digitális jólét
program

MAGYARORSZÁG DIGITÁLIS GYERMEKVÉDELMI STRATÉGIÁJA

digitális jólét program

TARTALOMJEGYZÉK

Köszöntő

A Kormány által az internetről és a digitális fejlesztésekről kezdeményezett 2015. évi nemzeti konzultáció, az InternetKon keretében a magyar polgárok egyértelmű véleményt fogalmaztak meg: a világháló ne fenyegesse gyermekeink biztonságát. Magyarország Digitális Gyermekvédelmi Stratégiájának megalkotását emellett elengedhetetlenné tette az is, hogy olyan új típusú veszélyforrások, fogalmak jelentek meg az elmúlt években a gyermekek internethasználatával összefüggésben, amelyek új megoldásokat, bizonyos körben új állami eszközrendszert igényelnek. A gyermekek már nem csupán passzív befogadók, aktívan kommunikálnak, ezért saját aktivitásukkal sodorhatják veszélybe magukat. Tájékozottságuk, tudatosságuk az internetes kommunikációban tehát fontosabb, mint valaha.

A Kormány az InternetKon eredményei alapján készítette el a magyar társadalom és a magyar nemzetgazdaság digitális fejlesztését célzó Digitális Jólét Programot. A program részeként elkészült Magyarország Digitális Gyermekvédelmi Stratégiáját a fentieken túl az a felismerés hívta életre, hogy a digitális kultúra egyre növekvő mértékben, meghatározó módon befolyásolja mindennapi életünket, társadalmunkat és gazdaságunkat. A tudatos internethasználat mint a digitális kultúrához való hozzáférés csatornája az egyik legfontosabb, rendkívül összetett képesség. Amennyiben a megfelelő képességekkel rendelkező fiatalok biztonságos környezetben tudják használni a digitális világ nyújtotta lehetőségeket, úgy nemcsak a saját egyéni versenyképességük javul, hanem közösségüké, így összességében az országé is. A stratégia megalkotásának elsődleges célja ezért annak biztosítása, hogy megvédjük gyermekeinket az internet veszélyes, káros tartalmaitól és módszereitől, valamint felkészítsük a gyermekeket, szüleiket, tanáraikat a tudatos, értékteremtő internethasználatra.

Magyarország Digitális Gyermekvédelmi Stratégiájának kiemelt célja a tudatos, értékteremtő internethasználat támogatása mellett, hogy az eddigieknél hangsúlyosabban érvényesüljenek a gyermekek védelmét szolgáló szabályok és intézkedések. Ennek érdekében fontos az internethasználat során a gyermekekre leselkedő veszélyek, kockázatok azonosítása, azok kiküszöbölése, ezáltal a káros hatások megelőzése, illetve lehető legnagyobb mértékű csökkentése. A stratégia további célkitűzése, hogy a rendelkezésre álló védelmi mechanizmusok megfelelőképpen, hatékonyan töltsék be funkciójukat.

A stratégia középpontjában a gyermekek állnak, de ezzel együtt a társadalom szinte valamennyi csoportja érintettnek tekinthető, ezért az állami eszközrendszer meghatározása mellett a kölcsönös tudásmegosztás és tanítás, valamint a társadalom különböző szereplőinek összefogása együttesen tehetik sikeressé a stratégia gyakorlati megvalósítását. Ennek érdekében Magyarország Digitális Gyermekvédelmi Stratégiája javaslatot tesz arra, hogy minden érintett szereplő – köznevelés, civil szervezetek, gyermekvédelmi intézményrendszer, bűnüldöző szervek – együttműködése valósuljon meg a káros, veszélyes és bűnös internetes tevékenységek ellen történő fellépésben.

dr. Deutsch Tamás

Digitális Jólét Program

összehangolásáért és megvalósításáért

felelős miniszterelnöki biztos

I. Helyzetértékelés

Bevezetés

A Kormány 2015 decemberében elfogadta az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (*InternetKon*) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról szóló 2012/2015. (XII. 29.) Korm. határozatot.

A Kormány annak érdekében, hogy a gyermekek és a személyiségi jogok védelmét szolgáló szabályok és intézkedések az eddigieknél hangsúlyosabban érvényesüljenek, felhívta a Digitális Jólét Programjával kapcsolatos kormányzati feladatok összehangolásáért és megvalósításáért felelős miniszterelnöki biztost, hogy az emberi erőforrások miniszterével együttműködve, az érintett szakmai és civil szervezetekkel, az NMHH elnökével, valamint az állami és piaci szereplőkkel egyeztetve 2016. június 30. napjáig készítse elő, és terjessze a Kormány elé a *Digitális Gyermekvédelmi Stratégiát* (Korm. határozat 4. *a)* pont).

A stratégia három pilléren nyugszik, amely szerkezet megjelenik a helyzetértékelésben, a célok meghatározásában, valamint az eszközök azonosításában is:

- Tudatosítás és médiaműveltség;
- Védelem és biztonság;
- Szankcióalkalmazás és segítségnyújtás.

1. Tudatosítás és médiaműveltség

A stratégia Tudatosítás és médiaműveltség pillérének elérni kívánt célja annak megteremtése, hogy az érintettek felelősen és tudatosan éljenek a technológia adta lehetőségekkel. A biztonságos internetezéssel kapcsolatos tudatosítás ahhoz szükséges, hogy elkerülhetőek – illetve legalábbis csökkenthetőek – legyenek a gyermekek és fiatalkorúak egészséges fejlődésére leselkedő veszélyek, káros hatások. A tudatos internethasználat tehát magában foglalja egyfelől az online világban rejlő lehetőségek lehető legnagyobb mértékben történő kihasználásának képességét, valamint az ennek során felmerülő lehetséges veszélyek, kockázatok ismeretének és felismerésének készségét egyaránt. A médiatudatosság mindezeken túl kiterjed az internet biztonságos használatát lehetővé tevő védelmi megoldások, illetve a sérelmes helyzetek nem várt bekövetkezte esetén igénybe vehető eszközök, intézmények létének, elérésének ismeretére is.

A tudatosítást azonban nem kizárólag a gyermekek tekintetében kell növelni, illetve megvalósítani, hanem legalább olyan fontos az őket közvetlenül körülvevő környezet vonatkozásában. A gyermekek mellett tehát legalább ilyen fontos a szülők, az oktatásukért, nevelésükért felelős pedagógusok ismereteinek bővítése, ahogyan az életükre kiemelt befolyást gyakorolni képes külső tényezők, mint például a média (vagy maga az internet) világa orientálásának szükségessége.
A stratégia helyzetértékelése azokat az információkat gyűjti össze és értékeli, amelyek jelen állapotban a gyermekek tudatosságát célozzák szolgálni, külön kitérve e körben az érintetteket fenyegető veszélyekre, amelyek nagyobb fokú tudatosság birtokában könnyen elkerülhetőek. A tudatosság meglévő pontos szintjének felmérése nyilvánvalóan nem megoldható, ugyanakkor az ennek megvalósítását célzó eszközök (például az oktatás terén), illetve ezek gyakorlati érvényesülése, hatékonysága ismert.

1.1 A tudatos internethasználathoz szükséges készségek

1.1.1 Technológiai ismeretek

A tudatos internethasználat elsőként az online térhez való csatlakozást lehetővé tevő eszközök használatának, működési elveinek és rendszerének ismeretét jelenti. Tekintettel a rohamos technológiai fejlődésre, a legfiatalabb generációk már e kultúrába születnek bele, és ezen eszközök környezetében nőnek fel. A tudatosítás növelésének első nehézsége már e ponton megmutatkozik: a gyermekek

életkorukból adódóan sokkal jobban tisztában vannak a digitális eszközök használatával, mint azok a környezetükben lévő felnőttek, akikre éppen a tudatosításban való aktív szerepvállalás hárulna.

1.1.2 Biztonságos internethasználatot elősegítő eszközök ismerete

Az internetezés tudatossága magában foglalja, hogy a gyermek tisztában van azokkal a rendelkezésére álló biztonsági eszközökkel, megoldásokkal, amelyek alkalmasak a káros hatásoktól, következményektől való megóvására. Ennek nem kell pontos, minden részletre és körülményre kiterjedő ismereteket jelenteni, így például nem feltétlenül jelenti az efféle eszközök pontos elérhetőségét, alkalmazását és használatát, azonban szükséges, hogy az ilyen lehetőségeknek legalább a létéről és alapvető funkciójáról rendelkezzenek ismeretekkel. Kiemelkedően fontos feladat, hogy a gyermekeken túlmenően a szülők, gondviselők, pedagógusok is legalább ugyanolyan – de inkább nagyobb – mértékben birtokában legyenek az efféle képességeknek, információknak.

Emellett hasonlóan lényeges az egyes, internethasználat során alkalmazott beállítások ismerete és felelősségteljes használata. Ilyennek tekinthető az adatvédelmi beállítások alkalmazása, egyes esetekben a felhasználási feltételek elfogadását megelőzően azok legalább alapszinten való átolvasása, az internetes vásárlásokkal kapcsolatos körülmények, lehetséges kockázatok ismerete.

1.1.3 A lehetséges veszélyekről általánosan

A gyermekekre (és sokszor nemkülönben a felnőttekre) számos további veszély leselkedik abban a világban, amelyben a digitális média – meghatározó társadalomszervező és identitásképző/szocializációs tényezőként – szinte minden tevékenységünket átszövi. Mediatizált és konvergens kultúránkban a gyermekeket (is) súlyosan fenyegető további veszélyek például:

- A tudatos megtévesztés, vagyis a manipuláció, mivel a médiaszöveg-fogyasztónak – különösen a kevéssé plurális nyilvánosság esetén – nincs lehetősége a média által közzétett információk igazságtartalmáról más módon, mint a médiából meggyőződni, márpedig így súlyosan sérülhet az őt megillető korrekt tájékozódáshoz, közérdekű információhoz jutáshoz való joga;
- A nehezebben szabályozható online médiakörnyezetben felerősödik a gyűlöletbeszéd vagy kódolt beszéd veszélye, ilyenkor a stigmatizáció, a kulturális értelemben vett bármiféle másság el nem fogadására való felhívás,

az előítéletek felerősítése, az idegen bűnösként való megjelenítésében felépülő rasszizmus a médiahasználattal összefüggő veszély forrása;

- Különösen erős veszély a függőségekkel, az addikcióval kapcsolatos „túlhasználatból” következik, a játékszenvedéllyel vagy a közösségi oldalak nonstop használatával, az internetre „költözéssel” egyre gyakrabban válnak a médiahasználók súlyos szenvedélybetegekké;
- Komoly veszélyforrás a virtuális világból származó élmények egyre fokozódó, túlzott részesedése az emberi tapasztalásban, a valós és virtuális információk nagyfokú keveredése, amely felkészületlenné, kiszolgáltatottabbá teheti az embert mindannak, amivel a valóságos életben kell megküzdenie;
- Súlyos probléma a valóságismeret gyengülése/tévedése a „kemény médiahasználók” könnyebb manipulálhatósága, összefüggésben azzal, ha bizonyos társadalmi csoportokat, jelenségeket kevéssé és nem a valóságnak megfelelően mutat be a média – vagyis a reprezentációk problémája;
- Az online világot jellemző nemlineáris olvasás, a linkhasználatra szerveződő szöveghasználat az ebben a textuális környezetben felnövekvő „klikkgenerációk” számára egyre nehezebbé teszi a hagyományosan strukturált szövegek végigolvasását, értelmezését – így nagyjából az iskolavilág által előírt komplett tudásanyag/szöveghalmaz elérését, feldolgozását, birtokba vételét;
- Az adatbiztonság sérülékenységének a problémája messze túlmutat a gyanútlanul kiadott személyes adatok kérdésén, mivel ide tartozik a – digitális – adatbázisok, archívumok sérülékenysége, amely részben súlyos és valós nemzetbiztonsági kockázatot jelent (kémkedés, terrorizmus), részben a hatalommal való visszaélés lehetőségét, a demokratikus alapjogokat megkérdőjelező korlátozásokat (akár indokoltan, akár a politikai-gazdasági erőfölénnyel rendelkezők hatalmának védelmében);
- A mediatizált testkultúra, a test átalakítása úgyszintén a populáris kultúrával/médiával kapcsolatos – és mai formájában újnak tekinthető – rendkívül fontos és problematikus jelenség (a tetoválástól a plasztikai műtéteken, a különféle szépészeti és egészségjavító szerkezetek beültetésen át a genetikai beavatkozásokig), mivel a testkultúra szoros kapcsolatban áll a férfi és női társadalmi szerepek alakulásával, a nemi identitások problémáival, és azon keresztül a kisebbségekkel kapcsolatosan a közvélemény formálásával;
- A konvergens kultúrában egyre inkább a média által közvetített kifejezési formák és minták alapján próbáljuk értelmezni saját magunkat és a környező világot, ami növeli a távolságot és csökkenti az átjárhatóságot az egyes generációk tapasztalata, értékvilága, informáltsága között;

- Mivel a konvergens kultúrában a technikai platformok egyre közelebb kerülnek egymáshoz, a tablet és az okostelefon egyszerre médialejátszó, fényképezőgép, kamera, online üzemmódban kommunikáló számítógép, így a médiatartalmak egyre nehezebben sorolhatóak markáns, éles kontúrokkal elkülöníthető műfajokba, szövegformákba – márpedig ez megnehezíti a szelekciót, a tudatos tartalomválasztást;
- A társadalmi egyenlőtlenségek növekedésével járhat a médiatechnológiák elérésének, a hozzáférésnek a korlátozottsága, a digitális analfabetizmus, a médiahasználathoz szükséges tudásból való kirekesztődés.

1.1.4 Káros tartalmak felismerése

Az ismeretek egyik legjelentősebb körét azon készségek képezik, amelyek révén a gyermekek fel tudják ismerni, és ennek következtében el is tudják kerülni az internetezés során felmerülő káros, veszélyes tartalmakat. Ezen kompetencia szoros összefüggést mutat a biztonságos internethasználatot elősegítő eszközök ismeretével kapcsolatban írtakkal; az egyes biztonsági megoldások (például a 18 éven aluliaknak nem ajánlott tartalmak előtt az e jellegükre való figyelemfelhívás) felismerése az internethasználat során kiemelt szempontnak számít. A gyermekeknek a káros tartalmakkal való szembetalálkozásuk során szintén rendelkezniük kell bizonyos alapvető kompetenciákkal; értelmüknek át kell fognia, hogy a számukra nem ajánlott tartalmakat valóban ne tekintsék meg (kíváncsiságuk ellenére se).
Emellett viszont, ha mégis szembesülnének káros, veszélyes vagy akár jogsértő tartalmakkal, akkor legyenek tisztában azoknak a fórumoknak, bejelentési lehetőségeknek (például hotline, rendőrség stb.) a létével, elérhetőségével, ahol a tapasztalt visszásságokat jelenteni tudják. (Nyilván az alapvető tudatosság kérdésén túlmutat, de megemlíthető, hogy a kívánt állapot esetében a gyermekek körében olyan kultúra kialakítása is szükséges volna, amely alapján nem mulasztják el az ilyen tartalmakat bejelenteni, ezzel is felelősséget vállalva a kevesebb ismerettel rendelkező társaik irányába, megóvva őket a veszélyektől.)

1.1.5 Káros magatartások felismerése

A káros tartalmak mellett az internetes úton elkövetett veszélyes, egyes esetekben kifejezetten jogsértést megvalósító magatartások felismerése, lehetőség szerinti elkerülése, illetve a szükséges járulékos intézkedések megtétele (például megfelelő fórumokon való bejelentés, jogi eljárások kezdeményezése) szintén a tudatos internethasználat körébe tartozik.

Az efféle magatartások megfelelő felismerése és kezelése egyben azt a képességet is magában hordozza, hordozhatja, hogy az illető gyermek, miután tisztában van az ilyen magatartások lehetséges hatásaival, következményeivel, vélhetően jóval kevesebb hajlandóságot fog mutatni ezek elkövetésére is.

1.1.6 A túlzott internethasználat káros hatásainak ismerete

Nem közvetlenül az internethasználat során, hanem annak hatására számos káros, veszélyes, és maga az érintett által nehezen felismerhető következmény alakulhat ki. E körben említhetők bizonyos függőségek, az internethasználat sajátosságaiból adódó koncentrációkészség-hanyatlás, a társas kapcsolatok megromlása, stb. Nyilvánvalóan nem minden, az online térben folytatott – hosszú ideig végzett – tevékenység hatására alakulhatnak ki ilyen következmények. A tanuláshoz szükséges információ keresése, olvasás, tájékozódás céljából történő barangolás más megítélés alá esik, mint az online játékok használata, vagy a közösségi oldalak üzenőfalainak puszta, csupán megszokásból történő lapozgatása.

1.1.7 Az internethasználat nyújtotta lehetőségek ismerete

A gyermekeknek tisztában kell lenniük az internethasználat által eléjük tárulkozó lehetőségekkel, amelyek az életük számos területén könnyítést, segítséget jelenthetnek. Ennek kapcsán elsődlegesen a tanulási folyamatok támogatására és az információgyűjtés, tapasztalatszerzés egyéb formáira indokolt gondolni. Megemlítendő, hogy egyes esetekben az – egyébként sokak által gyakran visszaélésre felhasznált – anonimitás is bizonyos előnyökkel szolgál e tekintetben. A gyermekek bizonyos területeken, kérdésekben (legtöbbször félelem vagy szégyenérzet által vezérelve) nehezen nyílnak meg mások előtt, nehezen osztják meg tapasztalataikat, lelki eredetű problémáikat. Az online tér adta fórumokon ezzel szemben könnyebben nyílik lehetőségük esetleges problémáik feltárására, és kor-, illetve sorstársaiktól nagyobb segítséget kaphatnak azok megoldásához.
Említhető a kapcsolattartás egyes formáira nyújtott lehetőségek (például közösségi oldalak, *social media*) feltételeinek, körülményeinek, alkalmazásának ismerete, használatuknak „egészséges” keretek között tartása, illetve a bennük rejlő lehetőségek kiaknázása. Ahogyan általában véve az internet sem eredendően „rossz”, úgy nyilvánvalóan e közösségi oldalak sem tekinthetők annak; olyanná válnak, amilyenné felhasználóik teszik, ahogyan azokat a gyermekek használják. E készségek elsajátítása révén nemhogy nem „veszélyként” jelentkeznek ezek a szolgáltatások, hanem éppen ellenkezőleg; a mindennapi élet számos területének megkönnyítéséhez járulnak hozzá.

1.2 A tudatos médiahasználat oktatásának helyzete

A köznevelésben a jelenlegi helyzethez képest jóval erőteljesebben meg kell jeleníteni a gyermekek védelmének, médiaműveltségük fejlesztésének kérdéseit. Különösen fontosnak tekinthető:

- A köznevelési intézményekben igénybe vehető szolgáltatások (pszichológusi, informatikai) tartalmának újragondolása;
- A pedagógiai munkát támogató szervezetek szerepvállalása (például az Oktatási Hivatal, azon belül pedig a Pedagógiai Oktatási Központok, a megyei és fővárosi Pedagógiai Intézetek és a civil szervezetek);
- A NAT és az egyes tantárgyi követelmények átdolgozása;
- A pedagógus- és tanárképzés követelményeinek módosítása;
- A pedagógusok és tanárok továbbképzési rendszerében meghatározott követelmények módosítása.

Ennek kapcsán figyelemreméltó információkat tartalmaz az alapvető jogok biztosának 2016 februárjában nyilvánosságra hozott jelentése (AJB-479/2016.), amelynek relevánsabb megállapításai az alábbiak szerint foglalhatók össze:

- A 2013-ban megjelent NAT újrarendezte a magyarországi médiaoktatás iskolán belüli helyét és rendszerét. A NAT-ban már valamennyi korosztály számára megjelennek a médiaműveltségre vonatkozó ismeretek, azok külön nevesítve épülnek be a vizuális kultúra tantárgyba;
- A Nemzeti alaptanterv kiadásáról, bevezetéséről és alkalmazásáról szóló 110/2012. (VI. 4.) Korm. rendelet alapján az iskolai tantervben szerepet kap a kritikai gondolkodás kialakítása, a médiában megjelenő erőszak, a jelenség értelmezése és hatásának tudatosítása, az online életforma hatása a személyiség fejlődésére, a társas kapcsolatokra, a tanulásra, a munkavégzésre, valamint a szabadidő eltöltésére. 2001-től pedig már választható közismereti érettségi vizsgatárgy is;
- Oktatási szakértők szerint azonban problémát okoz, hogy a médiaoktatás és -ismeret tekintetében meglehetősen nagy különbségek tapasztalhatóak a gyermekek tudása között attól függően, hogy milyenek a helyi, személyes és iskolai lehetőségeik. Emellett jelenleg a médiaértés-oktatás több műveltségi területhez is kapcsolódik, nem önálló tantárgyként szerepel, így a médiával kapcsolatos ismeretek átadása többnyire nem szakirányú végzettséggel rendelkező tanárokra hárul, hanem különféle más főszakkal rendelkező pedagógusokra;

- Az alapvető jogok biztosának álláspontja szerint az információ mennyisége, az információs csatornák elképesztő mérvű gyarapodása miatt még soha ekkora szükség nem volt arra, hogy a gyermekek, fiatalok olyan oktatásban részesüljenek, amely alkalmassá teszi őket a média világában való biztonságos eligazodásra. A gyermekek ugyanis akkor érthetik meg az őket körülvevő világot, ha képesek értően, kritikusan megítélni és befogadni a hallott és látott információkat. Ezt a célt szolgálja a médiaértés-oktatás;
- A köznevelésért felelős államtitkár kiemelte, hogy az iskolai média- és internethasználattal kapcsolatban nincs egységes szabályozás a nevelési-oktatási intézményekben. Ahol iskolai szintű szabályozást alkalmaznak, ott jellemzően a helyi tantervben, valamint az iskola szervezeti és működési szabályzatában rögzítik ezt. A szabályozás kérdését az is nehezíti, hogy a diákok jelentős része már rendelkezik okostelefonnal, tablettel, amelyek tanítási idő alatti működtetésére, használatára vonatkozóan szintén az iskolai szintű szabályozás az elfogadott. A szaktárca érzékelte az informatikai eszközök használatával járó kockázatokat és arra reagálva módosította a köznevelési törvényt;
- A médiaoktatásra fordított időkeret a valóságban rendszerint helyi, vagyis iskolai, illetve a tanár személyes döntése. Mivel pedig az iskolában zajló formális oktatás eredményességéről, azaz arról, hogy ténylegesen mi zajlik az osztálytermekben semmilyen kutatás nem áll rendelkezésre hazánkban, nincs arra vonatkozó adat sem, hogy az iskolákban ténylegesen milyen időkeretben történik az ismeretek átadása. A megkeresett szervek válaszai azonban arra engednek következtetni, hogy a médiaismeretre, a médiaértésre, illetve a tudatos médiahasználatra vonatkozó műveltségtartalmak átadására szánt időkeretet gyakran nem használják ki. Megállapítható, hogy az alacsony óraszám, az integratív jelenlét, valamint a kevés számú szakképzettséggel (és sokszor hiányos kompetenciával) rendelkező pedagógus iskolai jelenléte miatt a médiatudatosságra nevelés sok esetben nem valósul meg maradéktalanul és hatékonyan az oktatási rendszerben;
- A digitális környezet térhódítása miatt a pedagógusok nehéz helyzetben vannak, mert a legtöbb pedagógus képzésében még nem jelent meg hangsúlyosan az, hogyan kezeljék ezt a területet, hogyan tudják az oktatás során aktív és biztonságos módon alkalmazni a médiát. Az államtitkár utalt arra, hogy ezzel párhuzamosan pedig szükséges a diákokkal megértetni, hogyan lehet tudatosan és felelősen is használni a média nyújtotta lehetőségeket.

Az AJBH tájékoztatása szerint ritkának tekinthető az AJBH-hoz érkező közvetlenül, direkt módon az online gyermekvédelem területét érintő panasz; jellemző tapasztalat, hogy a panaszosok a sérelmek és kifogások között utalnak az online térben történő

jogsértésekre, említést tesznek azokról. Mindezek okán a terület ombudsmani gyakorlata nehezen számszerűsíthető vagy jellemezhető statisztikailag. A biztos szerint a tárgykörben beérkezett viszonylag csekély számú egyedi panasz és kérdés egyébiránt arra enged következtetni, hogy sok esetben nemcsak a gyermekek, de az érintett szülők, pedagógusok és iskolák sincsenek kellően tisztában az internettel kapcsolatos tényleges kockázatokkal, veszélyekkel, valamint azok kezelésének módjával, azaz az online térben a gyermekeket ért sérelem esetén eljárásra jogosult szervekkel. Ennek nyomán fogalmazta meg jelentésében annak szükségességét, hogy a pedagógusok képzése és továbbképzése során a tananyag részévé kellene tenni az online bántalmazási, zaklatási helyzetek iskolai kezelésével összefüggő ismereteket.

Ezen túl a biztos említi, hogy a panaszokban a beadványozók jellemzően sérelmezik a legnagyobb közösségi oldalak felhasználási feltételeit, a közösségi alapelveket sértő oldalakat, a közösségi oldalakon megjelenő és gyermekeket sértő véleményeket, hozzászólásokat. A szülők tartanak továbbá a közösségi oldalak használatából eredő azon következményektől, hogy az oktatási intézményen belül gyermekük esetleg negatív megítélés, megkülönböztetés alá esik.

1.3 Tapasztalatok az érintettek tudatosságát illetően

Számos vizsgálat, kutatás foglalkozik a tudatosság kérdésével, illetve egyéb programok során szerzett tapasztalat is felhasználható a jelenlegi állapot legalább vázlatos, a legjelentősebb pozitívumokat, illetve a releváns problémákat és hiányosságokat felszínre hozó értékeléséhez. A korábbiakban említettek szerint ahhoz, hogy a gyermekek a megfelelő képességek birtokába kerüljenek, jóval tágabb körben szükséges a tudatosítás stratégiáját kidolgozni, ehhez pedig a jelenlegi helyzetet értékelni. A gyermekek mellett tehát indokolt kitérni az alábbi szereplők internethasználathoz való viszonyára, meglévő készségeire, illetve a hiányok azonosítására és azok megszüntetésének lehetséges módjaira, eszközeire:

- szülők (közeli rokonok, illetve általában véve a család);
- pedagógusok;
- a gyermekvédelmi rendszer képviselői: iskolapszichológusok, szociális munkások, nevelők;
- kortársak.

A tapasztalatok között érdemes megemlíteni, hogy az UNICEF Magyar Bizottsága 2014 őszén végzett nem reprezentatív kutatást 1191 fő, 10-19 éves általános- és középiskolai diák körében a gyermekjogokról, benne az internetes biztonságról is. Bár a megkérdezettek 96%-ának van mobiltelefonja, és 88%-ának profilja közösségi oldalon, a gyermekek fele nem érzi biztonságosnak az internetet. Minden harmadik

gyermeket ért már kellemetlen piszkálódás az interneten. Ilyen esetben a gyermekek fele megpróbálta megvédeni magát, de segítséget csak minden tizedik kért. Az NMHH 2013-as felmérése szerint a 14 és 17 év közöttiek háromnegyede szokott úgy internetezni számítógépen, hogy nincs jelen felnőtt, de az óvodásokkal egy háztartásban élő internethasználók 10%-a is úgy nyilatkozott, hogy a velük együtt elő, hat évnél fiatalabb gyerekek szoktak táblagépen vagy telefonon egyedül, felnőtt segítsége nélkül internetezni. Az internetezők kis része számolt be arról, hogy ő, vagy szülője telepített szűrőprogramot a gyermek által használt számítógépre (18%) vagy telefonra, táblagépre (11%).

1.3.1 Szülők

A szülők – illetve a következő alpont alatt említett oktatók, pedagógusok – tudatossága kulcsfontosságú a terület szempontjából. Amennyiben a gyermekek oktatásában, nevelésében szerepet vállaló személyek nem rendelkeznek a tudatos internethasználattal kapcsolatos információkkal, valamint ezek átadásának szándékával és képességével, úgy az súlyos következményekkel járhat. Ha ugyanis azon szereplők, akiknek az információátadásban kulcsszerepet kellene szánni, maguk sem bírnak a megfelelő kompetenciákkal, úgy természetesen részükről nem várható el azoknak a gyermekek részére történő közvetítése sem.
A szülők (a család) felelőssége, illetve szerepe tehát kiemelt jelentőségű a tudatosság területén; ahogyan a mindennapi életben, úgy az online világban is hasonló mértékű segítség, támogatás várható el (jogosan) a részükről. Sajnálatos módon azonban a tapasztalatok szerint a szülők jelentős része az internet tudatos használatával és az ott előforduló veszélyekkel nincsen teljes mértékben tisztában. A veszélyekkel kapcsolatos ismeretek hiánya mellett a szülők esetében jellemző még a passzivitás, a problémák elhárítása, melynek oka elsősorban a tekintélyvesztéstől való félelem.
A szülők vonatkozásában tett megállapítások az idősebb generációkkal (így elsősorban a nagyszülőkkel) kapcsolatban még inkább helytállóak. Tévhit azonban, hogy egy bizonyos kor felett már nem lehetséges az átmenet az offline állapotból az online „írástudás" felé. Az élethosszig tartó tanulás *(„lifelong learning")* nyugat-európai társadalmakban sikeres, államilag támogatott kezdeményezés és folyamat, melynek pozitív hatása nem csak az érintetteken mérhető. A tudatosság növelésében nagy segítséget jelenthetne, ha a nagyszülők is megismernék a gyermekek internethasználatának sajátosságait, ezzel kapcsolatos gondolkodásmódját és szokásaikat, a nagyszülők és unokáik kapcsolattartásában ugyanis szintén nagy szerepet játszik az internet. A nagyszülők egy része például

skype- és/vagy viberfelhasználó, így e kommunikációs csatornáknál is kiemelt figyelmet kell fordítani a biztonságra.

1.3.2 Pedagógusok

A fentiek értelmében – noha a gyermekek tudatosításának növelésében az elsődleges felelősség nyilvánvalóan a szülőé (illetve tágabb értelemben a közvetlen családi környezeté) – kiemelt szerep, feladat hárul a pedagógusokra is. A pedagógus ugyanis az a felnőtt személy, aki – például egy *cyberbullying* esetében – nemcsak az áldozattal, hanem gyakran az elkövetőkkel és tanúkkal is közvetlen kapcsolatban áll, így a konfliktus észlelésében és megoldásában egyaránt kulcsszereplő. A pedagógusok szerepe tehát megmutatkozik egyfelől az ismeretek átadásában, másfelől „munkaköri kötelessége" a tudatosság készségének birtokában lenni az oktatási rendszer keretei között működő vita- és konfliktuskezelési mechanizmusok aktív résztvevőjeként.
A tapasztalatok szerint sajnálatos módon igen kicsi azon pedagógusok aránya, akik a szükséges készségekkel rendelkeznek. Megemlítendő, hogy számos civil szervezet folytat képzéseket, amelyek nem kizárólag a gyermekek, de a pedagógusok ismereteinek bővítését is célozzák (például a MediaSmart Hungary Oktatási Közhasznú Nonprofit Kft., a Safer Internet Plus Program vagy a Digitális Tudás Akadémia).
Ezzel összefüggésben indokolt szót ejteni az óvodai pedagógusokról is, a gyermekek ugyanis gyakran már iskolás koruk előtt is kapcsolatba kerülnek okoseszközökkel, azokon keresztül pedig az online térrel. Számukra is léteznek programok, amelyek elősegítik felkészültségük növelését, ilyen például a Televele Médiapedagógiai Műhely Egyesület által adaptált csomag. Szintén e körben említhető a Luxemburgból adaptált Bibianeten weboldal is (www.bibianeten.hu), amelyet a Nemzetközi Gyermekmentő Szolgálat működtet.

A továbbképzés, szakirodalom, oktatási segédanyagok terén elért eredmények között megemlíthető, hogy az NMHH 2015-ben 500 pedagógusnak 30-30 órás továbbképzési lehetőséget biztosított, akik elsajátították a médiaértést és a média használatát elősegítő új készségeket. A témák között szerepelt a digitális társadalom kultúrája, a digitális készségek, a digitális biztonság és közbizalom, a tudatos médiafogyasztási szokások kialakítása, a médiakultúra elsajátítása, a tudatos fogyasztói kultúra, valamint a tudatos és felelős állampolgári magatartás. Az NMHH 2015 őszén adta ki hiánypótló médiaértési szakkönyv- és oktatófilmcsomagját.

1.3.3 Kortársak

Kiemelt szerep hárul a kortársakra, számos program bizonyítja ugyanis, hogy a gyermekek, illetve az idősebb fiatalok jelentős segítséget tudnak nyújtani egymásnak, és az így megszerzett tapasztalataik, tudásuk átadása révén az idősebb korosztálynak is.
E körben említhető a közösségi szolgálat lehetősége, amely keretében fiatalok segítenek kortársaiknak eligazodni többek között az internetbiztonság, a közösségi oldalak, az adatvédelem kérdéseiben (például ilyen szolgálatot működtet jelenleg középiskolás diákok közreműködésével a Nemzetközi Gyermekmentő Szolgálat).

1.4 A tudatosság növelésében részt vevő szereplők

A gyermekek, illetve az előző pont alatt említett egyéb szereplők tudatosságának növelésében az elsődleges szerepet nyilvánvalóan az oktatási rendszernek kell vállalnia. A feladat fontosságára és súlyára tekintettel ugyanakkor e célkitűzés megvalósításában jóval szélesebb társadalmi felelősségvállalás tapasztalható már jelenleg is; a jövőre nézve továbbra is szükségesnek mutatkozik a széleskörű összefogás fenntartása a területen. Ennek értelmében az alábbi szereplők segítsége mutatkozik mindenféleképpen nélkülözhetetlennek a valódi eredmények elérése érdekében:

- köznevelés;
- állami szféra egyéb szereplői;
- civil szervezetek;
- piaci szereplők;
- egyéb szakmai, érdekképviseleti szervek;
- média.

1.4.1 Köznevelés

A gyermekek tudatosságának növelésében kiemelt feladat hárul a köznevelés rendszerére. A köznevelés helyzetével kapcsolatos tapasztalatok, ismeretek illetve a pedagógusok tudatosságának bemutatása az 1.2. és 1.3.2. alpontok alatt olvasható.

1.4.2 Állami szféra szereplői

Az állami szereplők, hatóságok és a köznevelés területén kívül eső egyéb intézmények szintén kiemelt szerepet töltenek be a tudatosítás terén. E szervezetek

feladatuknak saját humán és anyagi erőforrásaik felhasználása révén képesek eleget tenni, amelyek kiterjedhetnek többek között:

- közérdekű hirdetések és kampányok médiában való közzétételére;
- tudatosító hálózat üzemeltetésére;
- pedagógusképzések támogatására;
- felmérések, kutatások lebonyolítására.

1.4.3 Civil szervezetek

A tudatosság növelésében kiemelt szerepet kapnak a civil szféra szereplői, akik a digitális világ okozta rohamos változásokat működési elveikből, cél- és eszközrendszerükből következően igen gyorsan le tudják reagálni. Említésre méltó, hogy a gyermekek internetbiztonságának kérdésében együttműködés alakult ki a civil szféra, az ipar és az iskolák között, ami azt bizonyítja, hogy a duális oktatásnak alapvető szerepe és jövője van a tudatosítás tekintetében.

A Nemzetközi Gyermekmentő Szolgálat 2009 óta konzorciumvezető partnere az Európai Unió Safer Internet programjának (www.saferinternet.hu). Szakértői konferenciákat és képzéseket szervez. Oktatói az egész ország területén tartanak ingyenes interaktív foglalkozásokat gyermekeknek, fiataloknak, pedagógusoknak, szülőknek és mindenkinek, aki többet szeretne megtudni a biztonságos internetezésről.

A Digitális Tudás Akadémia (www.digitalisiranytu.hu) önkéntes oktatói hálózatot hozott létre és a gyermekek mellett pedagógusoknak, valamint szülőknek tart előadásokat.

Az UNICEF Magyar Bizottság Alapítvány és a Telenor Magyarország 2013-ban az Ébresztő-óra program elindításával kezdte meg együttműködését. Az UNICEF mára több mint 100 fős képzett önkéntes csapata 90 perces – az iskolák számára ingyenes – interaktív iskolai foglalkozásokon mutatja be a gyermekeket illető különleges jogokat, köztük kiemelt témaként a gyermekeket érő erőszakhelyzeteket (ideértve a *cyberbullying* és a digitális biztonság témáit). A gyermekjogok ismerete fontos a közösségbe való beilleszkedés szempontjából is, ami a „digitális bennszülött” fiatalok körében a biztonságos és zaklatásmentes internetezés alapja is lehet. A két szervezet évente 2000 gyermek elérését tűzte ki célul, de az iskolák részéről jelentkező igények kielégítését követően két év alatt több mint 11 000 gyermek vehetett részt Ébresztő-óra előadáson szerte az országban.

A civil szervezetek a szükséges ismeret, tapasztalat birtokában számottevő eredményeket képesek elérni a tudatosítás terén (is), jövőbeli tevékenységük támogatása érdekében aktív állami szerepvállalásra van szükség.

1.4.4 Piaci szereplők

A piaci szereplők aktivitása leginkább – a saját, tudatosítást ösztönző programok folytatása mellett – a törvényi követelményként előírt szűrőszoftver elérhetőségére vonatkozó követelmények teljesítésében nyilvánul meg. Elmondható, hogy a piaci szereplők (internethozzáférés-szolgáltatók) többsége igyekszik aktivitást mutatni e téren.

1.4.5 Egyéb szakmai, érdekképviseleti szervezetek

Az egyes piaci szereplőket tömörítő, szakmai, érdekképviseleti szervezetek szerepe a tudatosítás terén szintén jelentősnek mondható. E szervezetek a tagságukat képező szolgáltatók koordinálásával képesek hatással lenni a tudatosítás folyamatára. Példaként említhetők a médiapiac területén működő ön- és társszabályozási szervezetek (például Magyar Elektronikus Műsorszolgáltatók Egyesülete, Önszabályozó Reklám Testület, Magyarországi Tartalomszolgáltatók Egyesülete, Magyar Lapkiadók Egyesülete), amelyek mindegyike önálló magatartási kódexszel rendelkezik, ezáltal orientálva a piaci szereplőket; ugyanígy említhető a hírközlés területén tevékenykedő Hírközlési Érdekegyeztető Tanács vagy az Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége.

1.4.6 Média

A média feladata, szerepe, felelőssége, befolyásolási képessége – amiképpen az élet elég sok területén – a tudatosság terén is vitathatatlan. Az általa közvetített tartalmak révén önmagában is orientálja nemcsak a fiatalabb korosztályt, hanem a teljes társadalomra is jelentős hatással bír. A gyermekek tekintetében e képesség fokozottan igaz: élettapasztalatuk hiányából, sérülékenységükből adódóan még inkább „kiszolgáltatott” helyzetben vannak a média (internet) hatásait illetően.

Kiemelten fontos, hogy a média (értve ez alatt jelen esetben nem kizárólag a „hagyományos” médiaszolgáltatókat, hanem az internet világát egyaránt) felismerve e felelősségét, lehetőségeinek megfelelően vállaljon szerepet a tudatosítás terén. Ez hasonlóan például a civil szervezetekhez, megmutatkozhat önálló programok indításában, az általuk sugárzott tartalmak kapcsán tanúsított általános körültekintésben, a tudatossággal kapcsolatos kampányok számára megfelelő felület biztosításában, illetve kifejezetten a tudatosítást növelni képes műsorok közvetítésén keresztül.

1.5 Jó gyakorlatok a tudatosítás és a médiaműveltség növelése terén

A gyermekek tudatos média- és internethasználata érdekében számos program, kezdeményezés létezik. A felhalmozott tudásnak és tapasztalatnak köszönhetően a tudatosítás érdekében folytatott „küzdelem” igen előrehaladott állapotban van; e források hatékony felhasználása révén megvalósíthatónak látszanak a megfelelő és szükséges kompetenciák átadására irányuló törekvések.

A korábbiakban már esett szó a tudatosítással foglalkozó egyes szervezetekről, programokról, gyakorlatokról, így e helyütt nem tűnik szükségesnek ezeket ismételten felsorolni. Ami viszont világosan megállapítható a jelenlegi helyzet értékelése alapján az az, hogy a társadalom különböző területein számos program fut párhuzamosan egymás mellett, komoly erőfeszítéseket téve a gyermekek tudatos internethasználata érdekében. Ezen a téren alapvető fontosságúnak mutatkozik a résztvevő szervezetek, intézmények munkájának elismeréseként e jó gyakorlatok állam általi támogatása, illetve a feladatvégzés hatékonyságának növelése céljából tevékenységük koordinációja.

2. Védelem és biztonság

Az internet használata életünk és mindennapjaink szerves részévé vált, amely során – sajnálatos módon egyre gyakrabban – a veszélyekkel, azok lehetőségével egyaránt szembe kell nézni. A jogrendszernek éppen ezért megfelelő választ kell adnia, ha az internethasználó (jelen esetben kiváltképpen a kiskorú, gyermekkorú) káros tartalommal találkozik, sérelmes, esetleg kifejezetten jogsértő helyzetbe kerül. Amiként a felmerülő veszélyek forrása, formája és hatása igen különböző lehet, úgy az ezekre adandó megfelelő válaszok is sokrétűek.

Elsősorban természetesen az államra hárul a feladat, hogy az internethasználat káros következményeivel szembeni kellő szintű védelmet, biztonságot a maga eszközeivel biztosítsa. E célkitűzés egyfelől a szükséges jogszabályi keret és annak érvényesülését biztosító szervezetrendszer kialakításában, másfelől a civil szféra e téren kifejtett munkájának támogatásában ölt testet. Ez utóbbi szervek a szabályok végrehajtásában legalább olyan fontos szerepet töltenek be, mint az állami szektor; a társadalmi, az ön- és társszabályozó szervezetek feladatvállalása sok esetben gyorsabb és közvetlenebb válaszokat eredményez a felmerült problémákra, még akkor is, ha a rendelkezésükre álló eszközrendszer első látásra nem is tűnik olyan hatékonynak.

Nyilvánvaló, hogy ezen intézményrendszer nem kizárólag, illetve nem specifikusan a gyermekek védelmét szolgálja, azonban már a jelenlegi környezetben is megtalálhatók azok a megoldások, technológiák, amelyek kifejezetten a fiatal generáció online biztonságát hivatottak szolgálni.

2.1 A gyermekeket veszélyeztető tartalmak az interneten, tapasztalatok és hatások

2.1.1 A gyermekeket veszélyeztető tartalmak

A) *Cyberbullying* (online megfélemlítés): az online tér egyik legnagyobb veszélyévé nőtte ki magát, amely sokkal eredményesebben és hatásosabban félemlíti meg az áldozatot, mint a fizikai erőszak. A gyakori elkövetési formák közé sorolható az érintett személyes adatainak hozzájárulás nélküli közzététele (például más nevében regisztrálás egy közösségi vagy társkereső oldalra, és ezen a felületen valótlan és sérelmes adatok közzététele), a gyermekről olyan felvétel feltöltése közösségi, videó-, illetve képmegosztó oldalra, amit tudta vagy engedélye nélkül kínos helyzetben készített róla valaki.

Az internetes megfélemlítés nemcsak a személyes adatok hozzájárulás nélküli közzétételében merülhet ki, hanem számos más formája létezik még. A legjellemzőbb típusai:

Flaming („égetés”): online veszekedés dühös és trágár nyelvezet használatával, illetve – sokszor nem az adott témába vágó – támadó jellegű hozzászólások küldése valakiről nyilvános fórumra.

Harassment (zaklatás): az internetes zaklatás alatt azt értjük, amikor sorozatosan és hosszabb ideig fennálló szándékos sérelemokozás áldozatává válik egy tinédzser az interneten vagy mobiltelefonon. Megvalósulhat sorozatosan támadó, sértő, felzaklató üzenetek küldésével, célja lehet a fiatal megalázása, fenyegetése, nevetségessé tétele, kiközösítése, lejáratása, negatív színben feltüntetése.

Denigation (befeketítés): kegyetlen, a hírnév rontására alkalmas pletykák vagy szóbeszéd küldése, kiposztolása, terjesztése valakiről.

Exclusion (kiközösítés): az online közösség egy tagjának csoportból való kirekesztése.

Outing (kibeszélés): titkok, pletykák vagy egyéb személyes információk engedély nélküli megosztása másokkal.

Trickery („trükközés”, becsapás): személyes adatok csalással, megtévesztéssel történő megszerzése valakitől, majd ezeknek az információknak, adatoknak a közösséggel való megosztása.

Cyberstalking (online megfigyelés): az áldozat online szokásainak megfigyelése, folyamatos figyelemmel kísérése és támadó jellegű kijátszása, fenyegető, megfélemlítő üzenetek küldése és ezek felhasználása félelemkeltésre, hogy a másik a saját biztonságát veszélyeztetve érezze.

Cyberthreats (online fenyegetések): olyan közvetlen fenyegetések vagy nyugtalanító kijelentések, amelyekből úgy tűnik, hogy a szerző érzelmileg felkavart, és fontolgatja, hogy valaki mást vagy magát bántja, illetőleg öngyilkosságot követ el.

Sexting (szexting): a szó „text” (szöveg) és a „szex” szavak összemosásával jött

létre. A kifejezést olyan helyzetekre használják, amelyekben az elkövető szexuálisan provokatív és saját maga által készített meztelen, vagy félig meztelen képeket, vagy nyíltan szexuális tartalmú szöveget küld el online valakinek. A legnagyobb figyelmet a meztelen képek küldése kapja, mert az ilyen felvételek további, széles körű terjesztése sokkal valószínűbb, és a fiatalokat nagyobb kockázatnak teszi ki.

B) Online pedofília: a megfélemlítés mellett a legsúlyosabb veszély, mely a gyermekeket fenyegetheti, az internetes pedofília. A hamis profilok mögé rejtőző személyek gyakran másnak (legtöbb esetben szintén gyermeknek) kiadva magukat próbálják meg a gyermekek jóhiszeműségét és naivságát kihasználni, hogy bizalmas kapcsolatot építhessenek ki velük. Sok esetben az online „találkozók" után személyes találkozóra is invitálják az áldozatot. A fenyegető veszélyt súlyosbítja, ha a gyermekek úgy találkoznak online ismerősökkel, hogy arról szüleiket nem tájékoztatják, és kísérő nélkül kerül sor a személyes találkozóra.

C) Pornográfia: szintén veszélyforrásként említendő az online pornográf tartalmakkal való találkozás. Egyes felmérések alapján hozzávetőlegesen tízből négy gyermek már járt pornográf tartalmú oldalakon. Kisgyermekek esetében akár egy kéretlen reklám, vagy akár egy rossz helyre történő kattintás után a pornográf tartalmak könnyen hozzáférhetőek. Másik fő problémaforrás a területen, hogy a szolgáltatók nem megfelelően vagy egyáltalán nem látják el a pornográf tartalmú oldalakat figyelmeztetéssel.

D) Erőszak, agresszió, kegyetlen bánásmód: az erőszakos, agresszív, véres és brutális, tartalmak szintén károsak a gyermekekre, és gyakran előfordulnak mindenféle figyelmeztetés, *metatag* elhelyezése nélkül. Ezek az oldalak gyakran tesznek közzé állatkínzással kapcsolatos tartalmakat, illetve buzdíthatnak öngyilkosságra is.

E) Függőség: az online játékok, kiváltképpen függőséget okozó hatásuk miatt különösen veszélyesek lehetnek. Egyre több olyan esetről hallani, amikor a gyermek szinte beleragad egy online térbe, egy játék online valóságába, miközben elkezdi kerülni a saját, valódi életét. A korlátok, határok nélküli internetezés szintén függőséghez, személyiségtorzuláshoz vezethet.

F) Közösségi média felületek negatív hatásai: a közösségi média aktív részévé vált a gyermekek mindennapjainak. Sok esetben ezeken a felületeken hamis képek,

ideák kerülnek a gyermekek elé, melyekről úgy vélhetik, hogy azok elfogadott normák, melyeket példaként követnek. A manipulált fotók által közvetített kép egyfajta megfelelési kényszert eredményez a gyermekek körében. Sok esetben nincsenek tisztában azzal, hogy egy-egy ilyen megosztott fotó nem teljesen a valóságot tükrözi. Szeretnének ők is hasonlóvá válni, így az állandó tartalommegosztás, az állandó megfelelési kényszer és a visszajelzések figyelése nem csak adatvédelmi, de pszichológiai veszélyeket is hordozhat magában.

G) Adatvédelmi visszaélések: bármilyen adatvédelmi szabály megszegése adatvédelmi visszaélésnek minősül. Ilyen például az online adathalászat *(phishing)*, amely egy, a felhasználók megtévesztését szolgáló módszer arra, hogy felfedjék személyes és pénzügyi adataikat félrevezető e-mail üzeneteken vagy webhelyeken keresztül.

A személyiséglopás olyan internetes bűncselekmény, mely az utóbbi években terjedt el, és nagyrészt az adathalászathoz és a közösségi oldalakhoz köthető. Nagyon veszélyes, mivel súlyos hatással lehet az áldozat további életére. Azzal, hogy az elkövetők ellopják áldozatuk személyiségét (minden személyes adatát, sok esetben bizalmas információkat is az áldozatról), például hitelt vehetnek fel a nevében. A Wi-Fi elterjedése óta a helyzet romlott, mivel a megfelelő eszközökkel könnyen megszerezhető minden adat.

Az adathalászat és a személyiséglopás gyakori jelenség. Ezeknek a veszélyeknek értelemszerűen azok a személyek a legfőbb célpontjai, akik sok információt, személyes adatot (képeket, felvételeket) osztanak meg magukról, illetve közösségi oldaluk mindenki számára hozzáférhető.

A kockázatos internetes tevékenységek közé sorolandóak még például a személyes adatok gondatlan közzététele, kecsegtető nyereményjátékokra történő regisztráció, amelyek könnyen adatvédelmi incidenseket idézhetnek elő.

H) Online szolgáltatások igénybevétele (fizetések), online játékok: szintén veszélyforrásként említendő az olyan fizetési felületek (általában online játékokhoz kapcsolódóan), ahol nincs különösebb kontroll a fizetés folyamata felett, és pár kattintással online fizetést lehet alkalmazni, szolgáltatást lehet igénybe venni, vagy szerződést lehet kötni, amelyből aztán (anyagi, fizetési) kötelezettségek keletkeznek. Ez a veszélyforrás legfőképp az online játékok terén kiemelkedő.

2.1.2 A veszélyekkel kapcsolatos tapasztalatok, hatások

A) Amit a gyermek sem akar látni

A gyermekek szerte a világban egyre fiatalabb korban kezdenek megismerkedni az online világgal és az online tér kínálta lehetőségekkel. Elmondható, hogy ahogy a felnőtteknél úgy a gyermekeknél is az élet számos területén kap főszerepet az internetezés. A lehetőség természetesen sok előnnyel is jár, azonban a gyermekekre leselkedő veszélyek felett sem szabad szemet hunyni.
Az Európai Bizottság Biztonságos Internet Program támogatásával, közel 25 országot érintő adatfelvétellel készült el az EU Kids Online nemzetközi tanulmánysorozat. A kutatássorozat alapjául szolgáló modell felvetése, hogy a gyermekek internetezése és az online világban töltött ideje egyaránt rejthet lehetőséget és kockázatokat. A tanulmánysorozat legfőképp a kockázati tényezők feltárására összpontosított.
A kutatás kimutatta, hogy a magyar gyermekek átlagosan 9 éves korukban kezdik el önállóan használni az internetet. A jelenlegi tendenciák alapján a jövőben ez az életkor csökkeni fog, feltételezhető, hogy 5-6 éves kor környékén fog stabilizálódni. A 9-16 éves korosztály 60%-a naponta használja az internetet, azaz rendszeres internetfelhasználó, míg 35% köré tehető azoknak a gyermekeknek az aránya, akik hetente egy-két alkalommal interneteznek. Ez a korosztály aktív tagja közösségi oldalaknak, kétharmaduk rendelkezik saját profillal közösségi oldalakon. Az is kimutatható, hogy ebben a korosztályban a közösségi oldalakat használó gyermekek között a lányok aránya magasabb.
A kutatásban vizsgált öt kockázatos tevékenység közül legalább eggyel a magyar 9-16 éves korosztály 37%-a találkozott már az online térben, és átlagosan 0,74 ilyennel volt tapasztalata a fiataloknak. A leggyakoribb online tevékenység az online ismerkedés, ezt a gyermekek 26%-a már megtette. A gyermekek 16%-a böngészett már olyan tartalmak között, melyek veszélyeket jelenthettek számára. A pornográf tartalmak böngészése ennek ellenére elenyésző, csupán minden tizedik gyermeknek van ilyen tapasztalata. A megkérdezett gyermekek közel 70%-a arról számolt be, hogy online megfélemlítés áldozata volt. Szexuális tartalmú képekkel, videókkal való találkozás a gyermekek 30%-át érintette, szexuális jellegű üzenetekkel és cselekvésekkel kapcsolatos tapasztalatról a gyermekek 29%-a számolt be. Legkisebb arányban, a gyermekek 9%-a vett rész olyan rossz tapasztalattal végződő „offline” találkozón, melyet online ismerkedés előzött meg.
A kutatás alapján elmondható, hogy a magyar gyermekek internetezési szokásai követik a nemzetközi trendeket. A gyermekek többségének rendelkezésre áll a megfelelő infrastruktúra és életük mindennapi részévé vált az internet

használata. Fontos hangsúlyozni, hogy a kockázatos tevékenységek tekintetében a legmeghatározóbb tényező a kor. Minél idősebb a gyermek, annál valószínűbb, hogy effajta kockázatos tevékenységgel találkozik.
A kockázatot rejtő tevékenységgel való találkozást megakadályozni sajnos nem lehet. Ennek ellenére fontos, hogy a kockázatot rejtő tevékenység minél ritkábban forduljon elő, illetve ezek a helyeztek jól kezelhetőek legyenek a gyermekek számára.

B) A látencia, a kár

Az online veszélyekkel kapcsolatos látencia, a kár nehezen számszerűsíthető, becsülhető. Arra vonatkozóan léteznek adatok, hogy arányaiban melyik veszélyforrással találkoznak a gyermekek gyakrabban, illetve azt lehet felmérni, hogy melyik veszély bekövetkeztének nagyobb a káros hatása. Például egy online megfélemlítés és egy esetleges tettlegességbe fajult személyes találkozás nyilvánvalóan ártalmasabb, mint egy pornográf felvétel megtekintése. Az arányok, a gyakoriság, a tendenciák a nemzetközi és hazai kutatási eredményekből kikövetkeztethető és megfigyelhető.

2.1.3 Védelmi lehetőségek

A) A védelmi mechanizmusok funkcionálása

Egységes védelmi mechanizmus kialakítása az említett veszélyforrásokkal szemben nem megoldható, hiszen például egy online kapcsolatfelvételt máshogy kell kezelni, mint egy online játékot vagy pornográf tartalmat, és megint másként az adatvédelemmel kapcsolatos visszaéléseket. Nagyon fontos, hogy az érintettek (gyermekek) ismereteit alapvetően bővíteni kell, hogy ezáltal felkészültebben tudjanak reagálni az egyes helyzetekre, önállóan jobban meg tudják szűrni, hogy mely helyzetek lehetnek veszélyesek, mely oldalak tartalmazhatnak számukra káros tartalmakat. A tudatosításnak, az oktatásnak ezért rendkívül jelentős funkciója van. Sokkal fontosabb, mint az „utómechanizmusként” funkcionáló védelmi vagy segítségnyújtást támogató intézményeknek.
A védelem mint önálló, önmagában lévő segítség nem lehet teljes körű, mindig lehetnek rések a pajzson. A veszélyek és azok forrásai folyamatosan bővülnek, jellegük gyorsan változik. Ezért az első fronton, az ismeretek bővítésénél kell jelentős eredményeket elérni.

B) A védelem és a tudatosítás kapcsolata

A fentiek miatt kijelenthető, hogy az első és a legfontosabb védelmet a tudatosítás által kell elérni. A gyermekekben ki kell alakítani egy olyan szemléletet, amellyel önmagukat lesznek képesek megvédeni – függetlenül bármilyen további intézményesített védelmi megoldástól, rendszertől.
Míg az online kapcsolatfelvétel esetén például el lehet sajátítani bizonyos kommunikációs sémákat, megoldásokat, fel lehet tenni bizonyos kérdéseket a beszélgetés során, amelyekkel nagyobb eséllyel kiszűrhető, hogy ki a beszélgetőpartner, addig egy videómegosztó felületen ez a megoldás már nehezebben vagy egyáltalán nem működik.

2.2 Milyen megoldásokkal szigetelhető el a gyermek a rá veszélyes tartalmaktól, más felhasználóktól?

Veszélytípusonként eltérő, hogyan lehet kiküszöbölni azokat. A veszélyes tartalmak kiszűréséhez – többek között – az alábbi lehetőségek állnak rendelkezésre:

- Szűrőszoftverek használata, oldalak célzott blokkolása;
- Figyelemfelhívó tájékoztatás elhelyezése az adott oldalon a káros tartalomhoz való hozzáférést megelőzően;
- A gyermek elsajátított önvédelmi mechanizmusa, amellyel már előre ki tudja szűrni azokat a tényezőket, amelyek sejtetik, hogy káros tartalom található az adott felületen.

Mindezen védelmi mechanizmusok ellenére is előfordulhat, hogy a gyermek káros tartalomhoz fér hozzá. A szülőknek és a pedagógusoknak nagy felelősségük van abban, hogy ilyen esetekben nyitottak legyenek, továbbá képesek legyenek a gyermekkel a látottakat, illetve azok rájuk gyakorolt hatását megbeszélni, ezzel is csökkentve a későbbi hátrányos következményeket, negatív beidegződéseket.

2.2.1 Példák a védelmi mechanizmusokra, megoldásokra

A) Védelmi mechanizmusok

- Online kapcsolatfelvétel esetében: kommunikációs sémák, tipikus kérdések elsajátítása.
- Pornográf felvételek, képek: figyelemfelhívó tájékoztatás elhelyezése a tartalom betöltését megelőzően, és a születési dátum verifikálásának kérése. Megjegyzendő azonban, hogy a születési dátum megjelölésének kérése a

továbblépés engedélyezése előtt nem nyújt elegendő biztonságot a gyermeknek, ugyanis aki meg szeretné nézni az adott tartalmat, az nyilvánvalóan úgy fogja megadni a születési dátumát, hogy a 18+ korosztályhoz tartozzon, és ezáltal hozzáférhessen a tartalomhoz. Lényeges kérdés ennek kapcsán az is, hogy mi a cél. Csupán a gyermek tájékoztatása arról, hogy milyen jellegű tartalom következik, vagy az, hogy a tartalomhoz való hozzáférést szüntessük meg, blokkoljuk bizonyos korosztály számára.

- Agresszív, erőszakos, kegyetlen, véres felvételeket, képeket közzétevő oldalak: ugyanaz, mint a pornográf felvételek esetében.
- Adatvédelmi visszaélések: szükséges a megfelelő előzetes adatvédelmi ismeretterjesztés. Az egyes felületeknek megfelelő adatvédelmi tájékoztatást kell elhelyezniük, és az adatkezelést jogszabályszerűen kell folytatniuk. Az illetékes szerveknek sokkal nagyobb hangsúlyt kell fektetniük az érintettek ismeretterjesztésére és az adatkezelés kampányszerű, átfogó vizsgálatára. Ismeretterjesztéssel elérhető, hogy minden érintett fontosnak tartsa profilja adatkezelési beállításainak időről-időre történő ellenőrzését, hogy kialakuljon egy olyan attitűd, mely alapján minimalizálja – vagy legalább ellenőrzött keretek között tartja – a megosztott személyes adatokat.
- Online játékok, internetezés, nárcizmus, megosztáskényszer és visszajelzés-függőség: megfelelő alternatíva mutatásával a szülőknek, kortársaknak, pedagógusoknak segítséget kell nyújtaniuk azon gyermekeknek, akiket a határtalan internetezés és játék veszélye fenyeget, az ugyanis függőséget okozhat, amelynek végső soron személyiségtorzító hatása lehet. Szükséges ehhez, hogy a problémáról és ennek veszélyéről otthon és az iskolában is beszéljenek, és tudjanak kihez fordulni segítségért.
- Online megfélemlítés (*cyberbullying*): kettős megközelítést igényel a probléma. Egyrészt ki kell alakítani a gyermekekben azt a szemléletet, hogy ne legyenek elkövetők, másrészt arra is fel kell készíteni őket, hogyan tudnak az ilyen helyzetekben a megfélemlítővel szemben fellépni, illetve egyéb segítséget igénybe venni. Ehhez szintén a tudatosítás és az oktatás, a megfelelő szocializáció szükséges. Az ismeretterjesztésnek szintén nagy szerepe van abban, hogy az érintettek tudják, kihez forduljanak segítségért ezekben az esetekben.

B) Védelmi megoldások

- Az adatvédelmi visszaélésekkel kapcsolatosan szükséges lenne elérni egy olyan állapotot, amelyben a szolgáltatók is olyan alapvető adatvédelmi beállítással bocsátják a felhasználók rendelkezésére egyes szolgáltatásaikat,

hogy azokat a legszigorúbb adatmegosztással, a legkevesebb adat nyilvánosságra hozatalával használják. Meg kell követelni a szolgáltatóktól, hogy megfelelően tájékoztassák a felhasználókat az adatkezelés valamennyi mozzanatáról.

- Online játékok, internetezés, nárcizmus, megosztáskényszer és visszajelzés-függőség esetén iskolapszichológus rendszeres jelenléte szükséges minden iskolában. Pusztán fogadóórák kiírása azonban nem elegendő, a pszichológiai kérdésekkel proaktív módon is foglalkozni kell az iskolákban. Legyenek ilyen témákkal kapcsolatos foglalkozások, világítsanak rá a pszichológiai tényezőkre.
- Online megfélemlítés (*cyberbullying*): Az iskolai pszichológiai beszélgetések során szintén érdemes foglalkozni a témával. Nagyon gyakori, hogy a gyermekek elvesztik a kontrollt a megfélemlítés hatására, teljesen elkeserednek, nem találják a megoldást és kifejezetten káros következmények alakulnak ki. Az efféle helyzetek kezelésének nagyon fontos eszköze lehet az iskolai mediáció rendszerszintű beépítése.
- Online fizetések: célszerű megkövetelni olyan fizetési, szolgáltatás-igénybevételi megoldásokat, amelyek verifikációt kívánnak, tehát amelyek nem eredményeznek azonnali kötelezettségvállalást. Ezek alapvetően fogyasztóvédelmi és polgári jogi kérdések, így ilyen esetekben szükséges garanciákat beépíteni az igényérvényesítési folyamatokba. Sajnos a csalások ellen nehéz fellépni, különösen, ha külföldi elem is beiktatódik az online szolgáltatás nyújtásába, és ezért például a szolgáltatás nyújtóját nehéz elérni.

Ezekhez az esetekhez kapcsolódóan is jelentős segítséget nyújthat az, ha a gyermekek megfelelően tájékozottak az ilyen veszélyek előfordulásáról, és például megnézik az adott szolgáltatás felhasználási feltételeit, leellenőrzik, hogy ki a szolgáltatás nyújtója, hol lehet elérni. Meg lehet tanítani a gyermekeknek, hogy melyek azok a fontos szempontok, amelyre ügyelniük kell egy online szolgáltatás (akár játék) igénybevétele során, és arra is, hogy figyelmesen olvassák el a felugró ablakokban szereplő információkat, mielőtt a továbblépés vagy „ok” gombokra kattintanak. Különösen fontos felhívni a figyelmüket, hogy bankkártya adatokat vagy egyéb fizetéshez kapcsolható adatokat szülői kontroll nélkül ne adjanak ki.

2.2.2 A védelem hazai megoldásainak rendszere

A hazai szabályozásban fellelhető megoldásokat alapvetően két csoportra oszthatjuk. Az előzetes, aktív védelmi hálót biztosító megoldások, illetve a jogi

kívánalmakat meghatározó, azoknak keretet adó, és a reparációt segítő (a már megtörtént problémákra reagáló, azt orvosolni kívánó) megoldások.
Az aktív megoldások közé sorolandó a szűrőszoftverek alkalmazása, a reklámozással kapcsolatos előírások, tartalom-besorolások, klasszifikáció, illetve az azok biztosításával kapcsolatos jogi kötelezettségek. Ezek látják el a gyermekek internetezés közbeni védelmét. Míg a reparatívak közé sorolhatóak a polgári jogi és büntető jogi szankciók olyan esetekben, amikor a jogsértés már megtörtént.
A gyermekek online védelmét szolgáló eszközök komplex rendszert alkotnak. E téren egyfelől megemlítendők az egyes jogágak által biztosított jogszabályi követelmények, amelyek egy része kifejezetten gyermekvédelmi előírásokat tartalmaz (például médiaszabályozás, reklámszabályok, Ekertv.), míg más normák nem kizárólag a kiskorúak védelmét szolgálják, ugyanakkor alkalmazhatók az ő védelmükben is (például polgári jogi személyiségvédelem, büntetőjog, adatvédelem). A jogszabályi környezethez kapcsolódóan említendők egyes, kifejezetten a gyermekek védelmét szolgáló mechanizmusok, jogintézmények (például szűrőszoftver, kiskorúak személyiségi jogait sértő tartalmak esetén alkalmazandó értesítési-eltávolítási eljárás), amelyek érvényesüléséhez nem fűződik szigorú állami kényszer.
Szintén az állami szféra oldalán jelennek meg azok az intézmények, amelyeket elsődlegesen (vagy kizárólag) a gyermekvédelem, azon belül is az online gyermekvédelem támogatása érdekében hívtak életre. E körben említhető a Gyermekvédelmi Internet-kerekasztal, az oktatási jogok biztosának, vagy az alapvető jogok biztosának gyermekjogi tevékenysége. Ez utóbbi szervezetek által végzett tevékenységek jellemzője, hogy jogi kötőerővel nem bíró megnyilvánulásaikkal, a nyilvánosság erejét felhasználva igyekeznek egyfelől a jogalkotó figyelmét felhívni a tapasztalt hiányosságokra, másfelől a piaci szereplőket a jogkövető magatartás felé orientálni.
A család- és gyermekjóléti szolgálatok a jelenlegi gyermekvédelmi rendszer egyik legfontosabb, folyamatosan bővülő szerepkörrel rendelkező elemét jelentik. Mellettük megemlítendők a TÁMOP-5.6.2-10 projekt keretében bűnmegelőzési koordinátor képesítést szerzett személyek, akiknek tudása és tapasztalata hasznosítható lehet a gyermekek védelmének területén.
A következőkben e szervek gyermekek védelmével kapcsolatos tevékenységét tekintjük át röviden.

A) Emberi Erőforrások Minisztériuma

A Kormány tagjainak feladat- és hatásköréről szóló 152/2014. (VI. 6.) Korm. rendelet értelmében a gyermekek és az ifjúság védelméért, a gyermek- és ifjúságpolitikáért, valamint az oktatásért az emberi erőforrások minisztere felelős.

E feladatok körében a miniszter felel a Kormány gyermekek védelmével kapcsolatos politikájának kialakításáért, figyelemmel kíséri a gyermeki jogok érvényesülését, ellátja a gyermekeket és a fiatal felnőtteket érintő szolgáltatásokkal kapcsolatos kormányzati feladatokat, meghatározza a gyermek- és ifjúságpolitikához tartozó területek szakmai felügyeleti rendszerét és annak működését. A miniszter az oktatásért való felelőssége keretében előkészíti az iskolai nevelés-oktatás szakképesítés megszerzésére felkészítő szakaszára, a köznevelésre, a felsőoktatásra vonatkozó jogszabályokat, egyúttal felel a Kormány oktatáspolitikájának kialakításáért.
Elérhetőség: www.kormany.hu/hu/emberi-eroforrasok-miniszteriuma

B) Nemzeti Fejlesztési Minisztérium

A nemzeti fejlesztési miniszter az audiovizuális politikáért, az elektronikus hírközlésért és az informatikáért is felelősséggel tartozik. Ennek körében – a vonatkozó jogszabályok előkészítésére irányuló kötelezettségei mellett – a miniszter az informatikáért való felelőssége keretében irányítja az infokommunikációs infrastruktúra-fejlesztési és szolgáltatási politika végrehajtását, az irányítása vagy felügyelete alatt álló költségvetési szervek és az olyan állami tulajdonban lévő gazdasági társaságok esetében, amelyek felett tulajdonosi vagy vagyonkezelési jogot gyakorol, illetve felügyeli azok infokommunikációs infrastruktúra eszközrendszerének üzemeltetését és fejlesztését.
A Nemzeti Fejlesztési Minisztérium készítette el a Nemzeti Infokommunikációs Stratégiát (2014-2020).
http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf
Elérhetőség: www.kormany.hu/hu/nemzeti-fejlesztesi-miniszterium

C) Belügyminisztérium

A belügyminiszter – mások mellett – felelős a bűncselekmények megelőzéséért, illetve a szabálysértési szabályozásért. A miniszter – jogszabályban meghatározott kivétellel – a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. útján központosított informatikai és telekommunikációs szolgáltatásokat nyújt, gondoskodik az igénybevevők informatikai és telekommunikációs eszközökkel történő ellátásáról és az ilyen eszközök működtetéséről.
Elérhetőség: www.kormany.hu/hu/belugyminiszterium

A Belügyminisztérium égisze alatt működik a Nemzeti Bűnmegelőzési Tanács,

amelyet a Kormány 1087/2011. (IV. 12.) Korm. határozattal hozott létre. Feladata a magas szintű közbiztonság megteremtése és fenntartása, a bűnözés visszaszorítása, a bűnözést kiváltó jelenségek, a bűnalkalmak és a bűnelkövetők ellen történő következetes fellépés érdekében tett intézkedések erősítése, továbbá a bűnmegelőzés új modelljének hatékony működtetése, valamint a bűnmegelőzés érdekében szükséges cselekvési tervek kidolgozásának és végrehajtásának koordinálása. A stratégia egyik legsokrétűbb prioritása a gyermek- és ifjúságvédelem, ezen belül külön stratégiai pontként szerepel a média és internet veszélye, amely magába foglalja a jó gyakorlatok felkutatását és támogatását, foglalkozások tartását, a jogalkotói folyamat segítését.
Elérhetőség: www.bunmegelozes.info

D) Nemzeti Kiberbiztonsági Koordinációs Tanács

A Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról 2013 végén döntött a Kormány [484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről]. A tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását ágazati és funkcionális kiberbiztonsági munkacsoportok segítik; e kifejezetten nevesített területek egyike a gyermekvédelem. A munkacsoport javaslatára a tanács jogi kötőerővel nem rendelkező ajánlásokat adhat ki a kibertámadások kezelése és az elektronikus információbiztonság területén alkalmazandó legjobb gyakorlatokról.

E) Bűnüldöző szervek

A rendőrség bűnfelderítési, bűnmegelőzési feladatkörében általános bűnügyi nyomozó hatósági jogkört gyakorol, végzi a bűncselekmények megelőzését, megakadályozását és felderítését, ezen túl gyakorolja a szabálysértési hatósági jogköröket.
Elérhetőség: www.police.hu

F) Ügyészségek

Az ügyészség az igazságszolgáltatás közreműködőjeként az állam büntetőigényét érvényesíti. Az ügyészség üldözi a bűncselekményeket, fellép más jogsértő cselekményekkel és mulasztásokkal szemben, valamint elősegíti a jogellenes cselekmények megelőzését. Az ügyész a vádemelés feltételeinek

megállapítása végett nyomozást végeztet, felügyeli a nyomozó hatóság önálló nyomozását, illetve a büntetőeljárási törvényben meghatározott esetekben a nyomozást maga végzi. Az ügyész gondoskodik arról, hogy a nyomozás során a büntetőeljárás résztvevőinek jogai érvényesüljenek.
Elérhetőség: www.ugyeszseg.hu

G) Bíróságok

Az igazságszolgáltatási tevékenység ellátása a bíróságok feladata. A gyermekek különféle „minőségükben" kerülhetnek kapcsolatba az igazságszolgáltatással: lehetnek egy eljárás során tanúk (bizonyos esetekben), sértettek vagy akár elkövetők. A gyermekközpontú igazságszolgáltatás rendszere az elérhető legmagasabb szinten biztosítja a gyermekek jogainak tiszteletben tartását és hatékony érvényesítését, elsődleges szempontként juttatja érvényre a részvételükkel folyó, vagy őket érintő minden ügyben a gyermekek érdekeit.
Elérhetőség: www.birosag.hu

H) Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH 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 forintig terjedő adatvédelmi bírságot is kiszabhat. Emellett feladata az információs jogokkal kapcsolatos tájékoztatás, ismeretterjesztés.
Elérhetőség: www.naih.hu

I) Nemzeti Média- és Hírközlési Hatóság

2014. május 15-én nyílt meg az NMHH Bűvösvölgy Médiaértés-oktató Központja (Budapest, Hűvösvölgyi út 95.). A megnyitás óta több mint 12 000 gyermek vett részt a tematikus foglalkozásokon, akik közül mintegy kétezren hátrányos vagy halmozottan hátrányos helyzetűek voltak, a résztvevő pedagógusok száma pedig nyolcszázra tehető. A központ feladata, hogy bemutassa a gyermekeknek, hogyan használhatják tudatosabban és a veszélyeket elkerülve a médiát. A központ egyes szakmai tevékenységei a TÁMOP-3.1.14-12-2013-0001 sz. „A

Jövő tudatos médiafogyasztói – médiaműveltség és médiatudatosság elterjesztése" című projekt keretében valósultak meg. A hatóság üzemelteti továbbá az Internet Hotline szolgáltatást, amely lehetőséget biztosít az interneten található jogellenes, illetve a kiskorúak számára káros tartalmak bejelentésére.
Elérhetőség: www.nmhh.hu, www.buvosvolgy.hu

J) Nemzeti Média- és Hírközlési Hatóság Médiatanácsa

A Médiatanács hatósági felügyeletet gyakorol a médiaszabályozás gyermekek és kiskorúak védelmére vonatkozó előírásainak (Mttv. 9–11. §; Smtv. 19. §) érvényesülése tekintetében. E hatáskörével kapcsolatosan ajánlást bocsát ki a kiskorúak védelme érdekében előírt klasszifikációval, továbbá a kizárólag tizennyolc éven felüli nézők vagy hallgatók számára elérhetőséget biztosító hatékony műszaki megoldás követelményeivel összefüggésben. A konkrét (hatósági) hatáskörök mellett kezdeményező szerepet vállal a médiaműveltség, a médiatudatosság magyarországi fejlesztésében, ennek keretében összehangolja más állami szereplők médiaműveltségéhez kapcsolódó tevékenységét, segíti a Kormányt az Európai Unió felé e tárgyban esedékes időszakos beszámoló elkészítésében (Mttv. 132. § *k)* pont).
Elérhetőség: www.mediatanacs.hu

K) Gyermekvédelmi Internet-kerekasztal

A kerekasztal az NMHH elnökének huszonegy tagú, javaslattevő, véleményező, tanácsadó testülete, amelynek létrehozásáról az Ekertv. 2014. január 1. napjával hatályba lépett előírásai rendelkeztek (4/A–D. §). A kerekasztal kötelező erővel nem bíró, a médiatartalom-szolgáltatók, az elektronikus kereskedelmi szolgáltatók és az elektronikus hírközlési szolgáltatók jogkövető magatartását elősegítő ajánlások, állásfoglalások kiadására jogosult, feladata továbbá a kiskorúak és szüleik médiatudatosságát növelő intézkedések kezdeményezése. A testület a hozzá beérkezett bejelentések alapján jogosult egyedi ügyeket is megvizsgálni, és azok általánosított tapasztalatai alapján kötelező erővel nem rendelkező ajánlást vagy állásfoglalást kiadni.
Elérhetőség:
gyermekbarat.nmhh.hu/tart/index/1624/Gyermekvedelmi_Internetkerekasztal

L) Alapvető Jogok Biztosának Hivatala

Az alapvető jogok biztosa tevékenysége során – különösen hivatalból folytatott

eljárások lefolytatásával – megkülönböztetett figyelmet fordít a gyermekek jogainak védelmére. Az alapvető jogok biztosa a hatóságok tevékenysége során felmerült, az alapvető jogokkal kapcsolatos visszásságok megszüntetése érdekében hivatalból eljárást folytathat. A hivatalból indított eljárás természetes személyek pontosan meg nem határozható, nagyobb csoportját érintő visszásság kivizsgálására vagy egy alapvető jog érvényesülésének átfogó vizsgálatára irányulhat (Ajbt. 18. § (4) bek.).
Elérhetőség: www.ajbh.hu

M) Oktatási Jogok Biztosának Hivatala

Az oktatási jogok biztosának életre hívásáról az Oktatási Jogok Miniszteri Biztosa Hivatalának feladatairól és működésének szabályairól szóló 40/1999. (X. 8.) OM rendelet rendelkezik. A biztos – az általa vezetett hivatalon keresztül – a gyermeket, a tanulót, a hallgatót, a kutatót, a pedagógust, az oktatót, a szülőt, valamint azok közösségeit megillető, oktatással kapcsolatos állampolgári jogok érvényesülésének elősegítésében működik közre (1. § (1) bek.). A biztos eljárásának tárgya lehet olyan egyedi ügyben hozott határozat vagy intézkedés, valamint határozat (intézkedés) elmulasztása, amely bizonyos, a gyermek, a tanuló, a szülő, a pedagógus, a hallgató, a kutató, illetve az oktató számára biztosított jogokat sért, vagy a sérelem közvetlen veszélyét idézi elő. Azonos védelemben részesülnek a gyermekek, a tanulók, a szülők, a pedagógusok, a hallgatók, a kutatók és az oktatók közössége számára törvényben biztosított jogok is (3. §).
Elérhetőség: www.oktbiztos.hu

N) Gyermekvédelmi intézmények

A Gyvt. értelmében a gyermeki jogok védelme minden olyan természetes és jogi személy kötelessége, aki a gyermek nevelésével, oktatásával, ellátásával, törvényes képviseletének biztosításával, ügyeinek intézésével foglalkozik (11. § (1) bek.). A jogszabály a gyermeki jogok érvényesülését számos intézményen keresztül igyekszik biztosítani, ilyenek többek között a gyermekvédelmi gyám, továbbá a gyermekjogi képviselő intézménye, a bentlakásos gyermekintézmények, család- és gyermekjóléti központok, a gyermekotthonok, illetve a javítóintézetek.

O) Civil (érdekvédelmi) szervezetek

A társadalmi szervezetek igen széles köre tevékenykedik gyermekvédelem terén, jelentős részük foglalkozik speciálisan a gyermekek és a média, illetve az internet kapcsolatából adódó feladatokkal, segítségnyújtással, oktatással. E körben – a teljesség igénye nélkül – megemlítendő a Nemzetközi Gyermekmentő Szolgálat, a Kék Vonal Gyermekkrízis Alapítvány, az Eszter Alapítvány, a Hintalovon Alapítvány, a Nagycsaládosok Országos Egyesülete, a Médiaunió Alapítvány, a Gyermekmédia Egyesület, a Médiasmart Közhasznú Nonprofit Kft., az Egyszervolt Alapítvány, az Országos Gyermekvédő Liga, a Digitális Tudás Akadémia és az UNICEF Magyar Bizottság Alapítvány.
Elérhetőségek: www.gyermekmento.hu, www.kek-vonal.hu, www.eszteralapitvany.hu, www.hintalovon.hu, www.noe.hu, www.mediaunio.hu, www.gyermekmedia.eu, www.mediatudor.hu, www.egyszervolt.hu, www.ogyl.hu, http://digipedia.hu, www.unicef.hu

2.3 A szűrőszoftverek és az internetes tartalom-megjelölés

2.3.1 A hatályos szabályozás

A) A szűrőszoftverre vonatkozó követelmények

Az Eht. az internethozzáférés-szolgáltatóktól megköveteli, hogy honlapjukon bárki számára ingyenesen tegyenek elérhetővé a kiskorúak védelmét lehetővé tevő (magyar nyelvű, könnyen telepíthető és használható) szűrőszoftvert (149/A. §). Ehhez kapcsolódó előírás, hogy az előfizetői szolgáltatásokat nyújtó hírközlési szolgáltató általános szerződési feltételeiben szerepelnie kell a szűrőszoftverek, illetve az azokkal egyező célra szolgáló más szolgáltatások elérhetőségére és használatára vonatkozó tájékoztatásnak (131. § (1) bek. *l)* pont). Az internethozzáférés-szolgáltatást nyújtó szolgáltató továbbá köteles a szűrőszoftverek vagy azokkal egyező célra szolgáló más szolgáltatások elérhetőségére és használatára vonatkozó közérdekű tájékoztatót összeállítani, a tájékoztatót internetes honlapján közzétenni, a közzétételről és annak elérhetőségéről negyedévente az előfizetőt értesíteni (144. § (2a) bek.).
A nyilvános könyvtár az általa üzemeltetett, kiskorúak által is használható, míg a köznevelési intézmény a tanulók számára hozzáférhető, internet-hozzáféréssel rendelkező számítógépek használatát, a kiskorúak védelmét lehetővé tevő, könnyen telepíthető és használható, magyar nyelvű szoftverrel ellátva biztosítja a kiskorúak lelki, testi és értelmi fejlődésének védelme érdekében (1997. évi CXL. törvény a muzeális intézményekről, a nyilvános könyvtári ellátásról és a közművelődésről, 55. § (1a) bek.; Köznev. tv. 9. § (11) bek.).

B) Internetes tartalmak klasszifikációja

A fentiek mellett a médiaszabályozás szerinti médiatartalomnak nem minősülő azon internetes tartalmakat, amelyek súlyosan károsíthatják a kiskorúak egészséges fejlődését, a szolgáltató kizárólag e tényre történő figyelemfelhívás mellett teheti közzé. Mindemellett a hatályos törvényi előírások e klasszifikációs kötelezettség alkalmazása által azt is biztosítják, hogy a kiskorúak fejlődésére káros internetes tartalmak az előzőekben említett szűrőszoftver révén felismerhetők – és ezáltal szűrhetők – legyenek (Ekertv. 4/A. § (1) bek.).

A törvény által előírt követelményeknek jelenleg csak egyetlen cég által biztosított szoftver felel meg, azonban ez sem használható valamennyi operációs rendszeren. E probléma mellett azt is meg kell említeni, hogy miután semmi nem kötelezi a szoftver szolgáltatóját az ingyenességre, azt bármikor fizetőssé teheti, igencsak megnehezítve a törvényi előírásoknak való megfelelést. A szűrőszoftverekkel kapcsolatos egyéni visszajelzések alapján megállapítható, hogy a szűrőszoftverek nem alkalmazhatóak teljeskörűen, nem működnek teljes biztonsággal, és nem képesek valamennyi beállított káros tartalom kiszűrésére. Szintén probléma, hogy a szülő nem ismeri, nem tudja, hogyan kell megfelelően beállítani a szűrőszoftvert, és azt sem tudja, hogy ehhez kitől kérjen segítséget. Megállapítható továbbá, hogy a gyermekek gyakran jobban tudják alkalmazni a szűrőszoftvert, ennél fogva azt ki is tudják iktatni, tehát tényleges célját nehezen képes elérni.

Az említett követelmények érvényesülését az NMHH elnökének tanácsadó szerveként életre hívott Gyermekvédelmi Internet-kerekasztal – mint a médiatartalom-szolgáltatásban közzétett médiatartalmak mellett az elektronikus kereskedelmi szolgáltatás és az elektronikus hírközlési szolgáltatás útján hozzáférhető információk tekintetében meglévő, a kiskorúak védelmét célzó jogszabályi előírások hatékony érvényesítését, továbbá a médiatudatosság növelését elősegítő, támogató testület – kíséri figyelemmel. A kerekasztal hatósági hatáskörökkel nem rendelkezik, tevékenységének ellátása során a szolgáltatók jogkövető magatartását elősegítő – de kötelező erővel nem bíró – ajánlásokat, állásfoglalásokat adhat ki (Ekertv. 4/D. § (1) bek.).

2.3.2 A szűrőszoftver-fejlesztés támogatása

Az Eht. rögzíti, hogy az NMHH pályázati úton anyagi támogatást nyújthat az internethozzáférés-szolgáltatást nyújtó szolgáltatónak azon kötelezettség

teljesítéséhez, miszerint honlapjukon biztosítani kötelesek a szűrőszoftver ingyenes elérhetőségét és használhatóságát, amennyiben:

- A szűrőszoftver megfelel a Gyermekvédelmi Internet-kerekasztal ajánlásaiban foglalt követelményeknek;
- A szűrőszoftver a lakossági felhasználók, egyéni előfizetők általi használat mellett alkalmas azon nyilvános könyvtárak és köznevelési intézmények általi használatra is, amelyeknek törvényben előírt kötelezettsége az általuk nyújtott közszolgáltatásokat igénybe vevő kiskorú gyermekek internet-használatához szűrőszoftvert biztosítani;
- Az internethozzáférés-szolgáltatást nyújtó szolgáltató vállalja, hogy az előző pontban megjelölt intézmények részére közvetlenül vagy más szolgáltató közreműködésével a szűrőszoftverhez való hozzáférést ingyenesen biztosítja.

A pályázati eljárás lefolytatása az NMHH elnökének hatósági hatáskörébe tartozik, a pályázati eljárás részletes szabályait az elnök a gyermekvédelmi szűrőszoftverek biztosításával kapcsolatos kötelezettség teljesítésének anyagi támogatását szolgáló pályázat szabályairól szóló 4/2014. (VI. 18.) NMHH rendeletben határozta meg.

2.3.3 A szűrőszoftver gyakorlati alkalmazásának tapasztalatai

Az alapvető jogok biztosának AJB-479/2016. számú, a médiaértés-oktatás hazai helyzetéről készült jelentése szerint – hivatkozva a Nemzetközi Gyermekmentő Szolgálat elnökének beszámolójára – problémát jelent a szűrőszoftverek kapcsán, hogy nincsen olyan ismert és megfelelően transzparens minta, ajánlás, amely felhasználható lenne a köznevelési intézményekben, továbbá a szoftverekkel kapcsolatos költségek megoszlása, karbantartása vitatott, ahogyan az is, hogy milyen kifejezésre szűrjön a program. Az iskolák legtöbbször az iskolai internet-hozzáférés drasztikus korlátozását választják.

2.3.4 A Gyermekvédelmi Internet-kerekasztal ajánlása

Említést érdemel, hogy a kerekasztal a kiskorúakra káros internetes tartalmak és szolgáltatások esetén alkalmazandó figyelemfelhívó jelzésekre és szűrőszoftverekre vonatkozóan az Eht. 149/A. § (2) bekezdésében biztosított felhatalmazás alapján ajánlást fogadott el. Az ajánlás a figyelemfelhívó jelzések kapcsán az alábbi megoldásokat javasolja:

- A forráskódban elhelyezett *metatag* egyértelműen utaljon a tartalom kiskorúakra káros voltára (például *age*=18);
- A tartalomszolgáltató a tartalom elérésére szolgáló oldal megjelenítését megelőzően, illetőleg annak tartalmát bemutató tartalomjegyzékben vagy más

felületen (például a tartalomra mutató URL címsorában), jól látható módon, optikai azonosítással utaljon a kiskorúakra káros tartalomra;
- A tartalomszolgáltató a tartalom megjelenítése előtt ellenőrizze a felhasználó életkorát, a tartalom megtekintésére való jogosultságát (például jelenítsen meg egy kérdést, amelyben a néző életkorát ellenőrzi: *„Ön elmúlt már 18 éves? Igen – Nem”*). Ha az életkor-ellenőrzés alapján a felhasználó nem jogosult megtekinteni a tartalmat, akkor a tartalom letöltésére, elérésére ne legyen lehetőség;
- A tartalomszolgáltató az életkor-ellenőrzéssel egyidejűleg, azonos helyen, jól láthatóan hívja fel a felhasználó figyelmét a kiskorúakra vonatkozó veszélyekre, például az alábbi szöveg megjelenítésével: *„Figyelem! Ez a tartalom kiskorúakra káros elemeket is tartalmaz. Amennyiben azt szeretné, hogy az Ön környezetében a kiskorúak hasonló tartalmakhoz csak egyedi kód megadásával férjenek hozzá, kérjük, használjon szűrőprogramot. Szűrőprogram letöltése és további információk itt.”*

Az ajánlás a gyermekvédelmi szűrőszoftverekkel szemben támasztott követelményekkel kapcsolatban az alábbi területeken fogalmaz meg javaslatokat:
- A szűrőszoftver-megoldások elérhetősége és alkalmazásuk hatóköre;
- A szűrőszoftver-megoldások telepítése, beállítási lehetőségeik;
- Az online tartalmak elérhetősége korlátozásának módja;
- A kiskorúak interneten végzett tevékenységeinek monitorozása, riasztások.

2.3.5 Az ajánlásban foglaltak érvényesülésének vizsgálata

A Gyermekvédelmi Internet-kerekasztal a mintegy 120 – kiskorúakra káros tartalmakat is nyújtó – honlapra kiterjedő, 2014 végén, illetve 2015 elején lefolytatott vizsgálat eredményei alapján a 2015. június 17-i ülésén úgy döntött, hogy levélben szólítja fel az érintett tartalomszolgáltatókat a vonatkozó törvényi előírások és a kerekasztal szűrőszoftver-ajánlásának betartására.

A) A korábbiakban figyelemfelhívó jelzéseket már részlegesen alkalmazó tartalomszolgáltatókkal kapcsolatos megállapítások: a vizsgálat 85 olyan tartalomszolgáltatóra terjedt ki, amelyek már az első vizsgálat során is elhelyeztek valamilyen figyelmeztető jelzést a kiskorúakra káros tartalmak megjelenítése előtt. Az első és az ellenőrző vizsgálat során az alábbi figyelmeztető elemek meglétét, és alkalmasságát ellenőrizték:
- Forrás-file-ban *metatag* megléte, amely segítségével a szűrőszoftverek könnyen kiszűrhetik a kiskorúakra káros tartalmakat;

- Kiskorúakra káros tartalmakra figyelmeztető szöveg, továbbá életkor-ellenőrzés;
- Figyelem felhívása a szűrőszoftver alkalmazására, illetve szűrőszoftverre mutató link megléte.

A vizsgálat az alábbi eredményeket hozta:

- Az első vizsgálatkor a szolgáltatók mindössze 8%-a alkalmazott *metatag*-et a kiskorúakra káros tartalmak megjelenítése előtt. A kiküldött levél hatására a szolgáltatók számos honlap esetén elkezdték alkalmazni a *metatag*-eket, így a korábbi arány 26%-ra emelkedett.
- A honlapon a figyelemfelhívó jelzések elhelyezésében nem volt tapasztalható jelentős változás. Ugyanakkor megállapítható volt, hogy az érintett honlapok mintegy 75%-ánál tekinthetők elfogadhatónak a figyelemfelhívó jelzések. Ez nem azt jelenti, hogy teljesen megfeleltek az ajánlásnak, de legalább a kor ellenőrzése előtt nem jelent meg semmilyen kiskorúakra káros tartalom.
- A szűrőszoftverekre történő utalás az első vizsgálatkor a honlapok mindössze 22%-ánál volt megfigyelhető. Ez az arány lassú emelkedésnek indult. Jelenleg 34% esetén van utalás a szűrőszoftverre.

A második vizsgálatot követően is probléma volt, hogy a szolgáltatók által alkalmazott figyelemfelhívó jelzések rendkívül szerteágazóak, nem voltak egységesek és egyértelműek, ami megnehezítheti a szülők számára a káros tartalmakkal kapcsolatos veszélyek tudomásul vételét, és a szűrőszoftverek alkalmazása iránti igény kialakulását.

B) A korábbiakban figyelemfelhívó jelzéseket egyáltalán nem alkalmazó tartalomszolgáltatókkal kapcsolatos megállapítások: tekintettel arra, hogy az ebbe a csoportba tartozó mintegy 30 tartalomszolgáltató egyáltalán nem alkalmazott a korábbiakban semmilyen figyelemfelhívó jelzést, ők egységes tartalmú levelet kaptak a kiskorúakra káros tartalmak esetén alkalmazandó szabályok betartása kapcsán. Esetükben sajnos lényegesen rosszabbak lettek az eredmények, mint a valamilyen figyelemfelhívást már korábban is használó szolgáltatók esetében:

- Megállapítható, hogy körülbelül minden hetedik szolgáltató tett eleget a levélben szereplő felhívásnak. Ennek megfelelően a korábbi nullához képest 16% alkalmazott *metatag*-et, illetve helyezett el figyelemfelhívást a kiskorúakra káros tartalmak megjelenítése előtt;
- Szűrőszoftver használatára a honlapok mintegy 13%-a hívta fel a figyelmet, és ők ezzel egyidejűleg egy szűrőszoftverre mutató linket is szerepeltettek.

2.4 A gyermekek jogainak védelme a hatályos jogrendszerben

2.4.1 Nemzetközi jogszabályi háttér

Az ENSZ égisze alatt született, a Gyermek jogairól szóló, New Yorkban, 1989. november 20-án kelt Egyezmény 1. cikke szerint az egyezmény vonatkozásában gyermek az a személy, aki tizennyolcadik életévét nem töltötte be, s mint ilyet, kiemelt védelem illet meg. Az egyezmény 19. cikke kimondja a gyermekekkel szembeni erőszak minden formájától való tilalmat.

2.4.2 Alkotmányos háttér

A hazai jogrendszer alapját képező Alaptörvény XVI. cikk (1) bekezdése értelmében minden gyermeknek joga van a megfelelő testi, szellemi és erkölcsi fejlődéséhez szükséges védelemhez és gondoskodáshoz.

2.4.3 Polgári jog

A Ptk. Második Könyve foglalkozik a személyiségi jogok védelmével, amelynek körében általános jelleggel kimondja, a személyiség, az emberi méltóság védelmét (2:42. § (1) bek.: „Mindenkinek joga van ahhoz, hogy törvény és mások jogainak korlátai között személyiségét, így különösen a magán- és családi élet, az otthon, a másokkal való - bármilyen módon, illetve eszközzel történő - kapcsolattartás és a jóhírnév tiszteletben tartásához való jogát szabadon érvényesíthesse, és hogy abban őt senki ne gátolja.”).
A Ptk. külön nevesíti a magánélet, a becsület, a jóhírnév, a személyes adatok, a magántitok, a képmás és a hangmás védelmét (2:43. §: „A személyiségi jogok sérelmét jelenti különösen az élet, a testi épség és az egészség megsértése; a személyes szabadság, a magánélet, a magánlakás megsértése; a személy hátrányos megkülönböztetése; a becsület és a jóhírnév megsértése; a magántitokhoz és a személyes adatok védelméhez való jog megsértése; a névviseléshez való jog megsértése; a képmáshoz és a hangfelvételhez való jog megsértése.”). Ezeknek az intézményeknek a megsértése esetén a polgári jog eszközeivel fel lehet lépni, és a megfelelő szankciókat (kártérítés, sérelemdíj, jogsértő magatartás abbahagyására kötelezés stb.) igénybe lehet venni (2:51-2:53. §). A személyiséget nem csupán a való életben, hanem a digitális térben is meg lehet sérteni, és a jogsérelmet szenvedett felek között gyermekek is előfordulhatnak.
Az internetes veszélyforrásokból jogsérelem is kialakulhat, amelyet a polgári jog személyiségvédelmi részének keretei között lehet értelmezni, illetve reparálni.

Ahhoz, hogy a gyermekek is meg tudják védeni személyiségüket, szükséges, hogy ők és szüleik (törvényes képviselőik) ismerjék a polgári jog adta védelmi rendszert, a bírósági jogérvényesítés módját, lehetőségeit, de mindezeket megelőzően alanyi jogaikat. A jogok ismeretterjesztése tehát a védelemre irányuló fellépést megelőző állomás. Ezt az iskolai oktatásba szükséges beépíteni.
Ide kapcsolódóan megemlítendő azon speciális törvényi lehetőség, amely a kiskorúak személyiségi jogait sértő tartalmak online térből való egyszerűbb és hatékonyabb eltávolítását teszi lehetővé, megelőzve, illetve kiegészítve a polgári- és büntetőeljárások biztosította eljárásrendeket (Ekertv. 13. § (13)–(15) bek.).

2.4.4 Büntető- és szabálysértési jog

A büntetőjog keretein belül számos cselekmény nyert értékelést. A digitális térben való léttel kapcsolatban kiemelendőek a következő büntetőjogi tényállások:

- gyermekpornográfia
  (Btk. 204. §: aki a 18. életévét be nem töltött személyről pornográf felvételt készít, kínál, átad, megszerez, forgalomba hoz, azzal kereskedik. hozzáférhető teszi azt vagy tárolja az a személy bűncselekményt követ el);
- személyes adattal visszaélés
  (Btk. 219. §: ha egy állampolgár személyes adatait – például nevét, telefonszámát, lakcímét, fényképét – az érintett hozzájárulása, jóváhagyása nélkül teszik közzé);
- zaklatás
  (Btk. 222. §: ha valakivel, annak akarata ellenére más, mobiltelefonon, interneten, közösségi oldalakon vagy személyesen rendszeresen kapcsolatba akar lépni, őt zaklatják);
- magántitok megsértése
  (Btk. 223. §: aki a foglalkozásánál vagy közmegbízatásánál fogva tudomására jutott magántitkot alapos ok nélkül felfedi, ezzel jelentős érdeksérelmet okoz);
- levéltitok megsértése
  (Btk. 224. §: másnak közlést tartalmazó zárt küldeményét megsemmisíti, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, illetve elektronikus hírközlő hálózat útján másnak továbbított közleményt kifürkész);
- rágalmazás
  (Btk. 226. §: aki valakiről más előtt a becsület csorbítására alkalmas tényt állít, híresztel, vagy ilyen tényre közvetlenül utaló kifejezést használ);
- becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése
  (Btk. 226/A. §: aki abból a célból, hogy más vagy mások becsületét csorbítsa,

hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt készít);

- becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala
  (Btk. 226/B. §: aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt hozzáférhetővé tesz);
- becsületsértés
  (Btk. 227. §: a sértett munkakörének ellátásával, közmegbízatásának teljesítésével vagy közérdekű tevékenységével összefüggésben vagy nagy nyilvánosság előtt a becsület csorbítására alkalmas kifejezést használ, vagy egyéb ilyen cselekményt követ el);
- tiltott adatszerzés
  (Btk. 422.§: aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából:
  - más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
  - más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti,
  - más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
  - elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti);
- információs rendszer vagy adat megsértése
  (Btk. 423. §: aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad);
- információs rendszer védelmét biztosító intézkedés kijátszása
  (Btk. 424. §: aki jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja).

A Btk. mellett a szabálysértési törvény is tartalmaz tényállást, amely kiskorúak sérelmére (is) elkövethető online módon

- veszélyes fenyegetés
  (Szabs. tv. 173. §: aki mást félelemkeltés céljából a megfenyegetett személyre vagy annak hozzátartozójára vonatkozó, a becsület csorbítására alkalmas

tény nagy nyilvánosság elé tárásával komolyan megfenyeget).
Az egyes bűncselekmény-típusok elkövetésével kapcsolatos statisztikai adatok az 1. sz. mellékletben olvashatóak.

2.4.5 Médiaszabályozás

Az Mttv. rögzíti, hogy a lekérhető médiaszolgáltatás médiaszolgáltatójának vagy a szolgáltatását terjesztő műsorterjesztőnek hatékony műszaki megoldást kell alkalmaznia annak érdekében, hogy a tizennyolc éven aluliak fejlődését kedvezőtlenül befolyásolni képes műsorszámok kiskorúak számára ne legyenek elérhetők (emellett az V-VI. korhatári kategóriába tartozó műsorokat megfelelő minősítéssel is el kell látniuk). A hatékony műszaki megoldások tekintetében a Médiatanács – élve az Mttv. adta felhatalmazással – ajánlást tett közzé, a tapasztalatokat felhasználva pedig az abban foglalt javaslatokat, iránymutatásokat rendszeresen felülvizsgálja (Mttv. 11. § (1)–(3) bek.). Az ajánlás – többek között – kitér a digitális műsorterjesztési szolgáltatás keretében nyújtott lekérhető médiaszolgáltatások esetén alkalmazott gyermekzár megoldásokra (ajánlás IV. 4. pont), emellett a mobil hírközlési szolgáltatásokat nyújtó szolgáltatók által biztosított, illetve a vezetékes és mobil internet-hozzáférésen elérhető lineáris és lekérhető médiaszolgáltatások esetén alkalmazott hatékony műszaki megoldásokra (ajánlás V–VI. pontok).
A törvény értelmében a kiskorúak fejlődését súlyosan károsító médiatartalom lekérhető médiaszolgáltatásban csak abban az esetben tehető közzé, ha biztosított, hogy a kiskorúak rendes körülmények között nem férhetnek hozzá. Ehhez hasonlóan a sajtótermékben szintén korlátozni kell a kiskorúak hozzáférhetőségét, illetve azok csak a lehetséges veszélyről való tájékoztatást tartalmazó figyelmeztető jelzéssel tehetők közzé (Smtv. 19. § (2)–(3) bek.). Ilyen tartalomnak minősül az Smtv. értelmében a kiskorúak szellemi, lelki, erkölcsi vagy fizikai fejlődésének káros befolyásolására alkalmas azon médiatartalom, amely pornográfiát vagy szélsőséges, illetve indokolatlan erőszakot tartalmaz.
E törvényi előírások felügyeletét jelenleg a Médiatanáccsal közigazgatási szerződést kötött média-társszabályozó szervezetek látják el.
További gyermekvédelmi előírás – amely a kiskorúak védelmét (és egyben a szülők tájékoztatását) célozza – rögzíti, hogy a médiaszolgáltató műsorát közlő sajtótermékben, illetve a médiaszolgáltató internetes honlapján, képújságában és teletextjében – amennyiben rendelkezik ezek valamelyikével – szereplő tájékoztatásban valamennyi műsorszám minősítését jól látható módon fel kell tüntetni (Mttv. 10. § (7) bek.).

2.4.6 Adatvédelem

A hazai adatvédelem szabályozási keretét az Infotv. határozza meg. Az adatvédelem a gyermekek tekintetében különös rendelkezéseket nem tartalmaz, plusz védelmet nem ír elő. Mind a polgári jogi (kiskorú), mind a büntetőjogi (fiatalkorú) szabályozástól eltérő korosztályi megkülönböztetést tesz azzal, hogy a 16 év alatti és feletti korosztály rendelkezési jogosultságát eltérően rendezi. Az Infotv. 6. § (3) bekezdése szerint „a 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges” (14–16 év között azonban még közös döntésük szükséges).
Tehát a digitális térben való lét esetén adatvédelmi szempontból a 16 éves kor a vízválasztó. A szülői hozzájárulás hiányában lehet érvényesen adatkezeléshez hozzájárulni, adatot megadni, viszont egy ilyen esetnek lehetnek polgári jogi következményei, például az aktus vezethet szerződéskötéshez, amelynek érvényességéhez további lépések szükségesek, ez pedig könnyen veszélyforrássá válhat.
Az adatvédelmi tájékoztatásnak kiemelt fontossága van a gyermekek, fiatalok körében, ugyanis számos veszély, probléma kerülhető ki, előzhető meg tudatos eszközhasználattal, tudatos, biztonságos internethasználattal, amely szorosan kapcsolódik az adatvédelem témaköréhez.
A fentiek mellett kiemelten fontos és számon kérhető kötelezettség még a tisztességes és célhoz kötött adatkezelés elve.

2.4.7 Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény

2001 végén született meg az Ekertv., összhangban az Eker. irányelvvel, valamint a közös jogkezelő szervezetek által megkötött megállapodásokkal. A törvény rendelkezik a kiskorúak védelméről és kimondja, hogy a szolgáltató által közzétett és médiatartalomnak nem minősülő olyan információ, amely súlyosan károsíthatja a kiskorúak szellemi, lelki, erkölcsi vagy fizikai fejlődését, különösen azáltal, hogy meghatározó eleme az erőszak, illetve a szexualitás közvetlen, naturális ábrázolása, csak az információt tartalmazó aloldalon, az információ megjelenítése előtt közzétett, a kiskorúak lehetséges veszélyeztetéséről szóló tájékoztatást tartalmazó figyelmeztető jelzéssel, továbbá az aloldal forráskódjában szereplő olyan azonosítókkal tehető közzé, amelyek utalnak a tartalom kategóriájára.
A törvény rendelkezik továbbá a szolgáltató és a közvetítő szolgáltató felelősségéről,

az általuk közzétett információk jogszerűségéről. Mentesül a szolgáltató a felelősség alól, amennyiben nincs tudomása jogsértésről, vagy jogsértésre utaló körülményről, úgy jár el, ahogyan az az adott helyzetben általában elvárható, és lefolytatja a törvényben foglalt értesítési és eltávolítási eljárást.

2.4.8 Fogyasztóvédelmi törvény

A fogyasztóvédelmi törvény a gyermek- és fiatalkorúak védelmét szolgáló különös rendelkezések között megköveteli, hogy a játékszoftver gyártója az olyan játékszoftver forgalmazása esetén, amely alkalmas a tizennyolcadik életévüket be nem töltött személyek fizikai, szellemi, lelki vagy erkölcsi fejlődésének kedvezőtlen befolyásolására, különösen azáltal, hogy meghatározó eleme az erőszak, illetve a szexualitás közvetlen, naturális ábrázolása, köteles a *„Tizennyolc éven aluliak számára nem ajánlott!”* szöveget a játékszoftver csomagolásán jól észlelhető módon feltüntetni. A kötelezettséget az internetes lehívásra közzététel útján forgalmazott játékszoftver esetén a technikai sajátosságoknak megfelelő eltéréssel, a játékszoftver lehívása előtt kell teljesíteni.
A játékszoftver gyártója abban az esetben köteles az előzőekben említett kötelezettségnek eleget tenni, ha előzőleg nem csatlakozott az Egységes Európai Játékinformációs Rendszerhez (Pan European Game Information – PEGI) és nem alkalmazza a PEGI által megállapított, korhatár-besorolásra vonatkozó előírásokat. Ha az előző bekezdésben említett kötelezettséget a gyártó nem teljesíti, a játékszoftver forgalmazója a szoftvert az ott meghatározott szöveg feltüntetésével hozhatja forgalomba (Fgy. tv. 16/A. § (5)–(6) bek.).

2.4.9 Szerencsejátékról szóló törvény

A szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény szerint a szerencsejátékban – a nem folyamatosan szervezett sorsolásos játék kivételével – 18 éven aluli személyek nem vehetnek részt. A szerencsejáték-szervezőnek a játékosok részére a szerencsejátékban való részvétel biztosítása során figyelemfelkeltő módon tájékoztatást kell nyújtania a 18 éven aluli személyek játéktilalmáról, és a felelős játékszervezés elvének megfelelően el kell végeznie a 18 éven aluli személyek játéktilalmának biztosítását szolgáló intézkedéseket (1. § (5b) bek.).
A szervező távszerencsejáték-szervezéssel kapcsolatban használt honlapján a szerencsejáték-szolgáltatással kapcsolatban magyar nyelven kell feltüntetni – egyebek mellett – a 18 éven aluli személyek játéktilalmára vonatkozó figyelmeztetést (29/I. § (1) bek. *e)* pont).

2.5 Nemzetközi jó gyakorlatok

A hazai médiaszabályozás uniós hátterét is jelentő AVMS irányelv előírja, hogy azok a „lekérhető audiovizuális médiaszolgáltatások, amelyek súlyosan károsíthatják a kiskorúak fizikai, értelmi vagy erkölcsi fejlődését, csak oly módon legyenek elérhetők, amely biztosítja, hogy a kiskorúak rendes körülmények között nem láthatják vagy hallhatják az ilyen lekérhető audiovizuális médiaszolgáltatásokat” (12. cikk). Ez a követelmény kevésbé szigorú, mint ami a „hagyományos” (televíziós és rádiós) médiaszolgáltatásokra vonatkozik; utóbbiakban az ilyen jellegű tartalmak közzététele jogellenes.

A tagállamok különféle megoldásokat alkalmaznak a gyermekek védelmének terén, a lekérhető *(on demand)* médiaszolgáltatások vonatkozásában. Ezen előírások között megtalálhatók speciálisan a lekérhető szolgáltatásokra alkalmazandó klasszifikációs rendszerek (például Olaszország). Más országok a védelmet olyan formában próbálják biztosítani, hogy különböző műsorkatalógusokat nyújtanak a gyermekek és felnőttek számára (például Franciaország és Spanyolország). A technikai megoldások között megtalálható a PIN kódok alkalmazása (Olaszország), de gyakori védelmi eszköznek számít az úgynevezett „vízválasztók” *(watersheds)* alkalmazása, amelyek révén egyes káros tartalmak csak a késő esti/éjszakai órákban hozzáférhetők (például Finnország, Franciaország, Németország, Svédország).

Az Internet Watch Foundation-t (Internetfigyelő Alapítvány – IWF) 1996-ban hozták létre az Egyesült Királyságban. Az alapítvány egy non-profit szervezet, mely az Európai Bizottság támogatását élvezi. Céljaként tűzte ki, hogy felvegye a harcot az online jogsértő tartalmak ellen, és minimálisra szorítsa vissza az efféle tartalmakat az online térben. Különösen nagy hangsúlyt fektetnek a gyermekekkel készült pornográf tartalmakra, és a gyermekek ellen elkövetett online szexuális visszaélésekre. Szorosan együttműködve a kormánnyal, a bűnüldöző szervekkel és a szolgáltatókkal próbálják visszaszorítani az online jogsértéseket, és egy komplex rendszer létrehozásával védik a gyermekeket az online rájuk leselkedő veszélyektől. A szervezet sajátossága, hogy e tevékenysége mellett egy „forródrót” szolgáltatást működtet, ahol az állampolgároknak is lehetősége van jelenteni az online jogsértéseket. Ez a forródrót szolgáltatás Magyarországon sem ismeretlen, az NMHH által üzemeltetett Internet Hotline szolgáltatás és a Safer Internet Program támogatásával működő Biztonságosinternet.hu is hasonló tevékenységet végez.

Az IWF által alkalmazott modell jó nemzetközi gyakorlatként és mintaként szolgálhatna Magyarországnak, ahol egy központi szervezet foghatná össze az online gyermekvédelemmel kapcsolatos tevékenységet és hathatósan léphetne fel a gyermekekre leselkedő veszélyek ellen az online térben.

Az online gyermekvédelem egy sajátos megoldását alkalmazzák az Egyesült Királyságban, ahol az internethozzáférés-szolgáltatók – a kormányzattal kötött egyezség alapján – önként vállalták a pornográf tartalmak korlátozását, alapbeállításként 2013 végétől (ez kiterjedt a Wi-Fi szolgáltatásokra, és valamennyi eszközre egyaránt); a jogi szabályozás megalkotására nem került sor. A rendszer alapján a szolgáltatást újonnan igénybe vevők számára már eleve a Gyermekek Számára Biztonságos Internetszolgáltatást nyújtanak (hálózati szintű szűrőeszközökön – az Egyesült Királyságban használt terminológia szerint: *network level filtering measures*) – keresztül), de ez természetesen egyéni kérésre feloldható. Ez az elképzelés nem új keletű a szigetországban. 2002 óta az IWF listát tesz közzé azokról a tartalmakról, melyek károsak lehetnek a kiskorúakra és lista alapján, önkéntes módon blokkolják a szolgáltatók a tartalmakat. A lista a következő főbb kategóriák alapján tartalmazza a tiltani kívánt tartalmakat: drogok, alkohol, társkereső oldalak, pornográf, illetve öngyilkosságra buzdító tartalmak. A kezdeményezéshez csatlakoztak a legnagyobb szolgáltatók, emellett biztonságos internethasználattal és tudatosítással kapcsolatos oldalakat is létrehoztak, illetve biztosítják ügyfeleiknek az ingyenesen letölthető szűrőszoftvert. A későbbiekben megkezdték a könyvtárakban és iskolákban is a hálózati szintű szűrőeszközök bevezetését. 2016 végére szeretnék elérni, hogy az összes iskola csatlakozzon ehhez a kezdeményezéshez. A hálózati szintű szűrőeszközök „feloldására” kizárólag felnőttkorúak jogosultak.

A rendszer működését ért leggyakoribb kritika, hogy a szűrés több olyan oldalra is kiterjedt, amely online bántalmazás áldozatává vált gyermekek megsegítésével, oktatással, felvilágosítással foglalkozott.

Kifejezetten adatvédelmi szempontokat tart szem előtt az Egyesült Államokban 1998-ban a gyermekek (pontosabban a 13 év alatti kiskorúak) személyes adatainak online védelméről szóló törvény (*Children’s Online Privacy Protection 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 a fenti szolgáltatásaik során kiskorúaktól gyűjtenek adatokat. Ez nemcsak a kifejezetten a gyermekek felé irányuló honlapokat (például 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 az oldal üzemeltetőjének tudomása van arról, hogy a szolgáltatást kiskorúak is igénybe veszik.

2.6 A gyermekek számára készült biztonságos tartalmak választékának bővítése

A gyermekek káros tartalmaktól való megóvása mellett legalább ilyen fontos lehet a kifejezetten számukra készített, érettségi és szellemi fejlettségi szintjüknek megfelelő internetes tartalmak készítésének támogatása.

E téren jelenleg az állami szféra mellett a társadalmi, civil szervezetek is aktív szerepet töltenek be. A gyermekbarát internet európai stratégiájáról szóló európai bizottsági közlemény is kiemelten fontos elemként kezeli a gyermekeknek és fiatalkorúaknak szóló minőségi online tartalmak előállításának ösztönzését, amely a gyermekek érdeke mellett az egységes digitális piac javát is szolgálja. Kreatív, játékos természetű tartalmak révén a tudatos internethasználat készsége is könnyebben fejleszthető.

A civil szervezetek saját erőforrásból, illetve támogatások igénybevétele mellett állítanak elő kiskorúak számára szóló online tartalmakat.

Az állami szféra oldalán az NMHH Médiatanácsa által működtetett pályázati rendszer, a Magyar Média Mecenatúra program keretében lekérhető médiaszolgáltatásban megjelent, online műsorszámok elkészítésére lehet pályázni (NEUMANNJANOS pályázat). A támogatási rendszer – a médiaszabályozás adta keretekre tekintettel – némiképp kötött, így kizárólag a törvényi fogalom-meghatározás szerinti „műsorszám” támogatására nyílik módja a Médiatanácsnak, azaz jelenleg gyermekeknek készült játékok, internetes oldalak teljes körű támogatása nem lehetséges.

A Médiatanács animációs filmek gyártását is támogatja (MACSKÁSSYGYULA pályázat), ennek keretében az egyes pályázati eljárások az alábbi eredménnyel zárultak:

- 2012: 16 támogatott pályázat (122,9 M Ft összegben);
- 2013: 24 támogatott pályázat (206,4 M Ft összegben);
- 2014: 23 támogatott pályázat (182,6 M Ft összegben);
- 2015: 19 támogatott pályázat (178,2 M Ft összegben).

A hatóság emellett az általa már támogatásban részesített gyermek, ifjúsági és családi témájú animációs filmsorozatok további epizódjainak gyártását is támogatja, külön eljárás keretében (DARGAYATTILA pályázat). A 2014-ben meghirdetett pályázat eddigi két „teljes” évében a Médiatanács az alábbi számban (és keretösszeggel) nyilvánított kedvezményezetté pályázókat:

- 2014: 6 támogatott pályázat (215,2 M Ft összegben);
- 2015: 14 támogatott pályázat (244,9 M Ft összegben).

A két pályázati eljárás kapcsán elmondható ugyanakkor, hogy a NEUMANNJANOS pályázat feltétele az online közzététel, míg a DARGAYATTILA és a

MACSKÁSSYGYULA pályázatokban a gyermekeknek szánt tartalom, azonban mindkét feltételnek való megfelelés jelenleg egyik esetben sem egységes követelmény.
A fentieken túl a gyermekeknek szóló internetes tartalomkínálat bővítését segíti elő a közmédia tematikus gyermek- és ifjúsági csatornájának (m2) weboldala, ahol az egyes műsorok akár élőben, akár visszamenőlegesen is megtekinthetőek.

2.7 Esélyegyenlőség

Minden – az értékteremtő internethasználat támogatására, illetve a gyermekek védelmét szolgáló szabályok hangsúlyosabb érvényesülésére irányuló – eszköz, intézkedés kapcsán figyelembe kell venni a fogyatékossággal élő és sajátos nevelési igényű gyermekek szempontjait. Törekedni kell a médiaoktatás és képzés, valamint az internethasználatot elősegítő eszközök, hatékony műszaki megoldások integrálttá, hozzáférhetővé, akadálymentessé tételére, és ezeknek a lehetőségeknek széles körben történő megismertetésére, tudatosítására.

3. Szankcióalkalmazás és segítségnyújtás

A tudatosság növelését, továbbá a biztonságos környezet megteremtését szolgáló – meglévő, illetve a jövőben alkalmazandónak ítélt – intézkedések egyaránt azt a célt szolgálják, hogy a gyermekek ne legyenek kitéve semmiféle kockázatnak, veszélynek. A gyakorlatban azonban elkerülhetetlen a teljes körű védelem és biztonság megteremtése, éppen ezért indokolt áttekinteni azt a helyzetet, amikor a gyermekek az internethasználat során, illetve azt követően különféle nem várt negatív, káros következményekkel szembesülnek.

Ezt a helyzetet két tekintetben kell alaposan megvizsgálni: egyfelől segítséget, támogatást kell nyújtani az áldozattá vált gyermekek számára, másfelől pedig az internet felhasználásával elszenvedett (jog)sérelmet lehetőség szerint minél gyorsabban és hatékonyabban meg kell szüntetni, illetve a sérelem súlyától függően az elkövetőket megfelelő szankcióval (szankciókkal) kell sújtani. A sérelmek eltérő típusúak, jellegűek lehetnek, ebből következően hatásukat, és így a kezelésükre vonatkozó szabályozás körét (büntetőjog, polgári jog, médiaszabályozás stb.) és típusát (jogszabály, önszabályozás, etikai kódexek stb.) tekintve is igen szerteágazóak lehetnek.

Amiként a médiatudatosság-növelés, illetve a biztonságos internethasználat megteremtése körében, úgy a bekövetkezett sérelmes helyzet reparációja során is elengedhetetlen az érintettek széleskörű tájékozottságának elősegítése. Ez jelen esetben elsődlegesen a sérelmet szenvedettek számára rendelkezésre álló segítségnyújtási lehetőségek, megfelelő egyéb fórumok ismeretében, elérhetőségében, míg a potenciális elkövetők oldaláról nézve pedig cselekményük lehetséges hátrányos következményének ismeretében merülhet ki.

Megemlítendő, hogy a Nemzeti Infokommunikációs Stratégia (2014-2020) is külön foglalkozik a gyermekvédelem kérdésével, melynek körében a létező biztonsági kockázatokról és csökkentésük módjairól szóló átfogó tájékoztató program megvalósulásáról rendelkezett. Célul tűzte ki e veszélyek kezelésére vonatkozó jogszabályi háttér megalkotását, továbbá kívánatosnak tartotta, hogy váljon széles körben ismertté a gyermekvédelmi és kiberbűnözés elleni forródrót (minderre 2016-os céldátumot megjelölve).

3.1 Érintett szervezetek

Szükséges áttekinteni a jogsérelem bekövetkezte esetén a szankcióalkalmazásban, illetve a sérelem orvoslásában részt vevő intézmények, szervezetek körét.
A jogsérelem megtörténtét követően elsődlegesen az állami szerveknek kell ellátniuk a jogszabályok által hatáskörükbe utalt feladatokat. Ennek során a legsúlyosabb jogsértések, azaz a bűncselekmények esetén fellépő, illetve eljáró büntetőhatóságokat (rendőrség, ügyészség, bíróság) kell említeni. A közigazgatás szervezetrendszerén belül működő, eljárási jogosítványaikat, vizsgálati szempontjaikat és szankcióalkalmazási lehetőségeiket tekintve igen nagy eltéréssel működő intézmények közül megemlítendő az NMHH, a Médiatanács, a Gyermekvédelmi Internet-kerekasztal, a NAIH, valamint az AJBH.
A civil szervezetek e téren folytatott tevékenysége szintén kiemelkedő, amely nem a jogsértést elkövető személyek felelősségre vonásában, hanem elsősorban az áldozattá váltak számára történő segítségnyújtásban nyilvánul meg (ilyen például a Kék Vonal Gyermekkrízis Alapítvány).
Végül szükséges megemlíteni az állami szerepkört is átvállaló, de alapvetően civil szervezetnek minősülő azon szervezeteket, amelyek némi állami támogatás mellett saját piaci szegmensüket igyekeznek jogkövető magatartásra sarkallni, és ennek során az állami szereplőkhöz hasonló jogosítványokkal is rendelkeznek (például társszabályozó szervezetek a médiaigazgatási társszabályozás terén).
Mint látható, igen sokrétű az e területen tevékenykedő szervezetek köre és típusa, ami jellemzi munkájukat, hogy igen széttöredezetten, egymástól elkülönülve működnek. E szervezetek munkája alapvetően a különállósággal jellemezhető, hiszen valamennyi szervezet a saját hatáskörében eljárva, „önállóan” végzi feladatát. Mindenképpen hasznos volna egy olyan együttműködési rendszer, közös fórum kialakításának gondolata, amely segítségével a résztvevők a tapasztalatokat megoszthatják egymással, így az esetleges problémák könnyebben és hatékonyabban megoldhatók lennének.
A jogalkotó részéről erre irányuló kísérletnek, próbálkozásnak tekinthető a Nemzeti Kiberbiztonsági Koordinációs Tanács (gyermekvédelmi munkacsoport) vagy a Gyermekvédelmi Internet-kerekasztal életre hívása, amely testületek tagsága az állami szféra, a gyermekvédelmi szervezetek és a piaci szféra érdekképviseleti szervei által delegált személyekből tevődik össze. Hasonló kezdeményezésnek minősül a JOG-OK munkacsoport az alapvető jogok biztosának kezdeményezésére.

3.2 A jogsérelem megtörténtének felismerése

Elengedhetetlen a gyermekekben annak a tudatosítása, hogy mely cselekedetek azok, amelyek jogellenesnek minősülnek, és bizonyos körülmények fennállta esetén (súlyos) jogi következményekkel járhatnak. Igaz ez mind az elkövetők, mind pedig az áldozatok oldaláról nézve. E jogtudatosság az elsődleges kiindulópontja annak a helyzetnek, amikor a sérelmet szenvedett kiskorú felismeri, hogy jogellenes cselekmény áldozatává vált (vagy ennek közvetlen veszélye, lehetősége fennáll), és lépéseket tesz a sérelem orvoslására alkalmas eszközök, intézkedések igénybevételére.
A jogsértés bekövetkezte esetén elengedhetetlen a helyreállításhoz a megfelelő jogvédelmi eszköz megállapítása és igénybevétele.
Emellett szükséges annak tudatosítása, hogy a jogsérelem megtörténtét követően milyen lépések megtétele segítheti elő az elkövető felelősségre vonását. Ennek körében tudatosítani szükséges az alábbiakat:

- A jogsértés tárgyát képező fénykép, video, szöveges üzenet stb. elektronikus úton való rögzítésének megfelelő módja, lehetősége (lementés);
- Egyéb informatikai megoldások ismerete (értesítési beállítások az adott személlyel kapcsolatos információk interneten való megjelenése esetén);
- Jogi és egyéb (például eltávolítási) eljárás kezdeményezéséhez szükséges hasznos információk;
- Más (az észlelő által ismert) személlyel szemben elkövetett jogsértés észlelése esetén szükséges teendők ismerete.

3.3 Szankcióalkalmazás a médiaszabályozás területén

3.3.1 A társszabályozó szervek eljárása

A hatályos jogszabályi környezet az online tartalmak egy meghatározott körét tekintve felügyeleti, jogsértés észlelése esetén pedig szankcionálási jogkört telepít a Médiatanácsra. Az online tér viszonyában e szabályozás hatálya az internetes sajtótermékekre, illetve az internetes úton elérhető lekérhető médiaszolgáltatásokra vonatkozik. Megjegyzendő ugyanakkor, hogy a hatályos médiaszabályozás a szakmai tapasztalat és hatékonyság jegyében lehetőséget biztosít e téren az önszabályozó szervek szerepének növelésére. Ennek eredményeképpen a kiskorúak védelmére vonatkozó szabályok érvényesítése és esetleges jogkövetkezmény alkalmazása elsődlegesen az ön- és társszabályozó szervek feladat- és jogköre.
Egyes gyermekvédelmi szabályok – lekérhető médiaszolgáltatásokban és internetes sajtótermékekben a médiatartalmakra vonatkozó időbeli és közzétételi korlátok,

kiskorúak védelmét szolgáló reklámszabályok (Smtv. 19. §, Mttv. 11. és 24. §) – feletti felügyeleti jogkörrel jelenleg az alábbi – a Médiatanáccsal szerződéses viszony alapján – eljárási jogosultsággal rendelkező társszabályozó szervezetek bírnak:

- Magyarországi Tartalomszolgáltatók Egyesülete;
- Magyar Lapkiadók Egyesülete;
- Magyar Elektronikus Műsorszolgáltatók Egyesülete;
- Önszabályozó Reklám Testület.

Jogsértés esetén a társszabályozó szervezet kötelezettséget tartalmazó döntést hozhat, legfőbb ereje a nyilvánosság (ezen túl „szankcióként" az érintett szolgáltatót a normasértő tevékenység abbahagyására, az eredeti állapot helyreállítására, valamint elégtételadásra kötelezheti, illetve a társszabályozási rendszer hatályának rá nézve történő megszűnését és a hatósági eljárás alanyává „válását" állapíthatja meg).

A társszabályozás rendszerének hazai működését illető tapasztalatok szerint igen kevés panasz érkezik a szervezetekhez állampolgárok részéről, ezeknek pedig igen kis része érinti a gyermekek védelmének kérdését. A mostanra közel öt éve működő társszabályozási rendszerben mindösszesen három panasz érkezett, amely a kiskorúak védelmét célzó előírásokat érintette, ezekben az ügyekben pedig mindösszesen egy érdemi döntés született.

3.3.2 A Médiatanács eljárása

A Médiatanács széles körű hatósági felügyeleti eljárást biztosító hatáskörének egyik eleme a kiskorúak védelmét célzó előírások érvényesítése, ugyanakkor e hatásköre csak szűk körben érinti az internetes tartalmakat.

Amennyiben internetes úton elérhető lekérhető médiaszolgáltatással, illetve internetes sajtótermékkel szemben a Médiatanács jár el (mert az adott szolgáltató nem tartozik a társszabályozás hatálya alá), abban az esetben hatósági eljárásban érvényesíti a kiskorúak védelmét szolgáló előírásokat, és ennek keretében szankciót alkalmazhat.

Ez lekérhető médiaszolgáltatás esetében bírság kiszabását, közlemény közzétételére kötelezést, a jogosultság felfüggesztését és az MTVA pályázataiból való kizárást foglalhatja magában, sajtótermékre nézve az első kettő szankció alkalmazására nyílik mód. Ennél súlyosabb jogkövetkezményt jelent, hogy amennyiben a szolgáltató a jogerős, végrehajtható határozatban foglalt kötelezettségeit nem teljesíti, a Médiatanácsnak lehetősége nyílik a közvetítő szolgáltatót kötelezni az adott szolgáltatás közvetítésének felfüggesztésére.

Az eddigi tapasztalatok szerint a Médiatanács lekérhető médiaszolgáltatással, illetve sajtótermékkel szemben „közvetlenül" igen kevés alkalommal járt el.

A hatóság az Mttv. 10. § (7) bekezdésében foglaltak érvényesülését ugyanakkor rendszeresen vizsgálja, ez idáig összesen 23 alkalommal állapított meg jogsértést, évek szerint az alábbi megoszlásban:

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

3.4 Adatvédelmi szabályok megsértése esetén történő szankcióalkalmazás

Személyes adatok kezelésével kapcsolatos jogsérelem bekövetkezte esetén a NAIH-nál eljárás kezdeményezhető: ha jogsérelem vagy annak közvetlen veszélye fennállását megalapozottnak tartja, az adatkezelőt a jogsérelem orvoslására, illetve a közvetlen veszély megszüntetésére szólítja fel (Infotv. 56. § (1) bek.).

A személyes adatok védelméhez való jog érvényesülése érdekében a NAIH adatvédelmi hatósági eljárást indíthat. Az adatvédelmi hatósági eljárásban hozott határozatában az Infotv. 61. § (1) bek. alapján a NAIH:

- Megállapíthatja a személyes adatok jogellenes kezelésének vagy feldolgozásának tényét;
- Elrendelheti a valóságnak nem megfelelő személyes adat helyesbítését;
- Elrendelheti a jogellenesen kezelt vagy feldolgozott személyes adatok zárolását, törlését vagy megsemmisítését;
- Megtilthatja a személyes adatok jogellenes kezelését vagy feldolgozását;
- Megtilthatja a személyes adatok külföldre történő továbbítását vagy átadását;
- Elrendelheti az érintett tájékoztatását, ha azt az adatkezelő jogellenesen tagadta meg;
- Bírságot szabhat ki.

Ha a NAIH az eljárása során bűncselekmény elkövetésének alapos gyanúját észleli, büntetőeljárást kezdeményez az annak megindítására jogosult szervnél. Amennyiben szabálysértés vagy fegyelmi vétség elkövetésének alapos gyanúját észleli, szabálysértési, illetve fegyelmi eljárást kezdeményez a szabálysértési, illetve a fegyelmi eljárás lefolytatására jogosult szervnél (Infotv. 70. § (1) bek.).

A NAIH-hoz éves szinten kevés, csak 4-5 adatvédelmi panasz érkezik közvetlenül az érintett adatalanytól/szülőtől, általában közösségi oldalon nyilvánosságra hozott fényképpel összefüggésben, de ebben a körben sokkal inkább jellemzőek a hivatalból indított adatvédelmi hatósági eljárások, ahol az érintett kiskorúak száma ennél nagyságrendileg jelentősebb (például 2013-ban az online társkeresőknél jogellenesen regisztrált kiskorúak száma mintegy 8000, a jelenleg is folyó,

gyermekszépségversenyekkel kapcsolatos hatósági eljárásban érintett gyermekek száma több száz).

3.5 A polgári jogi jogkövetkezmények

A Ptk.-ban rögzített személyiségi jogok sérelme esetén (jellemzően a képmáshoz való jog, becsület és jóhírnév, illetve személyes adatok védelméhez való jog megsértése) a sérelmet szenvedettnek a polgári bírósághoz fordulás lehetősége biztosított.
Akit személyiségi jogában megsértenek, a Ptk. alapján (2:51. § (1) bek., 2:53. §) követelheti:

- A jogsértés megtörténtének bírósági megállapítását;
- A jogsértés abbahagyását és a jogsértő eltiltását a további jogsértéstől;
- Nyilvános elégtételadást;
- A sérelmes helyzet megszüntetését, a jogsértést megelőző állapot helyreállítását és a jogsértéssel előállított dolog megsemmisítését vagy jogsértő mivoltától való megfosztását;
- Sérelemdíjat az őt ért nem vagyoni sérelemért;
- Kárának megtérítését.

3.6 A büntetőjogszabályok megsértése

3.6.1 A Btk. szerinti szankcióalkalmazás

A 2.4.4. pontban említett bűncselekmények elkövetése esetén a Btk. szerinti büntetések (33. § (1) bek.) és intézkedések (63. § (1) bek.) alkalmazására nyílik lehetőség. (Speciális jogkövetkezmény az elektronikus adat elérhetetlenné tétele, amelyről részletesen a 3.7. pont alatt szólunk.)
Ezen felül a büntetőeljárási törvény bizonyos feltételek fennállta esetén közvetítői eljárás lefolytatására nyújt lehetőséget (Be. 221/A. §). Ilyen, a 2.1. pont alatt is említett, jellegzetesen az online térben, gyermekek sérelmére (vagy általuk) elkövetett bűncselekmények közül közvetítői eljárás lefolytatása biztosított többek között a zaklatás, a levél- és magántitok megsértése, vagy a személyes adattal való visszaélés bűncselekménye esetén (gyermekpornográfia esetében ugyanakkor nem). A közvetítői eljárás célja, hogy a bűncselekmény következményeinek jóvátételét és a gyanúsított jövőbeni jogkövető magatartását elősegítse. A közvetítői eljárásban arra kell törekedni, hogy a gyanúsított és a sértett között – a gyanúsított tevékeny megbánását megalapozó – megállapodás jöjjön létre (Be. 221/A. § (2) bek.).

A megállapodás akkor jön létre, amikor a sértett és a terhelt között a bűncselekménnyel okozott kár megtérítésében vagy következményeinek jóvátételében azonos álláspont alakul ki. A sikeres közvetítői eljárás eredményeképpen a 3 évi szabadságvesztésnél nem súlyosabban büntetendő bűncselekménycsoport esetében lehetséges a büntethetőség megszűnése, ennek okán pedig az eljárás megszüntetése; az ugyanezen felsorolásba eső, de 5 évi szabadságvesztésnél nem súlyosabban büntetendő bűncselekmények esetén pedig a büntetés korlátlan enyhítése.
(Az eljárás részletes szabályait a büntető ügyekben alkalmazható közvetítői tevékenységről szóló 2006. évi CXXII. törvény rendezi.)
A Belügyminisztérium Koordinációs és Statisztikai Osztály által közzétett bűnügyi statisztikai adatok között hozzáférhetőek az egyes bűncselekmény-típusok elkövetésének száma, különféle lebontásban (elkövetés helye, éve, tárgya, eszköze stb.). Ezek között azonban nem található információ a kifejezetten kiskorúak/gyermekek által/sérelmére, illetve online úton elkövetett bűncselekményekre vonatkozó adatok tekintetében.

3.6.2 A szabálysértési törvény szerinti jogkövetkezmények

A veszélyes fenyegetés (Szabs. tv. 173. §) elkövetéséért akár elzárás is kiszabható, helyette pedig bármilyen más szabálysértési büntetés vagy intézkedés alkalmazható.

3.7 A jogsértő tartalmak elérhetetlenné tételét szolgáló eszközök

Jelen pont alatt a szankcióalkalmazás egy sajátos formáját, nevezetesen a jogsértő online tartalom eltávolításának lehetőségét ismertetjük. Ennek az eljárási lehetőségnek az a sajátossága, hogy különféle esetekben, eltérő szabályozási rezsimbe tartozóan szabályozott módja van.

3.7.1 Kiskorúak személyiségi jogait sértő tartalmak eltávolítása

Az internetes gyermekvédelem területén 2014. január 1-jétől az értesítési-eltávolítási eljárás *(notice and take down)* alkalmazhatóságának köre kibővült. Ennek eredményeképpen a hatályos jogszabály lehetővé teszi, hogy a személyiségi jogok kiskorú jogosultjai, illetve a kiskorú jogosultak törvényes képviselői egy precízen szabályozott eljárási rend szerint, még a polgári peres, vagy a büntetőeljárás előtt vagy helyett, hatékony módon léphessenek fel a kiskorúak személyiségi jogainak védelme érdekében. Az eljárás eredményeképpen – hasonlóan a szerzői jogi

jogsértésekhez – lehetőség nyílik a kiskorú személyiségi jogait sértő tartalmak (információ) eltávolítására (Ekertv. 13. § (13)–(15) bek.).

A törvényi előírások érvényesítéséhez, kikényszerítéséhez ugyanakkor nem kapcsolódik hatósági jogkör. Amennyiben a szolgáltató nem tesz eleget a sérelmes információ eltávolítására vonatkozó kötelezettségeinek, vagy a kérelmet elutasítja, a kiskorú jogosult vagy a törvényes képviselője a kiskorú személyiségi jogai vélelmezett megsértése miatt az NMHH elnökének tanácsadó, javaslattevő szervéhez, a Gyermekvédelmi Internet-kerekasztalhoz fordulhat. A kerekasztal az ilyen bejelentéseket megvizsgálva, azok általános tapasztalatait tevékenysége során felhasználva elsődlegesen a nyilvánosság erejére építve érhet el eredményt.

A közel másfél éve hatályban lévő jogintézmény kapcsán ugyanakkor elmondható, hogy ez idő alatt a kerekasztalhoz egyetlen panasz sem érkezett, amelyben el kellett volna járnia. Ebből a tényből alapvetően kétféle következtetés vonható le:

- A szolgáltatók valamennyi esetben eleget tettek a személyiségi jogot vélhetően sértő tartalmak eltávolítására irányuló kérelemnek, amely miatt nem volt szükség a kerekasztal bevonására;
- A jogintézmény ismeretlen a közvélemény számára.

3.7.2 Hotline-ok

A) Az Internet Hotline

2005 óta működik hazánkban az Internet Hotline szolgáltatás, amely lehetőséget biztosít az interneten található jogellenes, illetve a kiskorúak számára káros tartalmak bejelentésére. A hotline üzemeltetője (2011 óta az NMHH) ezt követően – indokolt esetben – felhívja az érintett szolgáltatót a bepanaszolt tartalom eltávolítására, amely ezt önkéntes alapon megteheti, de erre kötelezni nem lehet (az eljárás tehát nem váltja ki és nem helyettesíti a jogsértés miatt indítható hatósági és bírósági eljárásokat).

Fontos hangsúlyozni, hogy az Internet Hotline tevékenysége nem hatósági eljárás, hanem egy olyan tevékenység, amelyet az NMHH a társadalmi felelősségvállalás jegyében végez. Az Internet Hotline, illetve az azt üzemeltető NMHH törvényi felhatalmazás hiányában a jogellenes tartalom esetében a törlésre, illetve a kiskorúakra káros tartalomra való figyelemfelhívásra kötelezni senkit nem tud. A kifogásolt tartalom eltávolítását az Internet Hotline csupán kérheti arra hivatkozással, hogy az jogszabályba ütközik. A kifogásolt tartalmat a honlapok szerkesztői, illetve a szerverek üzemeltetői általában eltávolítják, illetve feltüntetik annak kiskorúakra ártalmas voltát.

Az Internet Hotline bejelentési kategóriái:

- hozzájárulás nélkül hozzáférhetővé tett tartalom: ha az érintett hozzájárulása, engedélye nélkül tesznek az interneten hozzáférhetővé vele, vagy gyermekével kapcsolatos fénykép-, video-, hangfelvételt, vagy egyéb személyes adatot;
- pedofil tartalom;
- zaklatás, megfélemlítés: ha az érintett vagy gyermeke zaklatásnak, megfélemlítésnek esett áldozatul az interneten keresztül. Az olyan, weboldalakon, fórumokon olvasható szöveges tartalmak esetén, ahol kiskorúakra vonatkozóan szexuális jellegű megjegyzéseket, beszélgetést folytatnak, valamint olyan felhívás esetén, amelyben kiskorúakat keresnek szexuális együttlétre;
- rasszista, idegengyűlöletre uszító tartalom;
- erőszakot megjelenítő tartalom;
- drogfogyasztásra csábító tartalom;
- terrorcselekményre felhívó, terrorizmust népszerűsítő, elősegítő tartalom;
- adathalász honlapok, vírusokkal, kém- és féregprogramokkal fertőzött tartalmak;
- egyéb, a kiskorúakra veszélyes tartalom.

A hotline gyakorlatában „jogellenesnek” tekintendő az olyan tartalom, amely feltehetően a hatályos jogszabályokba, különösen a Btk., illetve a Ptk. rendelkezéseibe ütközik. Az internet világában a legjellemzőbb jogsértések a zaklatás, illetve a más képmásával vagy egyéb személyes adatával való visszaélés, például annak jogellenes közzététele. Kiskorúakra káros vagy veszélyes tartalom minden olyan tartalom, amely a kiskorúban félelmet, visszatetszést kelthet, szellemi vagy erkölcsi fejlődését károsan befolyásolhatja.
A hotline munkatársai felszólítják a vélhetően jogellenes tartalmat közreadó honlap szerkesztőjét vagy a tartalmat tároló szerver üzemeltetőjét, hogy távolítsa el a kifogásolt tartalmat. A törlést a szervertulajdonos (közvetítő szolgáltató) a közte és a tartalom feltöltője közt létrejött szerződés alapján teszi meg. Ezekben a szerződésekben szerepel, hogy a szerveren csak olyan anyagot, honlapot lehet elhelyezni, amelyeknek nem része jogellenes tartalom. Külföldi szerveren lévő tartalom esetén a hotline munkatársai tájékoztatják még az adott országban működő hotline-t is. Ha a jogsértő tartalom bűncselekményt vagy annak előkészületét is megvalósíthatja, akkor a hotline munkatársai a rendőrséget is értesítik.
A kiskorúakra káros, illetve veszélyes, ugyanakkor nem jogsértő tartalmak esetén a hotline munkatársai arra hívják fel a honlap szerkesztőjét vagy a szerver

üzemeltetőjét, hogy a honlapon egyértelműen jelezze, hogy az oldalon lévő tartalom a kiskorúak számára káros lehet.

Az Internet Hotline indulása óta – a 2016. márciusi adatok szerint – közel 3200 bejelentés érkezett. Ez éves szinten mintegy 700 bejelentést jelent. A leggyakoribb bejelentési kategóriák: a hozzájárulás nélkül hozzáférhetővé tett tartalom (az összes bejelentés 19%-a), a rasszista, idegengyűlöletre uszító tartalom (az összes bejelentés 19%-a), a zaklatás (az összes bejelentés 14%-a) és a pedofil tartalom (az összes bejelentés 8%-a).

A tapasztalatok alapján elmondható, hogy a hazai tartalom- és tárhelyszolgáltatók együttműködnek és a jogsértő tartalmat hozzáférhetetlenné teszik, illetve a kiskorúakra káros tartalmak esetén elhelyeznek korhatár figyelmeztetést. Pedofil tartalmak esetén az Internet Hotline együttműködik az INHOPE (International Association of Internet Hotlines – Internet Hotline-ok Nemzetközi Szövetsége) szervezettel. Ez a szervezet teremt lehetőséget arra, hogy a Magyarországra irányuló, de külföldön tárolt pedofil tartalmat is sikeresen el lehessen távolítani, illetve ezen a szervezeten keresztül jelzik, ha a jogsértő tartalom magyar szerveren található. A bejelentő szervek a saját országukban tárolt tartalom esetén felszólítják a tárhelyszolgáltatót az eltávolításra, illetve kapcsolatot tartanak a bűnüldöző hatóságokkal.

B) A Biztonságosinternet Hotline

A Biztonságosinternet Hotline 2011 májusától nyújt lehetőséget a jogsértő tartalmak bejelentésére. A hotline a Safer Internet Plus program keretén belül, európai uniós támogatással jött létre, része a magyar Safer Internet konzorciumnak. A hotline-t a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. működteti.

A Biztonságosinternet Hotline bejelentő oldalán a magyar jogszabály által meghatározott jogsértő online tartalmat jelenthet be a következők szerint:

- pedofil tartalom;
- erőszakos tartalom (zaklatás);
- idegen és fajgyűlöletre uszító tartalom;
- drogfogyasztásra csábítás;
- hozzájárulása nélkül sértő módon közzétett tett tartalom;
- egyéb káros tartalom.

3.7.3 Elektronikus adat elérhetetlenné tétele

2013. július 1-je óta tartalmazza a Btk. az „elektronikus adat végleges hozzáférhetetlenné tétele” elnevezésű intézkedést, amely alkalmazására azon elektronikus hírközlő hálózaton közzétett adat esetében nyílik mód:

- Amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg;
- Amelyet bűncselekmény elkövetéséhez eszközül használtak;
- Amely bűncselekmény elkövetése útján jött létre (Btk. 77. § (1) bek. a)–c) pontok).

E szankció alkalmazására akkor is sor kerülhet, amennyiben az elkövető nem büntethető vagy büntethetősége megszűnt. Az intézkedés alkalmazásához kizárólag a tényállásszerűséget és a jogellenességet kell vizsgálni, azaz az adat hozzáférhetetlenné tételéhez nem szükséges az elkövető személyének ismerete.

Ezen intézkedés alkalmazásához szorosan kapcsolódik a Be.-be ezzel egyidejűleg beiktatott kényszerforma, az „elektronikus adat ideiglenes hozzáférhetetlenné tétele”, amely az elektronikus adat feletti rendelkezési jog ideiglenes korlátozása. Ennek célja, hogy a büntetőeljárás idejére – visszaállítható módon – hozzáférhetetlenné tegye az olyan – bűncselekménnyel kapcsolatos adatot – amellyel szemben végleges hozzáférhetetlenné tétel intézkedése alkalmazható, és az ideiglenes hozzáférhetetlenné tétel a bűncselekmény megakadályozásához szükséges (Be. 158/B. § (2) bek.).

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele két formában valósulhat meg: elsődlegesen az „elektronikus adat ideiglenes eltávolításával”, amelyre a tárhelyszolgáltatót kell kötelezni (Be. 158/C. § (1) bek.). Az ideiglenes hozzáférhetetlenné tétel másik módja az „elektronikus adathoz való hozzáférés ideiglenes megakadályozása”, mely csak kivételes esetben, kizárólag bíróság által rendelhető el, amennyiben a büntetőeljárás gyermekpornográfia, állam elleni bűncselekmény, terrorcselekmény, kábítószer-kereskedelem, kóros szenvedélykeltés, kábítószer készítésének elősegítése, kábítószer-prekurzorral visszaélés, új pszichoaktív anyaggal visszaélés, illetve terrorizmus finanszírozása miatt indult, és az elektronikus adat e bűncselekménnyel áll összefüggésben (158/D. § (1) bek. a)–b) pontok), továbbá a tárhelyszolgáltató az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettségét nem teljesítette, vagy az elektronikus adat ideiglenes eltávolítására irányuló, külföldi hatóság felé küldött megkeresés a megkereséstől számított harminc napon belül nem vezetett eredményre. Ez esetben az elektronikus hírközlési szolgáltató a kötelezettség címzettje. A kényszerintézkedés végrehajtását az NMHH szervezi és ellenőrzi.

Az elektronikus adat végleges hozzáférhetetlenné tételére az elektronikus adathoz való hozzáférés végleges megakadályozása révén kerülhet sor (Be. 596/A. §).

3.7.4 Önszabályozás

A médiaszabályozásbeli társszabályozás mellett külön említést érdemel az önszabályozó (a 3.3.1. pont alatt említett négy szakmai szervezeten túli) szervezetek tevékenysége.

A Magyar Újságírók Országos Szövetségének (MÚOSZ) etikai kódexében – amelynek hatálya többek között az online sajtóra is kiterjed – szereplő magatartási szabályok megsértése esetén az etikai bizottság a szabályzata szerint lefolytatott eljárással etikai vétséget állapíthat meg. Az etikai kódex a gyermekek védelmével kapcsolatos előírást is tartalmaz, e szerint „etikai vétséget követ el, aki fiatalkorúak személyiségi jogait sérti. Akkor is megállapítható az újságíró etikai felelőssége, ha a fiatalkorú törvényes képviselője hozzájárult a nyilvánossághoz. Gyermekek csak a szülők, törvényes képviselők, tanítási, gondozási időben csak az osztályfőnök, óvodapedagógus engedélyével szerepeltethetők. Ha erre az anyag felvételénél nincs lehetőség, leadás előtt meg kell szerezni a hozzájárulásukat" (3.1.3. pont).

A 2015 decemberében megalakult Korrektor önszabályozó fórum (amely a Főszerkesztők Fóruma Egyesületének, a Magyar Lapkiadók Egyesületének és a Magyar Tartalomszolgáltatók Egyesületének együttműködése eredményeképpen jött létre) szintén biztosítja a sajtó valamennyi (így az online) területére kiterjedően a panasztételi lehetőséget. Eljárásának eredménye: az (esetleges) elmarasztaló döntést közzé kell tenni és nyilvánosságra kell hozni. A gyermekvédelmi szabályokat a személyiségi jogok védelme körében említi a szervezet etikai kódexe.

3.8 Alternatív vitarendezés a nevelési-oktatási intézményekben

A nevelési-oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról szóló 20/2012. (VIII. 31.) EMMI rendelet lehetőséget biztosít arra, hogy a tanulóval szemben lefolytatandó fegyelmi eljárást egyeztető eljárás előzze meg, amelynek célja a kötelességszegéshez elvezető események feldolgozása, értékelése, ennek alapján a kötelességszegéssel gyanúsított és a sérelmet elszenvedő közötti megállapodás létrehozása a sérelem orvoslása érdekében (53. § (2) bek.).

Ehhez hasonló jogintézmény az oktatásügyi közvetítő eljárása, amelyre abban az esetben kerülhet sor, ha a nevelési-oktatási intézmény a gyermeket, tanulót veszélyeztető okokat pedagógiai eszközökkel nem tudja megszüntetni, vagy ha a gyermekközösség, a tanulóközösség védelme érdekében indokolt, segítséget kérhet

konfliktuskezelési szaktanácsadótól, valamint az ifjúságvédelmi, családjogi területen működő szolgálattól (62. § (1) bek.).
Az oktatásügyi közvetítésre egyeztetési eljárás keretében is sor kerülhet, a rendelet tehát kifejezetten szól az alternatív vitarendezési formák közül a jóvátételi (resztoratív) mediáció lehetőségéről. Oktatásügyi közvetítő egyeztetési eljárásban való részvétele esetén a felek közötti megállapodás akkor jön létre, ha a sérelmet elszenvedő fél és a kötelességszegő tanuló között a kötelességszegéssel okozott kár megtérítése vagy a káros következményeinek egyéb módon való jóvátétele, enyhítése tekintetében azonos álláspont alakul ki (62. § (9) bek).
Megjegyzendő, hogy az egyeztetési eljárásban létrejött megállapodás nem érinti a sérelmet elszenvedőnek azt a jogát, hogy a fegyelmi eljáráson kívül a bűncselekményből, szabálysértésből származó igényét egyéb eljárás keretében érvényesítse (62. § (13) bek.).

3.9 Segítségnyújtás, áldozatsegítés

További fontos tényező az áldozattá váló gyermek kezelése, a negatív (vagy esetlegesen tragikus) következmények megelőzése, illetve megszüntetése. E téren alapvetően a gyermekek számára támogatást nyújtó, a sérelmes állapot feldolgozását, megfelelő kezelését és jövőbeli elkerülését szolgáló szervezetekről, intézményekről, emellett pedig a jogsérelem miatt sorra kerülő hivatalos hatósági eljárások során megfelelő körülmények biztosításáról kell beszélni. A területen kiemelendő a civil szervezetek által folytatott tevékenység.

3.9.1 Áldozatsegítés

Az áldozattá vált gyermekek kezelése, támogatása kiemelt feladat, külföldi példák alapján ugyanis látható, hogy az online térben elkövetett jogsértő cselekmények az események eszkalálódására tekintettel könnyen és igen rövid idő alatt tragikus következményekkel járhatnak. Az áldozatsegítés területén lényegében ugyanazon területeken kell megfelelő tapasztalattal rendelkezni, mint általában véve a kiskorúak védelme körében, így kiemelt feladat hárul a szülők mellett a pedagógusokra, az e téren működő társadalmi, civil szervezetekre, és természetesen magára az államra (az állam kiemelt feladata például a sérelmet szenvedettekkel szemben a hivatalos eljárás során megfelelő környezet kialakítása, lásd a 3.9.3 alpontot).
Elengedhetetlen e téren a szülők és pedagógusok számára a kellő szintű ismeretek biztosítása arra vonatkozóan, hogy elsőként milyen módon ismerjék fel a veszélyben

lévő gyermekeket, illetve ezt követően milyen módon tudnak számukra saját maguk, vagy akár erre avatott személyek, szervezetek közbenjárásával segítséget nyújtani.

3.9.2 A társadalmi és civil szervezetek tevékenysége

A szakmai szervezetek körében mindenképpen megemlítendő a Kék Vonal Gyermekkrízis Alapítvány. Az alapítvány tevékenységének egyik kiemelkedő területe az internet biztonságosabbá tétele érdekében, illetve a jogellenes káros tartalmak ellen folytatott hatékony küzdelem. Ennek keretében a szervezet ingyenes lelkisegély-vonalat működtet Magyarországon, a 116-111-es telefonszámon. Egyebek mellett fő tevékenységi körük a tanácsadás olyan gyermekeknek, akik káros, veszélyes tartalmakkal vagy visszaéléssel, zaklatással találkoznak az interneten.
Az UNICEF Magyar Bizottság Alapítvány 2016 májusában indította el – elsősorban felnőttek és szakemberek számára – jogsegély vonalát a Bibó István Szakkollégiummal együtt, ahová várják a jogi természetű kérdéseket a gyermekbántalmazás vagy a gyermekjogok más módon történő megsértése kapcsán; ideértve a biztonságos internethasználattal kapcsolatos ügyeket is (http://unicef.hu/unicef-jogsegely/). A 2014. évi „Biztonságosabb Internet Nap” rendezvény alkalmából a szervezet által életre hívott, gyermekeknek szóló okostelefon applikáció, a HelpAPP (http://www.unicef.hu/helpapp/) elnyerte az Év Legjobb Gyermekvédelmi Tartalma különdíjat. A világon elsőként kifejlesztett applikáció erőszak-helyzetekben azonnali segítséget nyújt a gyermekeknek. Ha a gyermeket bántják, vagy veszélyben van, egyetlen gombnyomással segítséget hívhat, vagy elküldheti tartózkodási helyének GPS koordinátáit. Az alkalmazás segítségével tanácsot kérhet arra vonatkozóan is, mit mondjon, vagy mit tegyen a gyermek, ha erőszak érte, vagy segíteni szeretne valakit, akit erőszak ért.
A gyermekekre káros és jogellenes tartalmak elleni küzdelemben szintén jelentős szerepet vállal a Nemzetközi Gyermekmentő Szolgálat.

3.9.3 A gyermekek érdekeinek védelme hivatalos eljárások (igazságszolgáltatás) során

Ahogyan arról a 2.2.2 pontban is szó esett, a gyermekek különféle „minőségükben” kerülhetnek kapcsolatba az igazságszolgáltatással: lehetnek egy eljárás során tanúk (bizonyos esetekben), sértettek vagy akár elkövetők. A gyermekközpontú igazságszolgáltatás olyan igazságszolgáltatási rendszer, amely az elérhető legmagasabb szinten biztosítja a gyermekek jogainak tiszteletben tartását és

hatékony érvényesítését, elsődleges szempontként juttatja érvényre a részvételükkel folyó, vagy őket érintő minden ügyben a gyermekek mindenekfelett álló érdekeit.

A gyermekbarát igazságszolgáltatás megteremtésének egyik eszköze az úgynevezett gyermekmeghallgató szobák létesítése, amelynek célja, hogy a nyomozó hatóság, illetve a bíróság a gyermekkorú meghallgatását olyan helyiségben foganatosítsa, amelyben a büntetőeljárás céljával összhangban biztosítható, hogy az eljárási cselekmény a gyermekkorú lehetőség szerinti kíméletével, a gyermek mindenekfelett álló érdekét szem előtt tartva valósuljon meg.

A gyermek mindenekfelett álló érdeke az ilyen életkorú tanúk esetében döntően azt jelenti, hogy a lehető legnagyobb mértékben megóvjuk őket a büntetőeljárás természetéből fakadó ártalmaktól.

II. SWOT analízis

Tudatosítás és médiaműveltség

Erősségek	Gyengeségek
➢ A tudatosság elterjedéséhez szükséges háttéranyagok, civil szervezetek, illetve a megfelelő tudással bíró szakértői kör rendelkezésre áll; ➢ A civil szféra, az ipar és az oktatási intézmények között együttműködés indult el a gyermekek biztonságos internethasználatához kapcsolódó egyes kérdésekben, ennek köszönhetően több pozitív eredménnyel járó program megvalósult; ➢ A gyermekek a médiahasználattal kapcsolatban sokszor jelentős tudás és tapasztalat birtokában vannak, amelynek hatékony kiaknázása nemcsak saját maguk, de kortársaik, illetve az idősebb generációk tudatosságának növelésére egyaránt jól felhasználható; ➢ A médiaműveltség erősítése érdekében erős elköteleződést nyilvánított ki valamennyi érintett szereplő; ➢ A hazai infrastruktúra fejlettségének, illetve a birtokukban lévő digitális eszközök nagy számának köszönhetően a gyermekek többsége rendelkezik tapasztalattal az internethasználatot illetően.	➢ A tudatos internethasználat szükségessége, a médiaműveltség kérdése nem bír a társadalomban kellő szintű beágyazottsággal; ➢ Az elméletben megfelelő szinten biztosított oktatás a gyakorlatban nem valósul meg maradéktalanul és kellő hatékonysággal; ➢ Az internethasználat kultúrájának megváltoztatásához és a médiaműveltség növeléséhez a társadalom valamennyi szereplőjének együttes közreműködésére lenne szükség; ➢ A tapasztalatok szerint a gyermekek számára legszorosabb kapcsot jelentő szülők túlnyomó része nincs teljes mértékig tisztában az internet tudatos használatának eszközeivel, illetve a veszélyeivel; ➢ A piaci szereplők aktív közreműködését elősegítő programok, állami támogatások rendszere nem alakult ki intézményesített és hosszú távra kiszámítható formában.
Lehetőségek	**Veszélyek**
➢ A köznevelési rendszer kisebb átalakítása oly módon, hogy abban a médiaműveltség kérdése a jelenleginél jelentősebb hangsúlyt kapjon; ➢ Aktív állami közreműködéssel nemcsak a gyermekek számára, de életkortól függetlenül biztosítható a tudatos internethasználat elsajátítása, amelynek hatása nem kizárólag az érintetteken fejti ki pozitív hatását; ➢ A pedagógusok alapvető digitális	➢ Az érintettek egy jelentős hányada nem tud, vagy nem akar tudomást szerezni a tudatos internethasználat hiányából fakadó, lehetséges káros következményekről; ➢ A médiaműveltség fejlesztésére irányuló törekvésnek a Nemzeti alaptantervben való feltüntetése önmagában nem biztosítja a téma köznevelésben történő tényleges megjelenését;

kompetenciájának megszerzése és fejlesztése (például az állam általi támogatáson keresztül) önmagában számos probléma felismerésére és megelőzésére alkalmas; ➢ A médiaműveltség növelésében kiemelt szerep hárul a médiára, azon belül is kifejezetten az internetes szolgáltatásokra.	➢ A gyermekeket óvni kívánó szülők, pedagógusok részéről az internethasználatra vonatkozó túlzott tiltás éppen az elérni kívánttal ellenkező eredményre vezethet; ➢ A gyermekek, illetve a szülők, pedagógusok médiaműveltségének fejlesztése érdekében tevékenykedő állami, szakmai és civil szervezetek egymástól elszeparált, párhuzamosságokat is magában foglaló tevékenysége a hatékonyság rovására mehet; ➢ Az internethasználat veszélyeinek túlzott hangsúlyozása, felnagyítása az abban rejlő lehetőségek háttérbe szorulása mellett a médiaműveltség megteremtését is hátráltatja.

Védelem és biztonság

Erősségek	**Gyengeségek**
➢ A társadalom egyes rétegeiben az uniós átlag körüli az internethasználat mértéke, így különösen a magasabban iskolázott társadalmi csoportok körében; ➢ A bűnüldöző szerveknél a kiberbűnözésre szakosodott külön szervezeti egységek működnek; ➢ A jogi szabályozást és jogalkalmazást támogató, kiegészítő Hotline-ok/forródrótok működnek; ➢ Több hatósági és civil kezdeményezés létezik a digitális gyermekvédelem és médiaműveltség terén (Internet Hotline, Bűvösvölgy, Gyermekvédelmi Internet-kerekasztal, Gyermekbarát Internet Program).	➢ Jóval az uniós átlag feletti a digitális írástudatlanság szintje; ➢ Az internethasználók között jelentős a kizárólag alapszintű szolgáltatásokat használók aránya; ➢ Jelentős mértékben hiányzik a tényleges társadalmi felelősségvállalás a területen; ➢ A köznevelésben az informatika tantárgyon kívül más tárgyak keretei között nem fejlesztik kellőképpen a digitális kompetenciákat; ➢ Nem áll rendelkezésre olyan, a legnépszerűbb operációs rendszerek mindegyikén működőképes szűrőszoftver, ami magyar nyelvű és ingyenesen letölthető; ➢
Lehetőségek	**Veszélyek**
➢ Olyan szűrőszoftver(ek) fejlesztése, mely megfelel a törvényi előírásoknak;	➢ A nem megfelelő szülői/pedagógusi felvilágosítás, iskolai oktatás

➢ Gyermekbarát böngésző fejlesztésének vizsgálata; ➢ A gyermekbarát, a gyermekek médiaműveltségnek növelését célzó online tartalmak választékának növelése; ➢ Az online megfélemlítés (*cyberbullying*) hatékonyabb kezelése a meglévő jogszabályi kereteken belül; ➢ A digitális írástudatlanság csökkentése, képzések, fejlesztések elindítása; ➢ A biztonságos internethasználatot lehetővé tevő hatékony műszaki megoldások követelményének bevezetése.	hiányában a gyermek nagyobb veszélynek van kitéve az online térben; ➢ A legkisebb korosztály egy része a rendelkezésre álló, a gyermekek védelmét célzó technológiai megoldások széles körű elterjedése hiányában olykor védtelen a veszélyekkel szemben; ➢ Nem minden tekintetben hatékonyan alkalmazható a jogszabályi háttér, a jogsértőket/elkövetőket nehéz felelősségére vonni; ➢ Sem a gyermekek, sem a pedagógusok nem kapnak megfelelő oktatást, képzést az online világ veszélyeiről, azok kezelési lehetőségeiről.

Szankcióalkalmazás és segítségnyújtás

Erősségek	Gyengeségek
➢ A kialakult veszélyhelyzetek, sérelmek megfelelő kezeléséhez szükséges háttéranyagok, illetve szakértői kör rendelkezésre áll; ➢ Állami és iparági szereplők, illetve a civil szféra egyaránt hangoztatott elkötelezettsége a digitális gyermekvédelem mellett; ➢ Jogrendszer valamennyi magatartás és felmerülő élethelyzet kezelésére elvben alkalmas lehet jelen állapotában is; ➢ A gyermekekre veszélyes tartalmak bejelentésére alkalmas hotline-ok üzemelnek (Internet Hotline, Biztonságosinternet Hotline).	➢ Az érintett szereplők párhuzamos tevékenysége sok esetben rontja a feladatellátás hatékonyságát; ➢ A veszélyes, káros, jogsértő tartalmak eltávolítását segítő eljárási lehetőségek ismertségének hiánya; ➢ Nem áll rendelkezésre minden tekintetben széles körű, az internetes gyermekvédelem hatékonyságának növeléséhez, az állami cselekvés megalapozásához szükséges adat, információ, kutatás; ➢ A sérelmet okozó, illetve azt elszenvedő gyermekek jogtudatosságuk hiányából fakadóan az online térben elkövetett tetteket nem értékelik megfelelően, jelentős a látencia aránya; ➢ Az áldozatsegítésben részt vevő személyek, intézmények nem minden esetben bírnak kellően alapos ismerettel a digitális gyermekvédelem területén felmerülő helyzetek kezeléséhez.

Lehetőségek	Veszélyek
➢ A piaci, iparági szereplők aktívabb szerepvállalásra, társadalmi felelősségvállalásra ösztönzése; ➢ Az alternatív, resztoratív vitarendezési eljárások, önszabályozási mechanizmusok szerepének és súlyának növelése; ➢ A gyermekek bevonása az egyes gyermekvédelmi programok megvalósításába (például kortárs mentorképzés); ➢ A hatáskörrel rendelkező állami szervek (nyomozó hatóságok, rendészeti szervek, bíróságok) részéről nagyobb hangsúllyal lehetnek vizsgálhatók az online térben megvalósuló, a gyermekekre veszélyes magatartások tényállásszerűsége, illetve szankcionálása; ➢ A leggyakrabban felmerülő internetes jogsértések (például a *cyberbullying*) megelőzésének, kezelésének hatékonysága különféle programok segítségével jelentősen javítható.	➢ A túlszabályozás nagymértékben gyengítheti az elérni kívánt célok érdekében alkalmazható eszközök hatékonyságát; ➢ A digitális világ gyorsan változó jellegére tekintettel a gyermekekre leselkedő veszélyeknek folyamatosan újabb formái és módjai jelennek meg; ➢ Nem minden, a gyermekvédelem területén érintett szereplő számára biztosított a kellő szintű (anyagi és humán) erőforrás a szükséges feladatok ellátásához; ➢ A szülők, pedagógusok, vagy maguk a gyermekek a cselekvési szabadságukba való beavatkozásnak tekinthetik az aktív állami szerepvállalást e területen; ➢ Az online tér sajátosságai révén könnyen megkerülhetőek a gyermekek digitális védelmét szolgáló intézkedések, nagyban csökkentve az erőfeszítések hatékonyságát.

III. Cél- és eszközrendszer

1. Jövőkép

Magyarország Digitális Gyermekvédelmi Stratégiájának célja, hogy elősegítse a gyermekek, a családok, a közösségek, a civil szervezetek, az oktatási intézmények és az állami intézményrendszer hatékonyabb felkészítését az értékteremtő internethasználatra. A digitális kultúra egyre növekvő mértékben, meghatározó módon befolyásolja mindennapi életünket, társadalmunkat és gazdaságunkat. Az információs társadalom polgára számára a tudatos internethasználat mint a digitális kultúrához való hozzáférés csatornája az egyik legfontosabb, rendkívül összetett képesség. A tudatos, értékteremtő internethasználat multiplikátor jellegű sikereket hoz mind az egyéni kapcsolattartás, életminőség, mind a társadalmi kapcsolatok, mind pedig az ország versenyképessége terén.

A tudatos, értékteremtő internethasználat támogatása mellett a stratégia kiemelt célja az internethasználat során a gyermekeket fenyegető veszélyek, kockázatok azonosítása és felmérése, a káros hatások lehető legnagyobb mértékű csökkentése, illetve kiküszöbölése érdekében. A stratégia foglalkozik az online térbe való belépést megelőzően szükséges tudás, ismeret átadásának, megszerzésének kérdései mellett a biztonságos internethasználat megvalósulásához szükséges feltételek biztosításának támogatásával, illetve az esetlegesen bekövetkezett káros következmények enyhítésével.

A stratégia épít a korábbi évek hasonló tárgyú kormányzati programjainak eredményeire, elsősorban az első (2012) és a második (2013) Gyermekbarát Igazságszolgáltatás törvénycsomag vívmányaira.

A stratégia középpontjában a gyermekek állnak, de ezzel együtt a társadalom szinte valamennyi csoportja érintettnek tekinthető; a gyermekekkel szoros, mindennapi kapcsolatban álló személyek (szülők, pedagógusok), az állami intézményrendszer, az iparági szereplők és az e területen működő civil szervezetek egyaránt. Az információs társadalom elsősorban hálózati társadalom; a nemzedékek közötti együttműködés, a kölcsönös tudásmegosztás és tanítás, a társadalom különböző szereplőinek összefogása elengedhetetlen a siker érdekében.

A kérdés megnyugtató kezelése tágabb perspektívát is igényel. A képzés a tanulás szempontjából is kiemelten fontos, különös tekintettel a gyorsan változó technológiai-munkaerőpiaci viszonyokhoz való alkalmazkodásra, valamint a jövőbeni érvényesülés szempontjára. Amennyiben a megfelelő képességekkel felvértezett fiatalok biztonságos környezetben tudják használni a digitális világ nyújtotta

lehetőségeket, úgy nemcsak a saját egyéni versenyképességük javul, de közösségüké, így az országé is. A stratégia elsődleges célja ezért annak biztosítása, hogy a gyermekek tudatos, az online tér lehetőségeit, kihívásait és veszélyeit egyaránt ismerő, tudásukat magas szinten használó felnőttekké válhassanak.

A gyermekek a technológiai fejlődés utóbbi évtizedekben történt rohamos felgyorsulásának köszönhetően az internethasználat terén sok esetben – bizonyos értelemben – jelentősebb tapasztalattal és szélesebb körű ismerettel bírnak, mint az oktatásukban, nevelésükben elsődleges szerepet játszó felnőttek. Éppen ezért elkerülhetetlen ez utóbbi személyi kör bevonása egyes stratégiai célkitűzések megvalósításába. Ezen sajátos helyzet kezelése a stratégia egyik kulcspontja, hogy a tudatos és biztonságos internethasználathoz szükséges információk megfelelő módon eljussanak a gyermekekhez; a tudást átadó személyi kör (szülők, oktatók stb.) médiaműveltség- vagy médiatudatosság-képzése így tehát kiemelt jelentőséggel bír a stratégiai célok megvalósulása érdekében.

A gyermekek magas szintű oktatása mint célkitűzés értelemszerűen magával vonja az oktatói bázis képzését is. Ennek kiindulópontjaként nem mellőzhető a jelenlegi állapot felmérése, hiszen megfelelő adatok, információ hiányában a szükségessé váló feladatok elvégzése sem valósulhat meg teljes hatékonysággal. A médiaműveltség fejlesztése terén számos kezdeményezés (az állami szereplők, valamint a civil szféra és az érintett iparág részéről is) létezik, így e gyakorlati tapasztalatok felhasználhatóak a további feladatok megvalósítása során. Fontos azonban már előre leszögezni, hogy a tudatos internethasználat jóval többet jelent a biztonságnál, magában foglalja az online tér nyújtotta lehetőségek kihasználásának képességét is.

A megfelelő szintű tudás átadása mellett a biztonságos internetezéshez szükséges – az internethasználók tevékenységén kívül eső – feltételek biztosítása is kiemelt cél. A biztonságos internethasználat feltételrendszere a kellő hatékonyságú védelmi mechanizmusok felállítása és működtetése nélkül nem valósulhat meg. Az előzőekben említettek szerint, míg a tudatosítás mind az internetezés veszélyeinek, mind pedig lehetőségeinek felismerésére vonatkozó készségek, ismeretek elsajátítását foglalja magában, addig a biztonság megteremtésének az online tér potenciálisan káros vagy veszélyes hatásaival szemben kell védelmet nyújtania. Ugyanakkor a biztonságos internethasználat előfeltétele a tudatos médiahasználat (médiaműveltség) képességének megléte az egyes felhasználóknál, illetve a rájuk befolyást gyakorló felnőtteknél; ilyen tekintetben az egyes célkitűzések szoros összefüggése, egymásra hatása magától értetődő.

A stratégia által kitűzött cél, hogy a rendelkezésre álló védelmi mechanizmusok megfelelőképpen, hatékonyan betöltsék funkciójukat. Az ehhez elvezető út nem elsősorban a további törvényi tilalmak felállításán keresztül vezet; a jogrendszer e

tekintetben nagyjából eljutott oda, ahová eljuthat, azaz széles körű korlátozások és tilalmak igyekeznek biztosítani a gyermekek online biztonságát. A jogrendszer jelenlegi állapotában csak kisebb korrekciók szükségesek, nem pedig új, büntetendő magatartások vagy korlátozó intézkedések törvénybe foglalása. A korlátozások hatékonyságának növelése részben a rendelkezésre álló technikai megoldások folyamatos monitorozásán, fejlesztésén keresztül valósulhat meg, kiemelt szerepet szánva a telekommunikációs iparág képviselőinek, részben pedig olyan – kifejezetten gyermekek számára készült – tartalmak előállítása által, valamint a megfelelő internetes felületek létrehozása révén, amelyeken keresztül a szükséges ismereteket, tapasztalatokat érettségi szintjüknek megfelelően elsajátíthatják.

A jövőkép kialakítása során nem szabad figyelmen kívül hagyni az egyes esetekben óhatatlanul bekövetkező sérelmek káros következményeinek enyhítését sem. A sérelmek, károk felismerése, a szankcionálásban és a kárt elszenvedők számára való segítségnyújtásban részt vevő szervezetek és alkalmazott módszerek ismerete szintén megfelelő szintű, tudatos internethasználatot feltételez. A sérelmek kezelése, illetve jövőbeli elkerülése érdekében aktív állami és civil fellépésre van szükség; e téren a hatékonynak bizonyult programok, eljárásrendek alkalmazási körének kiterjesztése, valamint alkalmazása hozzájárulhat a kívánt eredmények, illetve állapot eléréséhez.

2. A stratégia célrendszere

2.1 Átfogó stratégiai célok

Az internetes gyermekvédelemnek a stratégia helyzetértékelésében bemutatott keretei, illetve az elérendő célokat felvázolt jövőkép között meglévő eltérések, hiányok alapján felállítható a stratégia célrendszere. Ez a célrendszer nemcsak a hiányok pótlását, de a kialakított, működő rendszer hosszú távú fenntarthatóságát, üzemeltetését is szolgálja. A célrendszer kialakítása során segítséget nyújt a SWOT analízisben szereplő összefoglaló értékelés, amely segítségével azonosíthatóak mind a jelenlegi állapot, mind pedig az elérni kívánt célok tekintetében ismert pozitív és negatív körülmények, illetve a stratégia céljainak elérését befolyásoló feltételrendszer.

A célkitűzések megalkotásakor a Kormánynak mindenekelőtt figyelemmel kellett lennie az általa elfogadott Nemzeti Infokommunikációs Stratégia (2014-2020) vonatkozó elvárásaira, illetve az ott kitűzött célok eddigi megvalósulására. Jelen stratégiában megfogalmazott célok ezen túlmenően hasonlóságot mutatnak az Európai Bizottság által „A gyermekbarát internet európai stratégiája" címmel 2012-ben kibocsátott közleményben [COM(2012) 196] megfogalmazott elvárásokkal. A bizottsági közlemény az alábbi pillérek mentén fogalmazza meg javaslatait a tagállamok részére:

- A gyermekeknek és fiataloknak szóló minőségi online tartalmak;
- Tudatosságnövelő és felkészítő intézkedések fejlesztése;
- Biztonságos online környezet teremtése a gyermekek számára;
- Küzdelem a gyermekek szexuális zaklatása és kizsákmányolása ellen.

A stratégiának a gyermekek internethasználatára, illetve az ezzel szorosan összefüggő kérdésekre kell összpontosítania. A célrendszert ennek megfelelően oly módon szükséges meghatározni, hogy az egyes pillérek által lefedett területeken felmerülő kérdésekre, problémakörökre megfelelő választ, megoldást nyújtson. Tekintettel arra, hogy a gyermekek internethasználatához kapcsolódó kérdésekben az állami intézményrendszeren túl is számos egyéb szereplő érintett, a célok meghatározása során a társadalom széles rétegeire aktív szerep és feladatkör hárul.

Jelen stratégia átfogó célja tehát a biztonságos, tudatos és értékteremtő internethasználathoz szükséges ismeretek átadása a gyermekek számára, részben maguknak a gyermekeknek, részben pedig a velük napi szintű kapcsolatban lévő, fejlődésükre a legnagyobb hatást gyakorló személyek képzésén, oktatásán keresztül.

A stratégiának célja továbbá a biztonságos internethasználathoz szükséges hatékony védelmi megoldások ismeretének és elérhetőségének folyamatos

biztosítása, illetve a bekövetkezett sérelmek szakszerű, a későbbi káros hatások csökkentésével és a jogsértések megismétlődésének megakadályozásával járó orvoslása.
Mindezek fényében Magyarország Digitális Gyermekvédelmi Stratégiájának célkitűzése a helyzetértékelésben is követett pillérszerkezet alapján az alábbiakat foglalja magában:

I. pillér: Tudatosság és médiaműveltség

- Az egyes konkrét intézkedések megkezdése előtt átfogó felmérést kell elvégezni az iskolákban megvalósuló médiaértés-oktatás hatékonyságát, eredményességét illetően;
- A gyermekek médiaoktatása kapcsán alapvetően megvalósítandó célkitűzés szerint a gyermekeket fel kell készíteni az online szolgáltatások megfelelő használatára, a lehetőségek kiaknázására éppúgy, mint a veszélyek elkerülésére, illetve megfelelő kezelésére, valamint jogtudatosságuk megteremtésére;
- A tanárok képzése és a tananyagfejlesztés tekintetében a médiaoktatásban részt vevő tanárok számára friss, versenyképes, releváns tudás átadása a képzésben, valamint a megszerzett tudás folyamatos aktualizálásának lehetőségének megteremtése;
- A gyermekek médiaoktatása mellett figyelmet kell fordítani a szülők ilyen irányú tudatosságának és tudásának növelésére is;
- A szülők és egyéb érdekeltek ismereteinek bővítése keretében a gyermekek sérelmére elkövetett bűncselekményekkel vagy jogsértésekkel hivatásuknál fogva szükségszerűen kapcsolatba kerülő személyek (kiemelten az ilyen ügyekben eljáró nyomozó hatóságok, rendészeti szervek, bíróságok képviselői) médiatudatossági képzésének megteremtése – a szülők fakultatív képzésének lehetősége mellett;
- Egy gyűjtőhonlap létrehozásával az internetes gyermekvédelem területén rendelkezésre álló információk könnyű és mindenki számára rendelkezésre álló elérhetőségét kell megteremteni.

II. pillér: Védelem és biztonság

- A gyermekek számára biztonságos internethasználat feltételeit lehetővé tevő szűrőszoftver, illetve kifejezetten gyermekbarát böngésző elérhetővé tételének megvizsgálása, folyamatos fejlesztése;
- A káros tartalmak szűrésére alkalmas, a nemzetközi gyakorlatban bevett megoldások tapasztalatainak felmérése, lehetséges hazai megvalósításának előzetes értékelése;

- Az iparági részvétel erősítése elengedhetetlen, ez ugyanis nagymértékben előmozdíthatja az egyes védelmi megoldások hatékonyságát;
- Az állam aktív szerepvállalására van szükség a kifejezetten a gyermekek számára készült online tartalmak gyártásának támogatása érdekében.

III. pillér: Szankcióalkalmazás és segítségnyújtás

- Az online térben elkövetett jogsértő cselekmények számára, tendenciájára, hatására vonatkozó adatgyűjtés és rendszeres monitorozás szükséges a valós problémák megismerése és hatékony kezelése érdekében;
- A sérelemkezelés alternatív (jóvátételi) megoldásainak nagyobb szerepet kell kapnia a gyermekek által, illetve sérelmükre elkövetett cselekmények orvoslásakor;
- Az online megfélemlítés visszaszorítása, illetve az azzal szembeni hatékony fellépés megfelelő programok indítását, illetve a sérelmek kezelésében részt vevők képzését követeli meg;
- A meglévő jogorvoslati mechanizmusok szélesebb körű megismertetése szükséges.

2.2 Pillérenkénti célok

Az alábbiakban az egyes átfogó, stratégiai célkitűzések pillérek szerinti bontásban kerülnek részletes bemutatásra.

2.2.1 Tudatosítás és médiaműveltség

Átfogó cél: a gyermekek mellett a pedagógusok számára olyan rendszeres, a naprakész tudás elsajátítását segítő képzési lehetőségek biztosítása, illetve bizonyos esetben azoknak a számukra kötelezően előírt tananyag részévé tétele, amelyek segítségével a biztonságos internethasználathoz és egyben az online kultúra tudatos és kreatív alkalmazásához elengedhetetlen kompetenciák birtokába kerülhetnek. A cél részét képezi a szülők médiaműveltségének növelése is.

C1) Monitoring-rendszer felállítása és rendszeres mérések, kutatások végzése

A gyermek internethasználatát, annak folyamatos változásait, az őket ért károk és felmerülő veszélyek körét – lehetőség szerint korcsoport szerinti bontásban, az életkori sajátosságokat is figyelembe véve – rendszeres, legalább évente elvégzendő, nagymintás, megbízható, a döntés-

előkészítést szolgáló eredményeket adó mérésekkel kell vizsgálni. Az eredményeket nemcsak önmagukban és longitudinálisan, de nemzetközi összehasonlításban és kontextusban is értékelni kell, így más országok eredményeivel összevetve jobban kirajzolódnak a szükséges beavatkozási területek. A kvantitatív döntés-előkészítő mérések mellett (az intergenerációs együttműködés jegyében is) szintén szükséges egy – a gyermekek helyzet- és életmegélését kvalitatív módon feldolgozó – alapkutatás is.

C2) A gyermekek médiaműveltség-oktatása

A gyermekek médiaműveltségre való oktatását a köznevelés rendszerén belül új alapokra kell helyezni, hogy megfeleljen az online médiavilág által támasztott követelményeknek, ugyanakkor ne növelje jelentősen a gyermekek és a pedagógusok terheit sem.

C3) Tanárképzés és tananyagfejlesztés

A gyermekek köznevelésben való megfelelő oktatásának előfeltétele a tanárképzés megújítása a médiaműveltséggel kapcsolatos kompetenciák megszerzése tekintetében. A rendszeresen frissülő, nyomtatásban és online is elérhető tananyagok, tansegédletek, oktatói kézikönyvek előállítása – a meglévő anyagok felhasználásával – is alapvető fontosságú feladat. E folyamat során nemcsak a tananyagok, hanem maga a tanulás és a tanítás folyamata is jelentősen növelni fogja az értékteremtő internethasználatot.

C4) Az egyéb érdekeltek képzése

Az igazságszolgáltatás és a rendészet azon szereplőit, akik gyermekvédelmi kérdésekkel találkoznak munkájuk során, a médiaműveltség tekintetében folyamatosan képezni szükséges, valamint lehetővé kell tenni a képzésben való részvételt a szülők számára is. Az igazságszolgáltatás szereplői mellett kiemelt figyelmet kell fordítani a gyermekvédelem tágabb környezetének szereplőire – többek között az iskolapszichológusokra, a szociális munkásokra, a gyámügyi dolgozókra, a rendőrökre – is. E szereplők számára felelősségüket, szerepüket és lehetőségeiket, feladataikat egyértelműsítő, folyamatosan frissített sorvezetők elkészítésére és eljuttatására van szükség.

Az említett körön kívül a képzési lehetőséget javasolt kiterjeszteni magukra a szülőkre, továbbá az állami gyermekvédelem rendszerében dolgozó egyéb szereplőkre egyaránt.

C5) Gyűjtőhonlap és hitelesítés

Az internetes gyermekvédelem területén rendelkezésre álló információkat ingyenessé és könnyen elérhetővé kell tenni mindenki számára, valamint létre kell hozni egy olyan rendszert, ahol a ténylegesen hasznos, alkalmazható információt, tudást hordozó anyagokat megfelelően hitelesíti egy szakértőkből álló testület.

A fentiek alapján a tudatosítás és médiaműveltség-pillér célrendszere az alábbi:

C1) Rendszeres, átfogó internetes gyermekvédelmi mérések, kutatások elvégzése.

C2) A gyermekek médiaoktatásának átalakítása.

C3) A tanárok képzésének átalakítása és a szükséges tananyagok előállítása.

C4) Az igazságszolgáltatás érintett szereplőinek és az állami gyermekvédelemben rendszerében dolgozók kötelező képzése, a szülők képzési lehetőségének megteremtése.

C5) Az információk könnyű elérhetőségének megteremtése és a hitelesítés rendszerének felállítása.

2.2.2 Védelem és biztonság

Átfogó cél: a biztonságos internethasználathoz szükséges jogi és technikai feltételek és egyéb megoldások biztosítása, illetve elérhetővé tétele, emellett pedig a gyermekek érettségi szintjének megfelelő internetes tartalmak bővítése.

C1) Megfelelő szűrőszoftver-megoldások folyamatos biztosítása

A jelenlegi jogszabályi követelményeknek eleget tevő szűrőszoftver-megoldás elérhető és letölthető a szolgáltatók internetes oldalán keresztül, arra azonban nincs garancia, hogy a szoftver hosszú távon is ingyenesen

hozzáférhető marad. Emellett jelenleg nem alkalmazható a legelterjedtebb operációs rendszerek mindegyikére az említett szoftver, így alapvető célkitűzés, hogy állami támogatás mellett olyan szűrőszoftver-megoldások kerüljenek kifejlesztésre – az Eht. 149/A. §-ban foglaltakkal összhangban –, amelyek széles körben és hosszú távon ingyenesen elérhetők bárki számára; ezzel egyidejűleg hozzásegítve az internethozzáférés-szolgáltatókat a törvényi kötelezettségüknek való megfeleléshez. A szűrőszoftver fejlesztésekor figyelembe kell venni a mobil eszközök (okostelefon és tabletek) térhódítását is az internethasználatban.

C2) Káros tartalmak szűrésének alternatív megoldásai

A szűrőszoftver mellett a káros tartalmak gyermekektől való távoltartásának egyéb megoldásait is célszerű számba venni, amelyekre egyébként külföldi minták is rendelkezésre állnak. Szükségesnek mutatkozik e külföldi gyakorlatok számba vétele, hatékonyságának vizsgálata, az ezekkel kapcsolatos tapasztalatok összegyűjtése, kiértékelése, illetve esetleges hazai megvalósításuk várható hatásainak elemzése.

C3) Hatékony műszaki megoldások alkalmazása

A médiaszabályozás értelmében a kiskorúak számára különösen káros tartalmak csak hatékony műszaki megoldások alkalmazása esetén tehetők közzé; a Médiatanács ezen megoldásokra nézve ajánlást fogadott el (helyzetértékelés 2.4.5. pont). Az előbbiekben megfogalmazottak kizárólag a médiaszabályozás hatálya alá tartozó internetes tartalmakra (lekérhető médiaszolgáltatásokra, internetes sajtótermékekre) nézve fogalmazzák meg a követelményt; a Médiatanács ajánlása ezen túlmenően a műsorterjesztőkre nézve tesz javaslatokat a gyermekzár megoldásokat illetően. (Az ajánlást legutóbb 2014 márciusában módosította a Médiatanács, így – az azóta keletkezett tapasztalatok felhasználása mellett – ennek felülvizsgálata időszerű.)
Az internetes tartalmak (elektronikus kereskedelmi szolgáltatások) nagyobb hányadával szemben tehát jelenleg nincs törvényi követelmény a gyermekek hozzáférését szűkítő műszaki megoldások alkalmazását illetően. A védelem hatékony formája lehet a műszaki megoldások alkalmazási körének kiterjesztése a gyermekek számára káros tartalmakat illetően.

C4) Veszélyes és javasolt tartalmak kezelése (black list és white list)

Szükséges olyan listák összeállítása, amelyek egyfelől a gyermekek számára kifejezetten káros, esetleg jogsértő tartalmakat *(black list)*, másfelől pedig az elsődlegesen nekik szánt, kulturális-oktató jellegű online tartalmakat gyűjtik össze *(white list)*, amely listák nagy segítséget jelentenek a veszélyes tartalmak szűrésénél, illetve – a tudatos médiahasználat körében – a kiskorúak számára az életkoruknak megfelelő tartalmakhoz való hozzáférésben. A listák összeállítása és állandó frissítése folyamatában egy szakértői testület igénybevétele szükséges. A listák felügyeleténél figyelembe kell venni a különböző életkorú, társadalmi- és gazdasági helyzetű gyermekek esetlegesen eltérő szükségleteit és igényeit is.

C5) Az iparági társszabályozás erősítése

Célszerű a jelenleg már működő ön- és társszabályozó szervezetek tevékenységében rejlő előnyöket (például gyorsaság, hatékonyság) nagyobb mértékben kihasználni. A média- és hírközlési piacon tevékenykedő szervezetek számára olyan együttműködési lehetőségeket szükséges biztosítani, amelyek segítségével a piaci szereplők maguk is hozzájárulnak az online gyermekvédelem hatékonyabb érvényesüléséhez.

C6) A büntetőjog ultima ratio jellege

Az igazságszolgáltatás szereplőit megfelelő szintű képzésben kell részesíteni annak érdekében, hogy az online térben elkövetett jogsértő cselekményeket, azok sokrétű, sajátos jellegére tekintettel megfelelőképpen felismerjék és minősítsék. Az ismeretek átadása mellett elengedhetetlen a jogszabályok alkalmazásának hatásait, következményeit rendszeresen értékelni, és a tapasztalatokat felhasználni a későbbi képzések során.

C7) A gyermekek számára biztonságos és hasznos tartalmak körének bővítése

A káros, sérelmes tartalmaktól való védelem mellett szintén fontos annak támogatása, hogy a gyermekek lehetőség szerint minél nagyobb arányban találkozzanak kifejezetten számukra készült, nekik szánt tartalmakkal az online térben is. E tartalmak szerteágazó jellegűek és témájúak lehetnek; e

körbe tartoznak maguk a gyermekek által készített médiatartalmakat megjelenítő oldalak is.

A fentiek alapján a védelem és biztonság-pillér célrendszere az alábbi:

C1) A törvényi követelményeknek és a technológiai kívánalmaknak eleget tevő szűrőszoftver elérhetővé tétele.

C2) Az alapbeállításként bevezetett hálózati szintű szűrőeszközök várható hatásainak, következményeinek előzetes értékelése.

C3) A hatékony műszaki megoldások alkalmazási lehetőségeinek átgondolása a médiaszabályozás által nem érintett internetes tartalmak vonatkozásában.

C4) Gyermekek számára káros, jogellenes, továbbá a kifejezetten számukra javasolt internetes oldalakat tartalmazó listák összeállítása, és naprakészen tartása.

C5) Az ön- és társszabályozó szervezetekkel szorosabb és hatékonyabb együttműködés kialakítása.

C6) A jogalkalmazás szereplői számára megfelelő képzés és továbbképzés biztosítása a jogsértő magatartások megfelelő szintű felismerése és értékelése érdekében.

C7) Kifejezetten a gyermekek számára készített tartalmak mennyiségének és sokszínűségének növelése.

2.2.3 Szankcióalkalmazás és segítségnyújtás

Átfogó cél: a problémák valódi súlyát, hatását felmérni képes rendszeres nyomonkövetési, értékelési struktúra kidolgozása mellett a sérelemkezelés alternatív formáinak előtérbe helyezése.

C1) Információgyűjtés

Az interneten keresztül elsősorban gyermekek által vagy sérelmére elkövetett jogsértő cselekmények volumenét illetően nem állnak rendelkezésre megbízható kutatások alapján szerzett adatok, amely

nagymértékben megnehezíti az ezekkel szemben történő fellépés hatékonyságát is. A szankcióalkalmazás és a valódi segítségnyújtás lehetővé tétele érdekében elsődleges célkitűzés az információk rendszeres és folyamatos összegyűjtése, kiértékelése.

C2) Alternatív sérelemkezelési eljárások

A vitás helyzetek hatékony, az érintett gyermekek lehető legkíméletesebb módon történő kezelése alapvető fontosságú elvárás. Ennek érdekében azoknak az egyébként létező, a gyakorlatban is bevett alternatív vitarendezési eljárásoknak a körét kell kiterjeszteni, amelyek akár az elkövető, akár a sérelmet elszenvedő gyermekek érdekeit helyezik előtérbe, és hatékonyan, gyorsan képesek megfelelő módon rendezni a felmerült problémás helyzeteket.

C3) Az online megfélemlítés (cyberbullying) kezelése

Még ha teljesen pontos adatok nem is állnak rendelkezésre, tapasztalatok bizonyítják az online zaklatás, megfélemlítés gyakori jelenlétét és sérelmes mivoltát a gyermek körében. A stratégia kiemelt célkitűzései között szerepel a probléma átfogó, széleskörű összefogás keretében megvalósuló rendezése, amely kiterjed mind a megelőzés területére, mind pedig a már bekövetkezett sérelmek káros következményeinek csökkentésére, illetve lehetőség szerinti teljes orvoslására.

C4) Feladatok a meglévő jogorvoslati mechanizmusok szélesebb körű megismertetése terén

Fontos a jogrendszerben jelen lévő sérelemkezelési eljárások, lehetőségek szélesebb körben való ismertté tétele. Ha a sérelmet elszenvedett gyermekek, illetve szüleik, tanáraik nem ismerik a rendelkezésükre álló lehetőségeket, akkor a szabályozás hatékonysága, az általa elérni kívánt hatás elvész. A szélesebb körű megismertetésnek elsősorban a Btk. és az Ekertv. vonatkozó rendelkezéseire szükséges fókuszálnia.

A fentiek alapján a szankcióalkalmazás és segítségnyújtás-pillér célrendszere az alábbi:

C1) A hatékony fellépés érdekében össze kell gyűjteni és adatbázis keretei között rendszeresen frissíteni szükséges az elkövetett sérelmes magatartások számát, jellegét, típusát.

C2) A gyermekek által vagy sérelmére elkövetett online zaklatásokat, megfélemlítéseket *(cyberbullying)* indokolt esetben alternatív vitarendezési mechanizmusok keretében kell kezelni.

C3) Kereteket és feltételeket kell biztosítani az online bántalmazások megfelelő szintű kezeléséhez és számuk lehetőség szerinti visszaszorításához.

C4) A médiaoktatásban erőteljesen meg kell jeleníteni az elszenvedett károk kezelésének jogi lehetőségeit, az alkalmazható eljárásokat.

3. A stratégia eszközrendszere

3.1 Általános megközelítés

Az eszközrendszer meghatározásának alapvető feladata, hogy a jövőképben megfogalmazott általános, illetve a célrendszerben bemutatott konkrét célkitűzések megvalósulásához szükséges és elengedhetetlen eszközöket számba vegye. Alapvető elvárás, hogy az eszközrendszer egyes pontjai a célként kitűzött feladatok eléréséhez szükséges valamennyi elemre kiterjedjenek, azonban ne tartalmazzanak olyan eszközöket, amelyek egyik célkitűzés megvalósulását sem támogatják, még csak közvetetten sem.

3.2 Eszközök pillérek szerinti csoportosítása

Az alábbiakban – a stratégiában eddig is követett pillérszerkezetnek megfelelő bontásban – szerepelnek az egyes célkitűzések megvalósításához szükséges eszközök, a hozzájuk tartozó konkrét intézkedésekkel.

3.2.1 Tudatosítás és médiaműveltség

E1.1) Monitoring-rendszer felállítása és rendszeres mérések, kutatások végzése

A gyermekek internethasználatát, annak folyamatos változásait, az őket ért károkat és felmerülő veszélyeket, illetve a problematikus, az életmódra és értékvilágra komoly hatással lévő jelenségeket – lehetőség szerint korcsoport szerinti bontásban, az életkori sajátosságokat is figyelembe véve – rendszeres, legalább évente elvégzendő, nagymintás, megbízható, a döntés-előkészítést szolgáló eredményeket adó mérésekkel kell vizsgálni. A kvantitatív méréseket kvalitatív kutatással is ki kell egészíteni, mely során a gyermekek saját meglátásai, elképzelései, tervei és élethelyzet-megélései is felszínre fognak kerülni. A képzési terveket az eredményekhez kell igazítani.
Biztosítani kell a jogszabályok gyakorlati alkalmazásának folyamatos felmérését, különös tekintettel a büntetőjog határmezsgyéjén mozgó fiatalkori devianciák, így például a kortársak megfélemlítésének és bántalmazásának (*bullying, cyberbullying*) monitorozására. A vizsgálatnak ki kell terjednie a bejelentett esetek számára, az elkövetés típusára, az elkövetők és az áldozatok karakterisztikájának rögzítésére, valamint a büntetőeljárás kimenetelének figyelemmel kisérésére, különös tekintettel a

bíróság döntésénél figyelembe vett körülményekre. Az adatgyűjtés célja a döntési folyamat megkönnyítése, az eljárási irányelvek meghatározása – tekintettel a kiskorú sértettek és a fiatalkorú elkövetők speciális védelmi igényű társadalmi csoportjára.
A preventív intézkedéseket empirikus kutatásoknak kell megelőznie. Fel kell mérni az iskolákban a médiaműveltség fejlesztésének eredményességét. Ennek részeként vizsgálni szükséges, hogy a pedagógusok milyen módszereket használnak, hogyan és milyen eszközökkel integrálják a médiaértést, médiaműveltséget a tanórák anyagába. Az eredmények nyomán lehet javaslatokat tenni, hogyan lehetséges az oktatás során aktív és biztonságos módon alkalmazni az új médiát, valamint a tanulók médiaműveltségét, felelős médiahasználatát fejleszteni.
A mérésekhez, kutatásokhoz szükséges módszertan (indikátorok és adatfelvételi eszközök) fejlesztése szükséges, mivel ezek jelenleg vagy nem állnak rendelkezésre (például az iskolai médiaoktatás eredményességére vonatkozóan), vagy nem kellően differenciáltak, és kevéssé alkalmasak az internethasználat számos lényegi aspektusának feltárására.
A civil szervezeteknek és a vállalati szereplőknek köszönhetően látszólag sok „jónak tűnő gyakorlat” áll rendelkezésre a tudatosítás terén. Ezek összegyűjtését követően releváns indikátorok alapján el kell végezni a programok szakmai értékelését és hatásvizsgálatát is. Előírandó, hogy pályázati támogatásban csak olyan programok részesülhetnek, amelyek tartalmazzák a hatásvizsgálatot és az utánkövetést is.
Ezen felül szükséges a gyermekek mint fogyasztók digitális vásárlási szokásainak vizsgálata, ennek keretében felmérve azt is, hogy a gyermek-fogyasztók online vásárlásaik során milyen típusú veszélyeknek vannak kitéve. E vizsgálat eredményei a későbbiekben alapul szolgálhatnak az elektronikus kereskedelem területén a fogyasztóvédelmi szempontú továbblépési, esetleges beavatkozási lehetőségek kialakításához.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a1.1.1) A mérésekhez, kutatásokhoz szükséges módszertan (indikátorok és adatfelvételi eszközök) fejlesztése, a kutatások pontos tárgyának meghatározása.

a1.1.2) A mérésekben, kutatásokban szerepet vállaló felsőoktatási intézmények, kutatóműhelyek, civil szervezetek azonosítása, a velük való együttműködés kezdeményezése.

a1.1.3) A mérések, kutatások évenkénti lefolytatása, az eredmények kiértékelése és közzététele.

a1.1.4) Az a1.1.1-a1.1.3 pontokban meghatározott döntés-előkészítő tudásanyagokból konkrét ajánlások, a gördülő tervezést támogató változtatások jog- és szervezetharmonizált megfogalmazása és kommunikálása a döntéshozók felé.

a1.1.5) A digitális gyermekvédelem területén működő civil szervezetek és a hírközlési, valamint a tartalomszolgáltatói piacon jelenlévő iparági szereplők számára nyitva álló, a gyermekek médiaműveltségének növelését vagy az online világ jelentette veszélyekkel szembeni megóvását célzó pályázati lehetőségek áttekintése, a pályázati feltételrendszer módosítása annak érdekében, hogy a támogatott pályázatok szakmai színvonala biztosított legyen, valamint azok hatásvizsgálatot és utánkövetést is tartalmazzanak.

a1.1.6) A gyermekek mint fogyasztók digitális vásárlási szokásainak, továbbá annak vizsgálata, hogy a gyermek-fogyasztók online vásárlásaik során milyen típusú veszélyeknek vannak kitéve, és ezek eredményei alapján az elektronikus kereskedelem területén a fogyasztóvédelmi szempontú továbblépési, esetleges beavatkozási lehetőségek felülvizsgálata.

E1.2) A gyermekek médiaműveltségének fejlesztése

A) A médiaoktatás módosítása a köznevelés rendszerében – „médiahetek”

A gyermekek médiaműveltségének fejlesztését a köznevelés rendszeren belül részben új alapokra kell helyezni, hogy megfeleljen az online médiavilág által támasztott követelményeknek és kihívásoknak, ugyanakkor ne növelje jelentősen a gyermekek és a pedagógusok terheit sem.
A NAT-ban kifejezetten fontosnak tűnhet a médiaoktatás, a kerettantervben azonban – amely ténylegesen, iskolafokonként és iskolatípusonként szabályozza a médiaoktatás tényleges megvalósulását – már csak marginális, a valós fejlesztéshez szükséges minimális időkeretek nélküli mellékszereplőként jelenik meg a média.
A médiaoktatás óraszámának jelentős növelése kevéssé járható út, mert a kötelező tanórák kereteinek komolyabb átalakítását igényelné, miközben vagy a köznevelésben részt vevők terheinek növelésével járna, vagy pedig csak más, fontos tárgyak kárára történhetne meg.

Ahhoz, hogy a helyzetértékelésben vázolt problémák tudatosításával az oktatás valóban eredményes lehessen, a tanárképzési fejlesztést kiegészítő módszerre van szükség; ezt a célt szolgálja a tömbösített és projekt-elven szerveződő intenzív médiaoktatás beindítása a 6-7, 10, 13 és 17 éves korosztályokban, vagyis az első, a negyedik a hetedik és a tizenegyedik osztályban.

Ezeken az évfolyamokon mindkét félévben kerüljön bevezetésre a délutáni sávban a „médiahét" elnevezésű, programszerű, szekciókban, kiscsoportos formában és közös, plenáris eseményekben realizálódó oktatási forma, egy héten keresztül, naponta 14 és 17 óra között.

A médiaheteken a helyzetértékelés egyes elemei (például médiahasználat/függőségek; sztereotipizáció/gyűlöletbeszéd; valóság és virtualitás keveredése; valóságismeret gyengülése/reprezentációk; adatbázisok sérülékenysége; nemlineáris olvasás kontra hagyományosan strukturált szövegek/iskolai követelmények ellentmondásai; manipuláció; mediatizált testkultúra/nemi szerepek; generációk közti átjárhatóság csökkenése/túltiltás; tudatos tartalomválasztás problémái a konvergens technikai platformokon; társadalmi egyenlőtlenségek) adják egy-egy szekció programját. Azok feldolgozása széles módszertani skálán mozoghat (meghívott vendéggel, érintettek nyilvános diskurzusával, kutatási programokkal, prezentációkkal, szülők bevonásával). A programok egy része naponta ismétlődik más-más résztvevőkkel, a gyermekek maguk döntik el, hogy az adott napon hova mennek, melyik szekció programjában vesznek részt. A médiahetek szakmai garanciája hosszabb távon a megfelelő képzésben részesülő tanárok, különösen az iskolák médiaszakos tanárai (és a tartalmi/módszertani szempontból korszerű, a programot segítő szakanyag) lehetnek. Kellő számú szaktanár hiányában azonban a médiatanárok szaktudására egy-egy tankerületben is csak a későbbiekben építhető a program, ezért a képzési forma bevezetésének időszakában kitüntetett szerepe van a programot segítő külsős oktatóknak, szakembereknek. A médiaheteken nem kötelező, csak ajánlott a részvétel. A médiaheteket követően a tanulók feladatot kapnak, amelynek eredményeiről beszámolnak.

A médiahét az iskolában megvalósuló, központilag finanszírozott úgynevezett non-formal típusú oktatás színes, érdekes és korszerű formája, mely a tanárképzéssel összekapcsolva már valós esélyt ad a médiaműveltség szerteágazó problémakötegének tudatosítására, valamint a szükséges rezisztencia megszerzésére.

Az ezekhez (tanárképzés és médiahét-programok) szükséges szellemi innováció egy, már meglévő szervezeti alapokra épülő tartalom és módszertan fejlesztési/kutatási műhely (intézet) folyamatos működését követeli meg.

Mindezzel párhuzamosan szükség lesz továbbá annak kimunkálására és a tanárképzéssel összehangolt, mielőbbi bevezetésére is, hogy minden tanár saját szaktárgyán belül (annak példatárával és ismeretanyagával dolgozva) évente minimum 5-10 tanórányi média-fókuszú tanórát tartson, amely korrelál a problématérkép valamelyik elemével, reflektál arra, tudatosítja azt.

B) Az Országos Középiskolai Tanulmányi Versenyen való részvétel ösztönzése

A média tárgyú Országos Középiskolai Tanulmányi Verseny (OKTV) nem működik megfelelően tehetséggondozási eszközként, mert nem motivál eléggé a részvételre – a legjobbakat nem premizálja sem a szakirányú felsőoktatásba lépés lehetőségével, sem egyéb módon. A középiskolai médiaoktatás súlyának növelése érdekében ennek a megváltoztatása szükséges. Az ösztönzés eszköze lehet egy kutatási mentorprogram működtetése, az ebben résztvevő egyetemi kutatók, illetve civil szakemberek kutatási tapasztalatokkal, szakirodalmakkal, a szövegírás támogatásával segítik a kutató munkát. A mentorprogram természetes szövetségese és kiegészítője a *white* és *black list*-eket folyamatosan frissen tartó szakmai testületnek. A kutatási mentorrendszer létrehozatala szintén támogatja az D) pontban bemutatásra kerülő, képzéseket és tanácsadást végző mentorhálózat működését az alaptudás növelésével, illetve a mentorok képzésével.

C) A túltiltás veszélyeinek elkerülése

Ismert jelenség, ha a szülő úgynevezett morális pánikhelyzetben a veszélyekre hivatkozva, tiltott vagy túlkontrollált hálózati léttel oly mértékben korlátozza saját gyermekének választási és cselekvési szabadságát, hogy elzárja őt az internet nyújtotta lehetőségek kiaknázásától. A „túltiltás” kontraproduktív, az eredeti szándékkal ellentétes hatást érhet el, amellyel szemben szintén az iskolai médiaműveltség-képzés nyújthat ellenszert.

D) Kortárs mentorképzési rendszer kialakítása

Szükséges az előzőeken túlmenően kidolgozni egy kortárs mentorképzési rendszert, amelyben az internethasználat előnyeit és az annak során felmerülő veszélyeket a leginkább érintettek számára a hozzájuk hasonló korú iskolások mutatják be. (Alternatív lehetőségként felvethető néhány évvel idősebb mentorok bevonása a programba; ez különösen jól megoldható olyan oktatási intézményekben, ahol általános iskola és középiskola is működik egyben, így

utóbbiak közösségi szolgálat keretében érdekeltek lehetnek a minőségi mentorálás végrehajtásában.) A mentorok feladata egyéb (kapcsolódó) területekre (például konfliktuskezelés) is kiterjedhet, jelen esetben azonban központi elemének a biztonságos internethasználatnak kell lennie. A program lényege, hogy a mentorok rövid képzést követően rendszeresen segítséget nyújtanak az érintett diákoknak. Az iskoláknak szerepet kell vállalni a mentorok képzésében, de legalábbis ismereteik bővítésében, ezen túlmenően elengedhetetlen a tevékenység vonzóvá tétele a leendő mentorok számára.

E) Digitális eszközökhöz való hozzáférés felmérése

A médiaértés-oktatás hazai helyzetének elemzését nem lehet függetleníteni a rendelkezésre álló digitális eszközpark, illetve a digitális eszközök hozzáférésének kérdésétől, valamint a digitális kompetenciától. A tapasztalatok azt mutatják, hogy ma Magyarországon az egyes köznevelési intézményekben rendkívül eltérőek az adottságok és lehetőségek a digitális eszközök tekintetében. A médiaértés-oktatás teljes körű megvalósításának egyik fontos előfeltétele lenne a digitálisan jól felszerelt köznevelési intézmények kialakítása, a meglévő súlyos egyenlőtlenségek, hiányosságok pedig folyamatos orvoslásra, fejlesztésre szorulnak.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a1.2.1) A médiahetek-program lebonyolításához szükséges első generációs szak- és illusztrációs anyagok, módszertani ajánlások, feladatgyűjtemény, értékelési szempontok elkészítése.

a1.2.2) A médiahetek-program kísérleti programjának megszervezése, lebonyolítása és értékelése a 2017/2018. tanévben, az a1.2.1) akcióban írt szak- és illusztrációs anyagokra, módszertani ajánlásokra építve – az óvoda kivételével – köznevelési intézménytípusonként legalább 25 tanintézményben, köztük legalább két gyógypedagógiai intézményben.

a1.2.3) A médiahetek-program megvalósításához szükséges első generációs (azonnali) pedagógus-továbbképzés megszervezése és lebonyolítása akkreditált, 30-60 órás, tanfolyami rendszerű továbbképzési formában, kitüntetetten építve a már pályán lévő társadalomismeret, informatika, illetve a mozgóképkultúra- és médiaismeret szakos tanárokra.

a1.2.4) A 2018-ra tervezett új NAT, az ahhoz kapcsolódó kerettantervek, tankönyvek, valamint egyéb tanulást és tanítást segítő eszközök – ideértve a minta-tanmeneteket is – összehangolása Magyarország Digitális Gyermekvédelmi Stratégiájának intézkedéseivel, kiemelten a médiahetek-program tartalmaival.

a1.2.5) Médiaműveltség és pedagógia: tartalom és módszertan fejlesztési/kutatási műhely működtetése már meglévő szervezeti alapokon.

a1.2.6) A kortárs mentorprogram feltételrendszerének meghatározása, a mentorképzésben együttműködő civil és iparági szereplők felkérése, az iskolai bevezetés előkészítése és végrehajtása.

a1.2.7) A köznevelési intézmények digitális eszközállományának felmérése, a hiányosságok feltérképezése, illetve a szükséges fejlesztések elvégzésére vonatkozó javaslat összeállítása.

E1.3) Tanárképzés és tananyagfejlesztés

A médiát oktató tanárok szakirányú képzésének és továbbképzésének átalakítása is szükséges. Ennek három szintje lehet:

- Részben a pályán lévő tanárok 60-120 órás, tanfolyami rendszerű (vagyis nem a felsőoktatást terhelő) továbbképzése;
- Részben a felsőoktatás média- és kommunikáció szakjain indítható szakosító továbbképzési szak formában megvalósítható médiaszaktanár-képzése;
- Mindezzel párhuzamosan pedig minden, a tanári pályára készülő pedagógus kötelező médiaműveltségi képzése a tanárképzés során (a pedagógiatörténet és a pszichológia mint alapstúdiumok mellett, azokkal hasonló mértékű kreditszámokkal).

Más fókuszú és tartalmú képzésre lesz szüksége az óvodapedagógusoknak, a tanítóknak, a felső tagozatra készülő tanároknak és a középiskolai tanároknak, mert más a feladatuk az egyes fejlődési szakaszokban.

Az így új alapokra helyezett médiatanár-képzés eredményezheti azt az áttörést, amely ahhoz szükséges, hogy a köznevelés rendszerét mélységében átjárja a médiatudatosságra nevelés problematikája, jelentősége és pedagógiai módszertana. Ilyen mértékű tanárképzési innováció szükséges ahhoz, hogy a tanárok felismerjék,

napirendre tűzzék és kezelni is tudják a média szocializációs kihívásait (mivel a jelen iskolája – nem, vagy alig számolva a mediatizált kultúra jelenségeivel, a gyermekeket ugyanúgy pozícionálva, mint harminc vagy ötven évvel ezelőtt – lényegében „elbeszél” a gyermekek mellett).

A pedagógusoknak alapképzésben és továbbképzésben kell részesülniük a digitális eszközhasználatot, valamint a biztonságos és etikus internethasználatot illetően. A képzés az eszközhasználaton kívül foglalja magában az eszközök órai anyagba integrálásának módszereit. A pedagógusok képzésének legyen része az online megfélemlítés, bántalmazás kockázatainak megismerése, megelőzése és kezelése, valamint a problematikus, az életmódra és értékvilágra komoly hatással lévő médiajelenségek is.

Az iskolák legyenek felkészítve az online veszélyek, különösen az online bántalmazás okozta problémák felismerésére (áldozathibáztatás elkerülése), megelőzésére és kezelésére. Ennek érdekében megfelelő tudásbeli és szakszemélyzeti erőforrásokat kell biztosítani az iskolák részére. A pedagógusok igény szerint részesülhessenek szupervízióban és pszichológiai segítségben, amely segít feldolgozni a munkájukkal járó lelki terhet.

A tanárképzés megújításával egyidejűleg a szükséges tananyagfejlesztéseket is el kell végezni. Rövid időközönként (legalább háromévente) megújuló, a korábban említett médiahetekben rejlő potenciál kihasználására alkalmas tankönyvekre, azokhoz kapcsolódó online felületekre és tanári kézikönyvekre van szükség.

A médiapedagógusok szakirányú ismereteinek, készségeinek fejlesztése mellett a szakképesítéssel rendelkező pedagógusok létszámának növelése érdekében is szükséges intézkedéseket tenni.

Az eszközcsoporthoz tartozó intézkedés (akció):

a1.3.1) A tanító és tanárképzés rendszerében az általános médiaismereti és médiapedagógiai tartalmak, módszertani ismeretek és gyakorlat beépítéséhez szükséges tartalom- és curriculumfejlesztések kezdeményezése.

E1.4) Az egyéb érdekeltek képzése

A) Szülők médiaműveltség-fejlesztése

Lehetővé kell tenni a médiaműveltség-képzésben való részvételt a szülők számára is, olyan tanfolyamok szervezése útján, amelyek – megfizethető, elérhető áron – nyújtanak felkészítést az internethasználat kérdéseiben, abból a

célból, hogy az így megszerzett tudást a szülők gyermekük nevelése során alkalmazni tudják. Törekedni kell arra, hogy térítésmentes képzési lehetőségek is rendelkezésre álljanak (megfontolandó az eMagyarország pontok bevonása).

B) Az igazságszolgáltatás és a rendészet szereplőinek képzése

Az igazságszolgáltatás azon szereplőit, akik gyermekek sérelmére elkövetetett bűncselekményekkel vagy egyéb jogsértésekkel találkoznak munkájuk során (elsősorban a rendőrségi-, ügyészségi dolgozók és a bírók), folyamatosan képezni szükséges a médiaműveltség tekintetében, azon területekre kiterjedően, amelyek az érintettek munkájának elvégzéséhez szükségesek. Ennek a képzésnek a hatósági és bírósági dolgozók számára egyébként is kötelezően előírt képzések (a bíró- és ügyészképzés, a rendőrségi dolgozók képzése) rendszerébe kell betagozódnia. Aki online gyermekvédelemmel kapcsolatos kérdésekkel foglalkozik munkája során, annak meghatározott időközönként – de legalább háromévente – részt kell vennie médiaműveltség-képzésben.

C) A gyermekvédelem szereplőinek támogatása

Szükséges a gyermekvédelem szereplőinek (szociális munkások, gyámügyesek, gyermekpszichológusok, iskolapszichológusok, védőnők) képzése is, elsősorban letisztult, gyakorlati, az adott célcsoport felelősségének, lehetőségeinek és kihívásainak leírását tartalmazó útmutatók, segédletek készítésével. Ezen pont a Digitális Gyermekvédelmi Stratégiának a terület más intézkedéseihez, résztvevő csoportjaihoz való kapcsolódását is támogatja.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a1.4.1) A szülők által igénybe vehető médiaműveltség-tanfolyamok szakmai anyagának összeállítása, az együttműködő civil és iparági szereplők felkérése, a tanfolyamok meghirdetése a köznevelési intézményeken keresztül, valamint a tanfolyamok folyamatos megszervezése és lebonyolítása.

a1.4.2) A médiaműveltség-oktatás beépítése a bíróképzés rendszerébe, azon bírósági dolgozók képzését és továbbképzését szolgáló programok kidolgozása formájában, akik gyermekek sérelmére elkövetett bűncselekményekkel vagy egyéb jogsértésekkel kerülnek kapcsolatba.

a1.4.3) A médiaműveltség-oktatás beépítése az ügyészképzés rendszerébe, azon ügyészségi dolgozók képzését és továbbképzését szolgáló programok kidolgozása formájában, akik gyermekek sérelmére elkövetett bűncselekményekkel vagy egyéb jogsértésekkel kerülnek kapcsolatba.

a1.4.4) A médiaműveltség-oktatás beépítése a rendőrségi dolgozók képzésének rendszerébe, azon rendőrségi dolgozók képzését és továbbképzését szolgáló programok kidolgozása formájában, akik gyermekek sérelmére elkövetett bűncselekményekkel vagy egyéb jogsértésekkel kerülnek kapcsolatba.

a1.4.5) A médiaműveltség-oktatás beépítése az állami gyermekvédelem rendszerében dolgozók számára.

E1.5) Gyűjtőhonlap és hitelesítés

Az internetes gyermekvédelem területén rendelkezésre álló információkat ingyenessé és könnyen elérhetővé kell tenni mindenki számára, egy olyan honlapon, ahol e tartalmak összegyűjtve elérhetők, illetve ahol minden felmerülő praktikus kérdésre gyors és könnyen megtalálható választ kaphatnak az érdeklődők (elsősorban a szülők és a pedagógusok).
Ezzel párhuzamosan létre kell hozni egy olyan rendszert, ahol a ténylegesen hasznos, alkalmazható információt, tudást hordozó – e honlapon elhelyezett, vagy onnan könnyen elérhetővé tett – anyagokat megfelelően hitelesíti egy internetes gyermekvédelmi szakértőkből álló testület. Ez a szakértői testület foglal állást arról, hogy mely, az online gyermekvédelemmel foglalkozó tananyagot, oktatási segédanyagot, tájékoztató dokumentumot szükséges közzétenni e központi honlapon (is), ezáltal garantálva a felhasználók felé az anyagok szakmai megalapozottságát. A médiaoktatásban használt tankönyvek ellenőrzése és jóváhagyása egy ettől független eljárásban, a tankönyvekre, tananyagokra irányadó szabályok szerint történik.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a1.5.1) A gyűjtőhonlap tartalmának meghatározása, létrehozatala és működtetése.

a1.5.2) A gyűjtőhonlapon elérhető tartalmak szakmai hitelesítésére irányuló eljárás meghatározása és a hitelesítés rendszeres elvégzése.

3.2.2 Védelem és biztonság

E2.1) A szűrőszoftver-fejlesztés lehetőségei

Az elmúlt két év tapasztalatai azt mutatják, hogy a szűrőszoftver, noha alkalmas eszköz lehet a veszélyforrások egy jelentős részével szembeni védelemre, azonban több megoldást igénylő probléma is felmerült az elmúlt időben. A kiskorúakra káros tartalmak elérhetőségének szűrőszoftverrel történő hatékony korlátozásának legfontosabb feltételei, és azok teljesülése a jogszabályban, illetve a Gyermekvédelmi Internet-kerekasztal ajánlásában (helyzetértékelés, 2.3.4. pont) foglaltak fényében az alábbiak szerint foglalható össze:

- Elérhetőség, hozzáférhetőség: a legnagyobb szolgáltatók kivétel nélkül, illetve a kisebb szolgáltatók döntő többségben (>80%) kínálnak ingyenesen az ajánlásnak megfelelő szűrőszoftver(eke)t az ügyfeleik számára;
- Könnyű alkalmazhatóság: az internethozzáférés-szolgáltatók az esetek többségében a honlapjukról letölthető szöveges és videós telepítési útmutatót biztosítanak az ingyenesen elérhető szűrőszoftver(ek)hez;
- Operációs rendszerekkel való kompatibilitás: a szolgáltatók által ajánlott szűrőszoftver (Norton Family) az asztali gépek vonatkozásában a Linuxot, míg a mobil eszközök vonatkozásában az IOS, a WP és Firefox operációs rendszereket nem támogatja. Nem biztosított továbbá a Norton Family szűrőszoftver hosszú távú elérhetősége és ingyenessége sem;
- A közintézmények helyzete: a Norton Family szoftver központi menedzselhetőségének hiánya miatt nehézkes a kulturális intézményekben annak használata (mintegy 300 000 számítógép); az iskolai/könyvtári gépek 20%-án (mintegy 60 000 PC) Linux-alapú operációs rendszer működik, amelyre jelenleg egyáltalán nem érhető el szűrőmegoldás a hírközlési szolgáltatók oldalain;
- Problémát jelent, hogy nincsen olyan ismert és megfelelően transzparens minta, ajánlás, amely felhasználható lenne a köznevelési intézményekben. E szoftverekkel kapcsolatos költségek megoszlása, karbantartása vitatott, ahogyan az is, hogy milyen kifejezésre szűrjön a program. Az iskolák legtöbbször az iskolai internet-hozzáférés drasztikus korlátozását választják (helyzetértékelés 2.3.3 pont).

A szűrőszoftver megfelelő működéséhez elengedhetetlen olyan listák összeállítása, amelyek egyfelől a kiskorúak számára ajánlott, értékes és a fejlődési szintjüknek

megfelelő tartalmakat hordozó internetes oldalakat *(white list)*, másrészről pedig a számukra nem ajánlott, káros elemeket tartalmazó elérhetőségeket *(black list)* gyűjtik össze. Szintén elkerülhetetlen egyes tartalomkategóriák létrehozása, amelyek kiválasztásával meg lehet határozni, hogy egy adott kategória bizonyos korosztály esetén alapbeállításként elérhető legyen-e vagy sem. A listák segítségül szolgálhatnak a szűrőszoftver hatékony működéséhez.
A működés hatékonyságához nélkülözhetetlen a listák rendszeres frissítése. Tekintettel arra, hogy az Eht. 149/A. §-ának megfelelő (magyar nyelvű, könnyen telepíthető és használható) szűrőszoftver a piacon nem áll folyamatosan és megbízhatóan rendelkezésre, az államnak kell szerepet vállalnia a szoftver fejlesztésében. A négy legnépszerűbb operációs rendszerrel (Windows, IOS, Android és Linux) kompatibilis szoftvereket folyamatosan elérhetővé kell tenni. Ezek részben új fejlesztéssel, részben a meglévő szoftverek továbbfejlesztésével, valamint a licencek állam általi megvásárlásával is történhet. Fontos, hogy ezek mindenki számára ingyenesen elérhetőek legyenek, és frissítésük, karbantartásuk évente megtörténjen. A költségekre tekintettel (előzetes becsléssel: legfeljebb 100 millió forint költség operációs rendszerenként, a meglévő megoldások továbbfejlesztése esetén akár ennél alacsonyabb összeg) évente egy szoftver fejlesztése/továbbfejlesztése/megvásárlása várható el.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.1.1) A szűrőszoftver műszaki paramétereinek azonosítása, a fejlesztéshez szükséges közbeszerzés lebonyolítása és a fejlesztés ellenőrzése évente egy – eltérő operációs rendszeren alkalmazható – szoftver tekintetében (2017-2020 között).

a2.1.2) A fejlesztett szoftverek évenkénti frissítése és karbantartása.

a2.1.3) A fejlesztett szoftverekhez tartozó internetes ügyfélszolgálat, helpdesk működtetése (a témához kapcsolódó jogsegély szolgáltatást nyújtó szervezetek bevonásával).

a2.1.4) Konzultáció a szűrőszoftver ismertségét és elterjedését segítő eszközökről a hírközlési szolgáltatókkal.

a2.1.5) Tájékoztató anyagok elkészítése és folyamatos tájékoztatás nyújtása a szűrőszoftverről az óvodákban, iskolákban, illetve a szülők részére.

E2.2) Gyermekek Számára Biztonságos Internetszolgáltatás

Az online gyermekvédelemnek egy – a helyzetértékelés 2.5. pontjában ismertetett – sajátos megoldását alkalmazzák az Egyesült Királyságban, ahol az internethozzáférés-szolgáltatók – a kormányzattal kötött egyezség alapján – önként vállalták a pornográf tartalmak korlátozását, alapbeállításként 2013 végétől (ez kiterjedt a Wi-Fi szolgáltatásokra, és valamennyi eszközre egyaránt); ám a jogi szabályozás megalkotására nem került sor. A szolgáltatást újonnan igénybe vevők számára már eleve a Gyermekek Számára Biztonságos Internetszolgáltatást nyújtják hálózati szintű szűrőeszközökön keresztül, de ez természetesen egyéni kérésre feloldható. Ez az elképzelés azonban nem új keletű a szigetországban. 2002 óta az Internet Watch Foundation (Internetfigyelő Alapítvány) listát tesz közzé azokról a tartalmakról, melyek károsak lehetnek a kiskorúakra és lista alapján a szolgáltatók önkéntesen blokkolják a tartalmakat. A lista a következő főbb kategóriák alapján tartalmazza a tiltani kívánt tartalmakat: drogok, alkohol, társkereső oldalak, pornográf tartalmak, öngyilkosságra buzdító tartalmak. A kezdeményezéshez csatlakoztak a legnagyobb szolgáltatók, továbbá a biztonságos internethasználattal és tudatosítással kapcsolatos oldalakat üzemeltetnek és biztosítják az ügyfelek részére az ingyenesen letölthető szűrőszoftvert. Későbbiekben, a könyvtárakban és iskolákban is bevezették a hálózati szintű eszközöket, 2016 végére pedig szeretnék elérni, hogy az összes iskola csatlakozzon a kezdeményezéshez. A hálózati szintű szűrőeszközök „feloldására” kizárólag felnőtt korúak jogosultak.

A rendszer működését ért leggyakoribb kritika, hogy a szűrés révén több olyan weboldal is elérhetetlenné vált, amely online bántalmazás áldozatává vált gyermekek megsegítésével, illetve oktatással, felvilágosítással foglalkozott.

A rendszer üzemeltetéséhez a brit kormány e célra egy olyan weboldalt tart fenn (https://www.blocked.org.uk/), melyen egyszerűen ellenőrizhető, hogy az adott oldal blokkolásra került-e, illetve ha téves blokkolás történt, annak itt lehet kérelmezni a feloldását.

Az alábbi táblázatban a legnagyobb brit szolgáltatók egyes blokkolási kategóriáinak beállításai és blokkolási szintjei láthatóak. Szolgáltató egyéni vállalásától függ, milyen mértékű blokkolást állít be az adott kategóriákra, tehát a rendszer és a szabályozás nem egységes.

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

Megfontolandó lehet az Egyesült Királyságban már működő fenti rendszer hazai bevezetése, amely szerint az internethozzáférés-szolgáltatók alapbeállításként már eleve csak olyan, Gyermekek Számára Biztonságos Internetszolgáltatást biztosítanak az előfizetőik számára, amelyekkel egyes jogellenes, illetve a gyermekek fejlődésére súlyosan káros tartalmak nem érhetőek el. A megoldás alapján az előfizető aktív tevékenysége – a szűrés feloldásának kezdeményezése a szolgáltatónál – szükséges ahhoz, hogy a hozzáférés biztosított legyen e tartalmakhoz.

A javaslat lényeges eleme a szűrés feltételeinek meghatározása; azt kizárólag olyan tartalmakra kell alkalmazni, amelyek súlyos károkat tudnak okozni a kiskorúak fejlődésében, egyúttal ki kell küszöbölni, hogy a szűrés blokkolja azon tartalmakat, amelyek éppen ellenkező célt szolgálnak (például áldozatsegítő, oktató, felvilágosító oldalak). Éppen ezért e javaslat elfogadása esetén a szűrés feltételeinek kidolgozására kell a legnagyobb hangsúlyt fektetni.

Egy ilyen rendszer kötelező, jogalkotási eszközökkel történő bevezetése helyett konzultálni szükséges az internethozzáférés-szolgáltatókkal, és felmérni azt, hogy az illetékes állami szerv és a szolgáltatók közötti, önkéntesen létrehozott szerződéses viszonyrendszer alapján esetlegesen megvalósuló szűrés milyen előnyökkel és

hátrányokkal jár. A köznevelési intézményekben a gyermekek által használt gépeken könnyebben és jelentősen kevesebb alapjogi aggály mellett lehetséges a hálózati szintű szűrést megvalósítani. Jelen stratégia kizárólag egy lehetséges megállapodás előkészítését, az arról való végleges döntés megalapozását célozza.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.2.1) A hálózati szintű szűrőeszközöket alapbeállításként alkalmazó külföldi megoldások gyakorlati tapasztalatainak vizsgálata és kiértékelése.

a2.2.2) A hálózati szintű szűrőeszközök alapbeállításként való magyarországi bevezetésének lehetséges következményeinek, illetve várható hatásainak azonosítása és mérlegelése.

a2.2.3) Konzultáció lefolytatása a hírközlési szolgáltatókkal a hálózati szintű szűrőeszközök alapbeállításként való alkalmazásának kérdéseiről, a magyarországi bevezetés lehetőségeiről, valamint indokolt esetben javaslattétel a Kormány számára a szükséges lépések tekintetében.

a2.2.4) A köznevelési intézmények, önkormányzatok által biztosított hotspot szolgáltatások esetén azon lehetőség vizsgálata, hogy milyen hatékony módon lehetne megoldani, hogy az internetelérést igénybe vevő kiskorúak ne juthassanak hozzá rájuk nézve káros tartalmakhoz, illetve hogy a köznevelési intézményekben a gyermekek által használt számítógépeken megvalósuljon a Gyermekek Számára Biztonságos Internetszolgáltatás.

E2.3) Hatékony műszaki megoldások alkalmazási körének kibővítése

A gyermekek hozzáférésének korlátozása érdekében a hatékony műszaki megoldások alkalmazási körét a médiaszabályozás (Smtv. és Mttv.) hatálya alá nem tartozó internetes tartalmakra (az Ekertv. alapján elektronikus kereskedelmi szolgáltatásnak minősülő online tartalomszolgáltatásokra) is indokolt kiterjeszteni. A műszaki megoldások valóban hatékony alkalmazása érdekében – külföldi minták alapján – az életkor-ellenőrzés megvalósítására az alábbi javaslatok fogalmazhatóak meg:

- A kiskorúakra káros tartalmakra történő felhívás esetén a tartalom nyújtója egységes (jogszabályban szövegszerűen meghatározott) figyelmeztetést jelenítsen meg, melyben tájékoztat az oldal kiskorúakra káros tartalmáról,

ellenőrzi a látogató életkorát, elérhetővé tesz ingyenes szűrőszoftver-megoldást (lásd a Médiatanács ajánlását a hatékony műszaki megoldásokról);
- Hitelkártya vagy egyéb fizetési eszköz révén, amely megfelelően bizonyítja a kártyatulajdonos életkorát;
- A választási névjegyzékhez hasonlóan megbízható és hiteles adatbázisok felhasználásával (bár a más törvényi célra létrehozott állami adatbázisok felhasználása komoly és indokolt esetben jogalkotás útján kezelendő adatvédelmi kérdéseket vet fel);
- Olyan mobiltelefon-előfizetés igazolása által, amelyhez személyazonosításra alkalmas okmány (például személyi igazolvány, vezetői engedély) birtokában lehet csak hozzájutni;
- PIN kódok alkalmazásával.

Ezen megoldások alkalmazásának előírásához az Ekertv. módosítása lenne szükséges, amely megteremti a hatósági fellépés lehetőségét is a jogsértő – megfelelő megoldást nem alkalmazó – szolgáltatókkal szemben. Nyilvánvaló, hogy ez a szabály csak a magyar joghatóság alatt álló tartalomszolgáltatásokra terjedhet ki, de egyfelől ez is jelentősen csökkentheti a káros tartalmaknak a gyermekek általi hozzáférhetőségét, másrészt Európában széles körben írnak elő az egyes államok ilyen megoldásokat, azaz a szigorítás hozzájárulna az európai szintű fellépés egységesüléséhez is. Ebből eredően meg kell vizsgálni Ekertv. lehetséges módosításának indokoltságát a hatékony műszaki megoldások alkalmazásának kötelező előírása vonatkozásában. Ezzel párhuzamosan az Mttv. hatályos szabályozása, amely alapján a lekérhető médiaszolgáltatásokra (*video on demand*) nézve alkalmazandó „hatékony műszaki megoldás” mibenlétét a Médiatanács ajánlása rögzíti, megfelelő rugalmassága miatt változatlanul maradhat.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.3.1) A gyermekek fejlődésére veszélyes internetes tartalomszolgáltatásokkal kapcsolatban alkalmazott hatékony műszaki megoldások külföldi tapasztalatainak felmérése, egyúttal a leghatékonyabb megoldások azonosítása.

a2.3.2) Konzultáció lefolytatása a hírközlési szolgáltatókkal és a tartalomszolgáltatók szakmai szervezeteivel a hatékony műszaki megoldás bevezetésének egyes kérdései tekintetében.

a2.3.3) A kiskorúakra káros tartalmak esetén az egységes figyelemfelhívás alkalmazása érdekében az Ekertv. lehetséges módosítása indokoltságának vizsgálata.

E2.4) Veszélyes és javasolt tartalmak kezelése (black list és white list)

A) INTERPOL „*Worst of"-list*

2009-ben az International Criminal Police Organization (INTERPOL) közgyűlésének tagországai egyhangúan szavazták meg azt a rendeletet, amely korlátozza a gyermekekkel szembeni online szexuális visszaéléseket (gyermekpornográf felvételek). Az állásfoglalás arra ösztönzi a tagországokat, hogy a rendelkezésükre álló technikai eszközök segítségével támogassák az INTERPOL által közétett listán szereplő URL-ek blokkolását. Az INTERPOL feladata, hogy összeállítsa, frissítse és a tagországok rendelkezésre bocsájtsa az úgynevezett „*Worst of"-list* tiltólistát.

A fentiek alapján az INTERPOL a tiltólistát a tagállamaiban működő, vele szerződött internethozzáférés-szolgáltatók részére megküldi. A szolgáltatók az INTERPOL-lal kötött megállapodás alapján saját hálózatukban hozzáférhetetlenné teszik a listán szereplő, gyermekpornográf tartalmú oldalakat. 2011. december 1-jén szándéknyilatkozatot írt alá a hazai Telenor, az ORFK és az NMHH a gyermekek biztonságos internethasználatának megteremtése és a gyermekpornográf tartalmak internetes terjesztésének megakadályozása érdekében. A megállapodás alapján a Telenor Magyarország 2012. január 1-jétől elérhetetlenné teszi hálózatában az INTERPOL által összeállított és folyamatosan aktualizált tiltólistán szereplő, kizárólag gyermekpornográf tartalmú weboldalakat. A tiltólistát a Telenor Magyarország az anyacégén keresztül az INTERPOL-tól kapja meg.

A blokkolást nem végző szolgáltatók visszajelzései, álláspontja szerint a listán szereplő oldalak hozzáférhetetlenné tétele egyértelmű törvényi kötelezés, illetve bíróság vagy egyéb hatóság erről való rendelkezése hiányában nem jogszerű. Ezen szolgáltatók ezért a blokkolást – amíg annak jogszabályi feltételei nem kerülnek rendezésre – önkéntes módon nem vállalják.

A gyermekpornográf internetes tartalmak visszaszorítása terén jelentős előrelépést jelentene az INTERPOL által összeállított „*Worst of"-list* hazai internethozzáférés-szolgáltatók általi kötelező blokkolása, vagy legalább az ilyen irányú szűrési tevékenység kifejezett lehetővé tétele a vonatkozó jogszabályokban a szolgáltatók számára.

2015. június 30-án az Európai Tanács, az Európai Parlament és az Európai Bizottság között megállapodás született a TSM [Telecom Single Market – (EU) 2015/2120 európai parlamenti és tanácsi rendelet] szabályozásról. A 2016. április 30-tól hatályos új szabályozás alapján az internethozzáférés-szolgáltatók nem vezethetnek be olyan forgalomirányítási intézkedéseket, amelyek túlmutatnak a szabályozás-tervezetben foglaltakon, így nincs lehetőségük az INTERPOL-lista blokkolására sem. Az új szabályozás szerint a szolgáltatók kizárólag abban az esetben blokkolhatnak, amennyiben az a rájuk irányadó uniós és nemzeti jogszabályoknak való megfelelést szolgálja.

A TSM rendelet fenti rendelkezéseire figyelemmel, ahhoz, hogy a magyarországi szolgáltatók is jogszerűen blokkolhassák az INTERPOL által közétett listán fellelhető gyermekpornográf tartalmakat, azaz a „*Worst of"-list* szűréséhez az Eht. módosítása szükséges. A jogszabály-módosítás a hozzáférést biztosító elektronikus hírközlési szolgáltatókat és a kereső- és gyorsítótár-szolgáltatókat feljogosítaná arra, hogy az INTERPOL által fenntartott – gyermekpornográf felvételek elérhetetlenné tételét szolgáló – listán megjelölt weboldalakat hozzáférhetetlenné tehessék.

Az INTERPOL által közzétett listán szereplő weboldalak, illetve tartalmak kivétel nélkül büntetőjogi tényállást alapoznak meg, ezért a jelenleg hatályos jogi szabályozás alapján is lehetséges a hozzáférhetetlenné tétel elrendelése a Be. szerint. Ennek ellenére – döntően, mivel a rendőrség és a bíróságok kizárólag egyedileg tudják kezelni ezen ügyeket – nincs mód azok hatékony, az eljárási gyakorlatban is megfelelően működő végrehajtására. Mivel a büntetőeljárás alapvető célja a hazánk joghatósága alá tartozó bűncselekmények felderítése, bizonyítása és a bűnelkövetők felelősségre vonása, a büntetőeljárás keretében történő hozzáférhetetlenné tétel nem megfelelő mód az ilyen tartalmak, URL-ek tömeges tiltására.

Ahhoz hogy ezek a tartalmak egyszerűen blokkolhatóak legyenek, az Eht. megfelelő módosítása szükséges.

B) *Black list, white list* és tartalomkategóriák a szűrőszoftverhez kapcsolódóan

A káros és a hasznos weboldalakat tartalmazó listák, továbbá a tartalomkategóriák és a hozzá tartozó kulcsszó-listák összeállítása és folyamatos naprakészen tartása nagyban hozzájárulhat a szűrőszoftverek hatékony működéséhez, ezért kiemelten fontos ezek összeállítása és rendszeres aktualizálása. A cél- és eszközrendszer 2.2.2 C1 pontjában szereplő szűrőszoftver használatához – a megfelelő beállítások meghatározásához – szükségesek ezek a listák.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.4.1) A „*black list*” és a „*white list*” összeállítása, valamint rendszeres felülvizsgálata.

a2.4.2) Az INTERPOL „*Worst of*”-*list* bevezetéséhez szükséges egyeztetések lefolytatása.

a2.4.3) Az Eht. módosítása annak érdekében, hogy a hozzáférést biztosító elektronikus hírközlési szolgáltatók valamint a kereső- és gyorsítótár-szolgáltatók az INTERPOL listán szereplő weboldalakat – a TSM rendeletre figyelemmel – jogszerűen blokkolhassák.

E2.5) Az iparági társszabályozás erősítése

A) Az internethozzáférés-szolgáltatók társszabályozása

Az internethozzáférés-szolgáltatók jelenleg végzett tevékenysége a gyermekek tudatos internetezésének elősegítésében, a szülők felkészítésében, a biztonságos internetezést elősegítő szoftverek és alkalmazások elérhetővé tételében változatos képet mutat. Az államnak meg kell találnia azt a módot, amellyel ösztönözheti az iparágat – elsősorban az internethozzáférés-szolgáltatókat – a tudatos internetezéssel kapcsolatos társadalmi szerepvállalás hatékonyabb és integráltabb felvállalására, többek között a társszabályozás útján. Ehhez természetesen az is szükséges feltétel, hogy az iparág szereplőit összefogó érdekképviseleti szervezetek is hozzájáruljanak a biztonságos internethasználattal kapcsolatos szolgáltatói tevékenységek egységesítéséhez.
Az ön- és társszabályozás erősítése érdekében érdemes lenne fontolóra venni, hogy az állam a szolgáltatók hatékony gyermekvédelmi célú együttműködését bizonyos kedvezményekkel honorálja. Jelen stratégia ezért feladatul tűzi egy ilyen társszabályozási rendszer felállítási lehetőségének felmérését, a kormányzat és az érintett iparági szereplők közötti tárgyalások megkezdését egy új társszabályozási rendszer létrehozása érdekében.

B) A médiatartalom-szolgáltatók társszabályozása

A médiaszabályozásban létezik már egyfajta társszabályozási modell: az Mttv. lehetővé teszi, hogy a lekérhető médiaszolgáltatásokra és internetes

sajtótermékekre vonatkozó egyes törvényi előírások betartásának felügyeletét a Médiatanács a társszabályozó szervek feladatkörébe utalja (helyzetértékelés, 3.3.1. pont). A társszabályozó szervek eljárásait magatartási kódexek szabályozzák, ezen eljárási szabályok azonban meglehetősen bonyolultak és a gyakorlatban csak nehézkesen alkalmazhatók. Szükséges lenne ennek megfelelően ezen szabályok jelentős átalakítása, az eljárás formalizáltságának csökkentése, de ez a Médiatanács és a társszabályozó szakmai szervezetek közötti megállapodás módosításával érhető el.
A társszabályozási mechanizmusok erősítésének kívánalmát – külön kiemelve a gyermekvédelem területét – az Európai Unió is ösztönzi, valamint ennek megfelelően az AVMS irányelv módosításának 2016. májusi európai bizottsági javaslata is tartalmazza. Miután a társszabályozó szervek eljárásának lényege éppen a hatékonyság és a gyorsaság, javasolt lehet az eljárási szabályok olyan formában történő egyszerűsítése, illetve átgondolása, amely lehetővé teszi a gyermekvédelmi szabályok szélesebb körű érvényesülését.
Emellett megfontolandó, hogy a társszabályozó szervezetek nem kizárólag panaszra, hanem azon kívül is rendszeresen vizsgálják, hogy a tagságuk alá tartozó internetes szolgáltatások működése mennyiben felel meg a gyermekvédelmi előírásoknak (ehhez a hatóság anyagi támogatást nyújthat, a szervezetek pedig rendszeresen beszámolnak a vizsgálatok eredményeiről). E kérdésekben a megállapodás a Médiatanács és a társszabályozó szervek által megkötött szerződések módosítása útján történhet.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.5.1) Az internethozzáférés-szolgáltatókat tömörítő szakmai és önszabályozó szervezetekkel konzultáció lefolytatása, annak érdekében, hogy egy lehetséges új társszabályozási rendszer alapjai meghatározhatóvá váljanak.

a2.5.2) A Médiatanács felkérése arra, hogy dolgozza ki és kezdeményezze a médiatartalom-szolgáltatók szakmai szervezeteivel kötött társszabályozási szerződések módosítását, az ott alkalmazott eljárási szabályok egyszerűsítése érdekében.

E2.6) A büntetőjog ultima ratio szerepének hangsúlyozása

Fontos annak kiemelése és tudatosítása az online veszélyek megelőzésében és a

problémák kezelésében résztvevőkkel (szülők, iskolaigazgatók, pedagógusok, gyermekvédelmi szakemberek, gyermekpszichológusok, jogalkalmazók), hogy a büntetőjog csak legvégső megoldásként (*ultima ratio*) szerepeljen a gyermekek között megvalósuló online devianciák, különösen a megfélemlítés (*bullying*) és az online megfélemlítés (*cyberbullying*) ügyek elbírálásánál. Ezt indokolja, hogy a *bullying* és a *cyberbullying* legtöbbször súlyosabb cselekmények előkészületi vagy eszközcselekménye, amelyek közül általában csak az enyhébbek szándékossága bizonyítható. Ugyanakkor az iskoláskorú gyermekek körében előforduló esetekben az iskola mint szocializációs színtér felelősséggel tartozik az esetek megoldásában és megelőzésében. Európában és a világon számos olyan megoldás létezik, amely a fiatalok kriminalizációja helyett a nevelést, az iskolai szintű, illetve oktatással kapcsolatos szankciókat tartja elsődlegesnek. Kriminológiai kutatások szerint a fiatalkorban elkövetett bűncselekmények miatti, elzárással járó büntetésnek nincs preventív hatása, sőt a fiatalok kriminalizálása a felnőttkori kriminalitás előszobája lehet.

Magyarország büntetőjogi és polgári jogi szabályai biztosítják – ha nem is a *bullying*, de – a *bullying* határmezsgyéjén mozgó súlyosabb magatartások, valamint az eszköz- és előkészületi cselekmények szankcióval való fenyegetését. A *bullying* önálló tényállásként a jelenleg büntetőjogi tényállás keretében szabályozott cselekmények eredményeként előálló helyzetet megelőző lépéseket kriminalizálná. Ezek olyan absztrakt veszélyhelyzetek, ahol sokszor nem állapítható meg a károkozásra irányuló eshetőleges szándék sem, valamint – mivel a korosztály meglehetősen elterjedt magatartásairól van szó – a fiatalok tömeges kriminalizálásához vezetne, amelyet pedig sem kriminálpolitikai, sem pedagógiai, sem prevenciós szempontok nem indokolnak, sőt, kifejezetten ellenjavallnak.

Meg kell maradni a *bullying* eszköz- és előkészületi-jellegű cselekményeinek a jelenlegi szintű kriminalizálásánál, de mindenképpen fejleszteni kell a joggyakorlatot akképpen, hogy az eszköz- és előkészületi cselekmények beilleszthetők legyenek a meglévő tényállásokba.

Ennek érdekében biztosítani kell az igazságszolgáltatási rendszer különböző szereplőinek képzését, továbbképzését és a tudás folyamatos frissítését, ami az új típusú médiahasználatot (hogyan és milyen célokra használják a fiatalok az online felületeket, az okostelefont stb.), valamint ami a *bullying* és a *cyberbullying* jelenségét illeti. Ebben a körben a jogalkalmazóknak az alapvető megértés szintjére kell eljutnia a *bullying* szereplőit, dinamikáját, az elkövetési szándékot és a jóvátételi/szankcionálási célokat és lehetőségeket illetően. A nyomozó hatóság tagjait ki kell képezni a *bullying* körébe tartozó magatartások feljelentéskor történő felismerésére, és a feljelentett cselekmények megfelelő minősítésére, valamint az áldozatok megfelelő informálására (kioktatására), a segítségnyújtó szervezetek

ismeretére.
A szakértőknek szerepet kell vállalniuk a lakosság tájékoztatásában, a biztonsági óvintézkedéseken túl a tudatos használatot elősegítő, alternatívákat kínáló civil kezdeményezések megismertetésében. Fel kell térképezni és meg kell ismertetni a *startup* világ által kínált új lehetőségeket az intézményekkel, a pedagógusokkal és a szülőkkel.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.6.1) A munkájuk során gyermekek sérelmére elkövetett bűncselekményekkel, vagy egyéb jogsértésekkel kapcsolatba kerülő bírósági, ügyészségi és rendőrségi dolgozók képzését, illetve továbbképzését szolgáló programok kidolgozása.

a2.6.2) A gyermekek védelmére irányuló büntetőjogi szabályok gyakorlati alkalmazására vonatkozó folyamatos felmérések elvégzése, valamint a jogalkalmazók továbbképzésének e felmérések eredményeihez való igazítása.

E2.7) A gyermekek számára biztonságos és hasznos tartalmak gyártásának támogatása

A) Gyermekbarát online tartalmak támogatása

A tapasztalatok szerint a gyermekek online térben elszenvedett lelki sérülései sokszor nem találnak nyitott fülekre a felnőtt társadalomban. A probléma felismerésében és kezelésében a médiának is nagy szerepe van; az ott közölt tartalmaknak elő kell segítenie a mindennapi tudatosítást. A vizsgált problémakör legalább annyira a média tudatos használata (információbiztonság, adatkezelés, adatbiztonság, felelős, etikus médiahasználat), mint az informatikai műveltség (hardver-, szoftverismeretek, kódolás, eszközhasználat) felé mutat. Támogatni kell a média tudatos használatát fókuszba helyező médiatartalmak létrehozását; olyan, rendszeresen jelentkező műsorok gyártását (annak támogatását), amelyek világosan, közérthető és gyakorlatorientált módon szólnak a gyermekekhez és az egészséges fejlődésükért felelős felnőttekhez (szülők, pedagógusok).
A gyermekeket érdemes a számukra készített, vagy a tipikus tevékenységeik során használható tartalmak felé terelgetni, illetve támogatni a gyermekek által létrehozott tartalmak közül a hosszabb távon értékteremtőeket.

Ezt segíti elő többek között a honlapok online felületeken, rádióban, nyomtatott sajtóban történő népszerűsítése, reklámozása, mellyel célzottan a gyermekekhez, a célcsoporthoz juttatják el az információt.
Olyan megoldás is működhet, hogy az ilyen jellegű tartalmakról a pedagógus vagy a szülő tájékoztatja a gyermeket. Például a pedagógus egy honlap-listát ad át a tanulóknak azokról az oldalakról, amelyeket érdemes felkeresniük a tanulás során.
Szintén iskolai feladat lehet, hogy az általános tájékoztatás keretében informálják a gyermekeket a közvetlenül nekik szánt honlapok címeiről.
Gyermekbarát honlapokat szükséges létrehozni, amelyekről érdemes a gyermekeket tájékoztatni. Az ilyen honlapok létrehozását központilag, szervezetten, akár pályázat útján támogatni szükséges.
Tartalmukat tekintve ezek lehetnek: játékot, szórakozást tartalmazó honlapok, készségfejlesztő honlapok, jogaikról tájékoztató honlapok, segítséget nyújtó, informatív honlapok, ismeretterjesztő, tanulást segítő honlapok, játékosított, interaktív tanulást, illetve ismeretszerzést támogató honlapok.
Célszerű, ha a kifejezetten gyermekek számára létrehozott honlapok a hasonló jellegű honlapokra utalást tesznek, hogy a gyermekek az egyik ilyen jellegű tartalomról a másikra könnyen el tudjanak navigálni.
Az ilyen tartalmak támogatása különböző forrásokból történhet, elsődlegesen a Médiatanács által kezelt MTVA Magyar Média Mecenatúra-pályázatain, valamint a Nemzeti Kulturális Alap pályázati rendszerén keresztül. Fel kell kérni e döntéshozó testületeket, hogy rendszeresen írjanak ki pályázatot a gyermekbarát és a médiaműveltséget fejlesztő online tartalmak készítésére.

B) A közszolgálati média szerepvállalása

A Duna Médiaszolgáltató Nonprofit Zrt. mint közszolgálati médiaszolgáltató az Mttv. 83. § (1) bekezdés *h)* pontja alapján köteles a kiskorúak testi, lelki és erkölcsi fejlődését, érdeklődését szolgáló, ismereteit gazdagító műsorszámok, valamint a gyermekek védelmének céljait szolgáló ismeretterjesztő, felvilágosító műsorszámok közzétételére. Ebbéli tevékenységében a működését támogató MTVA is közreműködik. A médiaszolgáltató jelenleg ezt elsősorban az m2 lineáris audiovizuális médiaszolgáltatás által – illetve a csatorna interneten elérhető lekérhető szolgáltatása révén – teljesíti.
Meg kell vizsgálni annak a lehetőségét, hogy a közszolgálati médiarendszer szervezetei milyen módon tudnak a jelenleginél is hatékonyabban részt venni a gyermekek internethasználatának tudatosabbá tételében, elsősorban a közmédia internetes felületeinek ez irányú felhasználása által. Mindazonáltal a

közszolgálati média kormányzattól való függetlenségének megóvására is ügyelni kell. E stratégia célul tűzi ki az internetes gyermekvédelmi feladatot ellátó állami szervek és a közszolgálati média közötti együttműködési lehetőségek feltérképezését, amelyet az érintettek megállapodása útján lehet majd konkrét cselekvések formájában megjeleníteni.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a2.7.1) Támogatási programok kidolgozása a kifejezetten gyermekek számára készült online tartalmak gyártásának támogatására.

a2.7.2) A Magyar Média Mecenatúra program átalakításának kezdeményezése oly módon, amely a kifejezetten gyermekek számára készült, médiaműveltségük növelését célzó online tartalmak gyártásának támogatását a meglévő források terhére lehetővé teszi.

a2.7.3) A Duna Médiaszolgáltató Nonprofit Zrt., illetve a közszolgálati médiarendszer felkérése a jelenleginél is több, a gyermekek médiaműveltségének növelését célzó tartalom megrendelésére, előállítására, elsősorban a közszolgálati média online felületein való hasznosítás céljából.

3.2.3 Szankcióalkalmazás és segítségnyújtás

E3.1) Rendszeres monitoring és adatbázis építése

Igen nagy problémát jelent, hogy nem állnak rendelkezésre teljeskörűen és folyamatosan olyan naprakész adatok, információk, amelyek a gyermekek sérelmére az online térben elkövetett jogsértő cselekmények – köztük a bűncselekmények – számára, tendenciáira, hatására mutatnának rá. A jogsérelmek nagy része – többek között például a jogtudatosság hiányára is visszavezethetően – rejtve marad. Ezért fontos, hogy a hivatalos szervekhez, hatóságokhoz, rendőrséghez eljutott ügyek, eljárások, azok eredményei, illetve számarányuk megismerhető legyen. Ez a gyermekek védelme érdekében folyatott küzdelem egyik hatékony eszköze lehet, amely rámutathat arra, hogy melyek azok a területek, ahol az államnak, vagy akár az iparági és civil szereplőknek nagyobb szerepet kell vállalniuk.
Erre tekintettel rendszeres vizsgálatokat, kutatásokat szükséges folytatni arra vonatkozóan, hogy milyen mértékben vannak jelen a gyermekek által, illetve

sérelmére az online térben elkövetett jogsértések a társadalomban, és ezeket megfelelő értékelésnek kell alávetni.
A látencia felderítésének egy további lehetséges megoldását jelentheti egy anonim bejelentési forma létrehozása.
Ezt az adatbázist összehasonlító elemzés segítségével hozzá kell kapcsolni a longitudinális kvantitatív és kvalitatív alapkutatásokhoz.

Az eszközcsoporthoz tartozó intézkedés (akció):

a3.1.1) A kifejezetten gyermekek által, illetve sérelmükre az online világban elkövetett bűncselekményekre vonatkozó, a meglévő bűnügyi statisztikai rendszerben gyűjtött adatok gyakorlati használhatóságának felülvizsgálata, az adatok teljes körűvé tétele.

E3.2) Resztoratív sérelemkezelés

A vitarendezés alternatív formájaként jelenleg a jogi eljárások (lásd például a büntetőeljárásban alkalmazható közvetítői eljárást) mellett a nevelési, oktatási intézményekben működő egyeztetési eljárások lefolytatására is mód van. Az eljárások előnye, hogy a közvetlenül érintetteken kívül igen kevesen vesznek részt bennük, emellett sokkal gyorsabban és hatékonyabban orvosolhatóak az elkövetett sérelmek, mint a hivatalos, hosszadalmas, sokszor mind az elkövetőben, mind pedig a sértettben komoly károkat okozó eljárásokban.
Szükséges az ilyen típusú – elsődlegesen az elkövetett sérelmek helyreállítását, orvoslását szolgáló – mechanizmusok alkalmazási körének kibővítése, illetve az eljárási szabályok kapcsán eddig szerzett tapasztalatok felhasználása.
Az áldozatok számára biztosított segítségnyújtás területén szükség van az állami szervezetek és a civil szféra, valamint a szülők és a pedagógusok együttműködésre, kiegészítve a gyermekbarát igazságszolgáltatás feltételeinek biztosításával és követelményeinek betartásával.
A személyes bocsánatkérésen és az okozott kár megtérítésén alapuló jóvátételi eljárás a legjobb visszatartó erő a további bűncselekmények elkövetésétől. Ennek érvényesülése érdekében a fiatalkorúak által elkövetett *bullying*-típusú devianciák esetén a Btk. által (például a zaklatás esetén) lehetővé tett jóvátételi eljárás mellett a megelőzésben résztvevő szereplőknek (például iskola) biztosítani kell a büntetőjogon kívüli mediációt is. A pedagógusoknak és az iskoláknak megfelelő felvilágosítást kell kapniuk az alternatív konfliktuskezelési eljárások igénybevételéről, a szolgáltatást nyújtó civil szervezetekről és szakemberekről.

A *bullying* és a *cyberbullying* magatartásait a büntetőjogon kívüli területen, nevezetesen az igazgatási és az oktatási jog területén szükséges szabályozni. Ennek a szabályozásnak a lényege az iskolák felelősségének növelése, és hosszú távú célként a kötelezésük arra, hogy online megfélemlítés elleni programot, de legalábbis a biztonságos internethasználat előmozdítását szolgáló programot implementáljanak és mindennapi gyakorlatukban belső protokollok, speciális házirendek formájában készüljenek fel az online veszélyek kezelésére, valamint a megfelelő prevenciós stratégia elfogadásával biztosítsák a tanulók és a pedagógusok békés, kiszámítható szabályok szerinti egymás mellett élését. Az iskolai protokolloknak az online megfélemlítési esetekben a követendő eljárást, az adminisztratív válaszlehetőségeket, emellett végső megoldásként a polgári és büntetőjogi válaszokat is tartalmazniuk kell.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a3.2.1) Annak felmérése, hogy mely sérelmes helyzetek kezelése esetében alkalmazható a büntetőjog eszközei helyett hatékonyabb és a gyermekekre tekintettel megfelelőbb eljárásrend, ezen esetkörökre és az alkalmazható eljárásokra javaslatot kell tenni a köznevelési intézmények számára.

a3.2.2) A sérelmes helyzeteknek elsődlegesen az oktatási intézményekben megvalósuló rendezésével kapcsolatos jogszabályi hátterének kidolgozása, a szükséges jogszabály-módosítások előkészítése.

a3.2.3) A resztoratív sérelemkezelés szakmai koordinációja és a szükséges tanácsadás ellátása érdekében azon érintett pedagógus szakmai szervezetek bevonása, amelyek segítik az online megfélemlítés elleni protokollok, házirendek kidolgozását, az eszmecserét, valamint előmozdítják a szakmai párbeszédet.

E3.3) Feladatok az online megfélemlítés (cyberbullying) kezelése terén

Az állami-igazgatási szint, a civil szféra, valamint a vállalati-ipari szint szereplőinek együttes stratégiát kell kialakítaniuk. Meg kell találni azt a közös nevezőt, amely a digitális gyermekvédelem mindhárom potenciális szereplőjét ugyanazon cél elérése érdekében, egymással nem versengve, hanem a kompetenciákat és a feladatokat megosztva motiválja egy, a gyermekek számára biztonságosabb digitális eszközhasználat elérése érdekében.

El kell különíteni és tisztázni kell az igazságszolgáltatás, az oktatási intézmények, valamint a közösség – benne a társadalom és a szülők – szerepét és teendőit a *bullying* megelőzése és kezelése terén. Az online megfélemlítés elleni programok csak akkor bizonyultak sikeresnek, ha azokban aktív szerepet vállalt az egész iskola, a lakóközösség, valamint a szülők is.
A civil szervezetek által végzett segítségnyújtás, tudatosítás pályázati projektekre épül, amelyek nem biztosítanak működési támogatást. Ez megnehezíti az állandó és magas színvonalú segítségnyújtást. A pályázatok csak ciklusokat, innovatív, új dolgokat támogatnak, ami a segítő szolgáltatások működését megnehezíti. Az államnak – a meglévő pályázati források strukturáltabb elosztásával – támogatnia kell a civil szférát (mind az érzékenyítés, mind a segítségnyújtás szereplőit) annak érdekében, hogy képesek legyenek az együttműködésre. Szükséges olyan működési támogatások megteremtése, amelyek hozzájárulnak a már kidolgozott jó gyakorlatok továbbéléséhez.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a3.3.1) Az online zaklatások, megfélemlítések (cyberbullying) kezelésére és megelőzésére szolgáló programok létrehozása és működtetése, a meglévő programokhoz illeszkedve, azok szakmai tartalmának és tapasztalatainak felhasználásával.

a3.3.2) A jelenleg is meglévő online megfélemlítés elleni programok tapasztalatai alapján részletes akcióterv kidolgozása a jogsértő cselekmények számának visszaszorítása érdekében.

E3.4) Feladatok a meglévő jogorvoslati mechanizmusok szélesebb körű megismertetése terén

Problémát jelent, ha a jogrendszerben egyébként létező sérelemkezelési eljárások, lehetőségek széles körben nem ismertek. A tapasztalat az, hogy ha a sérelmet elszenvedettek nem ismerik az e tekintetben rendelkezésükre álló lehetőségeket, akkor a szabályozás hatékonysága, az általa elérni kívánt hatás elvész. Erre példa lehet a Btk.-ban foglalt szabályok alkalmazása éppúgy, mint más, internetspecifikus rendelkezések a jogrendszerben. Az Ekertv. 4/A.§ alapján a szolgáltató a gyermekek fejlődésére károsan ható információt csak a kiskorúak lehetséges veszélyeztetéséről szóló tájékoztatást tartalmazó figyelmeztető jelzéssel, továbbá az aloldal forráskódjában szereplő olyan azonosítókkal tehet közzé, melyek a szűrőszoftver számára felismerhetőek. Emellett 2013 óta van lehetőség például az Ekertv. 13. §

(13)–(15) bekezdései alapján a gyermekek személyiségi jogait sértő tartalmak online térből való egyszerű és hatékony eltávolítására, amely kiegészíti a polgári- és büntetőeljárások biztosította lehetőségeket, de ilyen kérelmeket az Ekertv. szerint eljáró Gyermekvédelmi Internet-kerekasztal nem kapott. E szabály rendkívül súlyos, és a tapasztalatok szerint gyakran előforduló problémát kíván kezelni. Szélesebb körű gyakorlati alkalmazásához szükséges lenne:

- Az Ekertv. eljárási jellegű szabályainak áttekintése, szükség esetén módosítása, az önrendelkezési jog tiszteletben tartása mellett;
- Az internethozzáférés-szolgáltatók és a kormányzat erre kijelölt szerve közötti olyan megállapodások megkötése, amely az Ekertv. ezen rendelkezésének alkalmazása során felmerülő gyakorlati kérdéseket dönti el, illetve rögzíti;
- A médiaoktatásban, illetve tájékoztató kampányok során a rendelkezés szélesebb körű ismertté tétele, mind a gyermekek, mind a szülők és a pedagógusok körében.

Az eszközcsoporthoz tartozó intézkedések (akciók):

a3.4.1) Az Ekertv. gyermekek megóvását célzó szabályainak, valamint az online-kereskedelemmel kapcsolatos fogyasztóvédelmi jogérvényesítést bemutató ismeretterjesztő és tájékoztató anyagok elkészítése és az iskolákba való eljuttatása, továbbá az egyes köznevelési intézmények honlapján az online gyermekvédelem területén alkalmazható jogszabályokról, védelmi lehetőségekről és a médiaműveltség növelését célzó programokról szóló naprakész információk elérhetővé tétele.

a3.4.2) Az Ekertv. szabályainak valamint az Internet Hotline szolgáltatásnak a szélesebb körű megismertetését célzó programok lebonyolítása, tevékenységek végzése.

RÖVIDÍTÉSJEGYZÉK

AJBH – Alapvető Jogok Biztosának Hivatala

Ajbt. – az alapvető jogok biztosáról szóló 2011. évi CXI. törvény

AVMS irányelv – Az Európai Parlament és a Tanács 2010. március 10-i 2010/13/EU irányelve a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv, kodifikált változat)

Be. – a büntetőeljárásról szóló 1998. XIX. törvény

Btk. – a Büntető Törvénykönyvről szóló 2012. évi C. törvény

Eht. – az elektronikus hírközlésről szóló 2003. évi C. törvény

Eker. irányelv – az Európai Parlament és a Tanács 2000. június 8-i 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól

Ekertv. – az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény

ENYÜBS – Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika

Fgy. tv. – a fogyasztóvédelemről szóló 1997. évi CLV. törvény

Gyvt. – gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény

Infotv. – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

Köznev. tv. – a nemzeti köznevelésről szóló 2011. évi CXC. törvény

Médiatanács – a Nemzeti Média- és Hírközlési Hatóság Médiatanácsa

Mttv. – a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény

MTVA – Médiaszolgáltatás-támogató és Vagyonkezelő Alap

NAIH – Nemzeti Adatvédelmi és Információszabadság Hatóság

NAT – Nemzeti alaptanterv

NMHH – Nemzeti Média- és Hírközlési Hatóság

Ptk. – a Polgári Törvénykönyvről szóló 2013. évi V. törvény

Smtv. – a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény

Szabs. tv. – a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény

digitális jólét program

MELLÉKLET

1. sz. melléklet – Statisztikai adatok az online megfélemlítés (*cyberbullying*) gyakorlatáról[1]

Eljárási adatok 2015

1978. évi IV. tv	2012. évi C. tv	Eljárások száma	*Ebből*				
			Feljelentés elutasítása	*Nyomozás megszüntetés*	*Vádemelés*	*Egyéb befejezés*	*Elterelés*
Kényszerítés 174. §	Kényszerítés 195. §	539	149	283	68	33	6
Zaklatás 176/A. §	Zaklatás 222. §	16 799	4 741	7 924	2 572	631	931
Visszaélés személyes adattal 177/A. § (1) a. pont		118	9	23	81	0	5
	Személyes adattal visszaélés 219. § (1) a. pont	1 288	247	213	674	132	22
Levéltitok megsértése 178. § (1) bek.	Levéltitok megsértése 224. § (1) bek.	36	13	18	1	4	0
Magántitok jogosulatlan megismerése 178/A. § (1),(2) bek.		1	0	1	0	0	0
	Tiltott adatszerzés 422. § (1) bek.	66	23	22	12	9	0
Rágalmazás 179. §	Rágalmazás 226. §	336	84	139	59	36	18
	Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése 226/A. §	1	0	1	0	0	0

[1] Az adatok forrása az Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika, amely úgynevezett követő statisztika; minden esetben a már lezárt eljárások számáról ad tájékoztatást. Az adatbázis nem az elkövetési idő, hanem a statisztikában való rögzítés időpontja szerint tartalmazza az adatokat. A számok a 2016. július 12-i adatállapotot tükrözik.

	Becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala 226/B. §	10	0	3	1	5	1
Becsületsértés 180. §	Becsületsértés 227. §	1 323	99	272	818	69	65
Kiszolgáltatott személy megalázása 180/A. §	Kiszolgáltatott személy megalázása 225. §	9	5	3	1	0	0
Számítástechnikai rendszer és adatok elleni bűncselekmény 300/C. § (1) bek.		58	1	38	18	0	1
	Információs rendszer vagy adat megsértése 423. § (1) bek.	622	64	179	64	280	35

Regisztrált bűncselekmények – sértetti oldal 2015

1978. évi IV. tv	**2012. évi C. tv**	**Regisztrált bűncselekmények száma**	**Ismertté vált természetes sértettek száma**	***Ebből 18 év alatti sérelmére***	***Ebből*** ***Számítástechnikai eszközzel elkövetett***
Kényszerítés 174. §	Kényszerítés 195. §	120	120	35	1
Zaklatás 176/A. §	Zaklatás 222. §	7 253	7 255	437	43
Visszaélés személyes adattal 177/A. § (1) a. pont		89	16	0	0
	Személyes adattal visszaélés 219. § (1) a. pont	838	0*	0	0
Levéltitok megsértése 178. § (1) bek.	Levéltitok megsértése 224. § (1) bek.	18	16	0	0

Magántitok jogosulatlan megismerése 178/A. § (1),(2) bek.		1	1	0	0
	Tiltott adatszerzés 422. § (1) bek.	22	19	1	1
Rágalmazás 179. §	Rágalmazás 226. §	181	176	7	0
	Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése 226/A. §	1	1	0	0
	Becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala 226/B. §	6	6	1	1
Becsületsértés 180. §	Becsületsértés 227. §	1 078	1 077	74	0
Kiszolgáltatott személy megalázása 180/A. §	Kiszolgáltatott személy megalázása 225. §	4	4	1	0
Számítástechnikai rendszer és adatok elleni bűncselekmény 300/C. § (1) bek.		25	10	0	0
	Információs rendszer vagy adat megsértése 423. § (1) bek.	406	0*	0	0

* A 2012. évi C. tv 2013.07.01-jei hatályba lépésétől az ENyÜBS nem gyűjti a sértett adatait.

Elkövetői oldal 2015

1978. évi IV. tv	2012. évi C. tv	Összes regisztrált elkövető	*Ebből 18 év alatti*	*Ebből*				
				Feljelentés elutasítása	*Nyomozás megszüntetés*	*Vádemelés*	*Egyéb befejezés*	*Elterelés*
Kényszerítés 174. §	Kényszerítés 195. §	52	13	3	3	6	0	1
Zaklatás 176/A. §	Zaklatás 222. §	2 806	120	5	58	33	7	17
Visszaélés személyes adattal 177/A. § (1) a. pont		3	0	0	0	0	0	0
	Személyes adattal visszaélés 219. § (1) a. pont	35	3	0	2	1	0	0
Levéltitok megsértése 178. § (1) bek.	Levéltitok megsértése 224. § (1) bek.	0	0	0	0	0	0	0
Magántitok jogosulatlan megismerése 178/A. § (1),(2) bek.		1	0	0	0	0	0	0
	Tiltott adatszerzés 422. § (1) bek.	8	0	0	0	0	0	0
Rágalmazás 179. §	Rágalmazás 226. §	55	14	0	9	3	0	2
	Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése 226/A. §	0	0	0	0	0	0	0
	Becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala 226/B. §	2	1	0	0	0	0	1
Becsületsértés 180. §	Becsületsértés 227. §	377	34	2	18	11	2	1

Kiszolgáltatott személy megalázása 180/A. §	Kiszolgáltatott személy megalázása 225. §	0	0	0	0	0	0	0
Számítástechnikai rendszer és adatok elleni bűncselekmény 300/C. § (1) bek.		6	0	0	0	0	0	0
	Információs rendszer vagy adat megsértése 423. § (1) bek.	59	14	0	12	0	0	2

A táblázatok a *cyberbullying* különböző magatartásaira ráilleszthető tényállásokat tartalmazzák. Ezek; a kényszerítés, zaklatás, a visszaélés személyes adattal, a levéltitok megsértése, a magántitok jogosulatlan megismerése, a tiltott adatszerzés, a rágalmazás, a becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése és nyilvánosságra hozatala, a becsületsértés, a kiszolgáltatott személy megalázása, az információs rendszer vagy adat megsértése és a tiltott adatszerzés bizonyos magatartásai.

Az Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika (ENyÜBS) nem ad teljes képet a *cyberbullying* elterjedtségéről, ennek okai a következők.

- A Btk.-ban nem szabályozott a *cyberbullying* magatartásainak teljes köre; az enyhébb súlyú *cyberbullying* magatartások, így például az online kiközösítés vagy a bántó, megalázó üzenetek online felületen való posztolása, megosztása nem érik el a társadalomra veszélyességnek olyan súlyos fokát, amely indokolná e magatartások kriminalizálását. A kriminalizálás ugyanakkor amiatt sem támogatandó, mert e magatartások tipikusan fiatalok, illetve gyermekkorúak között (általános- és középiskolás korban) fordulnak elő, és a kriminológiai kutatások nem javasolják a korai szankcionálást, a stigmatizálódás veszélye miatt.
- Az ENyÜBS adatbázisba került ügyek csak a jéghegy csúcsát jelentik, a legtöbb *cyberbullying*-magatartás rejtve marad. Ennek oka lehet, hogy a kiskorú sértett nem szól róla felnőttnek, vagy a körülötte lévő felnőttek nem jelentik a cselekményt a rendőrségnek.
- Bár a rendszer lehetőséget ad a „számítástechnikai eszközzel” elkövetett cselekmények leválogatására, ezen belül nem lehet elkülöníteni a számítógéppel, mobileszközökkel, illetve az interneten (online: e-mailen vagy

közösségi oldalon) való elkövetést. Míg minden, interneten megvalósuló cselekményt valószínűleg számítástechnikai eszköz használatával követnek el, addig ez fordítva nem mondható el, hiszen egy mobiltelefon megszerzése és az azon tárolt adatok törlése, módosítása, manipulálása nem feltétlenül kapcsolódik az online szférához. A *cyberbullying* magatartásai általában online kommunikációban (az online közösségi felületen, weboldalon, azonnali üzenetküldő felületeken stb.) valósulnak meg. Az ENyÜBS azonban nem tesz lehetővé finombontást az online cselekmények volumenének ellenőrzésére.

- Az ENyÜBS nem ad lehetőséget az elkövetői és sértetti oldal összekapcsolására. Míg a bűncselekményi statisztika tartalmazza a sértetti bontást, tehát a kiskorúak (18 év alatti személyek) sérelmére elkövetett cselekmények leválogathatók, addig az elkövetői statisztika a kiskorú elkövetők leválogatására ad lehetőséget, de nincs mód olyan csoportosítás létrehozására, hogy hány fiatalkorú elkövető által kiskorú személy sérelmére megvalósított *cyberbullying*-típusú cselekményt követtek el.

Az önbevallásos kutatások adatai és a hatóság tudomására jutó cselekmények különbsége adná azt a becsült számot, amely megmutatná a rejtve maradó cselekmények nagyságrendjét. Azonban Magyarországon sem a statisztika, sem pedig az önbevallásos látenciakutatások nem alkalmasak a gyermekek (az ENSZ Gyermekjogi Egyezménye szerint 18. évet be nem töltött személyek) között megvalósuló *cyberbullying* nagyságrendjének becslésére. A látenciakutatások mintavétele, mintanagysága, a minta súlyozása, a mintába került gyermekek életkora, valamint a vizsgálni kívánt magatartások, illetve a kérdésfeltevés miként nem ad lehetőséget egyfelől a látenciakutatások eredményeinek összehasonlítására, másrészt pedig az ENyÜBS adataival való összevetésre. A fiatalok közötti *cyberbullying* cselekmények volumenének felmérésére ezért a legideálisabb egy büntetőeljárási aktakutatás lenne, ami eddig szintén nem volt Magyarországon.

A *cyberbullying* elterjedtségéről a hatósági statisztikán túl jelenleg az önbevallásos látenciakutatások adnak orientáló jellegű képet. A magyarországi *cyberbullying* kutatások közül ehelyütt a TABBY (*Threat Assessment of Bullying Behaviour in Youth*) program, valamint a Megfélemlítés Elleni Program említhető.

A TABBY in Internet[2] 2011 és 2015 között budapesti és vidéki általános- és középiskolákban folyó komplex program a 10-18 éves diákok *cyberbullying*-fertőzöttségét mérte fel. A 2013-as felmérésben összesen 600 diák vett részt. A válaszolók több mint fele (59%) elszenvedett valamiféle enyhe online bántalmazást,

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

közülük mintegy 5% hetente lett áldozata *cyberbullying*nak. A kutatás egyik legfontosabb megállapítása, hogy a notórius online bántalmazók az iskolai (tehát offline) bántalmazás elkövetői és áldozati oldalán is részt vesznek.

A Megfélemlítés Elleni Program állapotfelmérése[3] 2014 tavaszán, két budapesti iskolában zajlott. Az anonim kérdőívet 704 diák töltötte ki a 10-18 éves korosztályból. Az összesített adatok szerint a válaszolók 22,2%-a szenvedett el és 20%-a követett már el életében valamilyen korosztályi bántalmazást vagy megfélemlítést (iskolai és/vagy *cyberbullying*ot). A kutatás által nevesített online bántalmazási formák valamelyikét a középiskolások 7%-a szenvedte el életében, míg ez az áldozattá válási arány az általános iskolások esetében némileg alacsonyabb: 6,2%. A középiskolások jóval nagyobb arányban vallották be valamilyen *cyberbullying* magatartás elkövetését (10,2%), mint a kisiskolások (2%). A két kutatás által nevesített *cyberbullying* fajták a következők voltak:

- Baráti társasága kiközösítette egy online közösségből;
- Megosztották személyes titkát vagy fényképét a neten az engedélye nélkül;
- Nevében bántó üzeneteket posztoltak, amellyel lejáratták őt a barátai előtt;
- Bántó, kegyetlen pletykát terjesztettek róla a neten;
- Megfélemlítő célú online üzenetet kapott.

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