznapi, fiatal vagy középkorú férfiaknak tündek, a filmben példaként egy 35 éves, kétgyerekes atlantai családapát emlitenek, aki 10 dollárt ajánlott Sweetie-nek, hogy levegye a ruháit.⁸⁴

F. ONLINE BEHÁLÓZÁS (grooming) és az online ragadozók (predators)

„Én 12 évesen mehettem haza az intézetből a nagymamámhoz” – kezdi a történetét az egyik 14 éves lány, Brigi, aki két éve van Esztergomban, idén nyáron „szabadul”. Hazagondozása után a Facebookon ismerkedett meg egy 45 éves férfival, aki profilképe alapján bejelölte, ő meg visszajelölte, mert nagyon boldog volt, hogy 12 éves létére azt írja neki valaki, hogy milyen szép. Attól kezdve sokat cseteltek, míg a férfi rábeszélte, hogy költözzön hozzá. Brigi éjjel indult el biciklivel. „Hogy mivel győzött meg? Hát, hogy mellette önálló lehetek. Saját házam és konyhám lehet, azt mondta, mellette én leszek a királynő. És ha akarom, reggel ágyba hozza a kakaót.” Brigit teljesen véletlenül látta meg a bátyja a buszmegállóban, majd a nagymama hívta a rendőröket, akik kimentek arra a címre, amit Brigivel találkozási pontként megbeszéltek. Ekkor derült ki, hogy a lányt már előre eladták külföldre. A lányt azonnal Esztergomba szállították védelmi okokból.”⁸⁵

⁸⁴ <http://kronika.ro/szines/ezer-pedofilt-fogott-a-virtualis-kislany>, (2016. 02.05.)

⁸⁵ idézet Kalas Györgyi cikkéből http://index.hu/kultur/2016/03/03/azt_mondda_szep_vagyok_es_agyba_hozza_majd_a_kakaot_nekem/ 2016.03.07.

Magyar kifejezés igazából egyelőre nincs rá, a behálózás, becserkészés szóval írhatjuk körül a jelenséget⁸⁶. A közösségi oldalak terjedésével leegyszerűsödtek az ismerkedés szabályai és a gyerekek gyakran olyan emberek közeledését is elfogadják, akikkel ugyan még nem is találkoztak, de ismerős ismerőse vagy van valami közös érdeklődésük. Számolnunk kell azzal is, hogy egy fénykép mögött rejtőző, magát 14 éves fiúnak mondó valaki a valóságban egy harminc, negyven vagy még idősebb férfi, aki szexuális vágyai kiéléséhez keres áldozatokat a világhálón. Az idősebb elkövetők zöme több hónapon át, tudatosan felépített stratégiával vadászik a közösségi hálókön lévő náluk jóval fiatalabb lányokra, fiúkra egyaránt. Bizalmukba férkőznek, kicsálnak tőlük személyes információkat, az interneten keresztül vonják be őket szexuális játékaikba, és végső esetben még személyes találkozóra is ráveszik őket. A gyerekek kezdetben – a jól kiépített bizalmi viszony révén – fel sem ismerik, hogy mi történik velük, nem okoz bennük törést, hogy aki kezdetben velük egykorúnak adta ki magát, a valóságban nem az. Az izgalom és kíváncsiság sokkal nagyobb bennük. Ha mégis személyes találkozóra kerül sor, akkor ezekről a gyerek nem beszél. Szégyenérzete miatt általában nem, vagy túl későn kér csak segítséget.

Az *online ragadozók* sokféleképpen próbálkoznak kapcsolatba lépni a gyermekekkel: ígéretesnek tűnő ajánlattétel, segítség kérés, segítség felajánlása, közös ismerősökre, eseményekre hivatkozás, internetes szokások megfigyelése, munkaajánlat, könnyű pénzkeresési lehetőség, modellkarrier ígérete. A különféle közösségi oldalak kiváló lehetőséget nyújtanak arra, hogy megismerjék a netező gyerekek szokásait, érdeklődési körét, akár személyes adatait. Sokszor pontosan nyomon lehet követni, hogy valaki éppen hol tartózkodik, vagy az elkövetkező napokban hol, milyen eseményeken fog részt venni. A cél a kapcsolat és bizalom kiépítése, elmélyítése, minél jobban kötődjön hozzá a gyermek, hogy aztán egyre több dologra lehessen rávenni: személyes találkozó, szexuális kapcsolat létesítése, pénz vagy értéktárgyak átadása, pornográf kép- vagy videófelvétel készítése, szexuális tartalmú beszélgetés folytatása. Sokszor csak akkor észleli valaki, hogy „grooming” áldozata lett, amikor ezek a dolgok szóba kerülnek, vagy már meg is történtek vele.⁸⁷

Egy tizenhárom éves kanadai kislány 2009-ben video chaten összeismerkedett egy idősebb férfivel, aki számtalan bók és dicséret után rávette, hogy mutassa meg a melleit. A férfi erre elkezdte zsarolni a lányt: ha nem mutat többet magából, a topless fotót elküldi mindenkinek. 2010-ben a rendőrség is nyomozást indított, mert a kép tömegekhez jutott el. Három év viszontagság és folyamatos netes zaklatás után végül is a kislány öngyilkosságba menekült.⁸⁸

86 Baracsi Katalin: Internetbiztonság Magyarországon és az Európai Unióban in.: Polgári Szemle 7. évf. 5-6. sz, 2012. febr. http://polgariszemle.hu/app/interface.php?view=v_article&ID=478, 2013-03-08

87 www.kek-vonal.hu/index.php/hu/internetes-biztonsag/212-mi-az-a-grooming (2015. 01.27.)

88 http://hvg.hu/plazs/20160126_Otven_lajkert_folteszek_magamrol_egy_fel (2016.02.23.)

G. „Égetés” (flaming)

A „flaming” az internetes fórumokon keresztül megvalósuló online zaklatás egy módja, tulajdonképpen egy online „háború”, támadás, dühös, trágár hozzászólások folyamata nyilvános fórumokon (gyakran online politikai, vallási, ideológiai vita).⁸⁹ Szándékosan sértő és ellenséges, a témához nem kapcsolódó hozzászólásokat küldenek szét nyilvános fórumokon, közösségi oldalakon, személyes blogokban, chat szobákban, e-mail levelező-rendszereken vagy videó megosztó oldalakon (például a YouTube). Az elkövetők – „flame-erek” – sokszor a dühükre, szomorúságukra, megalázottságukra, önbizalomhiányukra válaszul közölnek másokról „lejárató” tartalmakat. Míg egyesek célirányosan, konkrét témákban osztanak meg megalázó tartalmakat vagy más emberek faji, nemi, vallási hovatartozását, vagy éppen szexuális beállítottságát, gazdasági helyzetét veszik célkeresztbe, addig mások valós indok nélkül, pusztán szórakozásból járatták le az internetezőket.

Számos zaklató kifejezetten a sebezhetőnek tűnő internetfelhasználókra vadászik, akikről szívesen szereznek meg és használnak fel személyes információkat.

Ha valakiről lejárató, ciki tartalmat közölnek, a legrosszabb, amit tehet, ha reagál rájuk, főleg, ha abból kitűnik, hogy dühös, mérges és kiábrándult, hiszen pont ez a cél. Ha valaki a „flamerek” áldozatául esik, jelentheti a zaklatást az oldal üzemeltetőjének, aki törli a sérelmezett tartalmat, vagy letiltja az oldalról a zaklató felhasználót.⁹⁰

H. Online (szerep)játékok gyermekeknek

A szakirodalom csak a szerencsejáték szenvedélyt értékeli önálló szenvedélybetegségként, a számítógépes és online játékokhoz kötődő függő viszony még nem szerepel külön diagnosztikai kategóriaként, habár számos pszichológiai kutatás témáját adja a mai napig. Egy amerikai kutatás szerint a „komoly” online játékosok hetente átlagosan 23 órát töltenek el egy adott játékkörnyezetben és ezen felhasználók egynegyedének legjobb és legrosszabb heti élményei is a játékhoz kapcsolódnak.⁹¹ A játékküggőseget elsősorban tünetként értékelik a szakemberek: ha valóban súlyos következményekkel jár, nem kontrollálható, és nem egyszerűen a gyermekkorban természetes és egészséges játéktevékenység megnyilvánulása,

89 <http://www.kek-vonal.hu/index.php/hu/szolgaltatasok/internetbiztonsag/395-internetes-zaklatas> 2015. január 27.

90 <http://nobullying.com/what-is-flaming/> 2015. január 27. <http://www.wisegeek.com/what-is-flaming.htm> 2015. január 27.

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

akkor utalhat bizonyos magatartászavarokra, egyéb pszichés problémákra.⁹²

Magyarországon a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény (Sztjt.) 1. § (6) bekezdés értelmében online szerencsejátékokban főszabály szerint 18 éven aluli személyek nem vehetnek részt, ami alól csak a nem folyamatosan szervezett sorsolásos játékok (tombola) képez kivételt. A többi online játék, amely nem minősül szerencsejátéknak, azonban szabadon hozzáférhető bárki számára.

Játszani természetesen jó és az online játékoknál a gyermekek sok mindent megtanulhatnak, gyakorolhatnak, ami fejlődésük szempontjából fontos lehet. Történelmi, gazdasági, biológiai ismereteik biztosan fejlődnek, ha különféle specifikus szerepjátékokban vesznek részt, de van néhány buktató, amire nem árt odafigyelni. Először is nem szabad elfelejteni, hogy a játékok gyártóinak és a játékdalok üzemeltetőinek legfontosabb érdeke a profitszerzés, ezt pedig (legálisan) úgy érhetik el, ha minél drágább játékokat tudnak értékesíteni, az egyszeri kiadások mellett további vásárlásokra készítetik a felhasználót és minél hosszabb ideig „tartják meg” a játékost. Csak Németországban 2011-ben kb. 2 milliárd eurót költöttek számítógépes játékszoftverekre a felhasználók, akiknek jelentős hányada fiatalkorú. Egyre több, alapvetően ingyenes játéknál a „kiegészítők” vásárlása nélkül a játék megakad, vagy nem okoz olyan nagy örömet egy idő után.

Szintén német adatok szerint 2011-ben csak a virtuális kiegészítőkre, tárgyakra 233 millió eurót költöttek a fogyasztók, 100 millió euróval többet, mint előző évben⁹³. A kiegészítők vásárlása általában igen könnyen megoldható: egy emelt díjas telefonhívással vagy sms-küldéssel, illetve egyszerű bankkártyás fizetéssel (gyakran szülői telefont, illetve kártyát használva), és mivel a nyomás alatt álló gyermek egyre többször vásárol, sokszor csak a hó végi elszámolásnál derül ki a több száz eurós kiadás. Még ha meg is ígéri a weblap üzemeltetője, hogy a kiegészítők vásárlását havi szinten csupán meghatározott (egy-két) esetre korlátozza, ezen ígéretek alól gyakran találni kiskapukat.

A játékok kitalálói és üzemeltetői hajlamosak arra hivatkozni, hogy a gyermek a fejlesztő által, jellemzően egyoldalúan megszabott végfelhasználói szerződési feltételeket és a játékszabályokat megismerte és elfogadta. A komolyabb online játékokra csak bizonyos kor felett regisztrálhatnak a játékosok. A rendszer azonban – a közvetlen ellenőrzés hiánya miatt – könnyen kijátszható a gyermekek által. Nem egy olyan eset ismert, amikor a szülő jelszavának használatával történik valamilyen tranzakció. Például Nagy-Britanniában egy ötéves fiú egy ingyenes játék feltelepítéséhez kérte el édesapja jelszavát, azonban a kiegészítőért már fizetni kellett és a nem megfelelő beállításoknak köszönhetően a szülőknek komoly anyagi

92 Vida Andrea: Az információs és kommunikációs kultúra hatása a tizenéves korosztályra in.: <http://xenon.bibl.u-szeged.hu/~vidaa/holi/03/szenvbet/vidaa.pdf>, 2013. 03.

93 In der Kostenfalle – Kinderspiele im internet, Sendung vom 11.Dezember 2012, <http://www.zdf.de/ZDFmediat-hek/beitrag/video/1794584/#/beitrag/video/1794584/Kostenfalle-Kinderspiele-im-Internet>, 2013-03-08

kiadásai keletkeztek.⁹⁴

A számítógép, konzol, vagy okostelefon segítségével igénybe vehető online játékok sok esetben több játékos bevonásával játszhatók (ún. multi-player játékok), ekkor viszont már nem csak saját, hanem mások személyes adatai is tudomásunkra juthatnak. A szerepjátékosok először is létrehoznak egy személyre szabható virtuális karaktert, más néven *avatárt*, amely online megtestesítőjük lesz. A játékos a háromdimenziós – legtöbbször „emberszabású” – avatárt irányítva vesz részt a virtuális valóságot szimuláló játékvilágban. A játékosok viszonya sokszor olyan szoros saját digitális képmásukkal, hogy az avatár egy adott felhasználó személyes adatának tekinthető: a virtuális viselkedés, a felvett név vagy más személyes tulajdonságok alapján egyértelműen azonosítható az avatár mögött álló ember.

A rendszeresen játszó felhasználók hajlamosok arra, hogy párhuzamosan több online univerzumban is jelen legyenek, a játéktípusuk és az általuk kreált karakterek azonban nagyon hasonlíthatnak egymásra.

A játékba való belépés előtt fontos ezért megismerni az adatvédelmi nyilatkozatban foglalt információkat a program feltelepítésére vonatkozóan, hiszen az adatvédelmi irányelvekben rögzítik, hogy ki milyen adatainkhoz fér hozzá, milyen célból kezeli, esetleg mely harmadik félnek továbbíthatja azokat.

A számítógépes játékok sokféleképpen csoportosíthatók:⁹⁵

- megjelenítésük szerint szöveges (például *visual novel*), grafikus vagy vegyes;
- műfajuk alapján akció, kaland, stratégiai, szimulációs, szerepjátékok.

A magyar gyermekek körében a legnépszerűbb játékszoftver egy internetes szerepjáték, amely az úgynevezett MMORPG (*Massively Multiplayer Online Role-Playing Game*, vagyis *nagyszámú játékos egyidejű részvételével interneten keresztül játszható szerepjáték*) körébe sorolható.

Az online játékok regisztrációja során felhasználónevet, e-mail címet és születési dátumot kell megadni. A felhasználóhoz földrajzi értelemben legközelebb eső szervert legtöbbször a használt internetkapcsolat IP címe alapján automatikusan állítja be a szoftver. Az olyan joghatóság alá tartozó területeken, ahol a törvény életkor minimumot rögzít, általában megerősítést kérnek arra vonatkozóan, hogy a játékos nagykorú-e.

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

95 BALKU ANETT: VIRTUÁLIS KLÁNOK – CSOPORTKÉPZŐDÉS EGY INTERNETES SZEREJÁTÉKBAN (szakdolgozat), 3.1.-3.2. pont. Forrás: http://campuslet.unideb.hu/dokumentumok/tanulmányok1/Csoportkepzo_tenyezok/Virtualis_es_valosagos_csoportok_internetes_szerepjatekokrol/Balku_Anett_Virtualis_klanok_Csoportkepzoes_egy_internetes_szerepjatekban_SzakdolgozatMA.pdf, – 2013. 03. 25.

Néhány szolgáltatást ingyen igénybe vehetünk, míg másokért fizetni kell. Amennyiben internetes fizetés esetén használjuk a hitelkártyát, akkor jó, ha az erről készült jelentéseket rendszeresen ellenőrizzük. Azonnal fel kell venni a kapcsolatot a játék üzemeltetőjével, ha bizonytalan ügylet történt.

Meghatározhatjuk adatvédelmi beállításainkat, melynek mértéke a játékelülettől, a játékfejlesztő társaságtól és a játék jellegétől függ. A kifinomultabb játékoknál általában lehetőségünk van korlátozni beállításainkat, így ennek megfelelően az üzemeltető kivételével senki sem láthatja profilunk vagy személyes információink részleteit. A biztonság ezen szintje azonban nem igazán mozdítja elő a multi-player játékot vagy az online élmények közösségi aspektusait, sok játékos ezért kevésbé korlátozza a beállításait és így engedik, hogy mások láthassák a profiljukat. A létrehozott azonosítót azzal védhetjük meg, ha használjuk az alábbi eszközöket:

- erős, mások által nem könnyen kitalálható jelszót;
- HTTPS (Hypertext Transfer Protocol Secure), a webes alkalmazás olyan beállítását, mely kódolja a személyes információt és a játék közbeni kommunikációt (ahol ez a beállítási lehetőség biztosított);
- korlátozó adatvédelmi beállításokat, és
- minimális érzékeny természetű információt adunk ki (például el kell kerülni a lakcím, iskolával vagy a munkahellyel kapcsolatos részleteket);
- amennyiben a szolgáltatások jogi nyilatkozatai megengedik, úgy álnévvel vagy nick névvel is létre lehet hozni profilt, melyeket az üzemeltetők a közösségi oldalakkal abból a célból kapcsolják össze, hogy a játékosok értesíteni tudják online barátikat arról, ha egy játék elkezdődik. Ez esetben viszont ajánlott megismernünk a közösségi oldal adatvédelmi és jogi nyilatkozatát is

Az adatvédelmi irányelv és a jogi nyilatkozat az online játékra történő regisztráció folyamán, vagy épp egy program telepítését megelőzően, a személyes beállítások megadásakor képernyőn való ismertetés vagy egy hivatkozás formájában érhető el. Így láthatjuk, hogy kik és milyen információkat gyűjtenek össze rólunk, azok hová kerülnek, hogyan használják fel az adatokat, hová fordulhatunk probléma vagy kérdés esetén. Az üzemeltető társaságok kifejezetten széles körben osztják meg személyes adatainkat harmadik személyekkel különböző okokból (jogi kötelezettség, különböző jogellenes tevékenységek megfigyelése, szolgáltatási problémamegoldás, játékfejlesztés, fizetési mechanizmus biztosítása, lehetőség a játékosok közötti kommunikációra, valamint promóciós anyagok küldése). Személyes adatainkhoz így a szerződés hatálya alatt álló egyéni programozók, pénzügyi intézmények, online hosting vagy disztribúciós szolgáltatások, a technikai és játéktámogatást érintő ügy-

félsszolgálat, internetszolgáltatók, kutatók, hirdető, piackutatók, végrehajtók és egyéb más állami szervek is hozzájuthatnak. A játékosoknak ugyanakkor meg kell győződnie arról, hogy a cég vagy a játék fejlesztője szabályozta-e a felelősségre vonással kapcsolatos speciális feltételeket, továbbá a szolgáltatást érintő megállapodásokban rendelkezett-e az adatbiztonságot érintő szabályokról, melyek a személyes információk nyilvánosságra kerülése esetén létfontosságúak.⁹⁶

Kicsit meglepőnek tűnhet elsőre, de egyes, rendkívül részletes virtuális valóság szimulációként működő online játékokban (tipikusan ilyenek az MMORPG-k) egyes játékosok is hajlamossá válhatnak arra, hogy zaklassák, kizsákmányolják egymást, vagy akár közvetlen anyagi kárral járó tevékenységeket fejtsenek ki a másik sérelmére. Ezt a jelenséget a jogi szakirodalom a „*virtual crime*” (*virtuális bűnözés*) kifejezéssel illeti, melybe személy elleni és az egyes játékosok online vagyonát károsító cselekmények is beletartoznak.

A virtuális közösségekben a vagyont károsító bűncselekményeket olyan dolgok ellen követik el, amik értékkel bírhatnak egy játékos közösség szemében. Ez pedig nem más, mint a virtuális vagyon, ami nem azonos a vagyonról alkotott klasszikus, a polgári jog által is definiált fogalommal. Az online szerepjátékok virtuális piacokat szimulálnak, amelyek tényleges hatással rendelkezhetnek a való világbeli gazdaságra is.⁹⁷ A virtuális vagyontárgyakkal történt visszaéléseket – főleg olyan távol-keleti országokban, mint Kína, Japán és Dél-Korea – sűrűn dokumentálja a média. Klasszikus példa erre az az eset, amikor egy japán férfi visszaélve játéktársának bizalmával, annak belépési jelszavát felhasználva belépett az eredeti tulajdonos avatárjával az általuk játszott szerepjátékba, majd 50.000 japán yenért eladta a karakter tulajdonában lévő házat és az abban található minden ingóságot egy harmadik játékosnak az eBay-en.⁹⁸ Ebben az esetben bűncselekmény tényállása valóban megvalósulni látszik, hiszen az avatárt, és rajta keresztül annak tulajdonosát „meglopták”, majd annak virtuális vagyontárgyait valódi pénzért értékesítették.

A fenti esettel kapcsolatban érdemes kiemelni, hogy ha a virtuális valóságot szimuláló szoftverhez (online játékhoz) mellékelte, a felhasználó által elfogadott szerződési feltételek szerint az egyes virtuális tárgyakkal lehet a virtuális piacon kívül is kereskedni, akkor a tárgyak feletti használati jogosultság vagyoni értékű jognak minősül. Az ilyen tárgyak feletti használati jog jogtalan elvonása vagyon elleni bűncselekmény gyanúját kelti, mivel a jog megszűnése pénzben kifejezhető kárt, vagy vagyoni hátrányt keletkeztet a sértetti oldalon.⁹⁹

96 Forrás: http://www.priv.gc.ca/information/pub/gd_gc_201211_e.asp, (2013.04.15.)

97 Edward Castronova: On Virtual Economies. *Gamestudies.org*, 2003. december. <http://www.gamestudies.org/0302/castronova/>

98 Slasdot.org: Japanese Man Arrested for Virtual Theft. (2003. 02. 14). <http://www.slasdot.org/articles/03/02/14/0523248.shtml?tid=127>

99 Eszteri Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén a gazdaság és a tulajdon helyzetének magán- és bűn-

Ettől eltérő megítélés alá esik, ha a virtuális javak tulajdonosa saját maga egyezik bele abba, hogy tárgyait elpusztítsák, vagy tudatosan kerül olyan szituációba – akár a játékon belül –, ahol fennáll annak lehetősége, hogy megrongálódjanak értékei. Jó példa erre egy 2014 elején, milliós felhasználói bázissal bíró sci-fi szerepjátékban lejártszódott úrháború, aminek következményeképpen az abban résztvevők virtuális vagyonában egyes becslések szerint 70-114 millió USD közé tehető kár keletkezett.¹⁰⁰ Ebben az esetben az önkéntes veszélyvállalásba való sértetti beleegyezés kizárja azonban elkövetők büntetőjogi értelemben vett büntethetőségét.

A büntetőjogi világ is értékelhető magatartásoktól a szakirodalom megkülönbözteti az ún. „*griefing*” jelenségét. Ilyen magatartások közé sorolhatjuk mondjuk más, gyengébb játékos által irányított avatár folyamatos, feléledés utáni megölését (*corpse camping*), továbbá csapattársak indokolatlan hátbatámadását (*friendly fire*), szörnyek mások előli öncélú leölését és így fejlődésük hátráltatását (*kill stealing*), a játék közös chat ablakában értelmetlen mondatok gyors egymás utáni ismételtetését (*flooding*), más játékos útjának szándékos elállítását és hasonlókat. Közös a fenti cselekményekben, hogy azok célja a többi felhasználó idegesítése, ezáltal a játékelmény csökkentése. A legtöbb virtuális közösség üzemeltetői szigorúan lépnek fel a grieferek ellen, mivel azok közvetlenül a felhasználókat zavarják, és így akár a szoftver piaci szereplését is negatívan befolyásolhatják. A többi játékost zavaró avatárak tulajdonosai általában elsősre figyelmeztetésben részesülnek, majd újabb visszaélések esetén részleges vagy örökös kitiltásra is kerülhetnek a közösségből.¹⁰¹

Minden egyes online szerepjátékhoz csatolt dokumentációban található olyan rész, amely a játékosok közötti, illetve a játékos és a programozott környezet közötti kapcsolatokat szabályozza. Ezekben a dokumentumokban, illetve szerződésekben kerülnek kikötésre azok a szabályok, amelyek általánosan szabályozzák egy online közösség tagjaival szemben támasztott elvárható normákat. Ilyen például a csaló-programok és hackek használatának, vagy más játékosok zaklatásának tiltása. A rend fenntartásáért az adminisztrátorok felelnek. Ez a szabályozási módszer legtöbbször elég arra, hogy rendeződjene a virtuális világokban felmerülő feszültségek. A közösségek önszabályozó mechanizmusai mellett, az egyes csatornák, weboldalak, vagy szoftverek adminisztrátorai gyorsan fel tudnak lépni a visszaéléseket elkövetők ellen, ami legtöbbször a legobjektívabb és legcélszerűbb megoldás. Ha azonban a devianciák túlmútnak ezeken a kereteken, határozott külső, hatósági fellépésre is szükség lehet.

tetőjogi elemzése a virtuális közösségekben. Doktori értekezés, PTE Állam- és Jogtudományi Kar. <http://ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-vedes-ertekezes.pdf> (2016.02.02.)

100 HVG.hu: A neten kívül is hatalmas károkat okozott 24 óra alatt egy netes háború, (2014. 01. 30.) http://hvg.hu/tudomany/20140130_hatalmas_karokat_ozokzott_egy_netes_haboru

101 Parti Katalin: Actual Policing in Virtual Reality – A cause of moral panic or ajustified need? In: Ja Jin Kim (szerk.): Virtual Reality. InTech ISBN 978-953-307-518-1

Talán meglepően hangzik, de a legjobb védelem online játékok terén a gyermeknek az lehet, ha együtt játszik valamelyik szülővel vagy akár az egész család részt vesz – természetesen ésszerű keretek között – a játékban!¹⁰²

I. Személyes adattal való egyéb visszaélések

Mindennapi életünk elválaszthatatlan részét képezi az online világ. Életünk egy jelentős részében a virtuális környezetben létezünk, ahol hatékonyan tarthatjuk a kapcsolatot szeretteinkkel, könnyedén rendelünk meg árukat és szolgáltatásokat, követjük és kommentáljuk a világ eseményeit. Az online világ az elmúlt években egyre jobban behálózta életünket, főleg az első ránézésre csábítóan olcsó vagy „*gratis*” szolgáltatásai révén. Ezek a szolgáltatások azonban valójában nem ingyenesek, személyes adatainkkal fizetünk értük és minél jutányosabb az ár, annál több személyes adatot vagyunk hajlandóak megadni. Az Európai Hálózat- és Információbiztonság Ügynökség (ENISA) tanulmánya szerint hasonló árú szolgáltatások esetében az ügyfelek nagy része az adatvédelmi szempontból biztonságosabban választja, de amint az árak különbözőek, úgy az ügyfelek harmada már az olcsóbb szolgáltatást részesíti előnyben, akkor is, ha cserébe személyes adataikat áldozzák fel.¹⁰³

A Btk. 219. § (1) bekezdéséből a „jogtalan” szó kikerült, így jelenleg vétségnek minősül már minden, az Infotv. rendelkezéseinek megsértésével haszonszerzési célból vagy jelentős érdeksérelmet okozva elkövetett jogosulatlan vagy a céltól eltérő adatkezelés, az adatok biztonságát szolgáló intézkedés elmulasztása, illetve a tájékoztatási kötelezettség megszegése.

2011 januárjában az ombudsman gyermekjogi oldalára jelentkezett be az a panaszos, aki sérelmezte, hogy gyermekkorú felhasználóknak is továbbít az egyik levelezőrendszer (Freemail) pénisznagyobbításra vonatkozó reklámot tartalmazó **kéretlen elektronikus levelet (spam)**. Szerinte nem fogadható el az a védekezés, hogy a felhasználók életkorát a regisztrálásukkor megadott adatok alapján kezelik, hiszen az ott megadott információk hitelességét nem ellenőrizték, sőt, jogi értelemben az ott megadottak nem is tekinthetők nyilatkozatnak. Ellenben a gyermekjogok tömeges megsértése, ha e reklámok szórása ilyen adatokon alapul. Hatásköri korlátai miatt az ombudsman megküldte a panaszos levelét a Magyar Tartalomipari Szövetségnek (MATISZ) és a Magyar Reklámszövetségnek is. A MATISZ elnöke válaszában vázolta, hogy 2002-2003 között az USA-ban és Európában is életbe léptek a spam kezelésére hivatott törvényi szabályozások, ennek ellenére mára a globális e-mail

¹⁰² <http://mediasmarts.ca/blog/game-tips-parents>, (2013.04.15.)

¹⁰³ Study on monetising privacy An economic model for pricing personal information <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy>

forgalom 90-95%-át a spam-ek teszik ki, vagyis a probléma hatékony megoldása továbbra is várat magára. Ebben a felhasználói érdektelenség és tudatlanság is közrejátszik, hiszen a spam-ek terjesztéséért felelős hálózatok jelentős része fertőzött személyi számítógépekből áll. Az USA-ban a spam terjesztéséért elsődlegesen felelős ún. botnet-ek felderítését és lekapcsolását, üzemeltetőik és a fertőző botnet-komponensek fejlesztőinek elfogását és elítélését tartják a leghatékonyabb megoldásnak.

Magyarországon spam-ügyben elsődlegesen a Nemzeti Média- és Hírközlési Hatóság illetékes, amelynek honlapján bejelentés tehető a „Kéretlen hirdetést bejelentő űrlap” segítségével (<https://e-nmhh.nmhh.hu/e-nhh/4/urlopok/esf00101/>). Különösen az ismeretlen személyektől vagy idegen nyelven érkező, tárgybelihez hasonló tartalmú levelekre jellemző, hogy azok tartalma megtévesztő, továbbá vagy anyagi haszonszerzés, vagy a számítógép megfertőzése motiválta a spam-küldőt (többnyire ugyancsak anyagi haszonszerzésből). A legjobb védekezés a válasz nélküli azonnali törlés, a csatolmányokat, mellékleteket pedig értelemszerűen nem szabad megnyitni, mert nagy valószínűséggel ártalmas kódot tartalmaznak (amely akár a számítógépet is tönkretetheti). Ha bárkit kéretlen e-mailen keresnek meg bármilyen állásajánlattal, nyereménnyel stb., akkor az nagy valószínűséggel szintén átverés. Vannak szolgáltatói oldalú spam-szűrők (a levelező szervereken) és kliens oldalon (a saját számítógépen) is telepíthető levélszemét szűrők; többek között a modern vírusirtó szoftverek komplex védelmi csomagjai is tartalmazznak ilyen komponenst, tehát javasolt ezek telepítése. Tudni kell azonban, hogy a szolgáltató és kliens oldali spam-szűrés nem képes az összes spam eltávolítására.

Az **adathalászat**on (**phishing**) kívül a megszerzett információ sok mindenre felhasználható a zaklatástól a rágalmazásig és becsületsértésig, a zsarolástól, a személyiség lopásig, kihasználva, hogy nehezen ellenőrizhető, hogy ki is van egy profil mögött, azaz ki is az igazi elkövető, illetve, hogy a szolgáltatók többsége ösztönzi a felhasználókat minél több adat megadására a „használhatóság” növelése érdekében, ugyanakkor elmulasztja felhívni a figyelmet az ezzel járó veszélyekre. Mindezt tetézi, hogy a megvalósult ilyen jellegű cselekményekkel szemben egyrészt a szolgáltatók tehetetlenek, másrészt felelősségüket előzetesen kizárják.

A legtöbb szolgáltató lehetővé teszi, hogy a felhasználók különböző külső oldalakkal, programokkal, alkalmazásokkal is összekapcsolják a profiljukat (XSS, cross site scripting), ugyanakkor ezek a külső programok könnyen lehetnek ártalmas programokkal is fertőzöttek (vírus, féreg, trójai). A veszélyt az jelenti, hogy a közösségi oldalak többsége gyengén védett az ilyen fenyegetések ellen, mert a programot szolgáltató harmadik felet nem, vagy nem megfelelő mértékben ellenőrzik, illetve van módjuk ellenőrizni. Ráadásul a közösségi oldalakon keresztül a kapcsolati hálók miatt ezen kártékony programok gyorsabban és nagyobb károkat okozva is terjednek.

Ezen veszélyek következményei pedig gyakorlatilag beláthatatlanok, a profil kompromittálásától egészen az adathalászat miatti veszteségekig terjedhetnek.

Végül manapság szintén nagy népszerűségnek örvendenek az aukciós oldalak, melyek használata során adatvédelmi vonatkozásban is felmerül néhány kérdés. Egy népszerű magyar aukciós oldal üzemeltetője NAIH-nak küldött tájékoztatása szerint kiskorúak sérelmére vagy közreműködésükkel elkövetett visszaélésekről csak akkor szereznek tudomást, ha konkrét ügygel kapcsolatban az ügyfélszolgálatot megkeresik vagy rendőrségi nyomozást rendeltek el. Az első pont tekintetében tipikus eset, amikor *„egy felhasználó licitálást kér, mert állítása szerint gyermeke licitált (fix áras értékesítés esetén adott vételi ajánlatot), vagy gyermeke töltött fel termékeket. Ilyenkor a felhasználók tájékoztatást kérnek, hogy mit tehetnek, hogyan vonhatják vissza az online térben tett nyilatkozataikat.”* Az aukciós oldalak felhasználási feltételei azonban kifejezetten rögzítik, hogy 18 év feletti felhasználók számára nyitott a piactér, ám ezt az üzemeltetőnek nem áll módjában ellenőrizni. Ennek következményeként a szülők IT tudatosságát szükséges fejleszteni, hiszen felhasználói azonosítójukat védelem nélküli tárolás esetén tudják csak a 18 éven aluli személyek használni. Ezen megkeresések száma ritka: a napi 150-200 esetből évente körülbelül 10 a kérdést érintő jelzések száma. A második esetkört illetően már ténylegesen visszaélés történik, mely jellemző példája, mikor eladóként regisztrált felhasználó – néha nem létező – termékeket tölt fel, de nem ad el és a pénzt egy bankszámlán gyűjti. Az ilyen csalások vonatkozásában jogerős bírósági ítéletek is születtek már. A visszaélést elkövető személyek koráról a gazdasági társaság nem rendelkezik információval, továbbá azzal kapcsolatosan sem bír tudomással, hogy kiskorú személy (aki elvileg nem is lehetne az aukciós oldalak felhasználója) visszaélés áldozata lett volna. *„Olyan eset már előfordult, hogy a visszaélést elkövető személy kiskorú gyermekét nevezte meg, mint aki szórakozásból termékeket töltött fel – ebben az esetben a felhasználó nyilatkozatát „árnyalja” az a tény, hogy a bankszámlaszám, amire a termékek árát előre várta a felhasználó, az az apa kezelése alatt volt; tehát ebben az esetben a kiskorú is inkább áldozatnak tekinthető.”*

Az aukciós csalások elleni védekezésnél ügyelnünk kell arra, hogy túl kevés értékeléssel rendelkező eladótól ne vásároljunk, legyünk tisztába az értékelések tartalmával, ne vegyünk meg egyetlen terméket sem olyan felhasználótól, akik túl alacsony áron adnak el egy terméket, nem valódi lakcímmel vagy telefonszámmal regisztráltak, illetőleg az árut – különösen, amennyiben annak nagyobb az értéke – személyesen vegyük át.¹⁰⁴

104 http://www.penzcentrum.hu/vasarlas/tizezreket_bukhatnak_a_gyanutlan_vasarlok_tamadnak_az_atveros_netes_boltok.1035976.html, 2013-05-15

A. Portugália, Dadus Projekt

2008-ban a portugál adatvédelmi hatóság célul tűzte ki, hogy az adatvédelmet be kell építeni az iskolák tantervébe. A hosszú távú strukturális program első lépcsője az oktatási minisztérium támogatásával készült, a 10-15 éves korosztálynak szóló Dadus Project. Dadus egy fiatal srác, aki éli egy kiskamasz hétköznapjait és közben adatvédelmi szempontból értékelhető események történnek vele. A projekt tematikus egységekre van osztva és minden egység tartalmaz egy összegzést, a tanárok számára a témák mélyebb, a diákok számára pedig Dadus nyelvén – vagyis hétköznapi, „gyerekenyven” – megvalósuló összegzésben. A weboldalon (<http://dodus.cnpd.pt>) a tanárok a projekttel kapcsolatos anyagokat, összefoglalókat tölthetnek le, a diákok híreket, jogszabályokat ismerhetnek meg, a szülők pedig praktikus tanácsokat olvashatnak, valamint egy fórum segítségével megoszthatják egymással tapasztalataikat, véleményeiket. A Dadus Blog-on a diákok közvetlenül megbeszélhetik a Dadus által felvett témákat, közzétehetnek iskolai tanulmányokat. Az oldal – szórakoztatva tanítva – számos interaktív játékot, illusztrációt, valamint különböző tippeket és vicces anyagokat tartalmaz. A Dadus Project-et szimbolikusan 2008. január 28-án, az európai adatvédelmi napon indították el, de ezt megelőzően is regionális értekezleteket szerveztek országszerte. A Dadus Project pozitív hatására Portugáliában észrevehetően jobban törődnek az emberek – a szülők és tanárok – a gyermekeket érő internetes veszélyekkel. Korábban a szülők úgy gondolták, hogy nem képesek megbirkózni ezzel a problémával, főleg az infokommunikációs tudás hiánya miatt; a tanárok pedig napi szinten találkoztak az iskolában megoldásra váró esetekkel. A fő cél a gyermekek körében a tudatosság növelése, azáltal, hogy felelős döntéshozásra tanítják őket az alapvető jogaik, így a személyiség- és adatvédelem területén is önálló döntésekre képes embereket nevelnek.



B. Írország, „Private I, Public Eye” videóklip-verseny

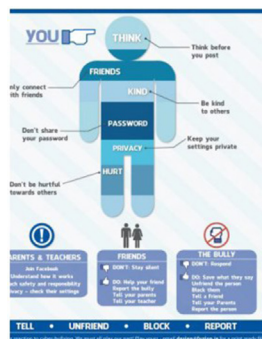
Az elmúlt években az ír adatvédelmi hatóság élénken foglalkozott a fiatalok online adatvédelmének kérdéseivel.¹⁰³ Két privacy tárgyú videóklip-versenyt is hirdetett diákoknak (www.youtube.com/dataprotection) valamint összeállított egy 92 oldalas, füzet formátumú színes oktatási segédanyagot iskolai felhasználásra.

Az ír gyermekjogi ombudsman 300, különböző szociokulturális háttérű általános iskolai tanulóval konzultált országszerte az online bullying kérdéséről. A gyerekek tapasztalatait összegző jelentésében felhívta a figyelmet, hogy az iskoláknak jóval nagyobb hangsúlyt kell az internetes zaklatás megelőzésére fordítani; a gyerekeknek meg kell tanítani, hogy felelősek az online szavaikért és a tetteikért is és szavaiknak, tetteiknek súlyos következményei lehetnek; valamint meg kell ismertetni a gyermekekkel, hogy kihez és hova fordulhatnak segítségért (<http://www.oco.ie/assets/files/OCO-Bullying-Report-2012.pdf>).



Szintén az ír gyermekjogi ombudsmanhoz kötődik a „Maradj biztonságban!” elnevezésű program, amely általános iskolások, szülei és a pedagógusok részére kíván alapos tájékoztatást nyújtani elsősorban a bántalmazás jelenségéről, megelőzéséről, köztük az internetes zaklatás elleni védekezésről is. A program folytatása a „Cool school” projekt, amely már a felsősöknek szól.

Egy ír kommunikációs cég, a Fuzion Communications képes formában ad tanácsot gyerekeknek a hálózati közösségek oldalaihoz (<http://www.thejournal.ie/safebook-how-to-stay-safe-online-657753-Nov2012/>).



C. Skócia, „Tisztelj engem!” Program

A Trinity College Anty Bullying Centre – <http://abc.tcd.ie/> „Tisztelj” – „Respect me” program (Skócia) <http://www.respectme.org.uk/> – mögé a skót gyermekjogi ombudsman is odaállt. A skót kormányzat által, a SAMH (Scottish Association for Mental Health), és az LGBT Youth Scotland támogatásával 2007-ben életre hívott program célja a (többek között az interneten történő) zaklatás megállítása, a megfelelő prevenciós programok kidolgozása, melynek érdekében ingyenes tréningeket is szerveznek országsszerte helyi szinteken. A projekt része a jogtudatosító, tájékoztató kampányok folytatása fiatalok számára.

<http://www.respectme.org.uk/What-do-I-do-if-a-child-tells-me-they-are-being-cyberbullied.html>

D. Norvégia, „Te döntesz!” Kampány

A norvég adatvédelmi hatóság, másokkal együttműködve “You decide” (Te döntesz!) címmel egy tudatosító kampányt indított az online környezet veszélyeiről, írásos és videó szemléltető anyagokkal mutatják be a fiatalok számára, milyen kihívások várják őket az online világban. A kezdeményezéshez bármely ország csatlakozhat. Alapvetően két korcsoportot céloznak meg: általános iskolásokat és középiskolásokat, a két anyag tematikájában és képi megjelenésében jelentősen eltérő, bár mindkét írásos szemléltető dokumentum leginkább egy tankönyvre hasonlít, sűrű, de jól tagolt információkkal. A szemléltető brosrák tanórai feldolgozásra készültek.

Az általános iskolások számára készített anyagban inkább rajzok szerepelnek, emellett a fiatalabb korosztály számára könnyebben feldolgozható feladatok találhatók. A tananyagban még fellelhető egy alap szótár, valamint érdekes figyelemfelkeltő statisztikák, adatok. Az általános iskolásoknak szóló anyag által felölelt problémák: egy viccnek szánt üzenet komoly következményekkel járhat, nem tudhatod ki van a chat másik oldalán, a neten sok a hamis információ.



A középiskolásoknak szóló anyag már fényképeket használ és sokkal lényegre törebb. Ez is tartalmaz feladatokat, de szótár helyett inkább a jogi fogalmakat próbálja közelebb hozni elmagyarázni (főbb gondolatok: mindenkinek joga van ahhoz, hogy magánszféráját tiszteltetben tartsák; az internet sosem lesz teljesen anonim; ne osszunk meg privát tartalmat viccből; hogyan osszunk meg privát tartalmat; mit tegyünk a cyberbullying ellen; ki mit tudhat rólad a netről; ki figyel a neten).

E. Lengyelország: Your Data – Your Concern Program

2009-ben a diákok és tanárok részére készített oktatási segédletet a lengyel adatvédelmi hatóság (GIODO) a gliwici Oktatási Centrummal közösen az oktatási minisztérium és Gyermekjogi Ombudsman fővédnöksége alatt. Fő cél, hogy a személyes adatok védelméhez kapcsolódó fő kérdéseket és a magánszférához való jogot beemeljék a pedagógus képzésbe és az általános- és középiskolák alaptantervébe Lengyelországban. A Your Data – Your Concern! (a Te adatod – a Te felelősséged)¹⁰⁵ program képzést is magában foglal, továbbá tanárok részére elérhető oktatási anyagokat, modell órákat, prezentációkat kínál, és arra ösztönzi a pedagógusokat, hogy legyenek tájékozottak a 7-16 év közötti diákok privacy problémáival kapcsolatban.

F. Franciaország, „More Rights For Your Personal Data”

A francia adatvédelmi hatóság honlapjának elkülönült részén „More rights for your personal data” (Több védelmet a személyes adatoknak)¹⁰⁶ címmel megtalálható egy tiniknek szóló magazin interaktív változata, illetve speciális témákat dolgoznak fel (például a helymeghatározásról, a személyes adatok online védelméről) további módszertani ismeretek és oktatási segédletek mellett.



¹⁰⁵ http://www.giodo.gov.pl/324/id_art/763/j/en/ (letöltve 2016. március 17.)

¹⁰⁶ <https://www.cnil.fr/en/more-rights-your-personal-data> (letöltve 2016. március 17.)

G. Spanyolország, „Pandi Projekt”¹⁰⁷



A spanyol adatvédelmi hatóság (AEPD) a honlapján a fiatalok (és érdeklődő szüleik) részére létrehozott egy „Pandi” elnevezésű kampányra épített weblapot, amely egy baráti kör történetét követi képregény formájában. A képregény megmutatja a gyerekeket az adatvéde-

lem fontosságára és a kritikus gondolkodásra. A weboldal hat oktatási anyagot tartalmaz alapvető ismeretekkel és helyzetgyakorlatokkal a személyes adatok és magánszféra; jogok és kötelezettségek és a legfőbb online veszélyek; digitális személyiség és online hírnév, közösségi hálók; képek a web 2.0-án: e-mail, chat, és üzenet küldés; hirdetés, vásárlás és online szórakozás; személyiség lopás, online megfélemlítés és sexting (erotikus tartalmú üzenetek küldése) témákban.

H. Új-Zéland, gyermekjogi projekt

2009-ben az új-zélandi adatvédelmi biztos olyan projekt kidolgozását tűzte ki célul, amely segítségével megtudhatják, hogy mennyire tájékozottak az új-zélandi fiatalok a magánélet vonatkozásában. A projektet egy 15 fős középiskolás tanulókból álló fókuszcsoporthal indították el. A diákok megvitatták, hogy a magánélet védelmének mely aspektusai okozzák számukra a legnagyobb aggodalmat, és hogy milyen tanácsokkal lehet segíteni a fiatal korosztályt, hogy tájékozottabbak legyenek az általuk kiszolgáltatott adataik sorsával kapcsolatban. A tudatosság növelése, valamint az információk megfelelő használata érdekében alakították ki egy koncepciót, ami a „fiatalok magánéleti csomagja” elnevezést kapta (www.privacy.org.nz/youth) és az alábbi elemekből áll:

- iránymutatások, ötletek előadók számára az adatvédelemmel kapcsolatos sikeres előadások megtartásához,
- magánélettel kapcsolatos történetek vitapontokkal, a történeteket eljátszhatják, majd utána megbeszélhetik azokat a főbb vitapontok mentén,

¹⁰⁷ <http://www.tudecideseninternet.es/menores-v2/?q=node/176> (letöltve 2016. március 17.)

- rövidfilm, ami arra készíti a fiatalokat, hogy gondolkozzanak el, mi minden történhet személyes adataikkal, a magukról kiadott információkkal,
- feladatok,
- kvíz, adatvédelemmel kapcsolatos igaz-hamis; vagy feleletválasztós kérdések,
- mini prospektusok,
- plakátok,
- valamint egy úgynevezett „felavató előadás”.

Minden egyes rész célja a fiatalok aktivizálása: gondolkodjanak el, játsszák el, éljék át a különféle helyzeteket, majd beszéljék meg mit kellett volna tenni, hogyan lehetett volna elkerülni a személyes adataikkal való visszaélést. Adjanak tanácsot egymásnak, és mondják el pozitív és építő jellegű negatív véleményeiket is egyaránt a különféle esetekkel kapcsolatban.

I. Kanada, képregény és tippek

A kanadai információs biztos valamennyi érdekelt félnek készített színes, lényegre törő ajánlásokat arról, miként lehet online környezetben megvédeni magánszféránkat. A fiataloknak szóló képregény – melynek magyar fiataloknak szóló verziója a Függelékben megtalálható! – a testvérpár történeteinek keresztül azt szemlélteti, milyen sok személyes adatot osztunk meg akaratlanul vagy észrevétlenül magunkról az interneten és keveredünk emiatt kellemetlen helyzetekbe. A szülőknek szóló 12 hasznos adatvédelmi tipp:

- *Tudd, milyen internetes szolgáltatásokat használnak gyermekeid.*
- *Próbáld ki a gyermekeid által használt internetes szolgáltatásokat.*
- *Tarts lépést a fejlődéssel.*
- *Tedd az adatvédelmi beállítások helyes beállítását vonzóvá.*
- *Tedd a jelszó védelmet prioritássá.*
- *Emeld ki a mobil eszközök védelmének fontosságát.*
- *Tudatosítsd gyermekeidben, hogy az interneten közzétett dolgokat mások is láthatják.*
- *Tanítsd meg gyermekeidnek, gondolják át, mielőtt bármire ráklikkelnek.*
- *Emeld ki, hogy csak a valós barátait vegyék fel ismerősnek.*
- *Tanítsd meg nekik, hogy személyes adataik nagyon értékesek.*
- *Mondd el nekik, hogy bármikor számíthatnak rád, ha önhibájukból illetékteleneknek kiszolgáltatták személyes adataikat.*
- *Mutass jó példát gyermekednek.*

Emellett a kanadai információs biztos egy iskolai tantervet is kiadott, amelyben 12 témát elemez, mindegyiket röviden bemutatva és vitaindító kérdésekkel ellátva:

- Gondolkozz, mielőtt bármire is ráklickelsz a neten!
- Oda szoktál figyelni az adatvédelmi beállításokra?
- Csak a valódi barátaidat szoktad visszajelölni?
- Válassz megfelelő jelszót!
- Véd meg online személyazonosságod és ügyelj oda személyes adataidra a neten is!
- Figyelj oda az internetes játékdalakra!
- Óvatosan viszonyulj az idegenektől kapott online üzenetekhez!
- Szülők a Facebookon
- Mobil applikációk
- Internetes randioldalak
- Sexting
- Cyberbullying

J. USA

Az Amerikai Egyesült Államokban 1998-ban a gyermekek (pontosabban a 13 év alatti kiskorúak) személyes adatainak online védelméről a tisztességtelen adatkezelések megakadályozása érdekében külön jogszabályt alkottak¹⁰⁸ (*Children's Online Privacy Act, COPPA*). A jogszabály a gyermekek felé irányuló kereskedelmi vagy online szolgáltatást nyújtó honlapok adatkezelőire többletkötelezettségeket hárít, amelyek betartását a *Federal Trade Commission* (Szövetségi Kereskedelmi Bizottság) hivatalból és panasz alapján induló eljárásaiban ellenőrzi. A törvény azokra a honlapokra vonatkozik, amelyek fenti szolgáltatásaik során kiskorúaktól gyűjtenek adatokat. Ez nem csak a kifejezetten a gyermekek felé irányuló honlapokat (pl.: egy játékbolt webshopja vagy egy rajzfilm online játékokat kínáló honlapja) jelenti, hanem az általános közönség számára kereskedelmi vagy online szolgáltatást nyújtó honlapokat is, ha a szolgáltatásokat kiskorúak is igénybe vehetik és a honlap üzemeltetőjének tudomása van arról, hogy a szolgáltatást kiskorúak igénybe is veszik. A honlapok üzemeltetői kötelesek:

- A kiskorúak adatainak kezeléséhez bizonyítható módon szülői hozzájárulást beszerezni.

¹⁰⁸ Children's Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2581–728, enacted October 21, 1998).

- A szülőnek külön felületet kell biztosítani, ahol átnézheti, töröltheti a gyermekéről kezelt személyes adatokat, illetve ahol megtilthatja a további adatkezelést, visszavonhatja az adatkezeléshez adott hozzájárulását.
- Egyszerűen szövegezett (azaz a gyermekek által is érthető, életkor semleges) és részletes tájékoztatást kell adni az adatkezelés valamennyi mozzanatáról.
- Az érintettől kért hozzájárulásként csak az aktív magatartással megadott hozzájárulás fogadható el.

A hamis születési dátummal történő regisztrációkat ki kell szűrni.

Például:

a) a születési dátum megadása közben lehetőség legyen 13 év alatti kort is beállítani, hogy a kiskorú ne kényszerüljön rögtön hamis évszám megadására, illetve a szolgáltató is tudomást szerezzen arról, hogy egy kiskorú szeretett volna regisztrálni;

b) a születési évszám megadásánál se legyenek jelzések arra nézve, hogy 13 év alattiak nem vagy csak szülői jóváhagyással regisztrálhatnak;

c) az oldal rövid ideig tiltsa le az adott IP címet, ha a felhasználó csak azért lép vissza, hogy megváltoztassa életkorát;

d) online vásárlást csak saját névre szóló hitelkártyával lehessen lebonyolítani

e) ha a megadott életkor alapján a felhasználó kiskorú, akkor a válaszüzenet ne egy pusztá elutasítás legyen, hanem tájékoztassa a gyermeket arról, hogy a honlap szolgáltatásait igénybe veheti, ha megkéri a szülőt, hogy regisztráljon [itt még arra is lehetőséget nyújt a törvény, hogy a szolgáltató megkérheti a gyermeket arra, hogy adja meg a szülő e-mail címét, amit természetesen a sikertelen vagy elutasított megkeresést követően törölnek].

- A szolgáltató munkatársainak megfelelő adatvédelmi képzéseken kell részt vennie, illetve a szolgáltatónak a belső szabályzatait a jogszabályban szereplő többletkötelezettségeknek megfelelően kell módosítania.

A jogszabály a megfelelő szülői hozzájárulás beszerzésére több lehetőséget is bemutat, amit a honlap által kínált szolgáltatások függvényében két részre bont:

1. Ha olyan szolgáltatásról van szó, amely a kiskorú adatait a nyilvánosság felé közvetíti (pl.: közösségi oldal, blog stb.), akkor

a) a szülőnek egy űrlapot kell kinyomtatnia, amelyet aláírva mailben vagy faxon meg kell küldenie a szolgáltatónak;

b) egy, a szülő nevére szóló bankkártyával egy minimális tranzakciót kell lebonyolítani;

- c) a szolgáltató által fenntartott ingyenes hívószámon az erre kiképzett ügyfélszolgálati munkatársnál azonosíthatja magát a szülő;
- d) digitális aláírással ellátott hozzájáruló e-mailt küldhet a szülő.

2. Ha olyan szolgáltatásról van szó, amely a gyermek adatait csak saját, belső használatra kezeli és nyilvánosság felé azokat nem közvetíti, akkor a fenti esetek mellett a szülő még az alábbi módon is megadhatja a hozzájárulást az adatkezeléshez:

a) a szülő egy e-mailben jelzi, hogy hozzájárul az adatkezeléshez, amelyben megjelöl egy postai vagy fax címet, ahonnan a szolgáltató megerősítő jóváhagyást tud kérni

b) a szülő egy e-mailben jelzi, hogy hozzájárul az adatkezeléshez, az email megérkezését követően egy meghatározott, de nem túl

rövid időintervallumon belül a szülő újabb mailt kap a szolgáltatótól, ahol meg kell erősíteni a regisztrációt.



A fentiekben túlmenően szigorúbb szabályokat ír elő a törvény a személyes adatok továbbítására (a vállalaton belüli továbbítást is ideértve), illetve az adatfeldolgozók igénybevételeire. A szülőt valamennyi igénybe vett adatfeldolgozóról, illetve az eredeti céllal nem szorosan összefüggő adattovábbításról tájékoztatni kell.¹⁰⁹

Az FTC 2011-ben kiskorú gyermekekkel kapcsolatos mobil applikációkról, 2012 decemberében az Apple és a Google alkalmazásboltjaiban (App Store) található alkalmazások adatkezelési gyakorlatáról tett közzé nyilvános jelentéseket¹¹⁰. Az alkalmazások felhasználói (sem a gyermekek, sem a szüleik) a kellő tájékoztatás hiányában nagyon sok esetben egyáltalán nincsenek tisztában azzal, hogy a mobilok és tabletek azonosítóját (számokból és betűkből álló egyedi azonosítók) a cégek titokban, piaci elemzőkkel, közösségi oldalakkal és reklámügynökségekkel is megosztják, melyek aztán a különböző Appokat használó gyermekekről könnyűszerrel készítenek felhasználói profilt. A vizsgált alkalmazások többsége a felhasználókkal egyáltalán nem közölte, hogy milyen adatokat gyűjt róluk annak ellenére, hogy a készülék azonosítóját az esetek több, mint felében más piaci szereplőknek is továbbították. Az alkalmazások 17 %-a pedig gyermekek számára is megengedte, hogy valódi pénzért vásároljanak virtuális termékeket 30 dollár erejéig.

¹⁰⁹ <http://www.coppa.org/comply.htm>, 2013-04-15

¹¹⁰ <http://www.ftc.gov/opa/2012/12/kidsapp.shtm>, 2013-04-22

K. Uniós programok

Az uniós programok sorában a **Safer Internet** programot¹¹¹ kell elsősorban kiemelni, melyet az Európai Unió 1999-ben indított és jelenleg 30 ország csatlakozott hozzá (Magyarország 2009-ben). 2004-től a program neve Safer Internet Plus. A program minden országban összefogja a témával foglalkozó civil szervezeteket, jogalkalmazó szerveket, amelyek a párbeszéd és összefogás alapján rendkívül hatékonyan tudnak együttműködni. A magyarországi konzorcium tagjai a Nemzetközi Gyermekmentő Szolgálat, a Kék Vonal Gyermekkrízis Alapítvány és a Nemzeti Infokommunikációs Szolgáltató Zrt.). A program célja az internet és online technológiák biztonságosabbá tétele különösen gyermekek számára és a jogellenes és/vagy káros tartalom elleni küzdés. A legfontosabb vívmányok a forródrótok (hotline) és segélyvonalak (helpline) üzemeltetése (lásd 9. fejezet!), amiken keresztül bárki bejelentést tehet vagy segítséget kérhet. A kéretlen és káros tartalmak ellen szűrőrendszerekkel, információcserével, gyermekvédelmi intézkedésekkel, szorosabb rendőrségi/bűnüldözői együttműködéssel veszik fel a harcot. A biztonságos internet napját (február 9.) világszerte kiemelt programokkal, konferenciákkal, iskolai előadásokkal ünneplik.



A „Web We Want – Internet, ahogy mi szeretnénk”¹¹² című, tizenévesek számára tizenévesek által kidolgozott kézikönyvet 2013 februárjában, a Biztonságos Internet Napján adta ki az Insafe hálózat. A kiadvány többek között a jogok és köteleességek kérdéskörét járja körül, és arra ösztönöz, hogy az olvasó gondolkodjon el a saját és kortársaik viselkedéséről. A kézikönyv párját – Kézikönyv pedagógusok számára – pedagógusok dolgozták ki tanárok számára. A nemzeti kompetencia keretrendszerekhez illeszkedő interaktív óratervekkel és feladatlapokkal segít a pedagógusoknak integrálni a fiatalok internetes tevékenységéhez kapcsolódó kérdéseket a tantervbe. Minden egyes feladatnál egy jól áttekinthető jegyzékben szerepelnek az adott feladathoz kapcsolódó témák és célok. A kézikönyvben található anyagok felhasználása lehetővé teszi a diákok számára, hogy

111 www.saferinternet.hu 2016-03-11

112 <http://www.webwewant.eu/hu/web/guest/about> (2016. 03.17.)

- jobban megértsék, milyen lehetőségeket nyújt az internet, és milyen kihívásokkal szembesülhetnek annak használata során
- olyan készségeket sajátítsanak el, melyekre jövőbeli életük és pályafutásuk során is szükségük lehet.

A kiadványok szabadon letölthetők a <https://digital-skills-jobs.europa.eu/en/latest/news/safer-internet-day-together-better-internet>



Az EU Kids Online kutatássorozat (www.eukidsonline.net) egyrészt már meglévő kutatási anyagok tanulságait összegezte, másrészt egy 2011 őszén lezáruló, 25 országra kiterjedő felméréssel maga is új adatsorokat állított össze. A kutatás két alapfogalmán, a kockázaton és az ártalmon kívül foglalkozik még az ártalomra való fogékonysággal is. A kutatás legfontosabb magyarországi megállapításai még mindig időszerűek, sajnálatos, hogy azóta nem készült ilyen átfogó vizsgálat¹¹³.

- „A magyar 9-16 éves gyerekek 37%-a találkozott már legalább eggyel, a kutatásban vizsgált öt kockázatos tevékenység közül, és átlagosan 0,74 ilyenrel van tapasztalata a fiataloknak. A legelterjedtebb kockázatos cselekvéstípus az online ismerkedés, amit a gyerekek csaknem negyede megtett már. Ezt követi a veszélyeket rejtő felhasználói tartalmak böngészése (16%). Az internettel kapcsolatos előítéletekkel ellentétben a pornográf tartalmak böngészése korántsem olyan elterjedt: minden tízedik gyereknek

¹¹³ http://hvg.hu/tudomany/20140912_ilyen_az_atlagos_magyar_gyerek_9_eves_de, (2016.02.23.)

vannak ilyen jellegű tapasztalatai. A szexuális jellegű üzenetek, cselekvések még ennél is ritkábbak, hasonlóan az online zaklatáshoz (6-6%).

- A kockázatos tevékenységekkel kapcsolatos tapasztalatok a korral egyértelműen nőnek – a fordulópont 14 és 15 éves kor között van, amikor hirtelen megnövekszik az ilyen tapasztalatokkal rendelkezők aránya. A regressziós elemzés szerint más demográfiai változók kevésbé befolyásolják ezt a kérdést, ebben a tekintetben sokkal fontosabbak az internethasználat milyenségét leíró tényezők, illetve egyes pszichológiai és offline faktorok. A gyakori és változatos internethasználat, illetve az általános kockázatkereső viselkedés növelik a kockázatos tevékenységek kipróbálásának esélyét.
- Általánosságban a gyerekek 10%-a számolt be olyan rossz tapasztalatokról, amik internetezés közben érték őket. A részletesebben vizsgált négy cselekvéstípus esetében igen változó, hogy azok milyen arányban fordultak ártalomnak tekinthető tapasztalatba. A zaklatás esetében a legnagyobb az arány (72%), amit sokkal kisebb számokkal követ a szexuális tartalmú képekkel, videókkal való találkozás (30%) és a szexuális jellegű üzenetekkel, cselekvésekkel kapcsolatos tapasztalat (29%). Legkisebb arányban az online ismeretségekkel való offline találkozókat végződtek rosszul (9%). Mindent összevéve, és a rossz tapasztalat komolyságát is megvizsgálva ezekkel a tevékenységekkel kapcsolatban a korosztály 5%-a számolt be olyan eseményről, ami meglehetősen, vagy nagyon felzaklatta.
- Az internetfüggőség – a gyerekek saját bevallása, illetve a szülei véleménye alapján – a jelek szerint nem mondható elterjedtnek a magyar gyerekek körében.
- Az adatok azt mutatják, hogy azok, aki rossz tapasztalatokat szereztek nagyrészt képek voltak aktív módon kezelni a helyzetet és csökkenteni az ártalom mértékét. Ugyan a fatalista elemek is gyakran előfordulnak a válaszadási mintákban, az érintettek 40%-a kizárólag valamilyen aktív stratégiát választott (megbeszélte valakivel a dolgot, megelőző technikai lépéseket tett stb.), és csupán 10%-uk hagyatkozott kizárólag passzív eszközökre (pl. függesztette fel egy időre az internetezést).
- A 11-16 éves gyerekeknek mindösszesen 24%-a gondolta úgy, hogy nem igaz az az állítás, hogy ő többet tud az internetről, mint a szülei. 30% inkább egyetértett ezzel, míg a fennmaradó 46% határozottan úgy vélte, hogy a szüleinél nagyobb tudással rendelkezik. Azaz majdnem minden második gyerek esetében a szülő már eleve információk hátrányban van a gyerekével szemben.
- A kutatás során vizsgált (csak a 11-16 évesek körében kérdezett) nyolc ilyen használati készség közül a könyvjelzők (bookmark) elmentése volt a legszélesebb körben használt tudás: a kérdezettek 58%-a tudta, hogy hogyan menthet el egyes oldalakat. A gyerekek csaknem fele képesnek érezte magát arra, hogy a biztonságos internethasználattal kapcsolatos ismereteket megtalálja a világhálón, és ugyanennyien tudják, hogy hogyan

blokkolhatnak nem kívánatos személyektől érkező üzeneteket. 45% tudja, hogy hogy kell a közösségi oldalakon a biztonsági beállításokat megváltoztatni. A nem kívánatos üzeneteket már csak 38% gyerek tudja blokkolni, és kevesebb min harmaduk érezte képesnek magát arra, hogy a helyes információ megszerzése érdekében összehasonlítsa különböző weblapokat. Végül csupán minden ötödik kérdezett tudta, hogy hogyan kell gépeknek szűrési beállításait megváltoztatni.

- Abban a viszonylag kis számú esetben (ami egy ilyen nagyságrendű kutatás során felszínre kerülhet), amikor egy gyereket valóban negatívan érintett valamilyen online kockázat és veszély, az erre adott válaszreakciók az esetek túlnyomó többségében olyan aktív cselekvések voltak, amelyek egyértelműen segíthetnek a probléma megoldásában. Egy ilyen kérdőíves kutatás természetesen nem szolgáltathat elegendő információt ezeknek a konkrét eseteknek a valódi, komplex és hosszú távú hatásmechanizmusairól. Ezért adataink csupán jelezhetik azt, hogy a probléma jelen van, az arra adott reakciók pedig igen sokrétűek, a gyerekek többsége pedig – saját bevallása szerint – viszonylag jól tudja kezelni a kialakult helyzeteket.
- A megkérdezett szülők több mint negyede nem használja az internetet. Rendszeres, napi szintű internethasználónak a teljes minta 43%-a bizonyult. Négy 9-16 éves magyar gyerek közül egy olyan biztosan van, akinek a szülője nem internetezik, miközben a gyereke igen. Azaz itt az ismeret- és tudásbeli szakadék mindenképpen jelen van. Az internetet nem használó szülőket legnagyobb arányban a kistelepüléseken (10 ezer, illetve 2 ezer fő alatt) és az alacsony státuszú háztartásokban találjuk.
- A leginkább, korlátozások nélkül engedélyezett tevékenységek körébe az azonnali üzenetküldés, illetve a különböző videók, videóklippek nézése sorolható. Közösségi oldalon saját profilt a gyerekek valamivel több, mint fele hozhat létre engedély nélkül.
- A szülők háromnegyede (75%) szokott beszélgetni a gyerekével arról, hogy mit csinál az interneten. Az, hogy egy szülő beszélget-e a gyerekével arról, hogy mit csinál az interneten, leginkább attól függ, hogy a szülő maga használja-e a világhálót.
- A saját internetes tudásukat magabiztosnak ítéő szülők – természetesen – jóval nagyobb arányban tudnak segíteni gyerekeiknek akár valamilyen információnak a megkeresésével, akár pedig a biztonságos internethasználattal kapcsolatban.
- Az internetet otthonukban (is) használó gyerekek szüleinek több mint fele (52%) meg szokta nézni a gyerekek által látogatott honlapokat, közel 40% azok aránya, akik a gyerek közösségi oldalon lévő profiljára is rápillantanak, míg 35% a gyerek kapcsolatait is ellenőrzi az azonnali üzenetküldő programokban. A gyerek által kapott/küldött üzeneteibe – legyen szó emailről vagy azonnali üzenetről – a szülők 23%-a tekint bele.
- A gyerekek több mint kétharmada számíthatott valamelyik barátjára akkor, amikor nehézségei támadtak valamivel a megkeresésével az interneten. 24% azok aránya,

akiknek segítettek akkor, amikor valamilyen felháborító vagy nyugtalanító tartalommal találkoztak az interneten.

- *A tanárok ugyan nincsenek nagy „lemaradásban”, azonban általánosságban a szülők-től nagyobb arányban kapnak segítséget, támogatást a gyerekek, mint tőlük.”¹¹⁴*



114 Ságvári Bence: Az EU Kids Online magyarországi kutatásáról in.: www2.lse.ac.uk/.../EUKidsOnline/.../Hungary%20webpage.pdf, 2013.03.07

BAJ ESETÉN KIHEZ FORDULHATOK?

Kihez?	Elérhetőség	Milyen ügyben?
Nemzeti Adatvédelmi és Információszabadság Hatóság www.naih.hu  Nemzeti Adatvédelmi és Információszabadság Hatóság	1055 Budapest, Falk Miksa u. 9-11. Tel: +36 1 391 1400, e-mail: ugyfelszolgalat@naih.hu	Ha személyes adataim védelmével (adatvédelem) vagy a közérdekű adatok nyilvánosságával (információszabadság) kapcsolatos alkotmányos jogaimmal összefüggő kérdésem van vagy ezeket a jogaimat sérelem érte/érheti.
Alapvető Jogok Biztosa www.ajbh.hu 	1055 Budapest, Falk Miska u. 9-11. Tel: +36 1 475 7100 e-mail: panasz@ajbh.hu	Amennyiben egy hatóság tevékenysége vagy mulasztása alapvető jogom sérti vagy közvetlenül sértheti.
Nemzeti Média- és Hírközlési Hatóság www.nmhh.hu  NEMZETI MÉDIA- ÉS HÍRKÖZLÉSI HATÓSÁG	1133 Budapest, Visegrádi u. 106. Tel: +36 1 468 0673 e-mail: info@nmhh.hu	Ha hírközlési szolgáltatók ellen kívánok panaszt benyújtani (például mobiltelefon-, internet- vagy postai szolgáltatásokkal kapcsolatban, kényszerű elektronikus hirdetés, spam bejelentése), illetve médiatartalom-szolgáltatók elleni panasz esetén (például televíziós és rádióműsorokkal, ún. lekérhető médiatartalmakkal, nyomtatott és internetes sajtóban megjelenő és egyéb internetes tartalmakkal kapcsolatban).

Kék Vonal Gyermek- krízis Alapítvány http://www.kek-vonal.hu/index.php/hu/inter-netbiztonsag 	Tel.: 116-111 vagy +36 1 354 1029 e-mail: kek-vonal.hu/emil chat: http://chat.kek-vonal.hu	Ha gyerekként úgy érzem, bajba kerültem, zaklatnak a neten, rossz érzéseket keltő weboldallal vagy üzenetekkel találkoztam, vagy szülőként aggódok, mert gyermekemet rossz élmények érték a világhálón, és szeretnék valakivel együtt gondolkodva megoldásokat találni.
Nemzeti Média- és Hírközlési Hatóság Internet Hotline www.internethotline.hu 	1015 Budapest, Ostrom u. 23-25. e-mail: internethotline@internethotline.hu	Ha jogellenes, illetve gyerekekre veszélyes vagy káros internetes tartalmat szeretnék bejelenteni, erre az Internet Hotline bejelentő felületén (http://internethotline.hu/tart/index/31/Bejelentes) kilenc kategóriában (hozzájárulás nélküli hozzáférhetővé tett tartalom, pedofil tartalom, zaklatás, rasszista, idegengyűlöletre uszító tartalom, erőszakos tartalom, drogfogyasztásra csábító tartalom, terrorcselekményre felhívó, azt népszerűsítő tartalom, adathalász honlapok, illetve egyéb, kiskorúakra veszélyes tartalom) és az internethotline@internethotline.hu e-mail címen van lehetőség.

Nemzetközi Gyermekmentő Szolgálat www.gyermekmento.hu www.saferinternet.hu 	H-1066 Budapest, Teréz krt. 24. Tel: +36 1 475 7000 Fax: +36 1 302 4136 ngysz@gyermekmento.hu	Ha előadást, képzést szeretnék szervezni iskolákban gyermekek, pedagógusok, szülők vagy szociális szakemberek részére a biztonságosabb internetezésről, az internet határtalan lehetőségeiről, a felhasználókra leselkedő veszélyek elkerülésének hatékony és egyszerű eszközeiről, vagy ilyen képzésben szeretnék részt venni.
---	---	--

„MAGYAR RECEPT”

A nemzetközi példák alapján több olyan, könnyen és olcsón megvalósítható gyakorlatot szeretnénk az érdeklődő felnőttek és gyerekek figyelmébe ajánlani, amik reményeink szerint alkalmasak lehetnek az internet világáról való elmélkedésre készítésre és olyan empátikus készségek (ki)fejlesztésére, ami a kulturált internethasználat alapja.

Történetek

Az osztályközösség vagy egy kisebb csoport felolvas vagy szereplőkkel eljátszik a magánszféra/adatvédelem megsértésével járó kitalált vagy igaz történeteket, majd különböző szempontok alapján megbeszélik, feldolgozzák a látottakat (drámapedagógia). Elemzik a résztvevők cselekedeteit és a következményeket, majd konklúziókat vonnak le arról, hogy mit és hogyan lehetett volna jobban csinálni az adott esetben azért, hogy ne kerüljenek veszélybe a személyes adatok/információk.

„Magánéleti napló”

A diákok feladata, hogy egy meghatározott belátható, rövidebb időszakon (1 hét – 1 hónap) keresztül vezessenek naplót, amelybe feljegyzik, hogy a róluk szóló online információkkal az adott időszakon belül mi történt. Például:

- Milyen körben árultak el magukról a magánéletüket érintő adatot?
- Esetleg más, ismerős vagy ismeretlen mit írt, mondott róluk?
- Elárulták-e online valakinek/valakiknek a nevüket, telefonszámukat, e-mail címüket?
- Bejelentkeztek-e egy website-ra?
- Letöltöttek vagy feltöltöttek fájlt a számítógépre?
- Használták-e a mobiltelefonjukat online alkalmazásra?

Miután elkészültek a naplók, a csoport/osztály beszélje át és szabadon értékelje ezeket.

Önarckép készítése és profil alkotása másról

A naplók felhasználásával a gyerekek gyűjtsék össze magukról és/vagy egy általuk a valóságban is jól ismert személyről az összes általuk kiadott vagy a neten róluk fellelhető személyes adatokat és információkat, majd ezek alapján készítsenek egy profilt. Elemezze ki mindenki önállóan, hogy az online profil igaz képet ad-e a valós személyről.

A másik feladat, hogy a gyerekek válasszanak ki egy hozzájuk közel álló ismerőst (családtagot, osztálytársat, vagy tanárt), és a rendelkezésre álló összes online forrás segítségével (pl. internetre feltöltött képek, megjelölt kedvenc tevékenységek, megosztott internetes oldalak, klubok, szabadidős tevékenység stb.) készítsenek egy profilt az adott személyről.

Ezt mutassák meg az adott személynek, majd figyeljék a reakcióját, van-e olyan dolog, amit nem szívesen hall, vagy lát magáról viszont a többiek előtt, annak ellenére, hogy amúgy az információt egy „egész világgal” osztotta meg korábban.

Magánélet súlyos sérelmével (megfigyelés, személyiséglopás, gondolatrendőrség, zaklatás, nyilvánosság ereje stb.) összefüggésbe hozható művészeti alkotások privacy szempontú elemzése:

Filmek:

- Hátsó ablak (eredeti cím: Rear Window, 1954, Alfred Hitchcock)
- A Hálózat csapdájában (eredeti cím: The Net, 1995, Irwin Winkler)
- Játssz/ma (eredeti cím: The Game, 1997, David Fincher)
- Gattaca (1997, Andrew Niccol)
- Truman Show (1998, Peter Weir)
- A közellenség (eredeti cím: Enemy of the State, 1998, Tony Scott)
- Különnvélemény (eredeti cím: Minority report, 2002, Steven Spielberg)
- Útközéspont (eredeti cím: Changing Lanes, 2002, Roger Michell)
- A mások élete (eredeti cím: Das Leben der Anderen, 2006, Florian Henckel von Donnersmarck)
- Drága besügött barátaim, 2012, Cserhalmi Sára
- A közösségi háló (eredeti cím: The Social Network), 2010, David Fincher)
- Trust (2010, David Schwimmer)
- Cyberbully (2011, Charles Binammé)
- Caught in the Web (2012, Chen Kaige)
- Disconnect (2012, Henry Alex Rubin)
- Személyiségeltörő (eredeti címe: Identity Thief, 2013, Seth Gordon)
- Az ártatlanság eladó (eredeti cím: Selling Innocence, 2004, Pierre Gang),
- Kamaszok (eredeti cím: Adolescence, 2025 Philip Barantini)

Regények:

- George Orwell: 1984
- Heinrich Böll: Katharina Blum elvesztett tisztessége
- William Golding: Legyek ura
- Natascha Kampusch: 3096 nap
- Eve Ainsworth: 7 nap

Versek:

- József Attila: Levegőt!
- Kosztolányi Dezső: Beírtak engem mindenféle könyvbe
- Illyés Gyula: Egy mondat a zsarnokságról stb.

ONLINE SZÓTÁR – INTERNETES KIFEJEZÉSEK

MAGYARÁZATA

Ban: egy vagy több személy letiltása egy adott csatornáról (tehát nick névváltás után sem tud a felhasználó általában visszajelentkezni.) Hasonló tiltást jelent a „Kick” – chatszobából való kitiltás.

Banner: „szalaghirdetés”, az internetes reklámozás legáltalánosabban használt eszköze (a Button „gomb” pedig a bannernél kisebb pixel méretben megjelenő reklámhirdetés)

Botnet: „robot network”, zombi számítógépek hálózata, melyeket különböző vírusokkal és trójai szoftverekkel irányítása alá vesz egy cracker. A számítógép erőforrásait ezután a saját céljára használja, az esetek nagyobb részében a számítógép tulajdonosa, használója tudta nélkül. Az ilyen botokkal irányított gépeket spamküldők (a spambot zombigéppel óránként akár 25 000 spamet is kiküldhetnek), valamint más bűnözői csoportok is ártó szándékkal használják (károkozás, megfélemlítés stb.).

Bug: „bogár”, a programokban lévő hiba, zavar (következménye pl. lefagyott képernyő vagy teljes rendszerösszeomlás)

Chat: „csevegés”, két vagy több ember online társalog, melyhez a chatprogramok biztosítanak teret (chatroom)

Cloud computing: „számítástechnikai felhő”, „felhő alapú informatika”, a naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomná a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások (pl.: Gmail, Dropbox). Az ügyfél számára előny, hogy gazdaságos és személyre szabott informatikai rendszerhez jut hozzá, de az alkalmazás adatvédelmi aggályokat vet fel, mert az adatok mozgása nem igazán nyomon követhető.

Cookie: „süti”, rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén, elvileg a felhasználó engedélyével. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítás), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt.

Cracker: nagy számítógépes tudását mások megkárosítására használó rosszindulatú személy, internetes vandál

Cyberbullying: „internetes zaklatás”, az internet, mobiltelefonok és egyéb modern technológiák közvetítésével olyan szövegek vagy képi tartalmak továbbítása vagy nyilvánosságra hozatala, melyek alkalmasak egy másik személy megszegényítésére, megalázására. A zaklatás ismétlődő jelleggel irányul egy kiszemelt áldozat ellen, amelytől az nem tudja önmagát megvédeni.

Deleb: dead celebrity, „halott híresség”

Domain név: egy weboldal elérési címe, egyedi azonosítója (pl. www.naih.hu)

E-commerce: „elektronikus kereskedelmi szolgáltatás”

Electronic Signature (e-Signature): „elektronikus aláírás”, informatikai úton előállított és jogi értelemben is elfogadott hiteles aláírás

Flame: „égetni” valakit megalázó megjegyzésekkel az internetes közösség tagjai előtt

GDPR: uniós adatvédelmi rendelet

Grooming: „becserkészés”, hamis identitás megadásával történő ismerkedés a világhálón

Hashtag: „kettőskeresztelés”, a Twitter közösségi oldalon a hasonló hozzászólások keresése

Hoax: lánclevél, e-mailben terjedő álhírek, „kacsák”

Lame: „láma”, „béna”, negatív jelző, gyakran ezzel jelzik saját magukról is felhasználók, hogy adott témakörben járatlanok, jóindulatú türelmet kérnek, ha esetleg értelmetlen dolgot mondanának vagy kérdeznének. Az online játékosok a „noob” kifejezést is használják.

Lájkolni: like, „tetszik” (először a Facebookon bejelölt ismerősöket lehetett így értékelni, mára általánosan elterjedt minősítési kategória)

Mesterséges intelligencia: olyan gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet

Mém (meme): digitális fájl (többnyire kép) internetes terjesztése azért, hogy egy kínos eseten vagy akár egy hamis híren/manipulált képen, videón stb. minél többen szórakozzanak (mémelés).

Msg (privát): külön beszélgetés, amit csak a beszélgetőtárssal ketten láthatunk, sokan helytelenül privátszatsornának hívják, de ha valakivel MSG-zünk, nem szükséges az illetővel egy csatornán lennünk.

Netikett: viselkedési normák az interneten

Nick: a felhasználó által választott egyedi azonosító név

Offtopic: témán kívüli

Op vagy @ a másik neve előtt: olyan személy (vagy bot), akinek az adott csatornán – megbízhatósága miatt – operátori jogai vannak (eltávolíthat másokat a csatornáról)

Post: üzenet hagyása üzenőfalra vagy weboldalon

Smiley: „mosolytár”, kis ábrák/karaktercsoportok, amik általában hangulatot, ritkábban cselekvést fejeznek ki („emotikon”) JKL

Smartphone: „okostelefon”, külső alkalmazások telepítésére és használatára alkalmas mobiltelefon

Sexting: erotikus tartalmú képi vagy szöveges üzenet

Streaming: hang vagy videó valós idejű közvetítése

Teamspeak: hanggal való kommunikáció azért, hogy halljuk a csoportban részt vevők reakcióit (receive only), illetve mi is hozzá tudunk szólni

Topic: „téma”, a csatorna fejléce

Torrent: több számítógép között megosztott gyors letöltés központi szerver közbeiktatása nélkül (peer-to-peer), melynek során a letöltendő fájl feldarabolják több kisebb fájlra és ezeknek a letöltését több számítógép végzi egyszerre (általában zeneszámok, filmek sokszor illegális letöltéséhez használják)

Troll: provokáló, közösségellenes módon történő megnyilatkozás, „beszólás”. Hasonló kifejezés a „Flame” – mikor a kommentelő kifejezetten indulatos hozzászólásaival árasztja el a hírcsatornát.

Unfriend: közösségi oldalakon egy személy negatív minősítése, letiltása

URL: Uniform Resource Locator, szabványosított internetes cím, az internetes dokumentum helyét adja meg

Website: az egy elérési cím (Domain) alatt található, egymással szoros kapcsolatban lévő Weboldalak együttese

Webpage: „weboldal”, olyan dokumentum, amely a böngészőben egy oldalként jelenik meg. Tartalmazhat szöveget, hyperlinkeket, képet, hangot, animációt, videót, illetve aktív, az oldal megjelenésekor elinduló programot is. A homepage „kezdőoldal” a website bevezető oldala és általában tartalomjegyzéke, ahonnan a website szinte bármelyik részére eljuthatunk. A honlap általában az az oldal, ami egy domain név beírásakor megjelenik.

Felhasznált források:

Cambridge szótár

<http://dictionary.cambridge.org/topics/internet-terminology-and-abbreviations/>

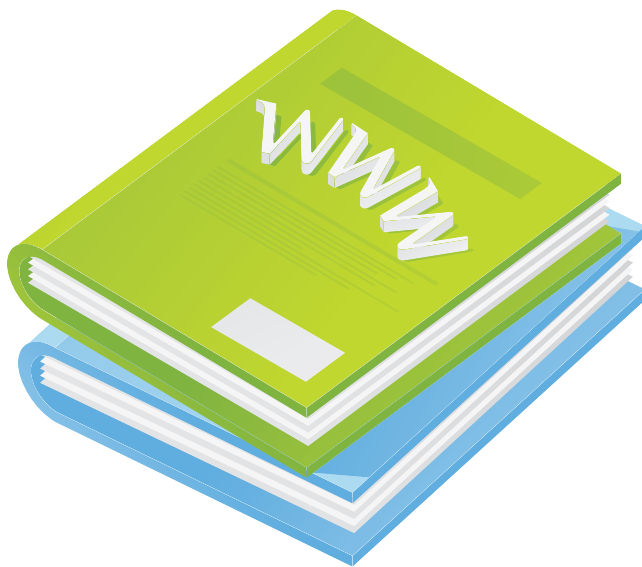
Gartner IT Glossary

<http://www.gartner.com/it-glossary/>

<http://www.logo92.hu/internetfogalom.html>

MI rendelet

Wikipédia



FÜGGELÉK

A MAGYAR ADATVÉDELMI HATÓSÁG GYERMEKEKNEK SZÓLÓ
TÁJÉKOZTATÓJA A TUDATOS INTERNETHASZNÁLATRÓL

FIGYELJ, EZ FONTOS!

Csak a Te döntésedon múlik, hogy a netet jóra vagy rosszra használod! Jó döntést azonban csak akkor tudsz hozni, ha tájékozott vagy, ezért ha közel áll Hozzád ez a téma, ismerkedj meg a valós életből vett példákkal és nézd át a hozzá tartozó információkat!



TUDTAD?

SZEMÉLYES ADAT: Egy személyre (az adataianyra) vonatkozó bármely információ személyes adat, melyet védeni kell illetéktelenek elől!

ADATKEZELÉS: személyes adatokkal végzett bármilyen művelet pl. lekérdezés, nyilvánosságra hozatal, megváltoztatás vagy törlés.

FELELŐSSÉG: Az internet virtuális világában a személyes adatok egy gombnyomással bárki számára megismerhetővé válhatnak és onnan senki sem távolíthatja el őket – az adatkezelő felelős és jogilag is felelősségre vonható azért, amit a mások adataival tesz!



Internetes szótár

ban:

egy vagy több személy letiltása egy adott csatornáról (tehát nick névváltás után sem tud a felhasználó általában visszajelentkezni.)

banner:

„szalaghirdetés”, az internetes reklámozás legáltalánosabban használt eszköze (a button „gomb” a bannernél kisebb pixel méretben megjelenő reklámhirdetés).

botnet:

„robot network”, zombi számítógépek hálózata, melyeket különböző vírusokkal és trójai szoftverekkel irányítása alá vesz egy cracker. A számítógép erőforrásait ezután a saját céljára használja, az esetek nagyobb részében a számítógép tulajdonosa, használója tudta nélkül. Az ilyen botokkal irányított gépeket spamküldők (a spambot zombigéppel óránként akár 25 000 spamet is kiküldhetnek), valamint más bűnözői csoportok is ártó szándékkal használják (károkozás, megfélemlítés stb.).

chat:

„csevegés”, két vagy több ember online társalog, a chatprogramok biztosítanak ehhez teret (chatroom)

choice mom:

szinglimami.

clicks and mortar:

hagyományos és virtuális kereskedés ötvö-zése

cloud computing:

„számítástechnikai felhő”, „felhő alapú informatika”, a naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál

a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások (pl.: Gmail, Dropbox). Az ügyfél számára előny, hogy gazdaságos és személyre szabott informatikai rendszerhez jut hozzá, de az alkalmazás adatvédelmi aggályokat vet fel (adatok mozgása nem nyomon követhető stb.)

cookie:

„süti”, rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén, elvileg a felhasználó engedélyével. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt.



cyber bullying / bullying:

„internetes zaklatás”, az internet, mobiltelefonok és egyéb modern technológiák közvetítésével olyan szövegek vagy képi tartalmak továbbítása vagy nyilvánosságra hozatala, melyek alkalmasak egy másik személy megszegényítésére, megalázására. A zaklatás ismétlődő jelleggel irányul egy kiszemelt áldozat ellen, amelytől az nem tudja önmagát megvédeni.

deleb:

dead celebrity, „halott híresség”

domain név:

egyedi azonosító az internet világában

e-commerce:

„elektronikus kereskedelmi szolgáltatás”

Electronic Signature (e-Signature):

„elektronikus aláírás”, jogi értelemben is elfogadott és informatikai úton előállított hiteles aláírás

grooming:

„becserkészés”, hamis identitás megadásával ismerkedés a világhálón

GDPR:

uniós adatvédelmi rendelet

hashtag:

„kettőskeresztelés”, a Twitter közösségi oldalon a hasonló hozzászólások keresése

hoax:

lánclevél, e-mailben terjedő álhírek, „kacsák”

lame:

„láma”, negatív jelző, gyakran ezzel jelzik saját magukról is felhasználók, hogy adott

témakörben járatlanok, jóindulatú türelmet kérnek, ha esetleg értelmetlen dolgot mondanának, vagy kérdeznének.

mém (meme):

digitális fájl (többnyire kép) internetes terjesztése azért, hogy egy kínos eseten vagy akár egy hamis híren/manipulált képen, videón stb. minél többen szórakozzanak (mémelés).

msg (privát):

külön beszélgetés, amit csak a beszélgetőtársal ketten láthatunk, sokan helytelenül privátcsatornának hívják, de ha valakivel MSG-zünk, nem szükséges az illetővel egy csatornán lennünk.



netikett:

viselkedési normák az interneten

nick:

„becenév”, a felhasználó által választott egyedi azonosító név.

offtopic:

témán kívüli

op vagy @:

a másik neve előtt: olyan személy (vagy bot), akinek az adott csatornán - megbízhatósága miatt - operátori jogai vannak (eltávolíthat másokat a csatornáról „kick”,

megtilthatja a belépésüket „ban”. Általánosságban fogalmazva megváltoztathatja a csatorna állapotát (mode).

plugin / social plugin:

tetszik és megosztás gombok

post:

üzénőfalon vagy a weboldalon üzenet hagyása

smartphone:

„okostelefon”, külső alkalmazások telepítésére és használatára alkalmas mobiltelefon
sexting: erotikus tartalmú képi vagy szöveges üzenet

streaming:

hang vagy videó valós idejű közvetítése (pl. egy online játékos az interneten közvetíti, ahogy éppen játszik).

teamspeak:

hanggal való kommunikáció azért, hogy halljuk a csoportban részt vevők reakcióit (receive only) illetve mi is hozzá tudunk szólni

topic:

„téma”, a csatorna fejléce



torrent:

több számítógép között megosztott gyors letöltés központi szerver közbeiktatása nélkül (peer-to-peer), melynek során a letöltendő fájlt feldarabolják több kisebb fájlra és ezeknek a letöltését több számítógép végzi egyszerre (általában zeneszámok, filmek sokszor illegális letöltéséhez használják)

troll:

provokáló, közösségellenes módon történő megnyilatkozás, „beszólás”. Hasonló kifejezés a „Flame” – mikor a kommentelő kifejezetten indulatos hozzászólásaival árasztja el a hírcsatornát.

unfriend:

ismerős elutasítása

URL:

Uniform Resource Locator, szabványosított internetes cím, az internetes dokumentum helyét adja meg

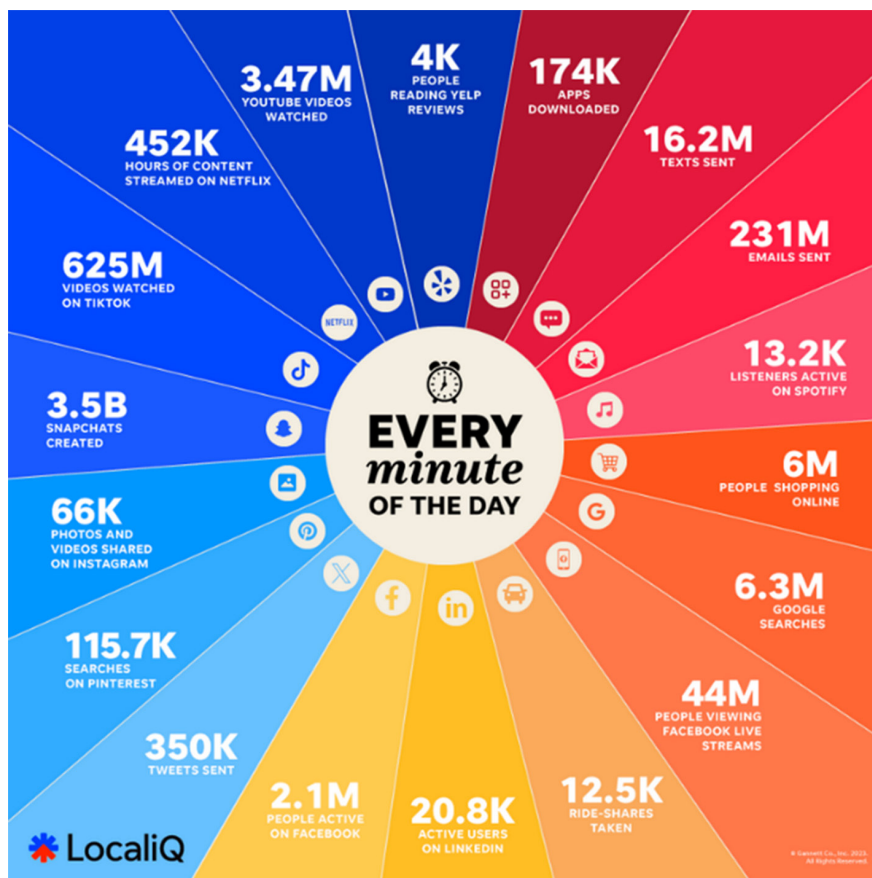
website:

az egy elérési cím (domain) alatt található, egymással szoros kapcsolatban lévő Weboldalak együttese

webpage:

„weboldal”, egy olyan dokumentum, amely a Böngészőben egy oldalként jelenik meg. Tartalmazhat szöveget, Hyperlinkeket, képet, hangot, animációt, videót, illetve aktív, az oldal megjelenésekor elinduló programot is. A Homepage „kezdőoldal” a Website bevezető oldala és általában tartalomjegyzéke, ahonnan a Website szinte bármelyik részére eljuthatunk. A honlap általában az az oldal, ami egy domain név beírásakor megjelenik.

Mi történik **egy perc alatt** az interneten?



Internet Minute 2023

VANNAK-E GYEREKJOGOK?

Természetesen igen, például tilos egy gyereket megalázni vagy vele szemben megtorlást alkalmazni szülei, családja vagy saját tulajdonságai, mondjuk vallása, nyelve, vagyoni helyzete, származása vagy véleménye miatt.

Joga van saját állampolgárságához, nevéhez, családjához és ahhoz, hogy az őt érintő kérdés eldöntésénél a hatóságok előtt kinyilváníthassa, hogy mit szeretne.

A neten keresztül sem lehet egy gyereket önkényesen megfigyelni és tilos a rá vonatkozó személyes adatokkal visszaélni!

Szabadon tájékozódhat, véleményét másokat nem sértő módon elmondhatja

Kit tart a jog gyerekeknek?

Aki a 18. életévét még nem töltötte be és nem nagykorúsították (például házasságkötés miatt.)

Szükséges-e szülői engedély az adatkezeléshez?

14 éves kor alatt: igen.

14-16 év között: a gyerek és szülő a szülő közösen dönt

16 év felett: a gyerek egyedül dönt



PÉLDA

- a kis elsősök diákigazolványán még a szülő aláírása szerepel
- 8. osztályban a továbbtanulási jelentkezést a gyerekek és a szülő(k) nek is alá kell írnia.
- az egyetemi felvételi papírokat már csak a diák írja alá

Biztos találkozottál már ezzel, csak esetleg nem gondoltok rá el rajta mélyebben, de sajnos az Internet gonosz vagy kellemetlen következményekkel járó célokra is használható:



Például:

- **internetes zaklatás (cyberbullying)**
- **internetes kibeszélés (mém)**
- **internetes „beszólás” (troll)**
- **erotikus képek küldözgetése (sexting)**
- **internetes pedofília**
- **személyes adattal való egyéb visszaélések (pl. adathalászat, személyiséglopás)**

INTERNETES ZAKLATÁS (CYBERBULLYING)



Az internetes zaklatás mindig személyes indítékkal indul, az elkövető hosszabb ideig, visszatérően kínozza áldozatát azért, hogy őt megfélemlítse vagy háborgassa (például valaki éjjel-nappal fenyegető vagy megalázó e-maileket küld, közösségi oldalon üzenget, bántó tartalmú kommenteket ír vagy blogos naplójában sértegeti társát).

A zaklatás bűncselekmény, mely akár egy évig terjedő szabadságvesztéssel is büntethető!

PÉLDÁK

Sajnos nem egyedi eset egy 13 éves amerikai kislányé, akivel „barátnője” egy közösségi portálon rendszeres e-mail váltások során elhitette, hogy egy 16 éves fiú szerelmes belé, majd nyilvánosan leleplezte és nevetségessé tette. A kislány elkeseredésében 2006-ban öngyilkos lett. Az eset miatt született meg Missouri államban az a törvény, mely az online sértegetőket vagy molesztálókat pénzbüntetéssel és börtönnel fenyegeti.

Egy magyar hatodikos kislány osztálytársnőjének szeretett volna segíteni és ezért fordult a Kék Vonalhoz. A duci, nehezen barátkozó kislány nem rég jött át egy másik iskolából, mert ott „halálra cikizték”, de a hívó úgy látja, itt sem lesz jobb sora. Az iskolában nem bántja senki, de a Facebookon már keringenek róla kellemetlen fotók, és az esti chatelésekben állandóan az új lány „bénasága” a téma. A betelefonáló kislány nem szeretne csatlakozni a bántalmazókhoz, de tart tőle, hogy ha az új lány mellé áll, ő is ki lesz téve hasonló bántásoknak.



INTERNETES KIBESZÉLÉS (MÉM KÜLDÉS)

Az internetes kibeszélés vagy mém (meme) küldés manapság főleg hamis hírek, káros videók vagy képek korlátlan terjesztéséből áll. A kárvallott általában idegen személy (ebben különbözik a cyberbullyingtól), akit az internetes közösség „kipécéáz” magának valamilyen tulajdonsága vagy megnyilvánulása miatt.



PÉLDA

Az egyetemről kikerült magyar fiatalember Facebook oldalán 2013 májusában köszönetet mondott hivatali feljebbvalóinak (ideértve még a miniszterelnököt is) hivatalnoki állása elnyeréséért – nevét és fényképét „percen belül” kikutatva nemsokára gúnyolódó mémek tömegének főszereplője lett. Az eredetileg csak ismerőseinek szánt üzenete miatt így vált egy nyilvános lejárató kampány áldozatává egy pályakezdő fiatal...

TROLL (PROVOKÁLÓ HOZZÁSZÓLÓ)



A troll egy olyan hozzászóló, aki ingerlő, provokatív módon, tárgyhoz nem is tartozó hozzászólásaival „bombáz” egy internetes közösséget (pl. fórum, chat, blog, levelező lista) vagy személyes véleményét erőlteti rá mindenkre azzal a szándékkal, hogy megzavarja az eszmecserét. A trollok ténykedése elszabadítja az indulatokat: mind a gyalázkodás, mind az ellenreakciók brutális stílusban zajlanak, gyakori a halálos fenyegetés is. Don't feed the trolls!, vagyis az ilyen hozzászólásokról jobb nem tudomást venni.

PÉLDA

A trollok között mostanában szokás híres sportolókat nyilvánosan gyalázni. Nemrég egy fiatal angol boxolóra „szállt rá” twitteres zaklatója, aki Jimmibob88 néven bejelentkezve változatos sértéseket vágott a sportoló fejéhez és gúnyolódott eredményein. A heves vérmérsékletű sportoló a Twitteren 1000 font „vérdíjat” ajánlott annak, aki elárulja a troll nevét és címét. Nemsokára rá is talált ellenfelére, még egy fotót is kipoztolt a házáról bizonyítva, hogy bármikor elkaphatja. A troll könnyörgésre fogta a dolgot és bocsánatot kért. A Twitteren az eset miatt a legnépszerűbb hashtagek közé emelkedett a #keyboardwarrior (billentyűzetharcos) és a #jimmybrownpants (kb. beszari Jimmy) minősítés.

EROTIKUS KÉPEK KÜLDÖZGETÉSE (SEXTING)



Szexi (bikinis, monokinis vagy meztelen) képeket vagy videókat egyre több tini lány küldözget magáról. Ráadásul meglepően sok gyerek látott már olyan képet, amit eredetileg egyértelműen nem neki szántak. A fő probléma ezekkel a képekkel, hogy a felvételek sorsa a későbbiekben a szereplőtől függetlenül alakul és számos komoly visszaélés történhet velük! Tartsd észbe, hogy az elhagyott barát vagy barátnő bosszúból aljasságokra is képes lehet...

Ráadásul vannak olyan honlapok, amik egyenesen ilyen képek beküldésére buzdítanak:

„Küldj be az interneten magukat kellettő 16 éves vagy annál fiatalabb csajokat! (myvip vagy iwiw adatlap címet feltétlen írd!)”...„Ha felkerültél az oldalra, és emiatt szomorú vagy, írd nekünk, és talán levesszük a képeidet az oldalról. Mivel bunkók vagyunk, és a szép szóból nem értünk, minél inkább mocskolódsz, annál biztosabb, hogy sikerrel jársz!”

PÉLDA

Egy lány a Miss MyVip Szépségkirálynő választás nevű versenyre fényképekkel nevezett a közösségi portálon és hamarosan ismerőse jelezte, hogy egy oldalon megtalálta őt pornográf képek között. Az oldal főszerkesztőjéhez címzett törlési kérelmére nem érkezett válasz.

Egy másik szülő 16 éves leányának fényképeit leszedték a közösségi oldalról, és feltették egy szexoldalra teljes nevével, lakhelyével, életkorával, telefonszámával. A lány fenyegető leveleket kapott és telefonon zaklatták, valamint trágár kommentárokat fűztek a képeihez. A törlési kérelmére csak annyit válaszoltak, hogy „innen soha a bűdös életbe nem fogsz lekerülni”.

A rendőrséghez 2013-ban egy 17 éves lány arról tett bejelentést, hogy egy korábban saját magáról készült ruhátlan képével - amelyet csak két ismerősének továbbított - egy ismeretlen új Facebook profilt hozott létre, melynek alapképe a kérdéses ruhátlan kép lett.



INTERNETES PEDOFÍLIA, BEHÁLÓZÁS (GROOMING)

A pedofil felnőtt beteg szexuális vágyat érez gyerekek iránt és az internet sajnos alkalmas terep a pedofil hajlamok kiélésére: ismerkedésre, kapcsolatépítésre, gyermekekről készült pornográf felvételek beszerzésére, cseréjére. Ráadásul a pedofilok és a más „internetes behálózók” nem nyílt kártyákkal játszanak: másnak adják ki magukat, így válhat rövid időn belül „ismerőssé” egy valójában veszélyes és ártó szándékú idegen. Az elkövetők zöme tudatos stratégiával, több hónapon keresztül cserkészti be a közösségi oldalon áldozatát, lányokat és fiúkat egyaránt.

PÉLDA

Negyvenes éveiben járó férfi 18 évesként regisztrál egy közösségi portálon vagy egy társskereső oldalon, feltölt „magáról” egy vonzó képet, elkezd tini lányokkal ismerkedni, egyre közelebb kerülnek egymáshoz, a kislány bizalmába fogadja a „fiút”, akinek kérésére esetleg további képeket küld magáról, jobb esetben ruhában, rosszabb esetben meztelen, vagy félmeztelen felvételeket.

A Kék Vonalhoz egy kisvárosból telefonált egy aggódó édesanya. 17 éves fia neten ismerkedett meg egy magát 19 évesnek való lánnyal és most szeretne hozzá felutazni Budapestre, hogy együtt töltsenek egy hétvégét. Az anya megnézte a lány Facebook oldalát, és az ismerősök alacsony száma, a fotók mesterkéltsége (csupa beállított „divatkép”) alapján rossz érzései támadtak.

INTERNETES JÁTÉKOK



Játszani nagyon jó, de azért akad néhány dolog, amire oda kell figyelni. A regisztráció során általában felhasználónevet, levelezési címet, születési dátumot kérnek – ugyanakkor el kell kerülni a lakcím, iskola kiadását és mindig használjunk korlátozó adatvédelmi beállításokat, erős jelszót!

Az „ingyenes” játékok sem mindig azok valójában, főleg a „kiegészítők” vásárlása esetén figyeljünk oda, nehogy az emelt díjas telefonhívás, sms a saját vagy szüleink pénztárcáját terhelje meg károsan nagy összeggel.

PÉLDA

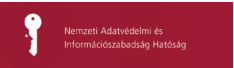
Bizonyos online játékoknál „megbüntetik” azt, aki túl korán kiszáll: eltilthatnak órákra-napokra-hetekre a játéktól, ami azzal a következménnyel is jár, hogy hiába fizetted ki a teljes részvételi díjat vagy vásároltál már kiegészítőket, az érvényességi idő csökkenése miatt ezek a befizetések elvesznek.

Az online játékoknál komoly gondot okozhat a függőség kialakulása. A Kék Vonalhoz egy 15 éves fiú apja telefonált, mert a fiú elhanyagolja az iskolát, a családját, már edzésekre se jár el. Online játékokkal tölti minden idejét, meg ki tudja, még mi mindent csinál az interneten... A szülők úgy érzik, semmit nem tudnak tenni, hogy megállítsák ezt a folyamatot és kétségbe vannak esve, mert világos, hogy a fiú egy lejtőn csúszik lefelé...



Baj esetén **kihez** fordulhatok?

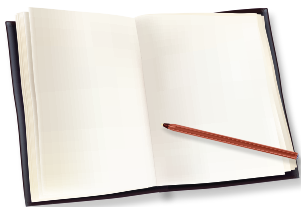


Kihez?	Elérhetőség	Milyen ügyben?
Nemzeti Adatvédelmi és Információszabadság Hatóság www.naih.hu 	1055 Budapest, Falk Miksa u. 9-11. Tel: +36 1 391 1400, e-mail: ugyfelszolgalat@naih.hu	Ha személyes adataim védelmével (adatvédelem) vagy a közérdekű adatok nyilvánosságával (információszabadság) kapcsolatos alkotmányos jogaimmal összefüggő kérdésem van vagy ezeket a jogaimat sérelem érte vagyérheti.
Alapvető Jogok Biztosa www.ajbh.hu 	1055 Budapest, Falk Miska u. 9-11. Tel: +36 1 475 7100 e-mail: panasz@ajbh.hu vagy külön gyerekeknek: kerdesemvan@obh.hu	Amennyiben egy hatóság tevékenysége vagy mulasztása alapvető jogom sérti vagy közvetlenül sértheti.
Nemzeti Média- és Hírközlési Hatóság www.nmhh.hu 	1133 Budapest, Visegrádi u. 106. Tel: +36 1 468 0673 e-mail: info@nmhh.hu	Ha hírközlési szolgáltatók ellen kívánok panaszt benyújtani (például mobiltelefon-szolgáltatással, internet-szolgáltatással, postai szolgáltatásokkal kapcsolatos panaszok, kéretlen elektronikus hirdetés, spam bejelentése), illetve médiatartalom-szolgáltatók elleni panaszok esetén (például televízió- és rádióműsorokkal, ún. lekérhető médiatartalmakkal, nyomtatott és internetes sajtóban megjelenő tartalmakkal és egyéb internetes tartalmakkal kapcsolatos panaszok).

Kihez?	Elérhetőség	Milyen ügyben?
Kék Vonal Gyermek- krízis Alapítvány www.kek-vonal.hu 	Tel.: 116-111 e-mail: gyerekjogasz@kek-vonal.hu chat: http://chat.kek-vonal.hu	Ha gyerekként úgy érzem, bajba kerültem, zaklatnak a neten, rossz érzéseket keltő weboldalakkal vagy üzenetekkel találkoztam, vagy szülőként aggódok, mert gyermekemet rossz élmények érték a világhálón, és szeretnék valakivel együtt gondolkodva megoldásokat találni, illetve jogi kérdéseimre választ kapni.
Nemzeti Média- és Hírközlési Hatóság Internet Hotline www.internethotline.hu 	1015 Budapest, Ostrom u. 23-25. e-mail: internethotline@internethotline.hu	Ha jogellenes, illetve gyerekekre veszélyes vagy káros internetes tartalmat szeretnék bejelenteni, erre az Internet Hotline bejelentő felületén (http://internethotline.hu/tart/index/31/Bejelentes) kilenc kategóriában (hozzájárulás nélküli hozzáférhetővé tett tartalom, pedofil tartalom, zaklatás, rasszista, idegengyűlöltre uszító tartalom, erőszakos tartalom, drogfogyasztásra csábító tartalom, terrorcselekményre felhívó, azt népszerűsítő tartalom, adathalász honlapok, illetve egyéb, kiskorúakra veszélyes tartalom) és az internethotline@internethotline.hu e-mail címen van lehetőség.

Kihez?	Elérhetőség	Milyen ügyben?
Nemzetközi Gyermekmentő Szolgálat www.gyermekmento.hu www.saferinternet.hu 	H-1066 Budapest, Teréz krt. 24. Tel: +36 1 475 7000 Fax: +36 1 302 4136 ngysz@gyermekmento.hu	Ha előadást, képzést szeretnék szervezni iskolákban gyermekek, pedagógusok, szülők vagy szociális szakemberek részére a biztonságosabb internetezésről, az internet határtalan lehetőségeiről, a felhasználókra leselkedő veszélyek elkerülésének hatékony és egyszerű eszközeiről, vagy ilyen képzésben szeretnék részt venni.

Az én **privacy-naplóm: mi történt az online adataimmal az elmúlt héten/két hétben/egy hónapban?**



Milyen körben osztottam meg magamról a magánszférámba tartozó adatot? Esetleg más, ismerős vagy ismeretlen mit írt, mondott rólam? Elárultam-e online valakinek/valakiknek a nevemet, telefonszámomat, e-mail címemet? Bejelentkeztem website-okra? Letöltöttem vagy feltöltöttem fájlt a számítógépre? Használtam-e a mobiltelefonom online alkalmazására? stb.

This image shows a full page of a worksheet designed for handwriting practice. It features ten sets of horizontal lines across the page. Each set consists of three lines: a solid top line, a dashed middle line, and a solid bottom line. These lines are evenly spaced and extend from the left margin to the right edge of the page, providing a guide for letter height and placement. The background is plain white, and there are no other markings or text present.

TESZTSOR

1. Megismerkedsz egy sráccal/lánnyal az interneten, aki nagyon bejön. Már régóta chateltek, mikor megkér, hogy küldj magadról neki képet:

- a) Na végre, annyira jól néz ki a profilképén, talán még össze is jöhetünk.
- b) Végülis, max nem tetszem neki.
- c) Dehogy küldök, elvégre látja a profil képen hogy nézek ki. Minek neki még több kép?

2. Bejelöl a Facebook-on egy személyt, akit még sosem láttál:

- a) Visszajelölöm, hogy minél több ismerősöm legyen.
- b) Még gondolkodom, hogy honnan ismerhetem.
- c) Nem jelölöm vissza. Sose láttam, nem is értem minek jelölt be.

3. Egy újságban ezt a feliratot olvasod: legújabb internetes örület, a mémelés:

- a) Na az meg mi?
- b) Valamit meséltek a suliban, valami ciki képekről van szó.
- c) Mármint arra gondolsz, amikor digitális fájl (többnyire képet) azért terjesztenek az interneten, hogy egy kínos eseten vagy akár egy hamis híren/manipulált képen, videón stb. minél többen szórakozzanak?

4. 15 évesen szeretnél meglepetésként egy oldalt, ami belépés előtt a következő lehetőségeket ajánlja fel: „elmúltam 18, meglepetésként az oldalt” vagy „még nem múltam el 18, elhagyom az oldalt”.

- a) Nem értem, minek a megkülönböztetés.
- b) Bár 15 éves vagyok, attól még el tudom dönteni, mit nézhetek meg a neten és mit nem.
- c) Lehet, hogy valami kellemetlen élménytől kímélem meg magam, ha hanyagolom az oldalt?

5. Online játékon való regisztráláshoz bankszámlaszám megadása szükséges:

- a) Felőlem, a lényeg, hogy végre játszassak vele.
- b) Nem is tudom, meg kéne kérdezni valakit, aki jobban ért ehhez.
- c) Kizárt, még fizetős oldalakra irányítanak.

6. Meglátod egy közösségi oldalon, hogy a barátnőd bikinis képeket töltött fel magáról:

- a) Na ezt nem hagyhatom, én is töltök fel néhány fürdőruca képet.
- b) Bikiniben azért nem, de felrakok néhány jobban sikerült fotót magamról.
- c) Majd letöltik egy csomóan a saját gépükre, aztán rajtam szórakoznak. Én biztos nem akarom viszont látni magam más gépén.

7. Kapsz az e-mail címedre egy levelet, amelyben az áll, hogy te vagy egy egzotikus nyaralás szerencsés nyertese. Csak meg kell adnod a következő adatokat, és átveheted nyereményed: név, lakcím, telefonszám, bankszámlaszám, személyi igazolvány száma, adószám:

- a) Ezt a mázlit, már küldöm is az adatokat, nemsokára nyaralás!
- b) Mi alapján lettem én a nyertes? De végül is egy próbát megér.
- c) Ja persze, biztos kisorsolnak hetente. Ezek csak átverések, nem küldök nekik semmilyen adatot.

8. A barátod arról mesél, hogy valaki a nevében küldözget e-maileket az osztálytársaidnak:

- a) Ja persze! Hogy tudna más belépni az ő e-mail fiókjába?
- b) Szerintem megadhatta valakinek a jelszavát, aki most így megvicceli.
- c) Sajnos nem nehéz manapság feltörni más oldalát.

9. Azt hallottad az iskolában, hogy a fénykép személyes adatnak minősül:

- a) Nem. Személyes adat a név, cím, személyi igazolvány szám, stb. Ezt mindenki tudja.
- b) Nem, csak akkor, ha rá van írva az is, hogy kiről készült.
- c) Persze, hiszen egy kép alapján egyértelműen beazonosítható bárki.

10. Egy ismerősödnek visszaéltek a személyes adataival. Azt mesélte, hogy a NAIH-hoz fordult segítségért:

- a) Már akkor sem értettem mire gondolt.
- b) Ja, az biztos valami nemzetközi szerv, ami adatokkal foglalkozik.
- c) Ha jól tudom, a magyar adatvédelmi hatóságról van szó.

11. Egy diszkóban elkéri a telefonszámod:

- a) Megadom. Szeretek ismerkedni.
- b) Legyen, max nem veszem fel, ha rosszkor hív.
- c) Hallottam már különféle zaklatásos sztorikat. Inkább nem...

12. A 14 éves húgod csak a szüleid felügyelete mellett internetezhet:

- a) Elég gáz, hogy nem csinálhat azt a neten, amit akar.
- b) Minek ott ülni mellette, utólag is vissza lehet nézni a látogatott oldalakat.
- c) Biztos nem kellemes helyzet, de legalább nem lát olyat, ami nagyon nem neki való.

13. Egy haver feltöltött rólad az internetre egy kinos képet:

- a) Kicsit haragszom, de mindegy, megkérem, hogy törölje le és elfelejtve a dolog.
- b) Feltöltök én is róla valami ciki képet.
- c) Na szép... ezt már sosem szedem le a netről.

14. Azért regisztráltam a Faceobokra, hogy:

- a) Hogy minél több emberrel megismerkedhessek, hogy feltehessek magamról képeket, megoszthassak én is videókat, posztolhassam, épp mit csinálok, merre járok.
- b) Ne maradjak le a többiektől. Már szinte mindenkinek van Facebookja, ahol minél több ismerőst gyűjthet.
- c) Megkeressem a barátaimat, és a rég nem látott ismerősöket.

15. Ha arról kérdeznak, hogy odafigyelek-e a személyes adataim védelmére, kijelenthetem, hogy igen, hiszen:

- a) Csak a szimpatikus embereknek árurom el a személyes adatokat.
- b) Csak akkor adok ki magamról adatot, ha valaki kéri, magamtól nem.
- c) Nem szoktam csak úgy minden ok nélkül bárkinek is kiszolgáltatni a rám vonatkozó adatokat.

ÉRTÉKELÉS

I. Legtöbb a) válasz esetén:

A válaszaid alapján jobban oda kellene figyelned a személyes adataid védelmére. Nem igazán tudod felmérni, hogy egyes esetekben milyen következményekkel járhat, ha meggondolatlanul bárkivel megosztod a telefonszámod, vagy kiteszel magadról képeket a közösségi oldalakra. Jó tanácsként ajánljuk figyelmedbe a tanulságos eseteket és hasznos tippeket tartalmazó projektfüzet elolvasását!

Legtöbb b) válasz esetén:

A válaszaidból látszik, hogy hallottál már az adatvédelemről, vagy jó érzéked van hozzá, hogy egyes esetekben elkerüld a személyes adataid meggondolatlan közlését. Vannak olyan szituációk, amelyekben gyanakodsz, ha bizalmas adataidról kérdeznek - és ez így helyénvaló-, ám végül sok esetben mégis elárulod ezeket. Mivel tudásodon még lehet csiszolni, az ismereteid bővítésére jó szívvel ajánljuk a projektfüzet elolvasását!

Legtöbb c) válasz esetén:

Gratulálunk! Sikeresen teljesítetted az adatvédelmi gyorstesztet! Válaszaid alapján látszik, hogy tisztában vagy az adataid védelmét érintő kérdésekkel. A való életben, a hétköznapi helyzetekben is helyesen tudsz mérlegelni, hogy mikor szükséges adatot kiadnod magadról és mikor kerülhetsz bajba, ha túl sok információt osztanál meg. Csak így tovább, tudásod elmélyítésére kiváló segítséget nyújthat a projektfüzet elolvasása!

TIPPGYŰJTEMÉNY

Általános:

- A stílus maga az ember - ne jársd le Magad közönséges vagy durva megnyilvánulásokkal.
- Használj bonyolult jelszavakat és cseréld ezeket gyakran.
- Megnyitás helyett inkább töröld a gyanús eredetű vagy tartalmú üzeneteket, véleményeket.e klikkelj válogatás nélkül mindenre.

Közösségi háló:

- Ismerd és használd a biztonsági beállításokat!
- Posztolás előtt jól gondold át, hogy milyen információ kerül ki így Rólad a netre.
- Az online hírneved érték, ne rontsd le meggondolatlanul
- A valóban személyes infók ne legyenek nyilvánosak
- Jobban jársz egy szűkebb, de megbízhatóbb ismerősi körrel.
- Az egyenes út mindig a legrövidebb: légy őszinte barátaiddal, beszéljétek ki a sérelmeiteket, lehet, hogy csak egy buta félreértés az egész!
- Ha valaki fenyeget vagy zaklat a neten, azonnal jelentsd ezt az adminisztrátornak, nyomtasd vagy mentsd el a bizonyítékot és töröld a zaklatót az ismerőseid közül.

Mobil webes eszközök:

- Ne feledd, hogy a hálózaton soha sem vagy egyedül!
- Vigyázz, mert ha ellopják a készüléket, a rajta lévő adatok is illetéktelen kezekbe kerülnek!
- A telefonon is használd jelszó-és egyéb biztonsági védelmet.
- Ne add meg telefonszámod vagy e-mail címed akárkinek.
- Ha app-et vásárolsz, nézd előtte meg, hogy az alkalmazás mihez fér majd hozzá (pl. közösségi háló vagy helymeghatározás)
- Lehetőséged van a helymeghatározás ki-és bekapcsolására.
- A nyilvános hálózatok (Wi-Fi hotspot) nem biztonságosak, veszélyt jelenthetnek az adataidra.
- Netes vásárláskor külön ellenőrizd a pénzmozgást.
- Gyanús jelentkezésekre (hanghívás, sms stb.) inkább ne reagálj, a gyanús forrásokat blokkold!
- Fényképezés/videózás előtt mindig kérj engedélyt az érintettől.
- Hozzájárulás nélkül ne posztolj képeket/videókat másokról.

ÉS A LEGFONTOSABB:



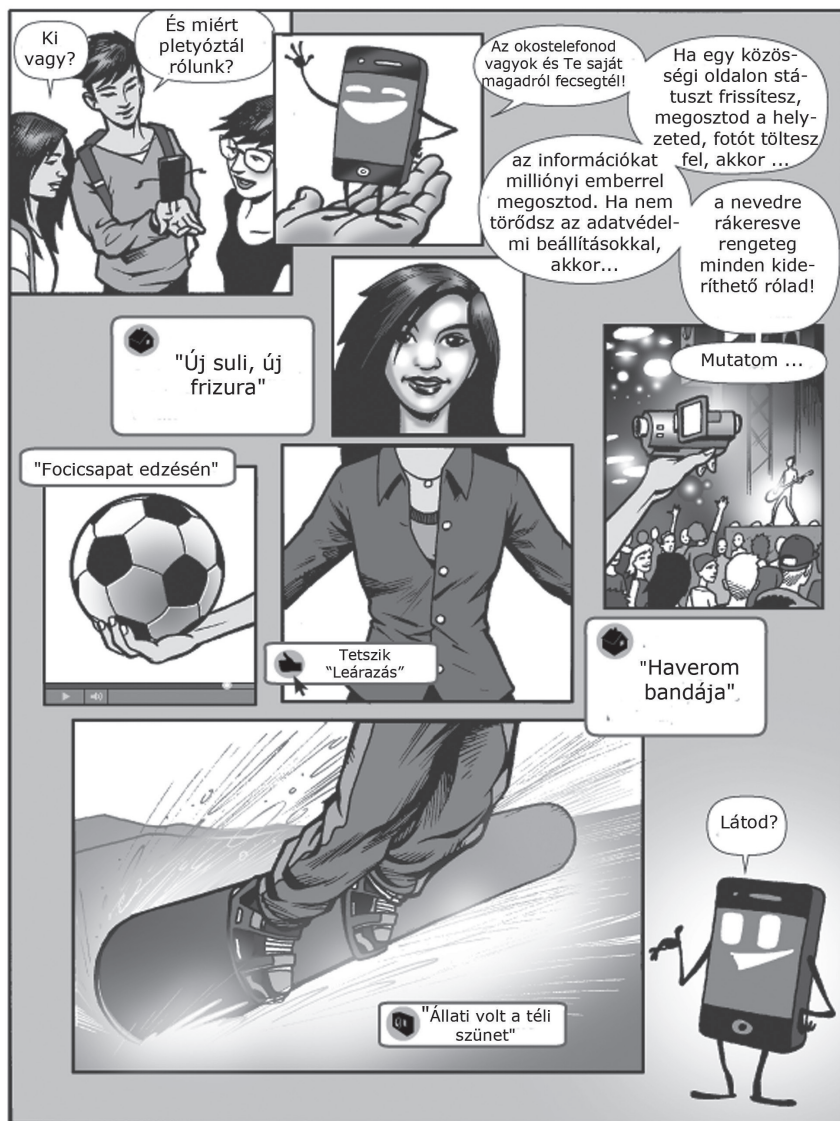
Másokkal ne tégy olyat, amit Te sem szeretnél soha átélni, de ha bajba kerülsz, gondolj arra, hogy biztosan nem Te vagy az egyedüli, aki ezzel a problémával küszködik és kérj azonnal segítséget!

Közösségi kulcskérdések

Adatvédelem és internet



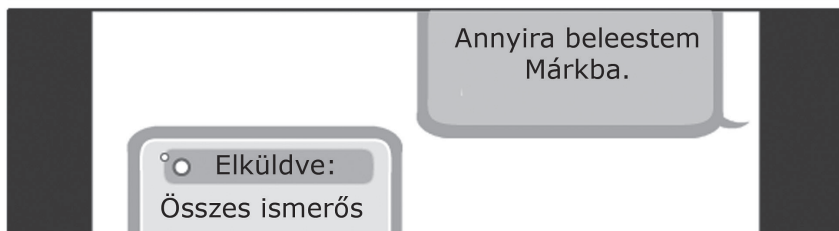
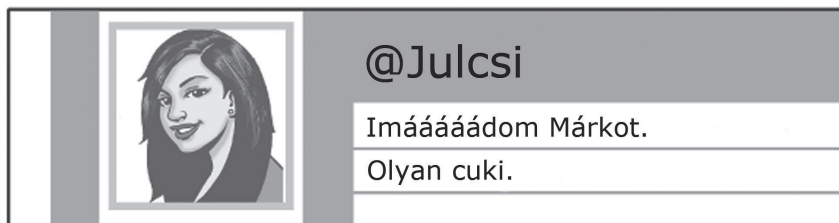
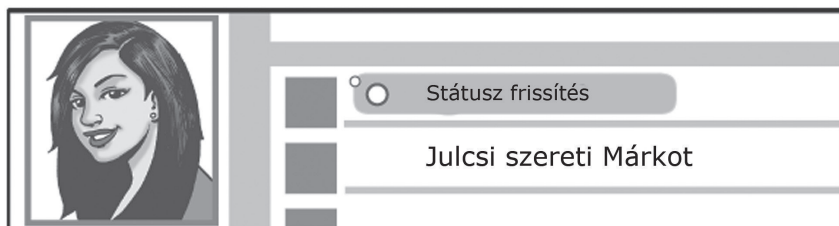






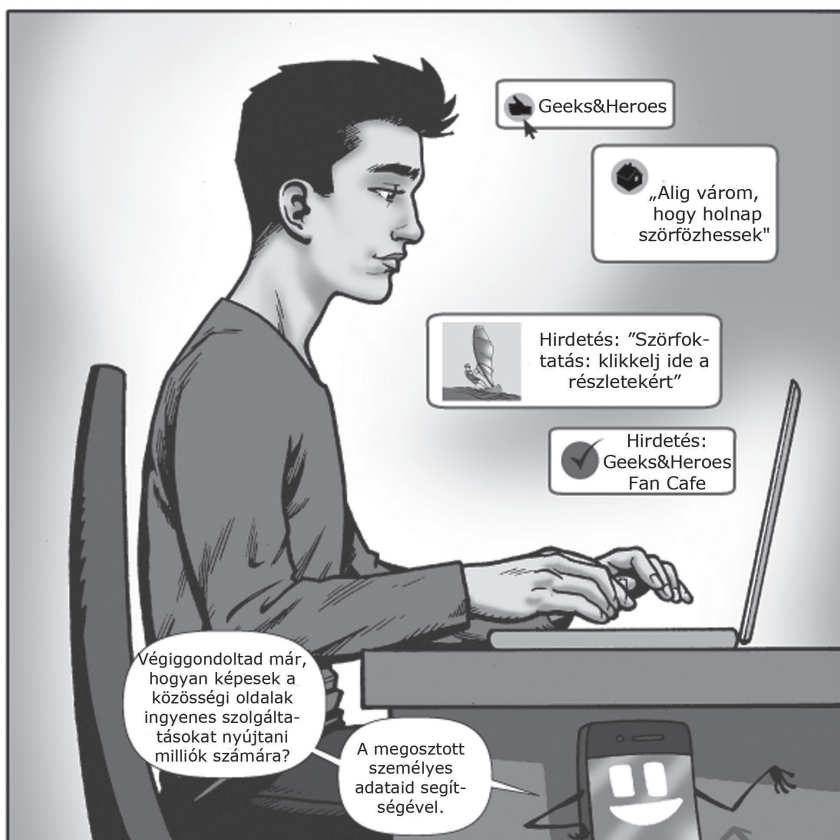




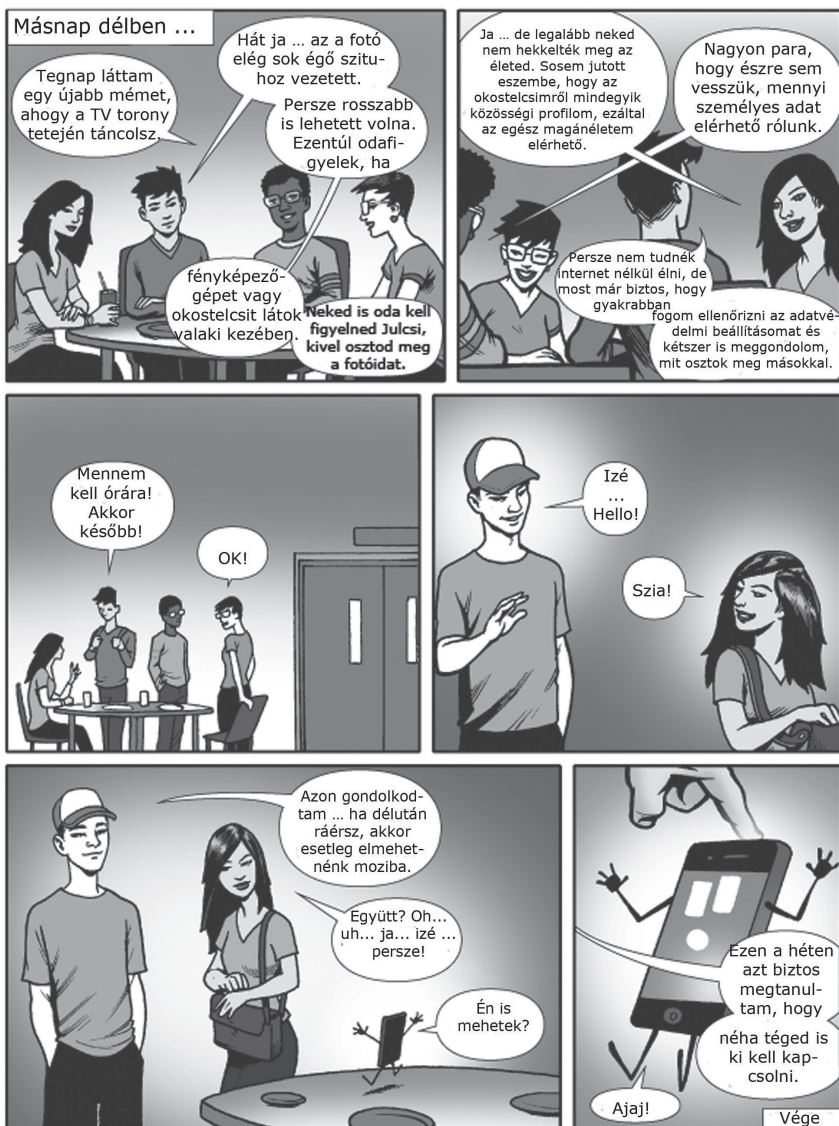












A képregény eredeti tartalma, illetve annak bármely alkotóeleme a kanadai adatvédelmi biztos hivatalának tulajdona és a kanadai adatvédelmi biztos előzetes engedélyével használható fel. A képregény fordítása a kanadai adatvédelmi biztos engedélyével és támogató hozzájárulásával készült. A honlap eredeti verziója az alábbi linken található meg: http://www.priv.gc.ca/youth-jeunes/fs-fi/res/gn_index_e.asp



Nemzeti Adatvédelmi és Információszabadság Hatóság



Nemzeti Adatvédelmi és Információszabadság Hatóság

1055 Budapest, Falk Miksa utca 9-11.
Levelezési cím: 1363 Budapest, Pf.: 9.

Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Internet: <http://www.naih.hu>
e-mail: ugyfelszolgalat@naih.hu

Kiadja: a Nemzeti Adatvédelmi és Információszabadság Hatóság

Felelős kiadó: Dr. habil. Péterfalvi Attila elnök

ISBN 978-615-82797-0-3