CYBERHŐSÖK

SZAKMAI HÁTTÉRTANULMÁNY

Gyermekek online biztonsága, digitális veszélyek és a megelőzés lehetőségei

Szakirodalmi áttekintés és szakmai megalapozás a CyberHősök gyermek-, szülő- és pedagógusprogramhoz.

2026

Kézirat – szakmai háttéranyag

Absztrakt

A gyermekek digitális környezete egyszerre kínál tanulási, kapcsolati, kreatív és részvételi lehetőségeket, miközben olyan kockázati helyzeteket is létrehoz, amelyek sajátosságai részben eltérnek az offline térben ismert veszélyektől. A háttértanulmány célja a CyberHősök program tudományos megalapozása: a gyermekek online jelenlétére, digitális készségeire, adatvédelmére, online bántalmazására, manipulációjára, szexuális megkeresésére, problémás közösségimédia-használatára, valamint a szülői és iskolai mediációra vonatkozó szakirodalom kritikai szintézise. A feldolgozás hierarchikus evidenciaszemléletet követ: elsőbbséget kapnak a szisztematikus áttekintések és metaanalízisek, majd a nagy mintás, több országra kiterjedő kutatások, ezt követően a longitudinális és kvalitatív vizsgálatok, végül a hiteles intézményi jelentések. A tanulmány hangsúlyozza, hogy az online kockázatnak való kitettség nem azonos a tényleges kárral; a gyermek életkora, fejlődési szintje, digitális kompetenciája, családi és kortárs kapcsolatai, valamint az adott platform architektúrája egyaránt módosítja a kimeneteket. A

szakirodalom alapján a pusztán tiltó vagy technikai kontrollra épülő megközelítés helyett a bizalom, az aktív szülői mediáció, a digitális és adatvédelmi műveltség, az érzelmi biztonság, a segítségkérési készség és az intézményi válaszrendszer együttes fejlesztése indokolt. A záró fejezet a CyberHősök program számára konkrét, mérhető és pilotvizsgálatban tesztelhető szakmai ajánlásokat fogalmaz meg.

Kulcsszavak: gyermekek online biztonsága; cyberbullying; online grooming; adatvédelem; digitális műveltség; szülői mediáció; prevenció; reziliencia.

A tanulmány célja és státusza

Ez a dokumentum szakmai háttértanulmány, nem klinikai diagnosztikai kézikönyv és nem jogi tanácsadás. Feladata, hogy a CyberHősök program edukációs tartalmait ellenőrizhető tudományos állításokra építse. Ahol a kutatási eredmények ellentmondásosak, ott a szöveg ezt kifejezetten jelzi; ahol oksági következtetés nem vonható le, ott asszociációról beszél. A prevalenciaadatokat különös óvatossággal kell értelmezni, mert a definíciók, mérőeszközök, időablakok és mintavételi eljárások jelentősen eltérhetnek.

Tartalmi áttekintés

1. Bevezetés és problémafelvetés

2. Módszertani keret és forráskritika

3. Elméleti és fejlődéslélektani háttér

4. A gyermekek digitális ökoszisztémája

5. Digitális műveltség, adatvédelem és digitális lábnyom

6. Online bántalmazás és cyberbullying

7. Online idegenek, megtévesztés, grooming és szexuális kockázatok

8. Közösségi média, problémás használat, alvás és pszichés jóllét

9. Szülői mediáció és családi digitális kultúra

10. Iskolai prevenció, pedagógusi szerep és intézményi válasz

11. Mit tegyünk, ha már megtörtént a baj?

juvenis

12. A CyberHősök program szakmai ajánlásai

13. Pilot, mérés és hatásvizsgálat

14. Következtetések

1/A. Magyarországi empirikus háttér és a hazai digitális gyermekkor

1/1. Miért szükséges külön magyar kontextus?

A nemzetközi kutatások nélkülözhetetlenek a gyermekek online kockázatainak mechanizmusaihoz, ugyanakkor egy magyar prevenciós program nem épülhet kizárólag más országokból származó prevalenciákra. A platformkínálat, a családi digitális kultúra, az iskolai gyakorlat, a hozzáférés és a szülői mediáció társadalmi mintázatai országonként eltérhetnek. Emiatt a CyberHősök szakmai modelljében a nemzetközi evidenciák a mechanizmusokat és beavatkozási elveket, a magyar adatok pedig elsősorban a célcsoport helyzetének és a program relevanciájának leírását szolgálják.

A Nemzeti Média- és Hírközlési Hatóság 2024 vége és 2025 eleje között végzett Digital parenting kutatása 2000, 7–16 éves gyermek és 2000 szülő bevonásával készült, országosan reprezentatív mintán. A kutatási program külön értéke, hogy ugyanazon témakörben 2017-es és 2020-as adatfelvételekhez is kapcsolódik, így nem pusztán pillanatfelvételt ad. Az NMHH adatai szerint 2024-ben a 7–16 éves gyermekek 84%-a internetezett rendszeresen; a saját mobiltelefon elterjedtsége életkorral meredeken nőtt, a 7–8 évesek 29%-ától a 15–16 évesek 99%-áig. Ezek az adatok nem önmagukban kockázati mutatók, hanem azt jelzik, hogy az online biztonság oktatása már az alsóbb életkorokban releváns, miközben a tartalom életkor szerinti differenciálása nélkülözhetetlen (NMHH, 2025).

1/2. Képernyőidő és használati szerkezet

Az NMHH 2025-ös Médiapiaci Jelentésében közölt adatok szerint a 9–16 évesek iskolaidőn kívüli internethasználata hétköznap átlagosan 121 perc, hétvégén 208 perc volt; a 15–16 éveseknél ugyanez 148, illetve 245 perc. Ezek a számok fontos kontextust adnak, de nem értelmezhetők önmagukban egészségügyi kockázati küszöbként. A szakirodalom egyre inkább különbséget tesz a puszta időtartam és a használat minősége között. A problémás, kontrollvesztett

vagy alvást, tanulást és kapcsolatokat kiszorító használat több vizsgálatban erősebb összefüggést mutat kedvezőtlen pszichés kimenetekkel, mint az általános használati idő (Shannon et al., 2022).

A párhuzamos médiafogyasztás életkorral szintén emelkedik. Az NMHH adatai szerint a 15–16 évesek 80%-a legalább heti rendszerességgel fogyaszt párhuzamosan médiatartalmat. Ez a CyberHősök számára azért releváns, mert a figyelemmegosztás, az értesítési környezet és a több platform közötti gyors váltás megnehezítheti a kockázati jelzések tudatos feldolgozását. A program azonban nem állíthatja, hogy a multitasking önmagában patológiás; inkább figyelemmenedzsmentet és tudatos megszakítási pontokat érdemes tanítani.

1/3. Közösségi média magyar gyermekek körében

A 2024–2025-ös hazai adatokban a napi közösségimédia-használat erősen életkorfüggő: a 7–8 évesek 10%-a, a 9–10 évesek 28%-a, a 11–12 évesek 46%-a, a 13–14 évesek 69%-a, a 15–16 évesek 82%-a látogatott napi rendszerességgel közösségimédia-oldalakat. A kutatásban szereplő platformok használata több esetben már a szolgáltatások tipikus minimumkorhatára alatt is megjelent. Prevenciós szempontból ezért nem elegendő azt mondani, hogy egy adott platform „13 éven felülieknek való”: a programnak számolnia kell a tényleges használattal, és a gyermekekhez eljutó biztonsági tudást nem kötheti kizárólag a platform formális korhatárához (NMHH, 2025).

A hazai adatok azt is mutatják, hogy a gyermekek digitális ökoszisztémája többplatformos. Ez módszertani következménnyel jár: a program példái nem rögzülhetnek egyetlen alkalmazás aktuális menüjéhez. A platformok gyorsan változnak, funkciók vándorolnak közöttük, és ugyanaz a kapcsolati kockázat – például idegen megkeresése, csoportos kiközösítés vagy intim tartalom továbbküldése – több szolgáltatáson is megjelenhet. A hosszú távon használható tananyag ezért funkció- és helyzetalapú.

1/4. Hazai szülői mediáció

Az NMHH Digital parenting kutatása a szülői stratégiákat korlátozó/tiltó, ellenőrző, aktívan mediáló és technikai korlátozó megközelítésekre bontotta. A 2024–2025-ös adatfelvételben a családok 57%-a alkalmazott korlátozó/tiltó módszert, 58% ellenőrzést, 47% aktív mediációt, 53% pedig valamilyen technikai megoldást. Ezek a kategóriák átfedhetnek, ezért nem adhatók össze. A nemzetközi szakirodalommal együtt értelmezve a hazai kép azt jelzi, hogy

a szülők jelentős része már aktívan próbálja szabályozni a digitális környezetet, ugyanakkor az aktív beszélgetés további fejlesztési cél lehet (Sevilla-Fernández et al., 2025; NMHH, 2025).

A szülő–gyermek kommunikáció gyakorisága témánként eltér. A hazai kutatás szerint az internetről és digitális világról a szülők 6%-a naponta, 41%-a hetente beszélgetett gyermekével; ez lényegesen ritkább, mint az iskolai ügyek napi megbeszélése. A CyberHősök szülői moduljának ezért nem egy újabb tiltó szabályrendszer létrehozása az elsődleges célja, hanem a rendszeres, nem krízisvezérelt digitális beszélgetés normalizálása.

Hazai indikátor	2024–2025-ös adat	Szakmai értelmezés
Rendszeres internethasználat, 7–16 év	84%	Az online biztonság általános gyermeknevelési kérdés.
Saját mobil, 7–8 év	29%	A prevenciót nem célszerű csak serdülőkorban kezdeni.
Saját mobil, 15–16 év	99%	Az autonóm használat miatt a készségfejlesztés kulcsfontosságú.
Napi közösségi média, 13–14 év	69%	Kortárs és platformkockázatok központi jelentőségűek.
Napi közösségi média, 15–16 év	82%	A tiltás helyett az autonómiát támogató biztonsági készségek szükségesek.
Aktív szülői mediáció	47%	A beszélgetéses mediáció fejlesztése reális programpont.

2 A digitális kockázatok integrált elméleti modellje

2/1. Kockázat, sérülékenység és protektív tényezők

A CyberHősök elméleti modelljében az online káresemény nem egyetlen ok következménye. Célszerű három réteget elkülöníteni: expozíció, sérülékenység és válaszkapacitás. Expozíció például az idegenekkel való kommunikáció vagy nyilvános profil; sérülékenységet jelenthet az életkori éretlenség, izoláció, korábbi áldozattá válás vagy alacsony társas támogatás; válaszkapacitás pedig a digitális készség, a segítségkérési hajlandóság, a szülői bizalom és az intézményi eljárásrend. A tényleges kár valószínűsége e tényezők kölcsönhatásából adódik.

Ez a modell megakadályozza, hogy a prevenció kizárólag a gyermekre terhelje a felelősséget. Egy jól képzett gyermek is kerülhet olyan helyzetbe, amelyben felnőtt segítség,

platformbeavatkozás vagy hatósági intézkedés szükséges. A reziliencia ezért nem sérthetetlenség, hanem a megfelelő erőforrásokhoz való hozzáférés és a káros folyamat gyors megszakításának képessége.

2/2. Platformaffordanciák és kockázati mechanizmusok

A digitális platformok úgynevezett affordanciái – például anonimitás, tartósság, kereshetőség, skálázhatóság, privát üzenetküldés, algoritmikus ajánlás és továbboszthatóság – módosítják a társas interakció természetét. Cyberbullying esetén a közönség nagysága és a tartalom tartóssága növelheti a megszégyenítés intenzitását; grooming esetén a privát kommunikáció, a folyamatos elérhetőség és a több csatorna közötti váltás segítheti a fokozatos bizalomépítést. Ezek nem „rossz funkciók”: ugyanazok a tulajdonságok pozitív kapcsolódást is szolgálhatnak. A kockázat a funkció, a szándék, a helyzet és a gyermek erőforrásainak kombinációjából keletkezik.

Az algoritmikus ajánlórendszerek külön figyelmet érdemelnek, mert a gyermek által látott tartalom nem kizárólag tudatos választás eredménye. A programnak ezért meg kell tanítania, hogy az ajánlás nem minőségi vagy igazságpecsét; az algoritmus jellemzően figyelmi és relevanciajeleket optimalizál. A kritikai médiaműveltség része annak felismerése, hogy a gyakran látott tartalom nem feltétlenül gyakori a valóságban, és a népszerűség nem azonos a hitelességgel.

2/3. Szociális tanulás és normák

A gyermek online viselkedését jelentősen alakítja az, amit kortársaitól és felnőttektől lát elfogadhatónak. A szemlélői reakciók cyberbullying esetén társas megerősítésként működhetnek: a továbbosztás, a nevető reakció vagy a csendes jelenlét növelheti az elkövető által érzékelt közönséget. Ez indokolja, hogy a CyberHősök ne csak potenciális áldozatként, hanem szemlélőként és közösségi normateremtőként is megszólítsa a gyermeket.

A felnőtt modellhatás ugyanezen logika része. Ha a szülő rendszeresen nyilvánosságra hoz családi részleteket, gyenge jelszavakat használ, vezetés közben üzenetet ír vagy étkezésnél folyamatosan a telefonjára figyel, akkor a gyermek számára a kimondott szabály és a megfigyelt norma eltér. A szülői programnak ezért önreflexiós elemet is kell tartalmaznia.

juvenis

2/4. Fejlődési autonómia és arányos védelem

Az online biztonság életkori differenciálása nem egyszerűen azt jelenti, hogy a kisebb gyermek kevesebb információt kap. A fejlődéssel változik a döntési autonómia, a kortársak szerepe, a romantikus és szexuális érdeklődés, az identitáskísérletezés és a privacy iránti igény. A szülői kontroll optimális formája ezért dinamikus. Kisgyermekkorban több közvetlen szabály és technikai korlát indokolt lehet; serdülőkorban fokozatosan nő a tárgyalásos szabályalkotás, a magyarázat és a saját döntési kompetencia szerepe.

A túlzott monitorozás paradox módon csökkentheti a felnőtt informáltságát, ha a gyermek rejtett fiókokkal, törölt üzenetekkel vagy más eszközökkel kerüli meg a kontrollt. Ez nem jelenti azt, hogy monitorozás soha nem indokolt. Magas kockázatú helyzetben, fiatalabb életkorban vagy konkrét veszély esetén intenzívebb felügyelet lehet arányos. A programnak nem univerzális szabályt, hanem kockázatalapú döntési keretet kell adnia.

3. Részletes módszertani és mérési keret a CyberHősök pilothoz

3/1. Programelmélet és logikai modell

A program értékelése előtt explicitté kell tenni, milyen mechanizmuson keresztül várunk változást. A javasolt logikai lánc: szakirodalomra épülő tartalom → életkorhoz illesztett helyzetgyakorlat → kockázatfelismerés és döntési készség → magasabb önhatékonyság és segítségkérési szándék → gyorsabb és biztonságosabb valós reakció → kisebb kár és jobb pszichoszociális kimenet. A lánc minden eleme külön mérhető, és nem feltételezhető automatikusan, hogy a tudásnövekedés viselkedésváltozást eredményez.

A szülői útvonal párhuzamos: tudás és kockázati kalibráció → kevésbé büntető, inkább támogató reakció → gyakoribb aktív mediáció → magasabb gyermekoldali segítségkérési bizalom. A pedagógusi útvonal: protokollismeret → magabiztos bejelentésfogadás → következetes dokumentálás és eszkaláció → gyorsabb intézményi válasz. A teljes program hatása e három útvonal kölcsönhatásából várható.

juvenis

3/2. Elsődleges és másodlagos kimenetek

Elsődleges rövid távú kimenetként célszerű szituációs döntési tesztet használni. A gyermek rövid vignettákat kap, amelyekben több válasz közül kell kiválasztania a legbiztonságosabbat. Ez közelebb áll a tényleges döntési kompetenciához, mint a definíciók visszamondása. A tételeknek külön kell mérniük az adatvédelmet, cyberbullyingot, manipulációt, groomingot és segítségkérést.

Másodlagos kimenet lehet az önhatékonyság, a segítségkérési szándék, a bystander-viselkedés, a privacy literacy, a szülői aktív mediáció és a pedagógusi protokollismeret. A tényleges incidenciák rövid távon problémás elsődleges végpontok: ritka eseményeknél nagy minta kell, és a program kezdetben akár növelheti is a bejelentett esetek számát azáltal, hogy javítja a felismerést és a segítségkérést. A több bejelentés ezért nem feltétlenül rosszabb biztonsági helyzet.

3/3. Mérőeszköz-fejlesztés

A saját mérőeszköz fejlesztésekor tartalmi validitást szakértői bírálattal, érthetőséget kognitív interjúkkal, belső konzisztenciát megfelelő pszichometriai mutatókkal kell vizsgálni. A tudásteszt esetében a Cronbach-alfa önmagában nem elegendő, mert heterogén biztonsági kompetenciák esetén a túl magas belső konzisztencia nem feltétlenül cél. A vignettaalapú tételeknél itemnehézség és diszkrimináció is vizsgálható.

A gyermekek önbeszámolóját lehetőség szerint több információforrással kell kiegészíteni. A szülői és pedagógusi kérdőív nem „ellenőrzi” a gyermek válaszát, hanem más konstrukciót mér. A különböző nézőpontok közötti eltérés maga is informatív lehet: például a szülő magasnak ítélheti saját aktív mediációját, miközben a gyermek ritkának éli meg a digitális témájú beszélgetéseket.

3/4. Kutatási elrendezés és elemzés

Megvalósíthatósági pilotban első lépésként egycsoportos pre–post mérés használható, de ez nem alkalmas erős oksági következtetésre, mert a változás történhet ismételt tesztelés, érés vagy külső esemény miatt. A következő szint kontrollcsoportos kvázi-kísérlet, majd – ha

juvenis

szervezeti és etikai feltételei adottak – klaszterrandomizált vizsgálat. Iskolai programnál a randomizáció természetes egysége gyakran az osztály vagy iskola, nem az egyes gyermek.

Klaszterezett adatnál a hagyományos, független megfigyeléseket feltételező próbák alábecsülhetik a standard hibát. Többszintű modell vagy klaszter-robosztus becslés indokolt. A jelentésben nemcsak p-értéket, hanem effektusnagyságot és konfidenciaintervallumot is közölni kell. Előzetesen rögzíteni kell az elsődleges kimenetet, hogy a sok párhuzamos teszt ne növelje indokolatlanul a téves pozitív eredmények esélyét.

3/5. Implementációs fidelitás

Egy prevenciós program hatástalansága két különböző okból következhet: a programelmélet hibás, vagy a programot nem úgy hajtották végre, ahogyan tervezték. Ezért mérni kell az implementációs fidelitást: hány foglalkozás valósult meg, milyen hosszban, mely komponenseket adták át, hány résztvevő volt jelen, történt-e lényeges adaptáció, és mennyire fogadták el a programot a résztvevők.

A kvalitatív visszajelzés ebben a szakaszban különösen értékes. Rövid fókuszcsoportok vagy strukturált interjúk megmutathatják, mely helyzetek voltak hitelesek, mely fogalmak voltak túl absztraktak, és hol jelent meg ellenállás. A kvalitatív adat nem helyettesíti a hatásmérést, hanem segít megérteni a kvantitatív eredményeket és javítani a következő programverziót.

3/6. Etika és adatvédelem a programértékelésben

A kutatási adatminimalizálás elve szerint csak olyan személyes adat gyűjthető, amely a kutatási kérdéshez szükséges. Érzékeny online tapasztalatok mérésénél különösen indokolt az anonimizált vagy pszeudonimizált adatkezelés, a hozzáférési jogosultságok szűkítése és a megőrzési idő előzetes meghatározása. A kutatási adatbázis nem tartalmazhat szükségtelenül képernyőképeket, intim tartalmakat vagy azonosítható beszélgetéseket.

Az etikai protokollnak tartalmaznia kell a váratlan feltárás kezelését. Ha a gyermek aktuális fenyegetést, szexuális kizsákmányolást vagy önveszélyeztetést jelez, a kutató vagy programvezető nem hagyatkozhat általános titoktartási ígéretre. Előre rögzített safeguarding-eljárás, felelős személy és segítségkérési út szükséges. A gyermeknek a részvétel előtt életkorának megfelelően értenie kell e titoktartási határokat.

Mérési terület	Javasolt eszköz	Időpont	Értelmezés
Szituációs döntés	Vignettaalapú teszt	Pre, post, follow-up	Elsődleges készségkimenet
Önhatékonyság	Rövid Likert-skála	Pre, post, follow-up	Szubjektív cselekvési biztonság
Segítségkérés	Szituáció + megnevezett felnőtt	Pre, post	Kapcsolati védőfaktor
Szülői mediáció	Szülői kérdőív	Pre, follow-up	Családi folyamatváltozás
Pedagógusi protokoll	Esetvignetta	Pre, post	Intézményi válaszkészség
Fidelitás	Foglalkozásnapló	Minden alkalom	Megvalósítás minősége
Elfogadhatóság	Rövid kérdőív + interjú	Post	Implementációs információ

3/7. Előre rögzített értékelési kritériumok

A pilot sikerét nem célszerű kizárólag statisztikai szignifikanciához kötni. Előre meghatározható például legalább 80%-os foglalkozási részvétel, 85%-os tartalmi fidelitás, alacsony lemorzsolódás, a résztvevők többségénél elfogadható érthetőség, valamint a szituációs döntési tesztben kismértékű vagy nagyobb kedvező standardizált változás. Ezek a küszöbök a pilot előtt szakértői döntéssel pontosítandók.

A negatív vagy nulleredmény is értékes. Ha a tudás nő, de az önhatékonyság nem, akkor több gyakorlásra lehet szükség. Ha a gyermekmodul javulást mutat, de a segítségkérési szándék nem változik, a szülői és pedagógusi kapcsolati komponens erősítendő. Az értékelés célja nem a program „bizonyítása”, hanem a programelmélet tesztelése és javítása.

4. Módszertani megjegyzés a források ellenőrizhetőségéről

A háttértanulmány bibliográfiájában DOI-t csak olyan tételnél szabad feltüntetni, amelynek DOI-ja kiadói, Crossref-, PubMed- vagy intézményi rekordból visszaellenőrizhető. A DOI nélküli intézményi jelentés ettől még lehet magas minőségű elsődleges forrás, de a dokumentumtípust egyértelműen jelölni kell. A CyberHősök kommunikációjában a DOI megléte nem minőségi pecsét: a kutatási terv, minta, mérés és torzításkockázat továbbra is értékelendő.

A 2026-os kéziratban szereplő friss tanulmányok esetében különösen fontos az „online first” és a végleges kötet-/oldalszám megkülönböztetése. Ha a végleges bibliográfiai adatok még

nem állnak rendelkezésre, az APA 7 szerint a rendelkezésre álló online publikációs adatokat és DOI-t kell használni, majd a nyomdai vagy nyilvános véglegesítés előtt bibliográfiai auditot végezni.

5. Statisztikai helyzetkép és empirikus evidenciaatlasz

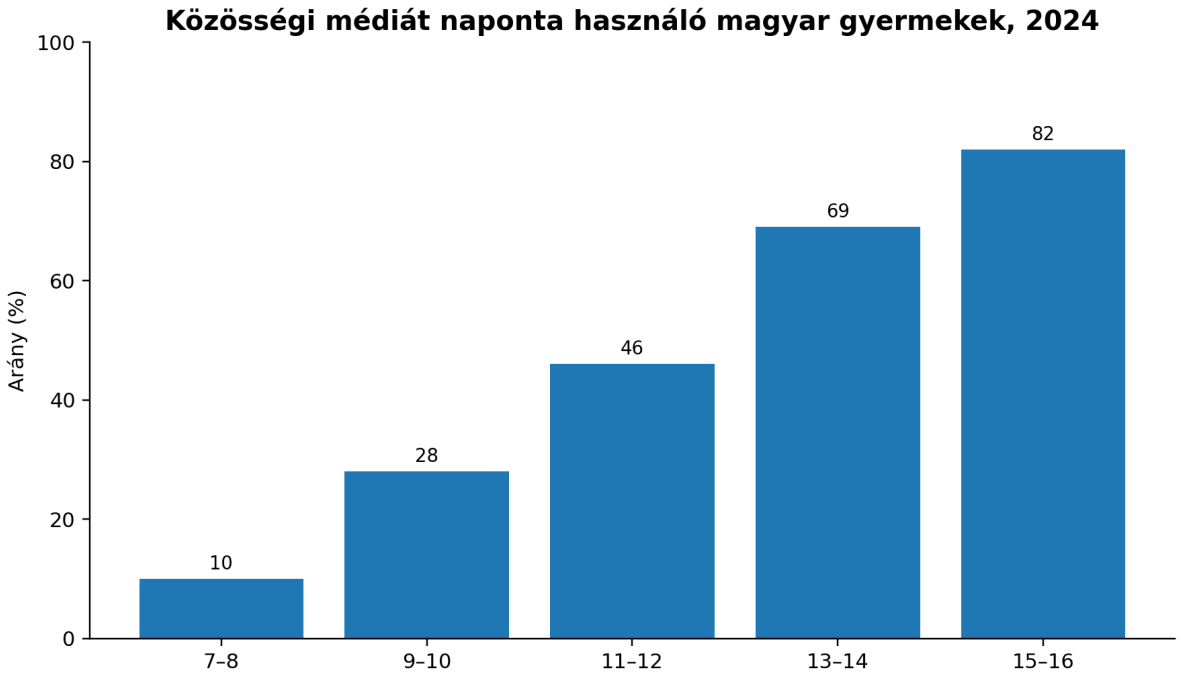
A CyberHősök szakmai megalapozásához nem elegendő annak bemutatása, hogy az online környezet kockázatokat hordoz. A programnak számszerűen is el kell helyeznie a gyermekek digitális jelenlétét, a kockázatok gyakoriságát, a pszichés összefüggéseket és a védőfaktorokat. E fejezet ezért elkülöníti a magyar reprezentatív adatokat, a több országra kiterjedő survey-eredményeket és a metaanalitikus becsléseket. A különböző típusú számok nem cserélhetők fel: egy országos prevalencia, egy európai átlag és egy korreláció eltérő kérdésre válaszol.

Az APA 7 szövegközi hivatkozási elvét követve minden empirikus állítás közvetlenül a forráshoz kapcsolódik. A százalékok mellett – ahol a forrás lehetővé teszi – megadjuk a populációt, az életkort és a mintanagyságot. A látványos statisztika szakmai célja nem a veszélyérzet maximalizálása, hanem a kockázat kalibrálása. A túlzó vagy kontextus nélküli számok ugyanúgy ronthatják a program hitelességét, mint a veszélyek bagatellizálása.

5/1. A magyar digitális gyermekkor számszerű képe

Az NMHH legfrissebb Digital parenting kutatása országosan reprezentatív, nagymintás adatfelvétel: 2000, 7–16 éves gyermek és 2000 szülő vett részt benne; a harmadik hullám adatfelvétele 2024 vége és 2025 eleje között történt (Nemzeti Média- és Hírközlési Hatóság [NMHH], 2025). Ez a forrás a CyberHősök számára különösen értékes, mert ugyanazon kutatási program korábbi, 2017-es és 2020-as hullámaival is összevethető.

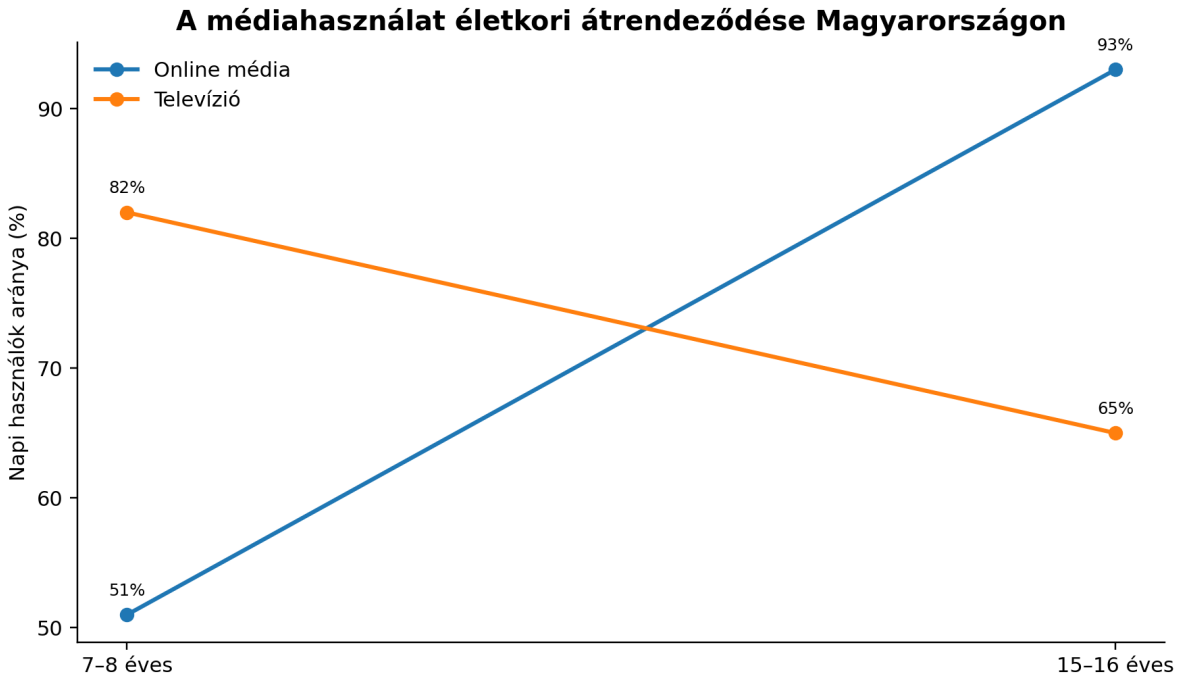
A közösségi média használata az életkorral meredeken emelkedik. A napi közösségimédia-használat a 7–8 évesek 10%-áról a 15–16 évesek 82%-ára nő. A köztes korcsoportokban 28%, 46% és 69% az arány (NMHH, 2025). Ez a minta önmagában cáfolja azt a programtervezési feltételezést, hogy az online kapcsolati kockázatok kizárólag „nagy kamaszok” problémái: a prevenciót korábban kell elkezdeni, de az életkorhoz igazított tartalommal.



1. ábra. A közösségimédia-oldalakat napi rendszerességgel látogató 7–16 évesek aránya korcsoportonként. Forrás: NMHH Digital parenting kutatás 2024–2025 (NMHH, 2025).

A médiahasználat szerkezete szintén életkori átrendeződést mutat. A 7–8 évesek 51%-a fogyaszt naponta online médiát, míg a 15–16 éveseknél ez 93%. A televíziózás ezzel ellentétes irányt mutat: 82%-ról 65%-ra csökken (NMHH, 2025). A CyberHősök szempontjából ez azt jelenti, hogy az idősebb korosztály digitális biztonságát nem lehet a „képernyőhasználat" általános fogalmával megragadni; a platformfunkciók, kommunikáció és algoritmikus tartalomterjesztés válik meghatározóvá.

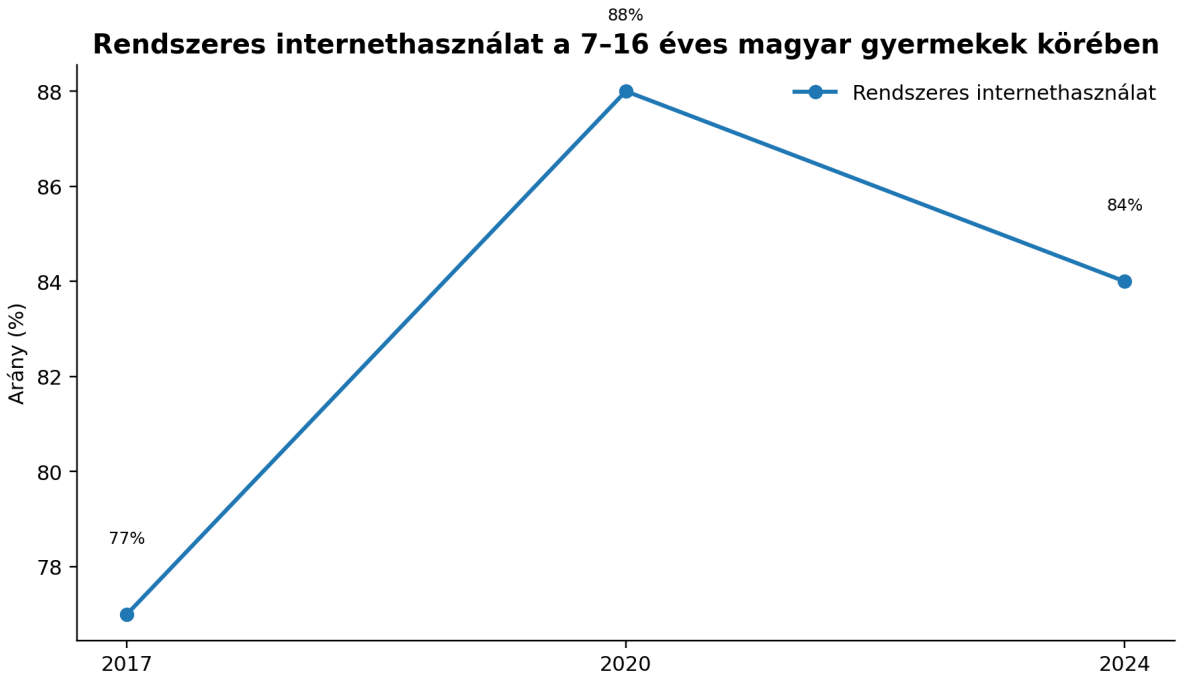
juvenis



2. ábra. Napi online médiafogyasztás és televíziózás a legfiatalabb és legidősebb vizsgált korcsoportban. Forrás: NMHH Médiapiaci Jelentés 2025 (NMHH, 2025).

A rendszeres internethasználat 2017-ben 77%, 2020-ban 88%, 2024-ben 84% volt a 7–16 évesek körében (NMHH, 2025). A 2020-as csúcs értelmezésében figyelembe kell venni a pandémiás időszak digitális oktatását. Ez jó példája annak, hogy az idősoros statisztika társadalmi kontextus nélkül félrevezető lehet.

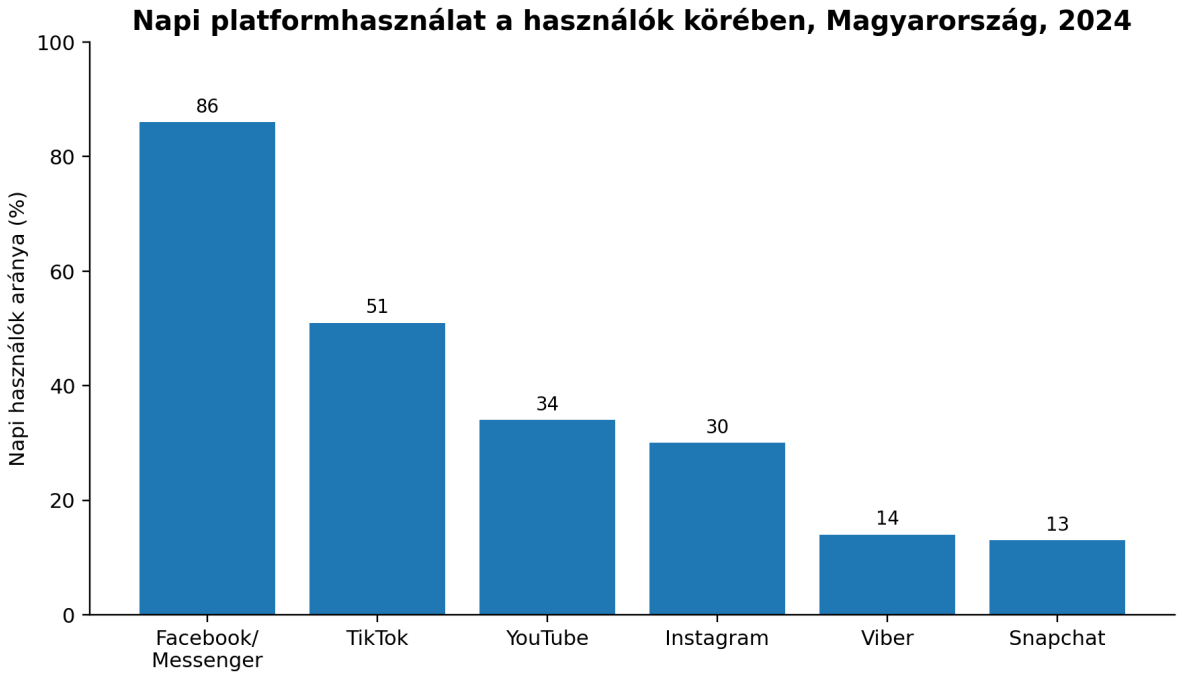
juvenis



3. ábra. A rendszeres internethasználat aránya 2017-ben, 2020-ban és 2024-ben. Forrás: NMHH Digital parenting kutatássorozat (NMHH, 2025).

A platformhasználati adatok szerint a TikTokot a vizsgált gyermekek 72%-a használja és 51% naponta, a YouTube-ot 64% használja és 34% naponta, az Instagram esetében 46%, illetve 30% az arány. A Facebook/Facebook Messenger a vizsgált használók körében rendkívül magas napi aktivitást mutatott. Az egyes platformmutatók értelmezésekor figyelembe kell venni a kérdezés és a használói bázis sajátosságait; az értékek nem adhatók össze egyetlen „közösségimédia-terheléssé” (NMHH, 2025).

juvenis



4. ábra. A vizsgált szolgáltatások napi használata az NMHH kutatásában. A platformmutatók eltérő használói bázisokhoz kötődnek, ezért nem adhatók össze. Forrás: NMHH (2025).

5/2. Európai helyzetkép: EU Kids Online 2026

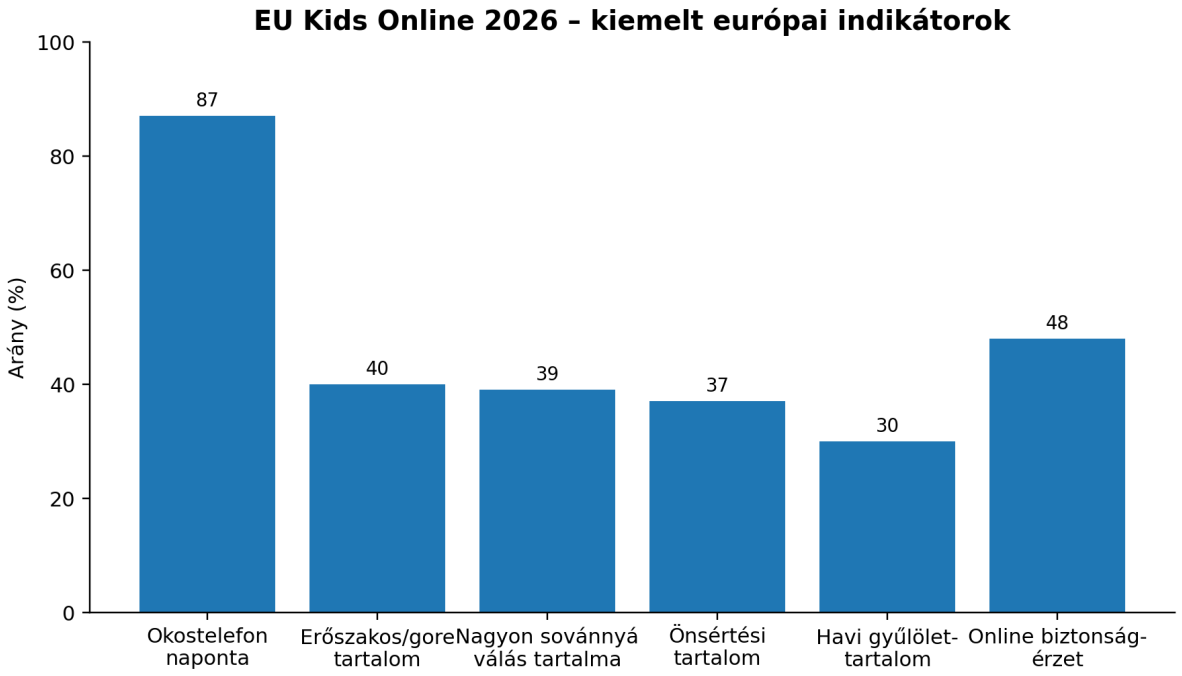
A 2026-os EU Kids Online összehasonlító vizsgálat 28 465, 10–16 éves gyermek reprezentatív mintájára épült 19 európai országban, az adatfelvétel 2025 áprilisa és 2026 áprilisa között zajlott (Staksrud et al., 2026). A mintanagyság és a közös módszertani keret miatt ez jelenleg az egyik legerősebb összehasonlító forrás a CyberHősök európai kontextusához.

A gyermekek 87%-a naponta okostelefonról vagy mobiltelefonról éri el az internetet. Ugyanakkor a digitális készségek nem egyenletesek: a technikai és kommunikációs készségek erősebbek, míg az online információk értékelése, az algoritmusok működésének megértése és a digitális tartalomalkotás gyengébb területek (Staksrud et al., 2026). Ez közvetlenül támogatja a CyberHősök azon elvét, hogy a technikai magabiztosság nem azonos a digitális kockázatokkal szembeni kompetenciával.

A káros tartalmaknak való kitettség jelentős: 40% számolt be véres vagy erőszakos képekkel való találkozásról, 39% olyan tartalomról, amely a nagyon sovánnyá válás módjait mutatta be, 37% pedig önsértéssel kapcsolatos tartalomról. Három gyermekből körülbelül egy

juvenis

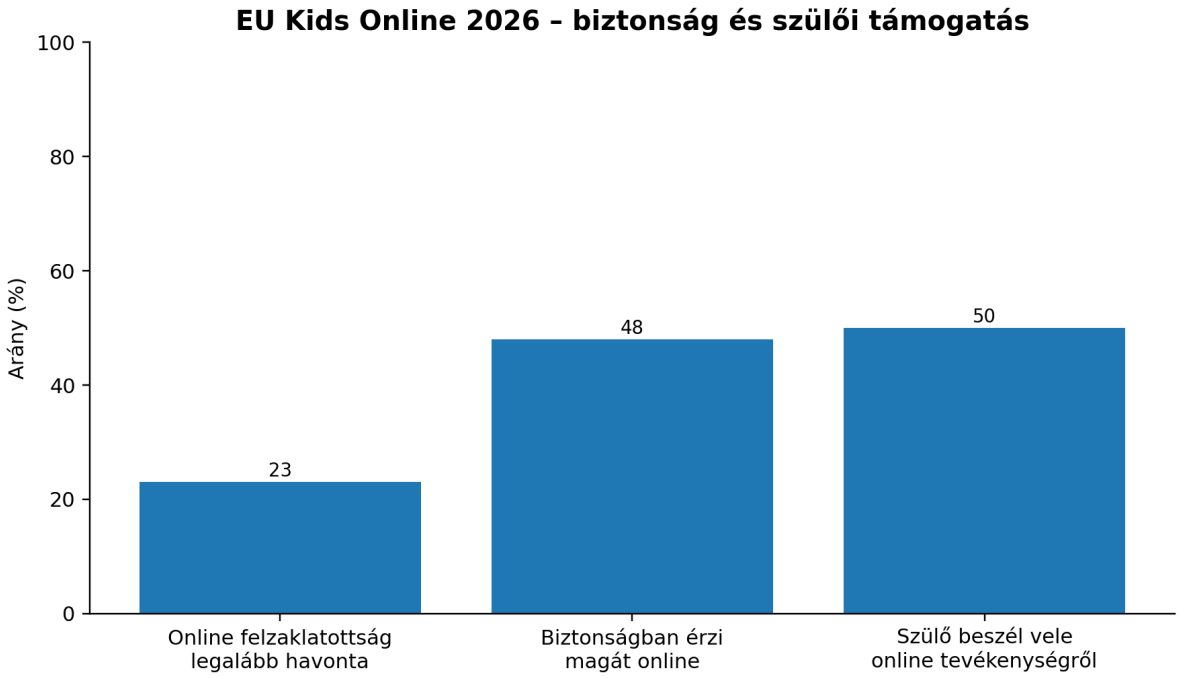
legalább havonta találkozik gyűlöletkeltő üzenetekkel (Staksrud et al., 2026). Ezek az adatok expozíciót mérnek; nem állítható belőlük, hogy minden találkozás pszichés kárt okozott.



5. ábra. Kiemelt indikátorok 28 465, 10–16 éves gyermek 19 országra kiterjedő reprezentatív vizsgálatából. Forrás: Staksrud et al. (2026).

A biztonságérzet különösen fontos indikátor. A 2026-os vizsgálatban mindössze 48% mondta, hogy biztonságban érzi magát online. A gyermekek 23%-át legalább havonta felzaklatta vagy zavarta valami az interneten. A szülői aktív támogatás egyik egyszerű indikátora – beszél-e a szülő a gyermekkel arról, mit csinál online – 50% volt (Staksrud et al., 2026).

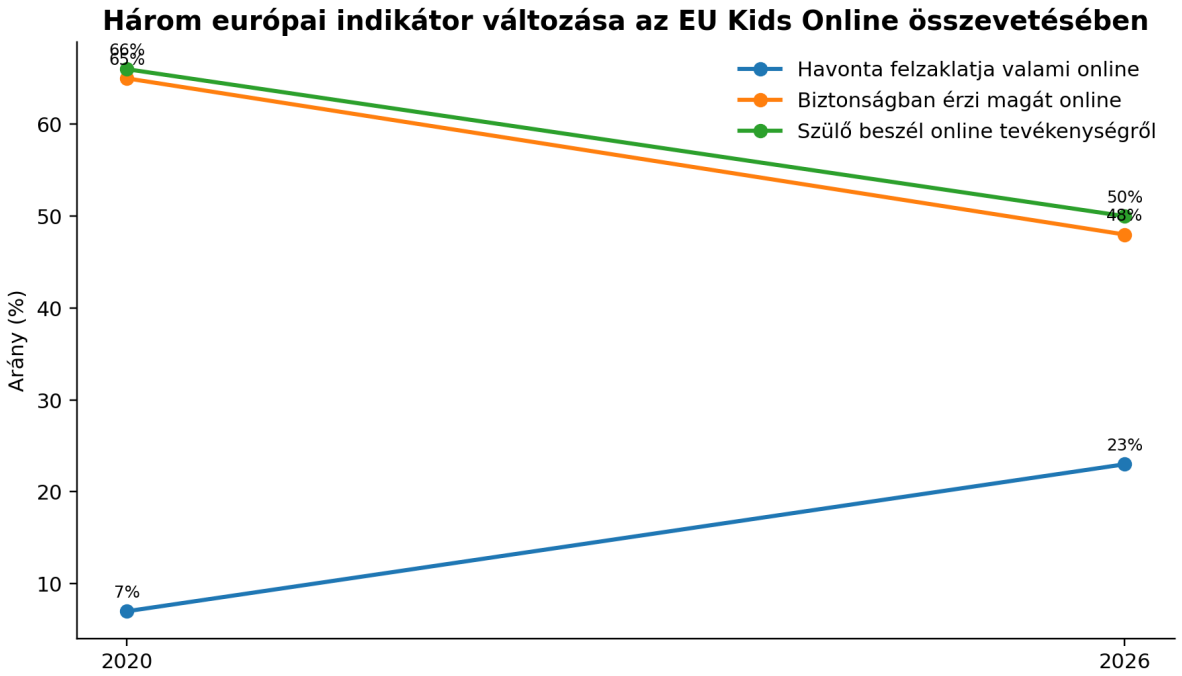
juvenis



6. ábra. A 2026-os összehasonlító kutatás fő biztonsági és szülői támogatási mutatói. Forrás: Staksrud et al. (2026).

A 2020-as és 2026-os összehasonlítás látványos változást jelez: a legalább havi online felzaklatottság 7%-ról 23%-ra nőtt, a biztonságérzet 65%-ról 48%-ra csökkent, miközben az online tevékenységről gyermekével beszélő szülők aránya 66%-ról 50%-ra esett (Staksrud et al., 2026). Az összevetést azonban nem szabad egyszerű oksági történetté alakítani: ebből nem következik, hogy a szülői beszélgetések csökkenése okozta a felzaklató élmények növekedését.

juvenis



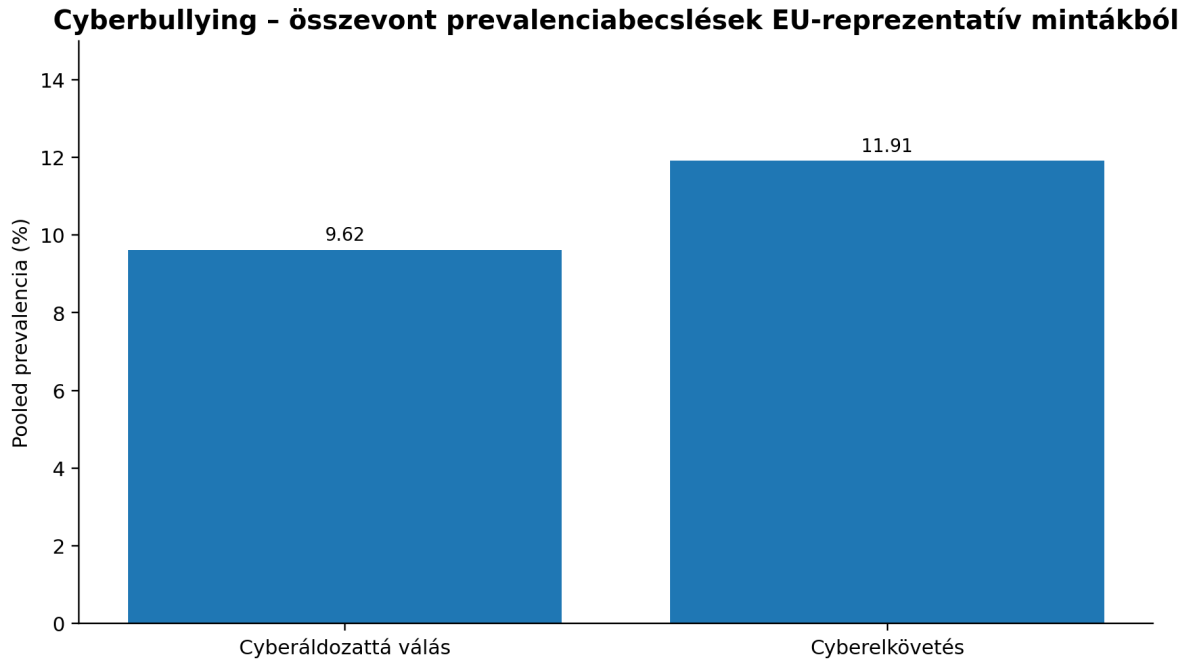
7. ábra. Az EU Kids Online által közölt összehasonlító mutatók 2020 és 2026 között. A két hullám módszertani különbségei miatt az értelmezés körültekintést igényel. Forrás: Staksrud et al. (2026).

A 2026-os eredmények új témát is behoznak: a generatív mesterséges intelligenciát. A gyermekek mintegy kétharmada rendszeresen használ AI-eszközöket; a külön tematikus EU Kids Online vizsgálat 25 592, 9–16 éves gyermek kvantitatív adatait és 244, 13–17 éves serdülő kvalitatív interjúját dolgozta fel (Staksrud et al., 2026). A CyberHősök újabb moduljaiban ezért már nem elegendő a közösségi média és cyberbullying: az AI-val kapcsolatos pontatlanság, adatvédelem, manipuláció, deepfake és túlzott bizalom is tananyaggá válik.

5/3. Cyberbullying: mit mondanak a metaanalízisek?

A cyberbullying prevalenciája erősen függ a definíciótól, mérőeszköztől és referencia-időszaktól. Henares-Montiel és munkatársai (2022) kizárólag EU-tagállamok reprezentatív populációs mintáit bevonó szisztematikus áttekintése hét vizsgálat, 25 ország adatait összegezte. Az egyes kutatásokban a cyberáldozattá válás 2,8–31,5%, az elkövetés 3,0–30,6%, a szemlélői érintettség 13,0–53,1% között mozgott. A pooled prevalencia 9,62% volt az áldozattá válásra és 11,91% az elkövetésre (Henares-Montiel et al., 2022).

juvenis



8. ábra. Hét tanulmány, 25 ország reprezentatív mintáinak metaanalízise. Forrás: Henares-Montiel et al. (2022), DOI: 10.3390/ijerph19127364.

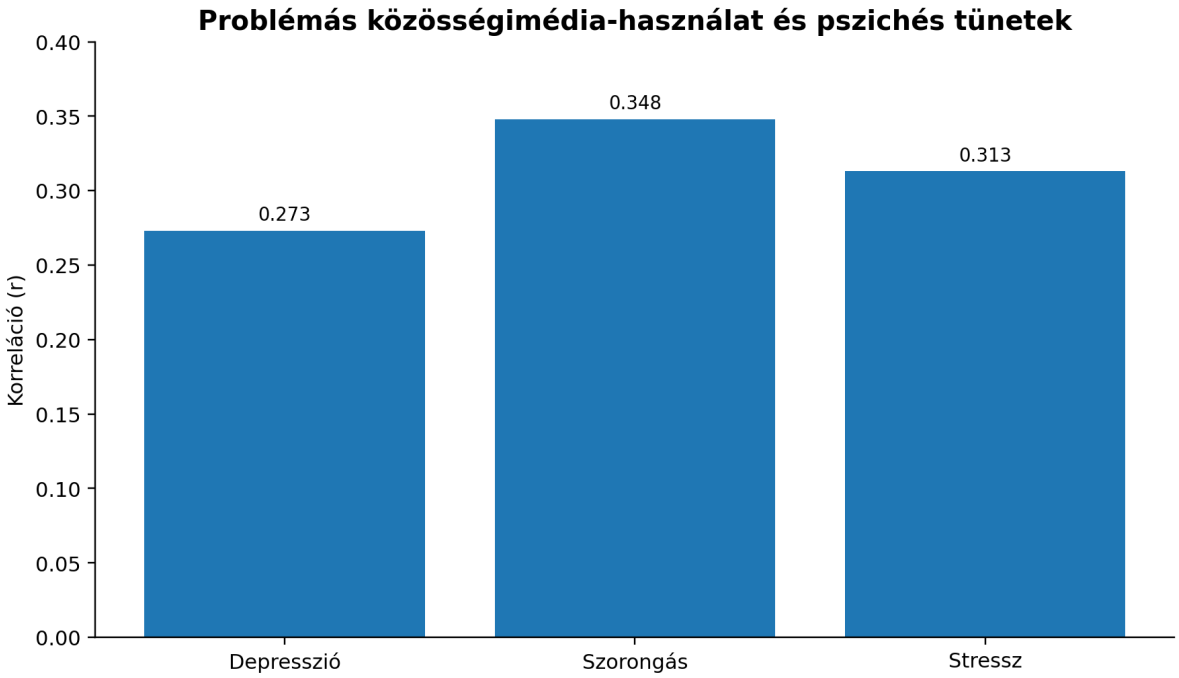
A széles tartomány módszertani figyelmeztetés. Egy plakáton szereplő „minden X. gyermek" állítás csak akkor védhető, ha pontosan megnevezzük a cyberbullying definícióját, a vizsgált időszakot, korcsoportot és földrajzi populációt. A CyberHősök publikációs standardja ezért azt javasolja, hogy a prevalenciaadatokat ne önálló figyelemfelkeltő számként, hanem rövid módszertani kontextussal együtt közöljük.

A cyberbullying következményeit vizsgáló szakirodalomban a depresszív és szorongásos tünetek, pszichés distressz, alvási problémák és egyes vizsgálatokban önsértéssel kapcsolatos kimenetek is megjelennek. Ugyanakkor a keresztmetszeti kutatások nem tudják kizárni a kétirányú kapcsolatot: a már sérülékenyebb gyermek nagyobb eséllyel válhat áldozattá, és az áldozattá válás tovább ronthatja a jóllétet. A longitudinális eredmények ezért nagyobb súlyt érdemelnek (Lee et al., 2026; Li et al., 2024).

5/4. Közösségi média és mentális egészség: effektusnagyságok helyes értelmezése

A problémás közösségimédia-használat nem azonos a gyakori használattal. Shannon és munkatársai (2022) 18 vizsgálat, összesen 9269 serdülő és fiatal felnőtt adatainak metaanalízisében mérsékelt, statisztikailag szignifikáns korrelációt találtak depresszióval (r =

.273), szorongással (r = .348) és stresszel (r = .313). Ezek az értékek kapcsolatot jeleznek, de nem bizonyítják, hogy a közösségi média okozta a tüneteket.



9. ábra. Metaanalitikus összefüggések 18 vizsgálat, 9269 résztvevő alapján. Korreláció nem jelent okságot. Forrás: Shannon et al. (2022), DOI: 10.2196/33450.

Az effektusnagyság kommunikációja kulcsfontosságú. Az r = .348 nem azt jelenti, hogy a közösségi média „34,8%-ban szorongást okoz". A korreláció irányt és erősséget fejez ki két változó között. A CyberHősök szülői anyagában ezért kerülni kell a statisztikai mutatók leegyszerűsítő százalékos átfordítását.

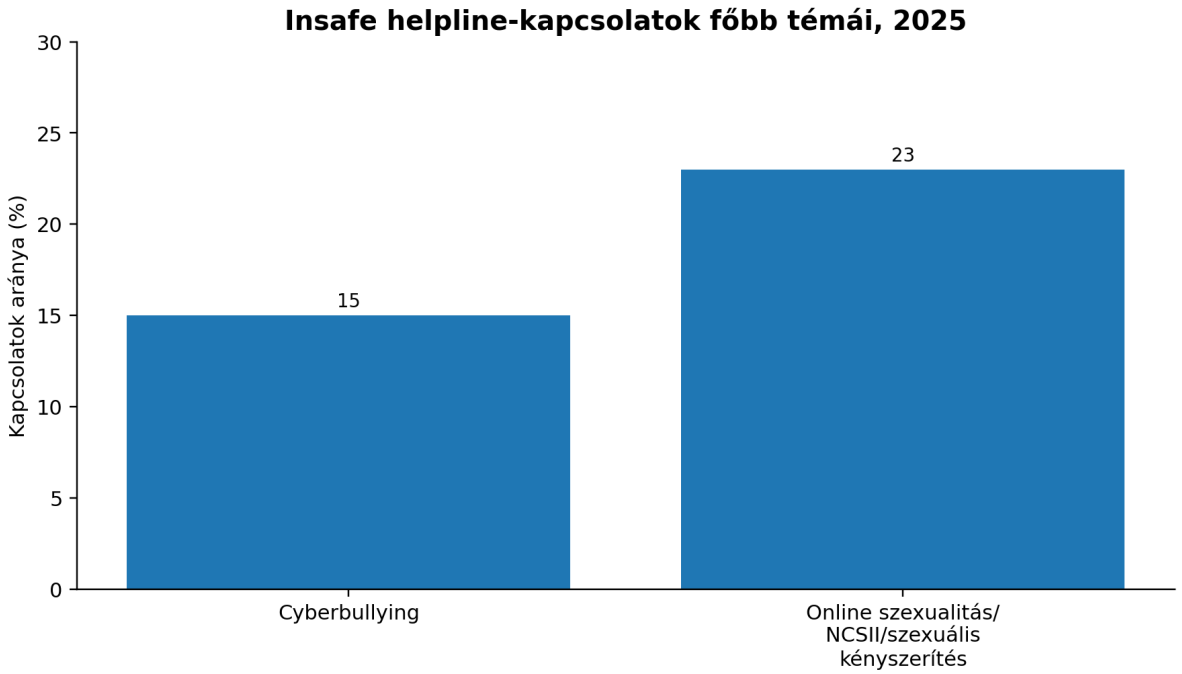
Az általános közösségimédia-használatról szóló umbrella review-k ennél heterogénebb képet mutatnak. Valkenburg, Meier és Beyens (2022) 25 áttekintést integráló elemzése szerint az átlagos összefüggések sokszor kicsik, miközben jelentős egyéni különbségek vannak. Ez azt indokolja, hogy a program a használat minőségét – például kényszeresség, éjszakai használat, konfliktus, társas összehasonlítás, káros tartalom – vizsgálja, ne pusztán az óraszámot.

5/5. Segítségkérés mint mérhető biztonsági kimenet

A Safer Internet Centre-ek európai Insafe helpline-hálózata 2025-ben több mint 57 000 kapcsolatot kezelt. A cyberbullying volt a leggyakrabban megjelenő önálló téma, a kapcsolatok 15%-ával; az online szerelem/szexualitás, a beleegyezés nélküli intimkép-megosztás és a

juvenis

gyermekek online szexuális kényszerítése és zsarolása együttesen mintegy 23%-ot tett ki. A kapcsolatok körülbelül 78%-a gyermekektől érkezett (Better Internet for Kids, 2026).



10. ábra. Az Insafe hálózat több mint 57 000 helpline-kapcsolatának kiemelt témái. A 23% összevont kategória. Forrás: Better Internet for Kids (2026).

A helpline-adat nem prevalenciabecslés: azt mutatja, milyen problémákkal kérnek segítséget azok, akik kapcsolatba lépnek a szolgálattal. Mégis fontos programtervezési jelzés, mert a segítségkérés tényleges mintázatát tükrözi. A CyberHősök hatásvizsgálatában ezért a „tudja-e, hová forduljon” és a „merne-e segítséget kérni” külön kimeneti változóként mérendő.

5/6. Statisztikai állítások publikációs protokollja

Kérdés	Kötelező elem a CyberHősök anyagban	Példa
Mit mér a szám?	Pontos konstrukció	„Legalább havonta felzaklatta valami online”
Kikre vonatkozik?	Életkor, ország/populáció	10–16 évesek, 19 európai ország
Mekkora a minta?	n, ha ismert	n = 28 465
Mikor mérték?	Adatfelvétel éve/időszaka	2025. április–2026. április
Milyen forrás?	Szerző–év + DOI/kiadó	Staksrud et al. (2026)
Mit nem jelent?	Oksági/prevalencia-korlát	Expozíció ≠ bizonyított pszichés kár

E protokoll különösen fontos a CyberHősök vizuális kommunikációjában. A látványos infografika szakmai kockázata, hogy a grafikai egyszerűsítés eltünteti a mérési kontextust. A megoldás nem a grafikonok elhagyása, hanem a rövid, szabványos forrás- és módszertani megjegyzés. A gyermekeknek szánt felületen ez rövidebb lehet; a háttértanulmányban minden ábra mögött teljes értelmezés szükséges.

6. Kockázati területek részletes szakirodalmi szintézise

6/1. Káros és életkornak nem megfelelő tartalmak

A tartalmi kockázatok közé nemcsak az erőszakos vagy szexuális tartalom tartozik, hanem az önsértést, szélsőséges testsúlycsökkentést, gyűlöletet vagy más veszélyes viselkedést normalizáló tartalom is. A 2026-os EU Kids Online adatok szerint a 19 országban vizsgált gyermekek 40%-a találkozott véres vagy erőszakos képekkel, 39% nagyon sovánnyá válással kapcsolatos, 37% pedig önsértéssel kapcsolatos tartalommal (Staksrud et al., 2026).

A kitettség és a kár elkülönítése itt is alapvető. Egy tartalom hatása függ a gyermek életkorától, előzetes állapotától, a megtekintés szándékosságától, ismétlődésétől és a társas kontextustól. A prevenció ezért nem épülhet kizárólag tartalomszűrésre; kritikai értelmezést, érzelmi önmonitorozást és segítségkérést is tanítani kell.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

6/2. Online gyűlölet és polarizáló tartalom

A 2026-os EU Kids Online vizsgálatban három gyermekből körülbelül egy legalább havonta találkozott gyűlöletkeltő üzenetekkel, országonként jelentős eltéréssel (Staksrud et al., 2026). A gyűlölettartalom egyszerre lehet content és conduct kockázat: a gyermek lehet szemlélő, célpont, továbbosztó vagy aktív résztvevő.

A programnak különbséget kell tennie sértő vélemény, célzott zaklatás és csoportidentitás alapján támadó gyűlölet között. A pedagógiai cél nem a politikai vagy társadalmi vélemények

homogenizálása, hanem az emberi méltóság, forráskritika, deeszkaláció és jelentési lehetőségek tanítása.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

6/3. Adatvédelem, célzott reklám és algoritmikus profilalkotás

A 2026-os EU Kids Online kutatásban a gyermekek fele aggódott amiatt, hogy személyes adatait célzott reklámozásra használják, négyből körülbelül egy helyett pedig négyből kettő attól tartott, hogy cégek beleegyezés nélkül osztják meg adatait harmadik felekkel; mindössze 30% bízott abban, hogy a vállalatok megfelelően védik a magánszféráját (Staksrud et al., 2026). Ezek az eredmények az adatvédelem kereskedelmi dimenzióját teszik láthatóvá.

Stoilova, Nandagiri és Livingstone (2021) evidence mappingje alapján a gyermekek interperszonális privacyval kapcsolatos tudása általában fejlettebb, mint az intézményi és kereskedelmi adatkezelés megértése. A CyberHősök adatvédelmi moduljának ezért a „ne add meg a címed” szintjéről tovább kell lépnie az adatnyomok, profilalkotás, algoritmikus következtetés és célzott reklám alaplogikájához.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

6/4. Generatív mesterséges intelligencia

A generatív AI 2026-ra a gyermekek digitális környezetének mindennapi részévé vált. Az EU Kids Online tematikus vizsgálata 25 592 gyermek kvantitatív adatait és 244 serdülő interjúját használta; a gyermekek főként oktatási, gyakorlati és kíváncsisági célokra használják az eszközöket, miközben pontossági, privacy- és készségvesztési aggályokat is megfogalmaznak (Staksrud et al., 2026).

A CyberHősök AI-moduljának minimumkompetenciái: az AI-válasz nem tekintélyforrás; érzékeny személyes adatot nem célszerű indokolatlanul megadni; generált kép, hang vagy videó lehet megtévesztő; az AI-val létrehozott megalázó vagy intim deepfake ugyanúgy súlyos károkat

okozhat; iskolai használatnál pedig a forrásellenőrzés és az intézményi szabályok betartása szükséges.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

6/5. Online szexuális megkeresés, sexting és sextortion

Madigan és munkatársai (2018) metaanalízise 31 mintában, 37 649 fiatal körében a nem kívánt online szexuális tartalommal való találkozást 20,3%-ra, kilenc mintában, 18 272 fiatal körében az online szexuális megkeresést 11,5%-ra becsülte. Ezek nem mai magyar prevalenciák; a tanulmány történeti és nemzetközi bizonyíték arra, hogy a jelenség populációs szinten is mérhető (Madigan et al., 2018).

A prevencióban el kell különíteni a konszenzuális kortárs sextinget, a nyomásgyakorlást, a beleegyezés nélküli továbbítást és a szexuális zsarolást. Az egy kategóriába mosás stigmatizálhatja a serdülőt és ronthatja a segítségkérést. A legfontosabb krízisüzenet: a zsaroló követelésének teljesítése nem garantálja a fenyegetés megszűnését; a gyermek ne maradjon egyedül, és felnőtt/szakmai segítséget kell bevonni.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

6/6. Online játék, közösségi funkciók és költési kockázatok

Az online játék nem kizárólag képernyőidő, hanem sok gyermek számára társas tér. A kockázatok ezért a játékon belüli kommunikációhoz, idegenekkel való kapcsolathoz, mikrotranzakciókhoz, lootbox-szerű mechanizmusokhoz, csalásokhoz és konfliktusokhoz is kapcsolódhatnak. A magyar NMHH adatok szerint a gyermekek online játéktevékenysége intenzívebb, mint a szülőké, ami növeli a generációs tudáskülönbség jelentőségét (NMHH, 2025).

A szülői programnak a játékot nem automatikusan problémaként, hanem megismerendő környezetként kell kezelnie. A jó kérdések: kikkel játszik a gyermek; van-e hangchat; lehet-e

pénzt költeni; milyen a jelentési rendszer; mi történik konfliktusnál; és mely adatok láthatók más játékosok számára.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

6/7. Digitális egyenlőtlenség

A digitális biztonságot gyakran eszközhozzáférési kérdésként tárgyalják, de az egyenlőtlenség a készségek, támogatás és használati lehetőségek szintjén is megjelenik. A 2026-os EU Kids Online eredmények a társadalmi-gazdasági háttér szerepét is hangsúlyozzák az online részvételben, biztonságérzetben és sérülékenységben (Staksrud et al., 2026).

Ez a CyberHősök implementációjában azt jelenti, hogy az otthoni technikai kontrollt feltételező ajánlás nem lehet az egyetlen védelem. Az iskola és a közösségi szolgáltatások szerepe különösen fontos azoknál a gyermekeknél, akik otthon kevesebb digitális támogatást kapnak.

Módszertani megjegyzés: az ebben az alfejezetben idézett arányok különböző kutatási tervekből származnak. A CyberHősök külső kommunikációjában csak azonos definíció és populáció mellett szabad közvetlen összehasonlítást végezni.

7. A CyberHősök kibővített szakmai modellje

A kibővített modell öt egymásra épülő szintet különít el: (1) digitális környezet és platformdesign; (2) gyermek egyéni fejlődési és pszichológiai sajátosságai; (3) családi és kortárs mediáció; (4) iskolai és intézményi válaszképesség; (5) társadalmi, szabályozási és szolgáltatói környezet. A program akkor tekinthető komplexnek, ha nem egyetlen szintre – például a gyermek „okosabb internethasználatára” – helyezi a felelősséget.

Szint	Kockázati példa	Védőfaktor	CyberHősök-beavatkozás
Platform	Ajánlórendszer, idegen kapcsolat, viralitás	Biztonságos alapbeállítás, jelentés	Platformlogika és biztonsági funkciók

Szint	Kockázati példa	Védőfaktor	CyberHősök-beavatkozás
Gyermek	Impulzív döntés, alacsony forráskritika	Digitális literacy, önhatékonyság	Szituációs készségtréning
Család	Büntető reakció, ritka beszélgetés	Aktív mediáció, bizalom	Szülői reakció- és kommunikációs modul
Iskola	Bizonytalan incidenskezelés	Eljárásrend, kijelölt felelős	Pedagógusprotokoll
Rendszer	Lassú eltávolítás, hiányos védelem	Helpline, hotline, hatóság, safety by design	Segítségkérési és eszkalációs térkép

A modell központi kimenete nem a „nulla online kockázat", mert ez reálisan nem elérhető és a digitális lehetőségek indokolatlan korlátozásához vezethet. A kívánt kimenet a kisebb káresemény, a gyorsabb felismerés, a kompetensebb reakció, a nagyobb segítségkérési hajlandóság és a biztonságosabb intézményi környezet.

A 2026-os európai adatok – különösen a 23%-os havi felzaklatottság, a 48%-os online biztonságérzet és a szülői beszélgetések 50%-os aránya – azt mutatják, hogy a gyermek egyéni készségeinek fejlesztése önmagában nem elegendő (Staksrud et al., 2026). A programnak ezért a szülő és pedagógus viselkedését ugyanúgy beavatkozási célként kell kezelnie, mint a gyermekét.

8. Tematikus evidence review: a CyberHősök program tudományos alappillérei

Ez a fejezet a program fő tématerületeit evidence review formában bontja tovább. Minden alfejezet három kérdésre válaszol: mit tudunk viszonylag stabilan a kutatásokból; hol vannak bizonytalanságok; és milyen programkövetkeztetés vonható le anélkül, hogy a bizonyíték erejét túlbecsülnénk. Ez a szerkezet a szakmai háttértanulmány és a későbbi kézikönyvek közötti átjárást biztosítja.

8/1. Kockázat és kár fogalmi szétválasztása

juvenis

Az online biztonságkutatás egyik legfontosabb elméleti különbsége a kockázat és a kár elválasztása. Az EU Kids Online kutatási kerete következetesen abból indul ki, hogy a kockázattal való találkozás nem szükségképpen eredményez negatív következményt. Ugyanaz az

aktivitás – például új emberrel való online kapcsolat – lehet fejlődési lehetőség és kockázati expozíció is. A 2020-as nemzetközi vizsgálatban az online felzaklató élmények aránya országonként jelentősen különbözött, miközben más online kockázatok ennél gyakrabban fordultak elő (Smahel et al., 2020).

A 2026-os adatok ezt a megközelítést még fontosabbá teszik. A káros tartalmaknak való kitettség magas, de ebből nem következik, hogy minden gyermek ugyanolyan mértékben sérül. A programnak ezért nem a veszélylista memorizálását kell céloznia, hanem annak felismerését, mikor nő meg a kár valószínűsége: ismétlődés, kényszerítés, személyes adat, izoláció, fenyegetés, szexuális tartalom, nyilvánosság vagy a gyermek erős distressze esetén (Staksrud et al., 2026).

Programkövetkeztetés: a CyberHősök minden témában külön jelölje a „találkozás", „kockázatos helyzet" és „káresemény" szintjét. Ez csökkenti a moralizálást és pontosabb incidenskezelést tesz lehetővé.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/2. Digitális készség és digitális sérülékenység

A gyermek technikai ügyessége könnyen keltheti azt a benyomást, hogy online biztonsági kompetenciája is magas. A digitális literacy szakirodalma azonban többdimenziós konstrukciót ír le: technikai, információs, kommunikációs, tartalomalkotási, kritikai és biztonsági készségek különülnek el (Tinmaz et al., 2022).

A 2026-os EU Kids Online eredményekben a technikai és kommunikációs készségek viszonylag erősek, miközben az információértékelés, algoritmusértés és tartalomalkotás kevésbé fejlett (Staksrud et al., 2026). Ez a „digitális bennszülött" mítosz egyik empirikus ellenérve: a gyakori használat nem automatikusan jelent kritikai műveltséget.

Programkövetkeztetés: a CyberHősök ne eszközkezelést tanítson, hanem bizonytalanságkezelést, forráskritikát, privacy-döntést és segítségkérési kompetenciát.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/3. Forráskritika és dezinformáció

A gyermekek online információs környezetében a tartalom hitelességének megítélése összetett feladat. A platformok vizuális egységessége miatt egy szakértői, reklám-, vélemény- és manipulált tartalom hasonló formában jelenhet meg. A generatív AI tovább növeli a valószerű, de pontatlan vagy teljesen hamis tartalom előállításának lehetőségét (Staksrud et al., 2026).

A forráskritikai oktatás nem korlátozódhat a „nézd meg, ki írta" szabályra. A gyermeknek meg kell tanulnia több forrás összevetését, az eredeti forrás keresését, a dátum és kontextus ellenőrzését, a túl erős érzelmi reakciót kiváltó tartalomnál a megállást, valamint annak felismerését, hogy a népszerűség nem bizonyíték.

Programkövetkeztetés: rövid, játékos fact-checking helyzetek kerüljenek a 11+ modulba, AI-generált és hagyományos példákkal egyaránt.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/4. Privacy literacy

Stoilova és munkatársai (2021) szisztematikus evidence mappingje azt mutatta, hogy a gyermekek privacy-tudása nem egységes. A közvetlen, interperszonális adatmegosztás könnyebben érthető, mint a háttérben zajló kereskedelmi adatgyűjtés és profilalkotás. A kvalitatív vizsgálatokban a gyermekek gyakran a „ki láthatja a posztomat" kérdésén keresztül értelmezik a privacyt (Stoilova et al., 2020).

A 2026-os EU Kids Online eredmények szerint a gyermekek fele aggódik a célzott reklámcélú adatfelhasználás miatt, és csak 30% bízik a vállalatok privacy-védelmében (Staksrud et al., 2026). Ez azt mutatja, hogy a kereskedelmi adatvédelem már a gyermekek saját aggodalmaiban is megjelenik.

Programkövetkeztetés: a „személyes adat" fogalmát ki kell bővíteni lokációval, metaadattal, böngészési mintával, eszközazonosítóval és kikövetkeztetett érdeklődési profillal.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/5. Jelszó- és fiókbiztonság

A fiókbiztonság az online gyermekvédelem technikai minimuma. A gyenge vagy újrahasznált jelszó, a kompromittált helyreállítási e-mail és a többfaktoros hitelesítés hiánya növeli a fiókátvétel kockázatát. A gyermek számára a technikai szabály akkor használható, ha kevés, konkrét és rendszeresen gyakorolható.

A fiókfeltörés gyakran társas kárral kombinálódik: az elkövető a gyermek nevében posztolhat, hozzáférhet privát beszélgetésekhez, képekhez vagy ismerősöket célozhat meg. Ezért a jelszóvédelem nem pusztán informatikai higiénia, hanem identitás- és kapcsolati védelem.

Programkövetkeztetés: minden korosztály kapjon életkorhoz illesztett „fiókmentő" forgatókönyvet: jelszócsere, aktív munkamenetek megszüntetése, 2FA, helyreállítási adatok ellenőrzése és megbízható felnőtt bevonása.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/6. Cyberbullying és offline bullying átfedése

A cyberbullying kutatása azt mutatja, hogy az online és offline bántalmazás nem két teljesen külön jelenség. Kowalski és munkatársai (2014) metaanalitikus áttekintése jelentős átfedést írt le a két forma között. A digitális környezet ugyanakkor sajátos affordanciákat ad: nagy közönség, állandó hozzáférés, tartósság, kereshetőség és részleges anonimitás.

Az EU-reprezentatív minták metaanalízisében a cybervictimizáció pooled prevalenciája 9,62%, az elkövetésé 11,91% volt, de a vizsgálatok közötti tartomány rendkívül széles (Henares-Montiel et al., 2022). Ez azt jelzi, hogy az iskolai esetkezelésnek nem egyetlen prevalenciaszámra, hanem világos definícióra és helyzetértékelésre kell épülnie.

Programkövetkeztetés: az iskolai modul kapcsolja össze az online és offline közösségi dinamikát, és külön tanítsa a szemlélők szerepét.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

juvenis

8/7. Szemlélői viselkedés

A digitális bántalmazás társas természetét jól mutatja, hogy a közönség reakciója a folyamat részévé válik. A továbbosztás, komment, emoji vagy akár a csoportos hallgatás is befolyásolhatja az áldozat megélését és az elkövető társas jutalmát. A cyberbystanding aránya az EU-reprezentatív vizsgálatokban 13,0–53,1% között mozgott (Henares-Montiel et al., 2022).

A szemlélői intervenció előnye, hogy nem kizárólag az áldozatra helyezi a cselekvési felelősséget. Ugyanakkor a gyermek biztonsága elsődleges: nem minden helyzetben indokolt közvetlenül konfrontálni az elkövetőt.

Programkövetkeztetés: tanítsunk többféle proszociális választ – nem továbbítani, privát támogatást adni, jelenteni, felnőttet bevonni – és különítsük el a biztonságos és kockázatos beavatkozást.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/8. Grooming és manipuláció

A grooming nem egyetlen üzenet, hanem adaptív kapcsolati folyamat. Ringenberg és munkatársai (2022) 93 tanulmányt összegző scoping review-ja bizalomépítést, kockázatfelmérést, izolációt, szexualizációt, titoktartást, megtévesztést és kényszerítést azonosított visszatérő stratégiaként.

Porcelli, Anderson és Kloess (2026) természetes környezetből származó adatokra épülő szisztematikus áttekintése tovább hangsúlyozta az elkövetői stratégiák individualizált és változó jellegét. Ezért szakmailag hibás lenne egy merev „öt lépéses grooming-receptet” tényként tanítani.

Programkövetkeztetés: a gyermek viselkedési vörös zászlókat tanuljon – titok, izoláció, gyors intimitás, határtesztelés, szexuális kérés, zsarolás –, ne profilképből próbálja felismerni az elkövetőt.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

juvenis

8/9. Online szexuális megkeresés

Madigan és munkatársai (2018) metaanalízise a nem kívánt online szexuális tartalommal való találkozás és megkeresés populációs jelentőségét mutatta meg. A becslések történeti jellegűek és különböző országokból származnak, ezért mai magyar prevalenciaként nem használhatók.

A kutatási kategóriák közötti különbség kulcsfontosságú: nem kívánt expozíció, nem kívánt megkeresés, beleegyezés nélküli képkészítés/megosztás, grooming és sextortion eltérő mechanizmusokat és válaszokat igényel.

Programkövetkeztetés: a szülői segédletben külön incidensút legyen szexuális tartalommal kapcsolatos zsarolásra, és első lépésként hibáztatásmentes segítségnyújtást írjon elő.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/10. Sexting és beleegyezés

A sexting szakirodalma módszertanilag érzékeny, mert a kutatások nem mindig választják külön a konszenzuális kortárs kommunikációt és a kényszerített vagy beleegyezés nélküli terjesztést. Benjamin és munkatársai (2026) szisztematikus áttekintése a jelenség serdülőkori szexuális viselkedéssel való kapcsolatát vizsgálta.

Gyermekvédelmi szempontból a legfontosabb határ a beleegyezés és a kényszerítés. A „soha ne küldj képet” üzenet önmagában nem készíti fel a gyermeket arra, mit tegyen, ha nyomást gyakorolnak rá, ha már elküldte, vagy ha más képét kapta meg.

Programkövetkeztetés: a prevenció tartalmazza a nemet mondás, tovább nem küldés, segítségkérés és zsarolásra adott válasz gyakorlását.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

juvenis

8/11. Közösségimédia-használat és depresszív tünetek

A közösségi média és mentális egészség kapcsolata heterogén. Az általános használati idő és a depresszív tünetek közötti átlagos összefüggések sok review-ban kicsik, és jelentős személyek közötti eltérést mutatnak (Valkenburg et al., 2022).

A problémás használat erősebb jelző. Shannon és munkatársai (2022) metaanalízisében a problémás használat depresszióval r = .273 korrelációt mutatott. Ez mérsékelt kapcsolat, nem oksági bizonyíték.

Programkövetkeztetés: a szülői modul a működésromlásra, kontrollvesztésre, alvásra, konfliktusokra és érzelmi következményekre kérdezzen rá, ne egyetlen „megengedett óraszámot" kezeljen diagnosztikai határként.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/12. Szorongás, stressz és problémás használat

Ugyanebben a metaanalízisben a problémás közösségimédia-használat szorongással r = .348, stresszel r = .313 összefüggést mutatott (Shannon et al., 2022). A három mutató közül a szorongással való korreláció volt a legerősebb, de továbbra is mérsékelt nagyságú.

A kapcsolat több mechanizmuson keresztül jöhet létre: társas összehasonlítás, FOMO, konfliktus, visszajelzéskeresés, alvászavar, illetve fordított irányban a szorongó gyermek fokozott online kapcsolódáskeresése.

Programkövetkeztetés: a pszichés tünetek és a médiahasználat kapcsolatát kétirányú kérdezéssel kell feltárni; kerülendő az automatikus oksági magyarázat.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/13. Alvás és esti digitális rutin

juvenis

Az alvás a digitális jóllét egyik legjobban operacionalizálható területe. Az eszközhasználat későbbi lefekvéssel, rövidebb alvással és rosszabb alvásminőséggel

kapcsolódhat össze, különösen problémás használati mintázatok mellett. A nagy áttekintések ugyanakkor heterogén mérési módszereket egyesítenek.

Az alvást több mechanizmus érintheti: időbeli kiszorítás, értesítések, érzelmileg aktiváló tartalom és a lefekvési rutin felbomlása. Ezek közül több közvetlenül módosítható családi szokásokkal.

Programkövetkeztetés: az esti értesítések, töltési hely és lefekvés előtti rutin legyen konkrét családi tervezési feladat, ne általános „kevesebb telefon” felszólítás.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/14. Szülői mediáció

A szülői mediáció többféle stratégiát foglal magában: aktív beszélgetés, közös használat, szabályalkotás, technikai kontroll és monitorozás. Sevilla-Fernández és munkatársai (2025) 32 tanulmány szisztematikus áttekintésében vizsgálták e stratégiák kapcsolatát a közösségimédia-használattal és kockázatokkal.

A magyar NMHH kutatás azt mutatja, hogy a családok többféle stratégiát kombinálnak. Ez fontos, mert a „szigorú vagy engedékeny” dichotómia túl egyszerű. A megfelelő stratégia függ a gyermek életkorától, a konkrét kockázattól és a kapcsolat minőségétől (NMHH, 2025).

Programkövetkeztetés: a szülői tréning ne egyetlen univerzális kontrollmódszert írjon elő, hanem döntési mátrixot adjon életkor és kockázat szerint.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/15. Szülői modellnyújtás

A szülő nemcsak szabályozó, hanem modell. Morawska és munkatársai (2026) áttekintésében a modellnyújtás, kommunikáció, monitorozás és határszabás visszatérő szülői tényezőként jelent meg.

juvenis

A parental phubbing kutatása arra utal, hogy a szülő saját telefonhasználata kapcsolatban állhat a gyermek szocioemocionális alkalmazkodásával, bár az evidencia jelentős része keresztmetszeti és kulturálisan koncentrált (Zhang et al., 2023).

Programkövetkeztetés: a családi digitális megállapodás tartalmazzon legalább egy, a felnőttekre is érvényes szabályt.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/16. Iskolai programok hatásossága

Polanin és munkatársai (2022) 50 vizsgálatot és 45 371 résztvevőt összegző metaanalízise szerint az iskolai cyberbullying-programok összességében képesek csökkenteni az elkövetést és áldozattá válást, de a programok heterogének.

Shi és munkatársai (2025) 44 randomizált kontrollált vizsgálat, 65 707 résztvevő adatai alapján kis, de szignifikáns hatásokat találtak. Az evidencia bizonyosságát ugyanakkor alacsonynak vagy nagyon alacsonynak értékelték.

Programkövetkeztetés: a CyberHősök ne állítsa előzetesen, hogy „bizonyítottan csökkenti a cyberbullyingot”. A korrekt megfogalmazás: evidenciaalapú komponensekre épül, saját hatásosságát pilot- és kontrollált vizsgálatokban kell tesztelni.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/17. Programdózis és ismétlés

A prevenciós programoknál a dózis nem egyszerűen az óraszám. Fontos az alkalmak száma, az ismétlés, a gyakorlás, a szülői és pedagógusi komponens, valamint az utánkövetés. A cyberbullying-intervenciók újabb metaanalízisében a hosszabb, legalább ötórás programok kedvezőbbnek tűntek (Shi et al., 2025).

Ez nem jelenti azt, hogy minden ötórás program hatékony, vagy hogy öt óra küszöbérték. Inkább arra utal, hogy egyetlen 45 perces előadás valószínűleg kevés a tartós készségváltozáshoz.

juvenis

Programkövetkeztetés: a CyberHősök alapprogram több alkalomból álljon, és 4–8 hetes booster vagy utánkövető elemet tartalmazzon.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/18. Segítségkérés és disclosure

A gyermekek biztonsága nagymértékben függ attól, hogy elmondják-e a problémát. A 2026-os európai eredmények szerint az online felzaklató élményt átélők egy része senkivel nem beszélt róla; a szülői beszélgetések gyakorisága pedig alacsonyabb, mint a korábbi hullámban (Staksrud et al., 2026).

A disclosure valószínűségét befolyásolja a szégyen, a büntetéstől vagy eszközelvételtől való félelem, az a feltételezés, hogy a felnőtt nem érti a platformot, illetve az elkövető fenyegetése. A programnak ezeket a gátakat explicit módon kell kezelnie.

Programkövetkeztetés: minden gyermekmodul végén legyen konkrét segítségkérési próba, minden szülői modulban pedig „első 60 másodperc” reakciógyakorlat.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/19. Generatív AI és deepfake

A generatív AI új kockázatokat hoz a hitelesség, privacy és identitásvédelem területén. A 2026-os EU Kids Online tematikus vizsgálat szerint a GenAI használata gyorsan beépül a gyermekek mindennapi digitális rutinjába (Staksrud et al., 2026).

A deepfake különösen érzékeny gyermekvédelmi probléma, mert megalázó, szexuális vagy megtévesztő tartalom létrehozásához nincs szükség arra, hogy az áldozat eredetileg ilyen képet készítsen. Ez átalakítja a hagyományos „ne küldj intim képet” prevenció korlátait.

Programkövetkeztetés: az AI-modulban külön jelenjen meg a generált tartalom jelzéseinek kritikája, a beleegyezés, az identitás-visszaélés és a deepfake incidenskezelése.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

8/20. Safety by design és a gyermek felelősségének határa

A gyermekvédelmi oktatás könnyen azt az üzenetet közvetíti, hogy a gyermeknek kell „elég okosnak” lennie a veszélyek elkerüléséhez. A 2026-os európai szakpolitikai és kutatási irány egyre inkább a safety by design megközelítést hangsúlyozza: a platformoknak alapértelmezetten biztonságosabb környezetet kell kialakítaniuk, nem kizárólag a felhasználóra hárítani a kockázatkezelést.

A gyermek készsége továbbra is fontos, de nem helyettesíti a megfelelő alapbeállítást, jelentési rendszert, moderációt, életkori tervezést és jogi védelmet. A CyberHősök szakmai hitelességéhez ezért rendszerszintű fejezet is szükséges.

Programkövetkeztetés: a program záró üzenete ne az legyen, hogy „védd meg magad”, hanem hogy „ismerd fel, cselekedj, kérj segítséget – és a felnőtteknek, intézményeknek és szolgáltatóknak is felelősségük van”.

Evidenciaértelmezési megjegyzés: a fejezetben szereplő összefüggések erősségét a kutatási terv határozza meg; a keresztmetszeti együttjárást nem kezeljük oksági bizonyítékként.

9. CyberHősök szakmai indikátorkészlet és kutatási adattár

A program hosszú távú szakmai fejlesztéséhez célszerű állandó indikátorkészletet létrehozni. Ennek célja nem az, hogy évente újabb és újabb „ijesztő számokat” gyűjtsön, hanem hogy ugyanazon konstrukciók változását követhetővé tegye. Az indikátorok három szintre bonthatók: környezeti expozíció, gyermekkompetencia és válaszrendszer.

Indikátorcsoport	Mutató	Javasolt forrás	Frissítés
Digitális jelenlét	Napi online média, közösségi média, saját eszköz	NMHH Digital parenting	Új hullámonként
Európai kockázat	Felzaklató élmény, káros tartalom, biztonságérzet	EU Kids Online	Új hullámonként
Cyberbullying	Áldozat, elkövető, szemlélő	Reprezentatív survey + metaanalízis	2–3 évente review
Mentális jóllét	Problémás használat kapcsolata tünetekkel	Metaanalízisek	Évente irodalmi frissítés
Szülői mediáció	Aktív beszélgetés, kontroll, monitorozás	NMHH + review	Új hullámonként

iuvenis

Indikátorcsoport	Mutató	Javasolt forrás	Frissítés
Segítségkérés	Helpline-témák, disclosure	Insafe / hazai szolgáltatások	Évente
AI	Használat, privacy, hitelesség	EU Kids Online / új review-k	Évente

Minden indikátorhoz metaadatlap tartozzon: definíció, kérdés pontos szövege, korcsoport, minta, adatfelvétel ideje, földrajzi hatókör, súlyozás, bizonytalanság és forrás. Így elkerülhető, hogy egy későbbi kommunikációs anyag azonos címkével eltérő konstrukciókat hasonlítson össze.

A CyberHősök honlapján a nyilvános statisztikai állításokhoz rövid forrásjegyzet, a háttértanulmányban pedig teljes APA 7 hivatkozás javasolt. A grafikonok saját újrarajzolása megengedhető, ha az adatforrás egyértelműen meg van nevezve, a számok változtatás nélkül kerülnek át, és a forrás felhasználási feltételeit betartják.

10. Annotált szakirodalmi áttekintés – kulcsforrások és felhasználhatóságuk

Smahel et al. (2020) – EU Kids Online 2020

A 19 ország 25 101, 9–16 éves gyermekének adataira épülő összehasonlító jelentés a hozzáférés, gyakorlatok, készségek, kockázatok, lehetőségek és társas kontextus közös modelljét használja. A CyberHősök számára elsősorban elméleti keretként és országok közötti összehasonlításként fontos. DOI: 10.21953/lse.47fdeqj01ofo.

Forráskritikai értékelés. Erősség: nagy, nemzetközi, összehasonlítható minta és dokumentált módszertan. Korlát: a nemzeti minták és egyes kérdésblokkok eltérései miatt a százalékok mechanikus rangsorolása kerülendő.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

juvenis

Staksrud et al. (2026) – EU Kids Online 2026

A legfrissebb összehasonlító hullám 28 465, 10–16 éves gyermeket vizsgált 19 országban. A klasszikus online kockázatok mellett AI-használatot, algoritmusértést, privacy-aggodalmakat és káros tartalmakat is mér. DOI: 10.21953/researchonline.lse.ac.uk.00140901.

Forráskritikai értékelés. Erősség: friss, reprezentatív, közös európai keret. Korlát: a 2020-as hullámmal közölt trendeket a kérdezés és korcsoport esetleges eltéréseinek figyelembevételével kell értelmezni.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

NMHH Digital parenting (2025)

A 2000 magyar gyermek és 2000 szülő országosan reprezentatív adatfelvétele a CyberHősök legfontosabb hazai kontextusforrása. A médiahasználat, saját eszköz, közösségi média, szülői tudás és mediáció egyaránt megjelenik.

Forráskritikai értékelés. Erősség: hazai, nagymintás és korábbi hullámokkal összevethető. Korlát: intézményi kutatási jelentés, nem lektorált folyóiratcikk; az egyes indikátorok kérdésszövegét a kommunikáció előtt ellenőrizni kell.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Henares-Montiel et al. (2022)

EU-tagállamok reprezentatív populációs mintáit összegző cyberbullying szisztematikus review és metaanalízis. A pooled cybervictimizáció 9,62%, a cyberelkövetés 11,91%, miközben az egyes vizsgálatok becslései széles tartományban mozognak. DOI: 10.3390/ijerph19127364.

Forráskritikai értékelés. Erősség: reprezentatív mintákra szűkített metaanalízis. Korlát: jelentős heterogenitás; a pooled érték nem tekinthető minden ország aktuális prevalenciájának.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Kowalski et al. (2014)

A cyberbullying kutatás klasszikus kritikai áttekintése és metaanalízise, amely az online és offline bullying átfedését, prediktorait és következményeit rendszerezi. DOI: 10.1037/a0035618.

Forráskritikai értékelés. Erősség: alapvető fogalmi és empirikus szintézis. Korlát: a platformkörnyezet 2014 óta jelentősen változott, ezért prevalencia- vagy platformspecifikus állításokhoz frissebb forrás szükséges.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Polanin et al. (2022)

Az iskolai cyberbullying-intervenciók metaanalízise 50 vizsgálat és 45 371 résztvevő alapján. A programok összességében kedvező hatást mutatnak az elkövetés és áldozattá válás terén.

Forráskritikai értékelés. Erősség: nagy intervenciós evidenciahalmaz. Korlát: a programok és kimenetek heterogenitása miatt nem következik belőle, hogy bármely edukációs program automatikusan hatékony.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Shi et al. (2025)

juvenis

Negyvennégy randomizált kontrollált vizsgálat, 65 707 résztvevő metaanalízise. Kis, szignifikáns hatásokat jelez, de az evidencia bizonyossága alacsony vagy nagyon alacsony. DOI: 10.1177/15248380251375480.

Forráskritikai értékelés. Erősség: randomizált vizsgálatokra fókuszál. Korlát: alacsony bizonyosság, heterogén programok. A CyberHősök saját hatásvizsgálatának szükségességét támasztja alá.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Shannon et al. (2022)

A problémás közösségimédia-használat depresszióval, szorongással és stresszel való kapcsolatát vizsgáló metaanalízis 18 tanulmány, 9269 résztvevő alapján. DOI: 10.2196/33450.

Forráskritikai értékelés. Erősség: effektusnagyságokat közöl. Korlát: az alapvizsgálatok jelentős része megfigyeléses; korrelációból okság nem következik.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Valkenburg et al. (2022)

Huszonöt áttekintést integráló umbrella review a közösségi média és serdülőkori mentális egészség kapcsolatáról. DOI: 10.1016/j.copsyc.2021.08.017.

Forráskritikai értékelés. Erősség: magas szintű szintézis, amely jól mutatja az átlagosan kicsi és heterogén összefüggéseket. Korlát: az umbrella review az alatta lévő review-k módszertani korlátait is örökli.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Stoilova et al. (2021)

A gyermekek személyesadat- és privacy-tudását feltérképező szisztematikus evidence mapping. DOI: 10.1080/1369118X.2019.1657164.

juvenis

Forráskritikai értékelés. Erősség: a privacy literacy több dimenzióját különíti el. Korlát: a technológiai és szabályozási környezet gyors változása miatt folyamatos frissítést igényel.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Stoilova et al. (2020)

Kvalitatív vizsgálat 169, 11–16 éves gyermekkel arról, hogyan értik és kezelik az online adatokat és privacyt. DOI: 10.17645/mac.v8i4.3407.

Forráskritikai értékelés. Erősség: részletesen feltárja a gyermekek gondolkodását. Korlát: kvalitatív kutatás, ezért nem prevalenciabecslés.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Ringenberg et al. (2022)

Kilencvenhárom tanulmány scoping review-ja a grooming stratégiáiról az internet előtti és utáni korszakban. DOI: 10.1016/j.chiabu.2021.105392.

Forráskritikai értékelés. Erősség: széles stratégiatérkép. Korlát: a scoping review célja a terület feltérképezése, nem egyetlen oksági modell bizonyítása.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Porcelli et al. (2026)

Friss szisztematikus review az online grooming és technológia által támogatott gyermek-szexuális visszaélések elkövetői stratégiáiról. DOI: 10.1177/15248380251411261.

Forráskritikai értékelés. Erősség: valós, természetes környezetből származó adatok hangsúlya. Korlát: az elkövetői stratégiák heterogének; nem alakíthatók merev lépéssorrá.

iuventis

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Madigan et al. (2018)

A nem kívánt online szexuális expozíció és megkeresés metaanalízise. DOI: 10.1016/j.jadohealth.2018.03.012.

Forráskritikai értékelés. Erősség: nagy összesített minta és világos kategóriák. Korlát: a digitális környezet gyors változása miatt prevalenciaadatai történeti kontextusban kezelendők.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Sevilla-Fernández et al. (2025)

A szülői mediáció és közösségimédia-használat kapcsolatának PRISMA-alapú szisztematikus áttekintése 32 tanulmánnyal. DOI: 10.1371/journal.pone.0312011.

Forráskritikai értékelés. Erősség: friss szintézis a szülői stratégiákról. Korlát: a mediáció definíciója és mérőeszközei vizsgálatonként eltérhetnek.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Morawska et al. (2026)

A serdülők közösségimédia-használatához kapcsolódó szülői tényezők szisztematikus áttekintése. DOI: 10.1002/jad.70062.

Forráskritikai értékelés. Erősség: a modellnyújtás, kommunikáció, monitorozás és határszabás együttes értelmezése. Korlát: az ok-okozati irány több vizsgálatban nem dönthető el.

iuvenis

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Wang & Jiang (2023)

Szülőkhöz kapcsolódó cyberbullying-intervenciók szisztematikus review-ja és metaanalízise. DOI: 10.1177/15248380221137065.

Forráskritikai értékelés. Erősség: a szülői komponens intervenciós jelentőségét vizsgálja. Korlát: programheterogenitás és eltérő mérési pontok.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Tinmaz et al. (2022)

A digitális literacy fogalmának szisztematikus áttekintése. DOI: 10.1186/s40561-022-00204-y.

Forráskritikai értékelés. Erősség: többdimenziós kompetenciamodell. Korlát: nem gyermekvédelmi intervenciós review, ezért közvetett alapot ad.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

UNICEF Innocenti (2025)

Globális összefoglaló a képernyőidőről, digitális készségekről és mentális egészségről, EU Kids Online és Disrupting Harm adatokkal.

Forráskritikai értékelés. Erősség: széles nemzetközi perspektíva és óvatos képernyőidő-értelmezés. Korlát: intézményi jelentés, több eltérő adatforrás szintézise.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

Better Internet for Kids (2026)

Az Insafe/Safer Internet Centre hálózat 2025-ös működési adatai több mint 57 000 helpline-kapcsolatról adnak gyakorlati képet.

Forráskritikai értékelés. Erősség: valós segítségkérési adatok. Korlát: szolgáltatáshasználati statisztika, nem populációs prevalencia.

CyberHősök-felhasználás. A forrás a háttértanulmányban közvetlen tudományos vagy intézményi alapként használható; a gyermekeknek szóló kommunikációban csak a korosztályhoz igazított, módszertanilag pontosan visszavezethető állítás emelhető át.

11. Fogalmi és módszertani szótár

Aktív szülői mediáció

A gyermek digitális tevékenységének beszélgetéssel, magyarázattal és közös értelmezéssel történő támogatása.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Algoritmikus ajánlás

Olyan automatizált tartalomrendezés, amely felhasználói és tartalmi jelek alapján választja ki, mit mutat a rendszer.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

juvenis

Asszociáció

Két változó statisztikai együttjárása; önmagában nem bizonyít oksági kapcsolatot.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Bystander

Olyan személy, aki bántalmazó esemény szemlélője vagy közönsége, de nem elsődleges áldozat vagy elkövető.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Cyberbullying

Digitális eszközökkel megvalósuló bántalmazás; definíciója kutatásonként eltérhet az ismétlődés, szándékosság és erőaszimmetria tekintetében.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Cybervictimizáció

Online bántalmazás áldozataként megélt tapasztalat.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

juvenis

Digitális lábnyom

A digitális tevékenység során közölt, megfigyelt vagy kikövetkeztetett adatok összessége.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Digitális literacy

Technikai, információs, kritikai, kommunikációs és biztonsági kompetenciák összessége.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Doxxing

Személyes vagy azonosító adatok beleegyezés nélküli nyilvánosságra hozatala.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Effect size

A vizsgált különbség vagy kapcsolat nagyságának statisztikai mutatója.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Expozíció

Egy tartalommal, személlyel vagy kockázati helyzettel való találkozás; nem azonos a kárral.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

juvenis

Fidelitás

Annak mértéke, hogy egy intervenciót mennyire a tervezett módon valósítottak meg.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Grooming

Kapcsolati és manipulációs folyamat, amelyben az elkövető bizalmat épít és határokat lép át kizsákmányolás céljából.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Impersonation

Más személy identitásának online utánzása vagy jogosulatlan használata.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Incidencia

Új esetek előfordulása egy meghatározott időszakban és populációban.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Káresemény

Olyan online tapasztalat, amely tényleges negatív következménnyel jár a gyermek számára.

juvenis

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Korreláció

Két változó lineáris együttjárásának mutatója; az r értéke -1 és +1 között mozog.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Metaanalízis

Több empirikus vizsgálat eredményeinek statisztikai összegzése.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

NCSII

Non-consensual sharing of intimate images; intim képek beleegyezés nélküli megosztása.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Parental phubbing

A gyermekkel való interakció megszakítása vagy háttérbe szorítása a szülő telefonhasználata miatt.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

juvenis

Prevalencia

Egy jelenség előfordulási aránya meghatározott populációban és időkeretben.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Privacy literacy

A személyes adatok, adatáramlás, láthatóság és adatkezelési kockázatok megértésének és kezelésének képessége.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Problémás közösségimédia-használat

Kontrollvesztéssel, konfliktussal vagy működésromlással jellemzett használati mintázat; nem azonos a gyakori használattal.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Protektív faktor

Olyan tényező, amely csökkenti a káros kimenet valószínűségét vagy mérsékli annak hatását.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

juvenis

Randomizált kontrollált vizsgálat

Olyan kísérleti elrendezés, amelyben a résztvevőket vagy klasztereket véletlenszerűen osztják intervenciós és kontrollfeltételbe.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Reziliencia

A káros helyzetekkel való adaptív megküzdés rendszerszintű képessége; nem jelent sérthetetlenséget.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Safety by design

Olyan tervezési elv, amely a biztonságot a szolgáltatás alaparchitektúrájába és alapbeállításaiba építi.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Sextortion

Szexuális tartalommal, képpel vagy információval történő zsarolás.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

juvenis

Sharenting

A gyermekről szóló információk, képek vagy videók szülő általi online megosztása.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Szisztematikus áttekintés

Előre meghatározott keresési és beválasztási módszerrel készült szakirodalmi szintézis.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Vignetta

Rövid, standardizált helyzetleírás, amely döntési vagy attitűdkérdés alapjául szolgál.

CyberHősök-módszertani használat: a fogalmat a szakmai dokumentumokban következetesen ebben az értelemben célszerű használni; gyermekeknek szóló anyagban egyszerűbb, életkorhoz illesztett magyarázat szükséges.

Evidenciaszint	Tipikus forrás	Erősség	Fő korlát
1	Szisztematikus review / metaanalízis	Több vizsgálat szintézise; heterogenitás becslése	A bevont vizsgálatok minőségét örökli
2	Randomizált / kvázi-kísérleti vizsgálat	Erősebb oksági következtetés	Implementáció és általánosíthatóság
3	Longitudinális kohorsz	Időbeli sorrend vizsgálható	Reziduális konfúzió
4	Reprezentatív keresztmetszeti felmérés	Jó populációs becslés	Okság nem állapítható meg
5	Kvalitatív vizsgálat	Mechanizmusok és jelentések mély megértése	Nem prevalenciabecslés
6	Intézményi szakmai jelentés	Gyakorlati és szabályozási relevancia	Nem mindig lektorált

Jelenség	Jellemző	Elsődleges válasz
Egyszeri online konfliktus	Kölcsönös vita, nincs tartós erőfölény	Deeszkaláció, kommunikáció, szabályok

Juvenis

Evidenciaszint	Tipikus forrás	Erősség	Fő korlát
Cyberbullying	Ismétlődő/terjedő bántalmazás, erőaszimmetria	Védelem, dokumentálás, intézményi beavatkozás	
Doxxing	Személyes adat nyilvánosságra hozása	Adatvédelem, eltávolítás/jelentés, kockázatértékelés	
Impersonation	Más nevében létrehozott/használt profil	Fiókvédelem, platformjelentés, bizonyítékmegőrzés	
Kiközösítés	Csoportból szándékos kizárás, megalázás	Közösségi norma és támogató kapcsolat	
Folyamatelem	**Lehetséges jel**	**Pedagógiai üzenet**	
Kapcsolatfelvétel	Gyors, intenzív érdeklődés	Az online identitás ellenőrzése korlátozott	
Bizalomépítés	Különlegesség, ajándék, állandó figyelem	A kedvesség nem kötelez viszonzásra	
Izoláció	„Ezt ne mondd el senkinek”	A titoktartási nyomás figyelmeztető jel	
Határtesztelés	Személyes/intim kérdések fokozása	Bármikor lehet nemet mondani	
Eszkaláció	Kép, videó, találkozó kérése	Megállás, segítségkérés, bizonyítékmegőrzés	
Kényszerítés	Fenyegetés, zsarolás	Nem a gyermek felelőssége egyedül megoldani	
Lépés	**Kérdés**	**Teendő**	
1. Biztonság	Van közvetlen veszély?	Sürgős segítség / hatóság szükség szerint	
2. Kapcsolat	El meri mondani a gyermek?	Nyugodt, hibáztatásmentes meghallgatás	
3. Dokumentálás	Mi őrizhető meg jogszerűen?	Felhasználónév, időpont, üzenet, URL	
4. Technika	Fiók vagy adat veszélyben?	Jelszócsere, 2FA, munkamenetek, privacy	
5. Platform	Jelenthető/blokkolható?	Jelentés, tiltás, eltávolítás kérése	
6. Intézmény	Érintett az iskola?	Kijelölt kapcsolattartó, dokumentált ügykezelés	
7. Utánkövetés	Maradt pszichés hatás?	Beszélgetés, szükség esetén szakember	
Célcsoport	**Minimum programkomponens**	**Mérhető kimenet**	
Gyermek	Helyzetgyakorlat + segítségkérés + privacy	Tudás, önhatékonyság, döntési pontosság	
Szülő	Aktív mediáció + családi szabály + krízisreakció	Kommunikációs önhatékonyság, szabályok minősége	
Pedagógus	Bejelentésfogadás + eszkaláció + dokumentálás	Protokollismeret, reakcióbiztonság	
Intézmény	Eljárásrend + kijelölt felelős + utánkövetés	Válaszidő, esetkezelési teljesség	
Programgazda	Forrásellenőrzés + pilot + hatásmérés	Adatminőség, pre–post változás, utánkövetés	

juvenis

Felhasznált szakirodalom

Ahmed, O., Walsh, E. I., Dawel, A., Alateeq, K., Espinoza Oyarce, D. A., & Cherbuin, N. (2024). Social media use, mental health and sleep: A systematic review with meta-analyses. Journal of Affective Disorders, 367, 701–712.https://doi.org/10.1016/j.jad.2024.08.193

Akay, O. (2026). Children's privacy, autonomy, and digital identity in sharenting research: A scoping review with bibliometric mapping. Frontiers in Psychology, 17, 1845715.https://doi.org/10.3389/fpsyg.2026.1845715

Benjamin, T. N. E., Saengsri, W., Lin, W.-H., Huang, S.-L., & Waits, A. (2026). Associations between sexting and sexual behaviours in adolescents: A systematic review and meta-analysis. Journal of Adolescence, 98(3), 678–697.https://doi.org/10.1002/jad.70101

Better Internet for Kids. (2026). Better Internet for Kids: Review of the year 2025. European Commission / European Schoolnet.https://better-internet-for-kids.europa.eu/en/about/bik-annual-reports

Henares-Montiel, J., Benítez-Hidalgo, V., Ruiz-Pérez, I., Pastor-Moreno, G., & Rodríguez-Barranco, M. (2022). Cyberbullying and associated factors in member countries of the European Union: A systematic review and meta-analysis of studies with representative population samples. International Journal of Environmental Research and Public Health, 19(12), 7364.https://doi.org/10.3390/ijerph19127364

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137.https://doi.org/10.1037/a0035618

Lee, J., Choo, H., Zhang, Y., Cheung, H. S., Zhang, Q., & Ang, R. P. (2026). Cyberbullying victimization and mental health symptoms among children and adolescents: A meta-analysis of longitudinal studies. Trauma, Violence, & Abuse, 27(2), 391–406.https://doi.org/10.1177/15248380241313051

Li, C., Wang, P., Martin-Moratinos, M., Bella-Fernández, M., & Blasco-Fontecilla, H. (2024). Traditional bullying and cyberbullying in the digital age and its associated mental health problems in children and adolescents: A meta-analysis. European Child & Adolescent Psychiatry, 33(9), 2895–2909.https://doi.org/10.1007/s00787-022-02128-x

juvenis

Madigan, S., Villani, V., Azzopardi, C., Laut, D., Smith, T., Temple, J. R., Browne, D., & Dimitropoulos, G. (2018). The prevalence of unwanted online sexual exposure and solicitation among youth: A meta-analysis. Journal of Adolescent Health, 63(2), 133–141.https://doi.org/10.1016/j.jadohealth.2018.03.012

Morawska, A., Adina, J., Khan, A., & Turner, K. M. T. (2026). Parental factors associated with social media use in adolescence: A systematic review. Journal of Adolescence, 98(1), 51–68.https://doi.org/10.1002/jad.70062

Nemzeti Média- és Hírközlési Hatóság. (2025). Digital parenting-kutatás 7–16 éves gyermekekkel és szüleikkel III. rész – 2025 (teljes kutatás).https://nmhh.hu/cikk/256682/Digital_parentingkutatas_716_eves_gyermekekkel_es_szuleikkel_III_resz__2025_teljes_kutatas

Nemzeti Média- és Hírközlési Hatóság. (2025). Médiapiaci Jelentés 2025: A gyermekek médiahasználati szokásai.https://nmhh.hu/kiadvany/1/Mediapiaci_Jelentes_2025/74/A_gyermekek_mediahasznalati_szokasai

Polanin, J. R., Espelage, D. L., Grotpeter, J. K., Ingram, K., Michaelson, L., Spinney, E., Valido, A., El Sheikh, A., Torgal, C., & Robinson, L. (2022). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. Prevention Science, 23, 439–454.https://doi.org/10.1007/s11121-021-01259-y

Porcelli, C., Anderson, F., & Kloess, J. A. (2026). Unraveling the complexities of offender strategies as part of online sexual grooming and technology-assisted child sexual abuse: A systematic review. Trauma, Violence, & Abuse. Advance online publication.https://doi.org/10.1177/15248380251411261

Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2022). A scoping review of child grooming strategies: Pre- and post-internet. Child Abuse & Neglect, 123, 105392.https://doi.org/10.1016/j.chiabu.2021.105392

Saleem, N., Young, P., & Yousuf, S. (2024). Exploring the relationship between social media use and symptoms of depression and anxiety among children and adolescents: A systematic narrative review. Cyberpsychology, Behavior, and Social Networking, 27(11), 771–797.https://doi.org/10.1089/cyber.2023.0456

JUVENIS

Sevilla-Fernández, D., Díaz-López, A., Caba-Machado, V., Machimbarrena, J. M., Ortega-Barón, J., & González-Cabrera, J. (2025). Parental mediation and the use of social networks: A systematic review. PLOS ONE, 20(2), e0312011.https://doi.org/10.1371/journal.pone.0312011

Shannon, H., Bush, K., Villeneuve, P. J., Hellemans, K. G. C., & Guimond, S. (2022). Problematic social media use in adolescents and young adults: Systematic review and meta-analysis. JMIR Mental Health, 9(4), e33450.https://doi.org/10.2196/33450

Shi, Y., Lau, Y., Chan, H. H. H., Choi, J. K. K., Calvo-Morata, A., & Wong, S. H. (2025). School-based intervention on cyberbullying-related outcomes and psycho-social well-being in children and adolescents: A systematic review and meta-analysis. Trauma, Violence, & Abuse. Advance online publication.https://doi.org/10.1177/15248380251375480

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online, London School of Economics and Political Science.https://doi.org/10.21953/lse.47fdeqj01ofo

Staksrud, E., Helsper, E., Livingstone, S., Lobe, B., Mascheroni, G., Stoilova, M., & Ólafsson, K. (2026). The EU Kids Online 2026 comparative study: Children's views, experiences, opportunities and risks in a digital world. London School of Economics and Political Science & University of Oslo.https://doi.org/10.21953/researchonline.lse.ac.uk.00140901

Staksrud, E., Mascheroni, G., Milosevic, T., Ní Bhroin, N., Ólafsson, K., Şengül-İnal, G., & Stoilova, M. (2026). European children's use and understanding of generative AI. EU Kids Online V. London School of Economics and Political Science & University of Oslo.https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/reports-and-findings/AI

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. Media and Communication, 8(4), 197–207.https://doi.org/10.17645/mac.v8i4.3407

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online – a systematic evidence mapping. Information, Communication & Society, 24(4), 557–575.https://doi.org/10.1080/1369118X.2019.1657164

juvenis

Tinmaz, H., Lee, Y.-T., Fanea-Ivanovici, M., & Baber, H. (2022). A systematic review on digital literacy. Smart Learning Environments, 9, 21.https://doi.org/10.1186/s40561-022-00204-y

Tølbøll, K. B. (2026). Social media use and adolescent mental health – an umbrella review and power analysis. Child and Adolescent Mental Health. Advance online publication.https://doi.org/10.1111/camh.70071

UNICEF Office of Strategy and Evidence – Innocenti. (2025). Childhood in a digital world: Screen time, digital skills and mental health. UNICEF.https://www.unicef.org/innocenti/reports/childhood-digital-world

Valkenburg, P. M., Meier, A., & Beyens, I. (2022). Social media use and its impact on adolescent mental health: An umbrella review of the evidence. Current Opinion in Psychology, 44, 58–68.https://doi.org/10.1016/j.copsyc.2021.08.017

Wang, L., & Jiang, S. (2023). Effectiveness of parent-related interventions on cyberbullying among adolescents: A systematic review and meta-analysis. Trauma, Violence, & Abuse, 24(5), 3678–3696.https://doi.org/10.1177/15248380221137065

Wang, L., Wang, W., Fei, W., & Wang, Z. (2026). Online risk behavior in adolescents: A systematic review. Trauma, Violence, & Abuse, 27(4), 1303–1321.https://doi.org/10.1177/15248380251343194

Zhang, J., Dong, C., Jiang, Y., Zhang, Q., Li, H., & Li, Y. (2023). Parental phubbing and child social-emotional adjustment: A meta-analysis of studies conducted in China. Psychology Research and Behavior Management, 16, 4267–4285.https://doi.org/10.2147/PRBM.S417718



juvenis

Melléklet A. Szakmai ellenőrzőlista a CyberHősök tartalmak publikálása előtt

- Van-e minden számszerű állításhoz pontos, visszakereshető forrás?
- A forrásból valóban ugyanaz a korcsoport, populáció, időablak és definíció következik-e?
- Az asszociációt nem fogalmaztuk-e át oksági állítássá?
- Elkülönül-e a kockázat, az expozíció és a tényleges kár?
- A szöveg kerüli-e a gyermek hibáztatását és a morális pánikot?
- Az ajánlás arányos-e a bizonyíték erejével?
- A szülői tanács támogatja-e a segítségkérést, és nem ösztönöz-e titkolózásra?
- A pedagógusi anyag tartalmaz-e egyértelmű eszkalációs és dokumentálási útvonalat?
- Az érzékeny témákhoz tartozik-e segítségkérési információ?
- A programállítások között elkülönül-e az evidenciaalapú tény, a szakmai ajánlás és a program saját hipotézise?



juvenis

Melléklet B. Javasolt minimumindikátorok a pilothoz

Dimenzió	Példaindikátor	Mérés
Tudás	Biztonsági döntési pontok felismerése	10–15 szituációs tétel
Önhatékonyság	„Tudom, mit tennék, ha…”	Likert-skála
Segítségkérés	Megbízható felnőtt azonosítása	Szituáció + nyitott kérdés
Privacy	Adatmegosztási döntés	Vignetta-alapú feladat
Bystander	Támogató reakció választása	Viselkedési szándék
Szülői mediáció	Aktív beszélgetés és szabályalkotás	Szülői kérdőív
Pedagógusi kompetencia	Bejelentésfogadási protokoll	Tudás + esetvignetta
Implementáció	Részvétel, dózis, lemorzsolódás	Programnapló



juvenis

Készítette:

Juvenis Ifjúsági Jogvédő Alapítvány



juvenis

Nemzeti Együttműködési Alap

Társadalmi Kapcsolatokért és Kultúráért Felelős Minisztérium

Bethlen Gábor Alapkezelő Zrt.



juvenis