
STUDIA IURIS

JOGTUDOMÁNYI TANULMÁNYOK / JOURNAL OF LEGAL STUDIES

2025. II. ÉVFOLYAM 3. SZÁM



Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

A folyóirat a Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskolájának a közleménye. A szerkesztőség célja, hogy fiatal kutatók számára színvonalas tanulmányaik megjelentetése céljából méltó fórumot biztosítson.

A folyóirat közlésre befogad tanulmányokat hazai és külföldi szerzőktől – magyar, angol és német nyelven. A tudományos tanulmányok mellett kritikus, önálló véleményeket is tartalmazó könyvismertetések és beszámolók is helyet kapnak a lapban.

A beérkezett tanulmányokat két bíráló lektorálja szakmailag. Az idegen nyelvű tanulmányokat anyanyelvi lektor is javítja, nyelvtani és stilisztikai szempontból.

A folyóirat online verziója szabadon letölthető (open access).

ALAPÍTÓ TAGOK

BODZÁSI BALÁZS, JAKAB ÉVA, TÓTH J. ZOLTÁN, TRÓCSÁNYI LÁSZLÓ

FŐSZERKESZTŐ

JAKAB ÉVA ÉS BODZÁSI BALÁZS

OLVASÓSZERKESZTŐ

GIOVANNINI MÁTÉ

SZERKESZTŐBIZOTTSÁG TAGJAI

BOÓC ÁDÁM (KRE), FINKENAUER, THOMAS (TÜBINGEN), GAGLIARDI, LORENZO (MILANO),
JAKAB ANDRÁS DSc (SALZBURG), SZABÓ MARCEL (PPKE), MARTENS, SEBASTIAN (PASSAU),
THÜR, GERHARD (AKADÉMIKUS, BÉCS), PAPP TEKLA (NKE), TÓTH J. ZOLTÁN (KRE),
VERESS EMŐD DSc (KOLOZSVÁR)

Kiadó: Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola

Székhely: 1042 Budapest, Viola utca 2-4

Felelős Kiadó: TÓTH J. ZOLTÁN

A tipográfia és a nyomdai előkészítés: CSERNÁK KRISZTINA (L'Harmattan) munkája

Nyomdai kivitelezés: Prime Rate Zrt., felelős vezető: TOMCSÁNYI PÉTER

Honlap: <https://ajk.kre.hu/index.php/jdi-kezdolap.html>

E-mail: doktori.ajk@kre.hu

ISSN 3057-9058 (Print)

ISSN 3057-9392 (Online)

URL: KRE ÁJK - Studia Iuris

<https://ajk.kre.hu/index.php/kiadvanyok/studia-iuris.html>

ÁRTATLAN SZEMEK, SÖTÉT TUDATOK, AVAGY A GYERMEKEK ONLINE ÁLDOZATTÁ VÁLÁSÁNAK PSZICHOLÓGIÁJA

INNOCENT EYES, DARK MINDS, THE PSYCHOLOGY OF CHILD ONLINE VICTIMISATION

ZSIRAI LILLA¹

ABSTRACT ■ Digital technology and social media have become an integral part of everyday life, and children's internet use is no longer the exception but the norm. However, this growing digital presence has introduced new forms of risk, making young users particularly vulnerable. This paper aims to explore the psychological dynamics of children's victimization in online environments, with special attention to the mechanisms of grooming and manipulation. The research applies the routine activity theory to examine how children's internet usage patterns influence their likelihood of becoming victims. The analysis focuses on the role of rapidly developing digital technologies and social media platforms, especially those that facilitate child exploitation. The paper also reviews the European Union Strategy on the Rights of the Child and Hungary's National Cybersecurity Strategy, assessing their effectiveness and practical implementation. The objective is not only to map out the risks but also to shed light on the often invisible psychological consequences that online abuse can leave on developing children. This study contributes to a broader dialogue aimed at balancing technological advancement with effective child protection in the digital age.

KEYWORDS: child protection, online abuse, networking, routine activity theory, social media, digital psychology, cybersecurity, children's rights, EU strategy on the rights of the child, national cybersecurity strategy

ABSZTRAKT ■ A digitális technológia és a közösségi média mindennapjaink szerves részévé vált, és a gyermekek internethasználata ma már nem kivétel, hanem norma. Ezzel párhuzamosan azonban újfajta kockázatok is megjelentek, amelyek a legfiatalabb felhasználókat különösen sebezhetővé teszik. A dolgozat célja, hogy feltárja a gyermekek online áldozattá válásának pszichológiai hátterét, különösen a behálózás és manipuláció lélektani mechanizmusait. A kutatás a rutintevékenység-elmélet mentén vizsgálja, hogyan befolyásolják a

¹ Doktorandusz, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Doktori Iskola; bírósági fogalmazó, Budapest Környéki Törvényszék.

gyerekek internethasználati szokásai az áldozattá válás esélyét. Elemzésre kerül a fejlődő digitális technológiák és a közösségi média szerepe, valamint azok a platformok és alkalmazások, amelyek különösen kedveznek a gyermekek online kihasználásának. A dolgozat kitér az Európai Unió gyermekjogi stratégiájára, valamint Magyarország Nemzeti Kiberbiztonsági Stratégiájára, értékelve azok hatékonyságát és gyakorlati érvényesülését. A vizsgálat célja nem csupán a veszélyek feltérképezése, hanem annak bemutatása is, hogy a digitális térben zajló bántalmazás milyen mély, gyakran láthatatlan pszichés nyomokat hagyhat egy fejlődésben lévő gyermekben. A dolgozat ezzel hozzájárul egy olyan átfogóbb párbeszédhez, amely a technológiai fejlődés és a gyermekvédelem közötti egyensúly megteremtését célozza.

KULCSSZAVAK: gyermekvédelem, online bántalmazás, behálózás, rutintevékenység-elmélet, közösségi média, digitális pszichológia, kiberbiztonság, gyermekjogok, EU gyermekjogi stratégia, nemzeti kiberbiztonsági stratégia

1. BEVEZETÉS

A modern kor gyermekei számára a digitális világ egyszerre ígér felfedezést és rejthet veszélyt. Miközben a gyerekek egyre fiatalabb korban csatlakoznak az online térhez, lévén, hogy már digitális bennszülötteknek számítanak, a bűnelkövetők is egyre kifinomultabb módszerekkel hálózák be őket – gyakran úgy, hogy a felnőttek csak későn, vagy egyáltalán nem veszik észre. Ez a dolgozat annak a pszichológiai folyamatnak jár utána, amely a gyermekek online áldozattá válásához vezet. Igyekszem a gyermekek online áldozattá válásának pszichológiai és társadalmi vetületeit feltárni, különös hangsúlyt helyezve a gyermekek internethasználati szokásainak feltérképezésére, valamint arra, hogy a rutintevékenység-elmélet miként segíthet megérteni azokat a körülményeket, amelyek elősegítik az áldozattá válást. A dolgozat bemutatja, hogyan válik egy gyermek napi online rutinja – akár a közösségi oldalak, játéklatformok vagy üzenetküldők használata – egy olyan mintázattá, amelyet a bántalmazók tudatosan kihasználhatnak. A gyermekpszichológia szempontjából a digitális tér olyan „játszótér”, amelyet felnőtt jelenlét nélkül is könnyen elérnek, és amelyben a határok könnyen elmosódnak. A gyermekek kognitív, érzelmi és társas fejlődése még nem biztosítja azt az érettséget, amellyel felismerhetők lennének az online manipuláció, a megtévesztés vagy a kizsákmányolás jelei. A bizalom, az identitáskeresés és a társas elfogadás iránti vágy természetes sajátosságai ennek az életkornak, ezek pedig sebezhetővé teszik őket azokkal szemben, akik az online térben rejtőzködve, tudatosan építenek bizalmat, majd élnek vissza vele. A dolgozat külön fejezetben elemzi a behálózás ('grooming') folyamatát,

amely nem csupán technikai, hanem mélyen pszichológiai jelenség is. A gyermek bizalmának apró lépésekben történő elnyerése, a határok fokozatos tágítása, a manipuláció, mindez egy láthatatlan hálónak válik, amelyből nehéz menekülni, különösen akkor, ha a gyermek saját maga sincs tudatában annak, hogy bántalmazás áldozata lett. Része továbbá a digitális technológia és a közösségi média szerepének kritikai vizsgálata: ezek a platformok ugyanis nemcsak lehetőséget nyújtanak a kapcsolattartásra, hanem új terepet biztosítanak a visszaélés különböző formáinak is – különösen, ha a gyermekfelhasználók nincsenek megfelelően védve. A dolgozat jogi és stratégiai keretrendszerek elemzésével is foglalkozik: bemutatja az Európai Unió gyermekjogi stratégiáját, valamint Magyarország Nemzeti Kiberbiztonsági Stratégiáját, és értékeli, milyen mértékben képesek ezek a dokumentumok reagálni a gyorsan változó online környezet kihívásaira.

2. A MODERN KOR GYERMEKE ÉS AZ INTERNET KAPCSOLATA

Az Ofcom² 2024-es felmérései szerint az 5–7 évesek 38%-a social media felhasználó, bár az életkori korlátok tiltják ezt. Az online kommunikáció (üzenetküldés, videóhívás) és élő közvetítés is emelkedést mutat náluk. 26% saját profillal rendelkezik 41% játszik online játékokat, 15% pedig „lövöldözős” játékokat – miközben a szülők fele nem követi rendszeresen ezeket az aktivitásokat.

Az 5–7 évesek mintegy 65%-a üzeneteket küld (2023-ról 2024-re emelkedve 59%-ról). A 3–5 évesek 37%-a önállóan használja a közösségi médiát (ez 11%-os növekedés egy év alatt). A korosztályoknál jelentős az aggodalom a fake news, AI-s csalások miatt: az erre figyelő szülők aránya 70%.

Ezen adatok már kellőképpen megdöbbentőek, főleg, ha figyelembe vesszük, hogy milyen fiatal gyermekekről is van szó. Azonban a gyermekek online tevékenysége nem merül ki a social media, és a játékok használatában. Az Ofcom felmérései alapján ugyanis a 8–14 éves gyermekek körében legalább 8% nézett már pornográf tartalmat az interneten.

Egy 2025-ös, szintén az Ofcom által 3–17 évesek körében végzett kvantitatív és kvalitatív kutatás azt mutatja, hogy 89% játszik online, 81% rendszeresen YouTube-ot néz, és 40% már social media profil tulajdonosa 13 év alatt is.³ A 3–5 éves korosztályban 19%–30% rendelkezik saját okostelefonnal, a 6–7 évesek között ez az arány 30%.

A fiatalok számos okból használják az internetet, többek között olyan pozitív és konstruktív tevékenységek folytatásához, mint a tanulás – elég csak a 2019-es

² Online safety rules: what you need to know – Ofcom.

³ Article – Ofcom Media Use & Attitudes Report 2025 – KIDSONLINEWORLD.COM.

Covid-járványra gondolni –, vagy egyéb szórakozási tevékenységek, de ezenkívül az is fontos számukra, hogy az internet-hozzáférés megkönnyíti a valós idejű online játékokban való részvételt, a kortársaikkal és a családjukkal való kapcsolattartást, illetve új barátok megismerését olyan kínos, személyes kommunikációs helyzetek elkerülésével, amiktől az életkoruk és esetleges tapasztalatlanságuk miatt tarthatnak a fizikai világban.

Véleményem szerint nyugodtan kijelenthetjük, hogy nincs ma már olyan gyerek, aki nem használ valamilyen felületet. Legyen ez akár videómegosztó portál pl. YouTube, TikTok, social media felület pl. Facebook, Instagram, de ide-sorolandók a különböző üzenetküldő alkalmazások is pl. Messenger, WhatsApp, Viber stb. Ezen alkalmazások használata a gyerekek mindennapjainak szerves részét képezi, és egyben magában foglalja azt is, hogy az alkalmazásokhoz felhasználói fiókok is tartoznak, tehát a gyerekek nagy része nemcsak „passzív” felhasználó, hanem „aktív” tartalomgyártóként is jelen van az online világban, ami még inkább sebezhetővé teszi őket.

Már THOMAS HOLT, ADAM BOSSLER, KATHRYN SEIGFRIED-SPELLAR 2017-ben megjelent *Cybercrime and digital Forensics* c. könyve is kiemeli, hogy az olyan nyíltan hozzáférhető, közvetlen kommunikációs csatornák használata, mint a Messenger és a Discord, az egyének láthatóságának fokozásával megnövelték az interszónális viktimizáció lehetőségét az online térben. Ez azt jelenti, hogy a kibertérben töltött több idő potenciálisan megnövekedett veszélynek teheti ki a gyermekeket. Ennek megelőzése és hatékony kezelése érdekében érdemes a kriminológia elméleti kereteiben vizsgálni az internet néhány olyan egyedi jellemzőjét, amelyek befolyással lehetnek a gyermekek online védelmére és biztonságára a világhálón, beleértve a közösségi média működési elveinek sajátosságait, illetve a dinamikusan fejlődő modern digitális technológiák hatását, főként a gyerekeket érintő online áldozattá válására.

3. A KÖZÖSSÉGI MÉDIA SZEREPE A GYERMEKEK

ONLINE ÁLDOZATTÁ VÁLÁSÁBAN

A digitális technológiák gyors ütemű fejlődése – különösen az olyan eszközök elterjedése, mint az élő közvetítést lehetővé tevő szoftverek, a végpontok közötti titkosítással működő kommunikációs platformok, valamint az anonim tranzakciókat biztosító fizetési megoldások, például a kriptovaluták – jelentős mértékben elősegítette a gyermekek online térben történő szexuális kizsákmányolását. E technológiai innovációk nemcsak a behálózás folyamatát tették kevésbé észlelhetővé a felnőtt felügyelet számára, hanem hozzájárultak a gyermekeket ábrázoló

szexuális tartalmak előállításának és terjesztésének kockázatához is. Az elkövetők számára biztosítják, hogy nehezen felderíthető és kinyomozható módokon működjenek. A hálózatok kiépítése, információk egymással történő megosztása, illetve a kiskorúak ellen, lényegében bárholnan elkövethető bűncselekmények megvalósítását is könnyebbé tették. Ebben az esetben fontos kiemelni, hogy a bűncselekményeket egyszerűen több áldozat sérelmére is el lehet követni.

Az Instagram, a Facebook, a TikTok és a többi, kiskorúak körében rendkívül népszerű közösségimédia-platform működési módja – például a moderálás formája, alapossága és intenzitása – nagyban befolyásolhatja, hogy az ezeket használó gyerekek könnyen „elérhető” és megközelíthető célpontot jelentenek-e az elkövetők számára vagy sem. Az, hogy milyen szintű védelmet, például szűrő és jelző eszközöket építettek be ezekbe az alkalmazásokba, meghatározza, hogy mennyire biztonságos a gyerekek számára a használatuk. Az Európai Unió az online biztonság elősegítése érdekében ezért 2022 májusában bemutatta „a gyermekbarát internet új európai stratégiáját”,⁴ illetve legújabb, a gyermekek online szexuális bántalmazásának megelőzése és az ellene folytatott küzdelem érdekében kidolgozott és előterjesztett uniós rendeletjavaslatát,⁵ melynek keretében az Európai Bizottság kötelezné az alkalmazás áruházakat üzemeltető közösségimédia-vállalatokat annak biztosítására, hogy a gyermekek ne tölthessenek le olyan alkalmazásokat, amelyek a behálózás magas kockázatának tehetik ki őket, illetve azonosítsák őket, amennyiben már felhasználókká váltak, és előzzék meg a szolgáltatások általuk történő további használatát. A rendeletben szorgalmazza továbbá egy európai központ létrehozását, melynek feladata lesz a gyermekek szexuális kizsákmányolásának megelőzésére és leküzdésére szolgáló szervezetek koordinációja, kapcsolódó kutatási és szakértői tevékenységek, az áldozatok támogatása, valamint – megkönnyítve a nemzeti rendészeti szervek munkáját – a gyermekek online szexuális bántalmazásával összefüggő ügyek felderítésének, bejelentésének és kezelésének támogatása is.⁶

Az egyre szigorúbb nemzetközi szabályozások és társadalmi nyomás ellenére sem sok vállalat hajlandó a gyermekek online védelme melletti elköteleződést deklaráló nyilatkozatokon túlmutató érdemi lépéseket tenni, és a profitjuk egy részét a gyakorlatban is a gyerekek érdekét szolgáló, az áldozattá válásukat megelőző

⁴ Európai Bizottság COM (2022) 212 final. Digitális évtized a gyermekek és az ifjúság számára: a gyermekbarát internetre (BIK+) vonatkozó új európai stratégia.

⁵ Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. COM/2022/209 final.

⁶ MEGYESFALVI BOGLÁRKA: Kockázati tényezők a digitális térben. A gyerekek internet- és közösségi média használata és az online áldozattá válás. *Belügyi szemle*, 2023 (12). Kockázati tényezők a digitális térben megtekintése | Belügyi Szemle (letöltés: 2025. június 01.).

biztonsági fejlesztésekre fordítani, jelenleg világszerte vita tárgyát képezi, hogy a végpontok közötti titkosításnak és az életkor-ellenőrzési ('age-verification') technológiáknak milyen szerepet kellene játszaniuk a gyermekek online védelmében. A gyermekek biztonságáért kampányoló jótékonyági szervezetek, digitális technológiai szakértők, és áldozattúlélők brit koalíciója ezen technológiák megfelelő szabályozását követelve indította el a Nincs hová bújni ('No place to hide') elnevezésű kampányt, azzal a céllal, hogy megakadályozzák azt, hogy a Messengerhez hasonló szolgáltatásokat nyújtó közösségimédia-vállalatok az üzenetküldő szolgáltatásaik részeként bevezessék a végpontok közötti titkosítást.⁷ Ez a technológia az üzeneteket úgy alakítja át, hogy a megosztott tartalmakat csak a feladó és a címzett láthatja, ami a kampányt szervező koalíció szerint szinte lehetetlenné teszi az online behálózások felderítését, többek között azért, hogy sem a moderátorok, sem a gépi algoritmusok nem lesznek képesek a gyanús vagy káros tartalmakat azonosítani. A végpontok közötti titkosítás technológiájának alkalmazása körüli globális vita már régóta folyik a politikai döntéshozók, nemzetközi szervezetek és az adatvédelmi érdekekért kampányoló társulások között, mindkét oldalon olyan fontos, egyetemes emberi jogok védelmére hivatkozva, mint a gyermekek mindenek felett álló érdeke és (online és offline) biztonsága, illetve a szólásszabadsághoz és a magánélet védelméhez való jog.⁸

A közösségimédia-vállalatok széles körben elterjedt jelenlegi rutinja, hogy irányelvek és szabályozások révén elhatárolódnak az oldalaikon generált tartalmakért és tevékenységekért vállalt felelősségétől, áthárítva azt más szereplőkre, például a felhasználókra, a jogalkotókra, vagy a bűnüldöző szervekre. A bűnüldöző szervek azonban egyedül nem képesek megvédeni a gyerekeket az egyre növekvő számú online szexuális ragadozótól, és az oldalakat üzemeltető üzleti vállalkozásokéhoz képest aránytalanul kevés technológiai tudással, eszközzel és rálátással rendelkeznek a közösségimédia-platformok hatékony ellenőrzéséhez. Kiemelendő továbbá az is, hogy a bűnüldöző szerveknek nem is áll rendelkezésére olyan technikai eszköz, amellyel sikeresen fel tudnák deríteni az elkövetőket. Így az ilyen típusú bűncselekmények legtöbb esetben felderíthetetlenek maradnak. Másrészt az ilyen típusú bűncselekmények esetében kiemelő, hogy sokszor maguk az áldozatok nem tesznek jelentést. Itt nem a rendőrségnél tett feljelentésre gondolok, hanem a közösségimédia-platformon megtehető jelentésről. Ezen akadályok – technikai hiányosságok, jelentés elmulasztása – nagyban megnehezíti az online térben elkövetett bűncselekmények elleni harcot.

⁷ Ibid.

⁸ Ibid.

4. ÁLDOZATI MAGATARTÁS MEGJELENÉSÉNEK EGYES ELEMEI AZ ONLINE VILÁGBAN

Az áldozati jellemzőkhöz tartozó korosztálybeli kategória oldalán rajzolódik ki némi különbség, az internetes színtér és annak használata leginkább azokra a fiatalokra jellemző, akik leginkább rendelkeznek a digitális kompetenciákkal. A mindennapi életük részévé vált virtuális interakcióban való nagyobb részvétel több lehetőséget biztosít arra, hogy gyakori célpontot jelentsenek (zaklatás, csalás, 'cyberbullying'). A részvétel egyben a korosztályok közti számszerű különbséget is jelenti az áldozattá válás tekintetében. A korosztályi meghatározottságnál az online színtéren aktív gyermekek viszont kiemelt kockázati kategóriába sorolhatóak, sőt, a kiskorúak digitális részvételének magas intenzitása és a sokkal lazább családi kontroll miatt még fokozódhat.

Míg az offline terepen az áldozattá válás szoros okozati összefüggésben áll a szegénységgel, az alacsony iskolázottsággal, a nélkülöző élethelyzettel, addig az internetes társadalomban ugyanez fordított irányban is megjelenhet. A kedvezőtlen szociális helyzet mindenképp nagy szakadéknak tűnik az offline és online környezet ez irányú összehasonlításában. Azoknak a társadalmi csoportoknak a tagjai, akik jövedelmi és képességbeli hiányosságaik okán nem rendelkeznek megfelelő eszközökkel és digitális tudással, kevésbé van lehetőségük aktív részvételre, és a virtuális környezetben is kisebb eséllyel válhatnak közvetlenül áldozattá. Mindez vonatkozhat a fogyatékkal élők azon köreire is, akik betegségeik okán kisebb arányú internetes részvétellel nem tartozhatnak közvetlenül az online áldozatok közé. A társadalmi csoportok közti szakadék digitális szakadékként értelmezve új kérdést vet fel az online áldozatiság tárgykörében, mégpedig azt, hogy milyen társadalmi státuszú közösségek tartozhatnak az internetes társadalom viszonyrendszerében a magasabb kockázati kategóriába. Ha csak azok sorolhatóak ezen keretek közé, akik meghatározott társadalmi státusz felett helyezkednek el, akkor az internethez való szabad és egyenlő hozzáférési esélyek növekedése esetén milyen mértékben bővíthet az internetes társadalom tipikus áldozatainak köre. Ha ez továbbra sem változik, akkor lehet-e az új környezetben homogénebb áldozati kategóriáról beszélni, azzal, hogy a szegénységet a bűnözés effajta terepén nem lehet az áldozattá válással szoros összefüggésbe hozni.

A színterek kapcsán ki kell emelni a család szerepét is. Ahogy a bűnelkövetővé válás elsődleges megalapozója a család – mint szocializációs színtér –, úgy az áldozattá válással is generális okozati összefüggésben állhat. Az instabil családi légkör, a bűnözői szülői minta, a szeretethiány, a pszichés betegségek, a kontrollhiány, és a családban előforduló örökös áldozati személyiségminta indokolja az áldozati személyiségvonások kialakulását. Noha kétségkívül kapcsolatban

áll a szocializáció az internetező személyiségével, döntéseivel és ezzel összefüggésben a bűnelkövetői és áldozati életúttal is, a válasz mégis inkább a szülő és a gyermek szoros kapcsolatának deficitjében, a szülő alacsony informatikai tudásában keresendő, és nem kizárólag a családi kiscsoport életkörülményeiben. Ebben a tekintetben már indokolható, hogy miért válhatnak magas számban a kimondottan „jó családban” nevelkedő kiskorúak az interneten vagy azáltal súlyos bűncselekmények áldozatául. Mivel a társadalmi kontroll az online színtéren alacsonyabb, mint a fizikai valóságban, ezért a kiskorú internetes jelenlétét nem lehet egy napon említeni a hagyományos „kulcsos gyermek” szabadságával, akit szabadidejében a lakókörnyezet vagy más közösség nagyobb eséllyel tartott kontroll alatt akkor is, ha a szülő nem volt jelen.

Az online identitás azokból az elemekből tevődik össze, amit az egyén vagy a közösség magáról ebben a közegben megformál és nyilvánosságra hoz. A virtuális profil a személyes adatokon túl gyakran megtörtént életesemények, valós életkörülmények, belső gondolatok, vágyak, célok halmaza, ami egyszerre jeleníti meg a múltat, a jelent és a jövőt. Az internethasználó a dolgok és az egyének másoktól való megkülönböztethetőségét, saját magáról alkotott tudást, az egyéni tulajdonságok halmazát, az egyén önálló entitását, a „ki vagyok én” és „mi vagyok én”-ről való ismeretet, vagyis az identitást ebben az érában képek, szövegtartalmak és egy rendszer tartalmaként testesíti meg. Az online „karakter” kissé képlékennyé teszi az identitást korábban stabil határaihoz képest. Ami azt jelenti, hogy a korábban markáns elképzelést önmagunkról már a vágyak és a képzelet is formálja, ezért a „ki és mi vagyok én” klasszikus értelmezés mellett a virtuális környezetben a „ki és mi lehetnék én” is fontos szerepet kapott. Másként fogalmazva, az online identitást tartalmazó profilokban saját magunkról alkotott kép már a vágyak szülte egyéniségünket is tartalmazza. Az online identitással az egyén egyszerre vesz részt egy virtuális világban és egy valós materiális környezetben, ezért a két tér közti ingázása folytán a valóságot virtuális környezetben (személyes adatok, fotók, videók) a virtuális karakterét a valóságban jeleníti meg (valós cselekvéssé alakítja át). A szereplő a két dimenzió közti vándorlása alatt nem minden esetben klimatizálódik, ekképp a cselekedeteit sem illeszti a színterek elvárásaihoz – de legfőképp a fizikai valóság elvárásaihoz. A virtuális karakter a valóságban azoktól a cselekedetektől válik igen kockázatosná, amilyen korlátokat lép át (például a jogi, a társadalmi és erkölcsi normákat sért), vagy közvetlenül fizikai akadályokba ütközik. Míg a személyes adatait tartalmazó információkat megosztja az online profiljában, és azzal bárki visszaél, addig a sértett és a bűnelkövető is meghatározható, amikor viszont a virtuális környezetben átvett szerepe miatt a valós térben áldozat pozícióba kerül, az elkövető meghatározása nem oly egyértelmű. Az utóbbi esetén egy virtuális rendszer lehetne felelős azért, mert a tudatos fizikai

valóságtól elszakítja, irreális szerepkörbe és cselekvésmintákba helyezve a fizikai valóságban áldozattá teszi. Azoknak az online cselekvésmintáknak az alapján, melyeket az online szereplő a valós szintén követ gyakran bűnelkövetőként, vagy társadalmi normasértőként definiálják, így könnyen kerülhet bűnelkövetői pozícióba az internetező, aki az internetes közösségekben, vagy az ott szerzett érzelmformáló ingereket követően erőszakos bűncselekményeket vagy öngyilkosságot követ el, vagy az elérhetetlen életszínvonal elérhetőségének hitében jogellenes eszközökkel vagyron elleni bűncselekményeket valósít meg. A virtuális terep gyenge kontrollfunkciója nyomán a belső kontroll sem alakulhat ki kellő hatásossággal, így hasonló módon eredményezhet olyan személyiséget, aki rögzült deviáns életpályára lép – függetlenül a család személyiségformáló erejétől és a valós társadalmi kontrolltól. Ebben a tekintetben ugyancsak felmerül az a kérdés, hogy áldozatnak tekinthető-e az online szereplő, aki az internetes társadalom részeseként egy virtuális rendszer által szenved testi és lelki sérelmeket vagy kerül olyan életpályára, amit a társadalom deviánsnak tart. Felelős-e a valós térben őt körülvevő környezet akkor, ha az internetes világban való részvétel szerves része a társadalomnak és alapvető joga az internetezőnek.

Az áldozat egyéni és kollektív megfogalmazását bővebben a Magna Carta, azaz az ENSZ 1985. évi Deklarációja taglalja, ami a hatalommal való visszaélés áldozatait és a bűncselekmény áldozatait egy definíción belül foglalja össze. Kissé szűkebb kereteket kapott az áldozat meghatározása az Európai Unió 2001. évi kerethatározatában, ahol az áldozat az a természetes személy, aki valamely tagállam büntetőjogába ütköző cselekmény (tevékenység vagy mulasztás) közvetlen következményeként sérelmet, így különösen testi vagy szellemi (mentális) sérülést, érzelmi szenvedést, avagy gazdasági veszteséget szenvedett. Magyarországon az áldozat fogalmát a bűncselekmények áldozatainak segítéséről és az állami kárenyhítésről szóló 2005. évi CXXXV. törvény (Ást.) fogalmazza meg pontosan. Magyarországon elfogadott áldozatfogalom a kriminálviktimológia által használt fogalom, így a bűncselekmény, vagy szabálysértés sértettjeit és szerepüket emeli ki. Sokkal szélesebb meghatározás az általános viktimológia fogalomköréhez kapcsolható, miszerint az áldozat kategóriájába beletartozik minden olyan esemény miatt testi, lelki sérelmet vagy kárt szenvedett egyén vagy kollektíva, akik nemcsak bűncselekmény elkövetése, hanem természeti katasztrófa, vagy valamely baleset elszenvedői is. A modern viktimológia a két fogalomkör közt helyezkedik el, áldozati kategóriába sorolja a hatalommal való visszaélés és az emberi jogok megsértését a bűncselekmények sértettjei mellé. A fogalmakat áttekintve érzékelhető, hogy egyik meghatározás keretei közé sem illeszthető az online áldozat. Mindez azért sem lehetséges, mert nem kézzelfogható az a virtuális tér, aminek szabályai szerint az egyén a valós térben

cselekedve normasértést követ el. Azzal szemben, hogy jó néhány olyan tartalom megjelenése és működése büntetendő, melyek hatására az egyén vagy kollektíva agresszív erőszakos bűnelkövetővé, vagy öngyilkossá válhat, a megszokottnak és legális működésűnek tartott hálózat (például társas oldalak), ezen hatása nem tetten érhető. Ebben a tekintetben az, hogy az online rendszer áldozata áldozatnak mondható-e, megválaszolatlan maradt.

5. AZ ONLINE ÁLDOZATTÁ VÁLÁS ÉS A RUTINTEVÉKENYSÉG-ELMÉLET

Az online környezet kétségtelenül számos előnnyel jár a gyermekek számára, ugyanakkor az internet az egyéni elkövetők és a szervezett bűnözői hálózatok számára is új és egyre szélesebb körű lehetőségeket kínál a sérülékenyebb személyek kizsákmányolására. A gyermekek ellen elkövetett számítógépes bűncselekmények és az online áldozattá válás folyamatának alaposabb megértéséhez alkalmazható kriminológiai megközelítés a rutintevékenység-elmélet.

A rutintevékenység-elméletet ('Routine Activity Theory') 1979-ben dolgozta ki két amerikai kriminológus: Lawrence E. Cohen és Marcus Felson. A rutintevékenység-elmélet szerint a bűncselekmények nemcsak az elkövető motivációjától függenek, hanem attól is, hogy a hétköznapi tevékenységek során találkozik-e három tényező: motivált elkövető, védtelen áldozat, hiányzó felügyelet vagy védelem.

A modell főként azokra a bűncselekményekre alkalmazható, amelyek napi rutintevékenységek (pl. közlekedés, internethasználat) közben, alkalmi lehetőségek kihasználásával valósulnak meg – ezért különösen hasznos az online áldozattá válás, így a gyermekek digitális sebezhetőségének vizsgálatában is.

A digitális tér jelentősen átalakította a rutintevékenység-elmélet értelmezését, különösen a gyermekek esetében, akik már egészen fiatal kortól aktívan jelen vannak online. Az alábbiakban bemutatjuk, hogyan illeszthető a modell az online behálózás és szexuális kizsákmányolás kontextusába:

1. Motivált elkövető: Az elkövető gyakran anonim módon lép be az online térbe, hamis identitással. A digitális környezet lehetőséget ad arra, hogy a bántalmazó következmények nélkül kísérletezzon és manipuláljon. A motiváció mögött pszichoszexuális devianciák, hatalmi kontrollvágy, vagy kriminális szocializációs minták állhatnak.
2. Alkalmas célpont – a gyermek: A gyerekek életkoruknál, érzelmi fejlettségükönél és naivitásuknál fogva könnyen befolyásolhatók. Az internetes rutintevékenységek (pl. játék, videónézés, közösségimédia-használat) során gyakran kerülnek kapcsolatba ismeretlenekkel. A gyerekek gyakran nincsenek tisztában azzal, hogy online viselkedésük áldozati kockázattal járhat.

3. Hiányzó felügyelet: A szülők vagy pedagógusok nem mindig értik vagy követik a gyermekek digitális tevékenységeit. Az algoritmus-vezérelt platformok (TikTok, Instagram, Discord stb.) nem biztosítanak megfelelő biztonsági szűrőket. A végpontok közötti titkosítás ('end-to-end encryption') korlátozza a hatóságok vagy a platformok beavatkozási lehetőségeit. Az online tér „láthatatlanná” teszi a bántalmazást – nincs fizikai közelség, nincs klasszikus „helyszín”.

Az online térben azonban több tényező is befolyásolhatja az áldozatok kizsákmányolását. Ilyen például az internet által legyőzött távolság, valamint a bűnelkövetők anonimitása.

6. AZ EU GYERMEKJOGI STRATÉGIÁJA ÉS A BARNAHUS-MODELL

A stratégia alapját többek között a gyermek jogairól szóló ENSZ-egyezmény és annak három fakultatív jegyzőkönyve adja. A stratégia főként az Európai Parlamenttől, a tagállamoktól, a gyermekjogi szervezetektől összegyűjtött javaslatokon alapul. A dokumentum hangsúlyozza, hogy a gyermekek a társadalom legkiszolgáltatottabb tagjai, akik egyedül nem képesek kezelni a társadalmi kirekesztés kockázatát. A gyermekek életében teljesen összeolvad az offline és az online tér. A stratégia olyan akadálymentes digitális környezet kialakítását szorgalmazza, amelyeket minden gyermek használni tud. A gyermekeknek joguk van ahhoz, hogy sokféle forrásból gyűjthessenek online információt, és ne legyenek áldozataik online bűncselekményeknek e tevékenységük során. Ehhez szigorú szabályozásra van szükség. A gyermekek, már egészen kicsi gyermekként is internetes megfélemlítés áldozataivá válhatnak, ami súlyos vagy akár végzetes mentális egészségügyi problémákat okozhat. A gyermekek online szexuális erőszaknak is áldozatul eshetnek. A stratégia 3. pontja összegzi a gyermekekkel szembeni erőszak jellemzőit. A gyermekek lehetnek erőszakos cselekmények áldozatai, tanúi és elkövetői – a saját otthonuktól kezdve az iskolán, a szabadidős és rekreációs tevékenységeken keresztül az igazságszolgáltatási rendszerig, offline és online egyaránt.⁹

2024. április 23-án az Európai Bizottság elnöklete alatt ajánlást ('Recommendation') fogadott el az integrált, több szektorra kiterjedő gyermekvédelmi rendszerek bevezetésére. Ez a következőket tartalmazza:

⁹ DOMOKOS ANDREA: Gyermekáldozatok védelme az online világban. In: HOMICSKÓ ÁRPÁD OLIVÉR (szerk.): *A technológia fejlődés társadalmi kihívásai és hatása a jogi szabályozásra*. Budapest, Patrocinium Kiadó, 2022. Gyermekáldozatok védelme az online világban (letöltés ideje: 2025. június 05.).

1. Átfogó nemzeti terveket sürget az erőszak minden formája – beleértve az online és offline helyzeteket –, elleni fellépésre.
2. Sokszereplős együttműködést ösztönöz – a bűnüldözéstől az oktatáson át a társadalmi szervezetekig.
3. Kiemeli a digitális írástudás fontosságát gyerekek, szülők és pedagógusok körében.

Az integrált gyermekvédelmi rendszerek előmozdítása szervesen kapcsolódik az erőszak megelőzéséhez és az azzal szembeni védelemhez. A gyermekközpontúságot szem előtt tartva, valamennyi érintett hatóságnak és szolgáltatnak együtt kell működnie a gyermek védelme és támogatása érdekében, a gyermek mindenek felett álló érdekének megfelelően. A Bizottság továbbra is támogatni fogja a gyermekházak ('Barnahus') létrehozását az EU-ban.¹⁰

Mivel a Barnahus-modell igen fontos pontja a gyermekvédelemnek, szeretnék néhány gondolat erejéig kitérni rá.

A Barnahus-modell, amelynek neve izlandi eredetű és szó szerint „Gyermekházat” jelent, egy integrált, gyermekközpontú szakmai beavatkozási forma, amelyet az 1990-es évek végén dolgoztak ki Izlandon a gyermekekkel szembeni szexuális bántalmazás és más súlyos abúzusok áldozatainak hatékonyabb védelme érdekében. A modell célja, hogy a gyermekek részére egy olyan komplex, multidiszciplináris ellátást biztosítson, amelyben a büntetőjogi, pszichológiai, egészségügyi és gyermekvédelmi eljárások összehangoltan, egy helyszínen, gyermekbarát környezetben zajlanak. A Barnahus tehát nem csupán egy fizikai helyszín, hanem egy szemlélet is: a gyermek érdekeit mindenek felett állónak tekinti, és arra törekszik, hogy az igazságszolgáltatás folyamata a lehető legkisebb pszichés megterheléssel járjon az érintett gyermek számára.

A modell egyik legfontosabb eleme, hogy a gyermekek kihallgatása – amely gyakran a büntetőeljárás legkritikusabb része – egy erre kiképzett, gyermekpszichológiai ismeretekkel rendelkező szakember által történik, egy barátságosan berendezett, nyugodt környezetben. A kihallgatást videóra rögzítik, és azt a büntetőeljárás során bizonyítékként lehet felhasználni, így elkerülhető a gyermek többszöri kihallgatása és ezzel a másodlagos traumatizáció. A kihallgatás során a többi érintett szakember – rendőr, ügyész, gyermekvédelmi szakember, pszichológus – egy külön helyiségből figyeli a beszélgetést, így biztosított az információmegosztás és az azonnali szakmai egyeztetés lehetősége. A Barnahus-modell további előnye, hogy a gyermek bántalmazásának gyanúja esetén minden szükséges vizsgálat és beavatkozás – például igazságügyi orvosi

¹⁰ Ibid.

vizsgálat, pszichodiagnosztikai értékelés, azonnali terápiás beavatkozás – helyben megtörténhet. A különböző szakterületek együttműködése nem csupán hatékonyabbá teszi a védelmi rendszert, hanem növeli a gyermek biztonságérzetét is, hiszen nem kell számára ismeretlen intézmények között mozognia, miközben érzékeny, traumatikus élményeiről kell beszélnie.

Jogi szempontból a Barnahus-modell számos országban példaértékűként szolgál. Európában több mint húsz állam – köztük Svédország, Norvégia, Litvánia, Horvátország és Lengyelország – vezette be vagy adaptálta saját nemzeti rendszerébe. Az Európa Tanács és az UNICEF is aktívan támogatja a modell terjedését. Magyarországon jelenleg kísérleti jelleggel működnek Barnahus típusú programok, illetve a Gyermekbarát Igazságszolgáltatás keretében több gyermekmeghallgató szoba is létesült az elmúlt években, amelyek egyes elemeiben követik a Barnahus alapelveit. A Barnahus szemlélete a traumaérzékeny igazságszolgáltatás elvére épül. Ennek értelmében a gyermekbántalmazás során szerzett pszichés sérülések nem csupán következmények, hanem az eljárás egészét meghatározó szempontok. A modell olyan támogató, megerősítő környezetet kíván teremteni, amelyben a gyermek nem csupán tanú vagy sértett, hanem egy védelmet igénylő, autonómiával rendelkező személy, akinek méltósága, biztonságérzete és mentális jólléte elsődleges fontosságú.

Összességében a Barnahus-modell az egyik legkomplexebb és leginkább gyermekbarát megközelítés a gyermekekkel szembeni súlyos visszaélések kezelésében. Sikere abban rejlik, hogy az áldozatot állítja a középpontba, miközben hatékony és együttműködésen alapuló szakmai rendszert épít ki. A modell hazai adaptációja lehetőséget teremt arra, hogy Magyarország is egyre magasabb színvonalon biztosítsa a gyermekek védelmét és a velük szemben elkövetett bűncselekmények hatékony, mégis kíméletes igazságszolgáltatási kezelését.

Visszatérve az EU gyermekjogi stratégiájához, 4. pontja felhívja a figyelmet arra, hogy nagy a látencia a gyermekek sérelmére elkövetett bűncselekmények esetében. A bűncselekmények gyermekáldozatai esetében az áldozat életkora, a jogaikkal kapcsolatos ismeretek hiánya, valamint az elérhető, életkornak és nemnek megfelelő bejelentési és támogató szolgáltatások hiánya miatt nagyon gyakran elmarad a bejelentés. A stratégia 5. pontja olyan EU képét vázolja fel, ahol a gyermekek biztonsággal használhatják a digitális környezetet, és kihasználhatják az abban rejlő lehetőségeket. A dokumentum kiemeli, hogy a gyermekek digitális jártasságuknak köszönhetően ügyesebben boldogulhatnak a fokozottan digitalizált és hálózati oktatásban, majd a későbbiekben a munkaerőpiaci rendszerekben. A gyermekek online jelenléte azonban növeli a káros vagy jogellenes online tartalmaknak, például a gyermekek szexuális bántalmazását vagy kizsákmányolását ábrázoló anyagoknak, a pornográfiának és felnőtt tartalmaknak,

a szextingnek, az online gyűlöletbeszédnek vagy a félretájékoztatásnak és dezinformációnak való kitettségüket. Hasonlóan komoly veszélyt jelent a kiberzsákmány és a gyermekek sérelmére megvalósuló kerítés, az internetes megfélemlítés vagy az online bántalmazás és internetes zaklatás.¹¹ Az emberkereskedelem a világban történő események hatására szárnyal, véleményem szerint elmondható, hogy a legjobban jövedelmező bűncselekmények egyike. Az az ellen folytatott harcot nagyban megnehezíti, hogy a kibertér olyan nagy fokú anonimitást és lekövethetlenséget biztosít az elkövetők számára, amivel a bűnüldöző szerveknek nagyon nehéz felvenni a versenyt. Nemzetközi szinteken persze vannak próbálkozások, azonban azt gondolom, hogy hosszú évek kellene még ahhoz, hogy hatékonyan tudjanak ellenük fellépni. A gyermekek súlyosan kiszolgáltatott csoportot alkotnak, az ő megvédésük prioritást kell, hogy élvezzen. Ezt már nemzetközi szinteken is felismerték, azonban – akár csak az elkövetők vonatkozásában – az áldozatok hatékony védelme is egy hosszantartó folyamat, amelyet nagyban nehezít a technika folyamatos és rettentő gyors fejlődése.

7. MAGYARORSZÁG NEMZETI KIBERVÉDELMI STRATÉGIÁJA¹²

Magyarország Nemzeti Kiberbiztonsági Stratégiája 2021 és 2030 közötti időszakra határozza meg az ország digitális biztonsági célkitűzéseit és az ezek eléréséhez szükséges intézkedési irányokat. A stratégia kiemelt célja, hogy a kibertérben is biztosított legyen a társadalom, a gazdaság és az állam zavartalan és biztonságos működése, valamint a lakosság – különösen a sérülékeny csoportok, például a gyermekek – hatékony védelme az online térben megjelenő fenyegetésekkel szemben. A stratégia alapját az a felismerés képezi, hogy a digitalizációval párhuzamosan nő a kiberfenyegetések súlya és összetettsége. A kiberbiztonság már nem kizárólag technológiai kérdés, hanem nemzetbiztonsági, társadalmi, gazdasági és jogi jelentőségű ügy is. A dokumentum szerint a kibertér védelme össznemzeti ügy, amelyben az állami szereplők mellett a gazdasági szféra, az akadémiai közösség, a civil társadalom és az egyének is felelősséggel bírnak. A stratégia három fő pillérre épül: a reziliencia, a reagálóképesség és a bizalom erősítésére. A reziliencia célja, hogy az intézmények, infrastruktúrák és felhasználók felkészültek legyenek a kiberincidensek kezelésére. A reagálóképesség keretében az incidenskezelő szervek, mint például a Nemzeti Kibervédelmi Intézet (NKI) megerősítése, a kibertér-felügyeleti és információmegosztási rendszerek

¹¹ Ibid.

¹² 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

fejlesztése történik. A bizalomépítés pedig a felhasználók tudatosságának növelését, az oktatás és képzés erősítését, valamint a szabályozási és etikai keretek finomítását foglalja magában. Külön figyelmet fordít a stratégia az állami és önkormányzati intézmények védelmére, a kritikus információs infrastruktúrák megerősítésére, a pénzügyi és egészségügyi szektor digitális biztonságának növelésére, valamint az oktatásban és a gyermekvédelemben megjelenő kihívásokra. A dokumentum hangsúlyozza, hogy a gyermekek fokozottan ki vannak téve az online térben megjelenő fenyegetéseknek – így például a zaklatásnak, a manipulációnak, vagy akár a gyermekekkel szembeni szexuális kizsákmányolásnak. Ezért a kiberbiztonsági stratégia a gyermekvédelem digitalizációs vonatkozásait is tartalmazza: a szülők, pedagógusok és gyerekek digitális írástudásának fejlesztésével, a biztonságos internethasználatra nevelés intézményesítésével és a prevenció eszközök bővítésével kíván reagálni a kockázatokra. Nemzetközi dimenzióját tekintve a stratégia hangsúlyozza Magyarország aktív részvételét az Európai Unió kiberbiztonsági politikájában, különösen az EU Cybersecurity Strategy 2020–2025 dokumentum célkitűzéseinek megvalósításában, valamint a NATO kibervédelmi együttműködésében. Összegzőként elmondható, hogy a Nemzeti Kiberbiztonsági Stratégia nem csupán technológiai fejlesztési irányokat határoz meg, hanem átfogó, társadalmi szemléletű megközelítést alkalmaz. Olyan eszközrendszert kínál, amely figyelembe veszi az egyének – köztük a gyermekek – védelmi szükségleteit, és célja, hogy Magyarország digitális környezete biztonságos, ellenálló és mindenki számára hozzáférhető legyen.

8. ÖSSZEGÉS

A gyermekek digitális térben történő áldozattá válása napjaink egyik legsúlyosabb és legsürgetőbb társadalmi kihívása, amely nem csupán jogi, de pszichológiai, szociológiai és kiberbiztonsági szempontból is átfogó megközelítést igényel. A vizsgált témák egy közös nevezőre vezethetők vissza: hogyan lehet hatékony, gyermekközpontú védelmi rendszert kialakítani egy gyorsan változó, technológiavezérelt világban. A rutintevékenység-elmélet (Cohen & Felson, 1979) mentén történő megközelítés kiválóan alkalmazható az online térben tapasztalható jelenségek, így a gyermekek behálózásának, kizsákmányolásának és digitális bántalmazásának megértéséhez. Az elmélet rávilágít arra, hogy az áldozattá válás lehetősége gyakran a mindennapi digitális rutinokban rejlik – különösen akkor, ha a gyermek védtelen célponttá válik, és hiányzik a megfelelő felügyelet, illetve kontrollmechanizmus. E védelmi rések megszüntetésére több szinten is történnek előrelépések. Az Európai Unió Gyermekjogi Stratégiájának legfrissebb

módosításai hangsúlyozzák az integrált gyermekvédelmi rendszerek fontosságát, a digitális tér biztonságosabbá tételét, valamint a gyermekek tényleges bevonását a róluk szóló döntésekbe. A gyermekek aktív részvételére épülő uniós platformok, valamint a Better Internet for Kids+ (BIK+) kezdeményezés erősítik a prevenció szemléletét, miközben új eszközöket is bevezetnek, például az online szexuális visszaélések automatikus felismerésére. Magyarország Nemzeti Kiberbiztonsági Stratégiája (2021–2030) e törekvésekkel összhangban áll, és egyértelmű célként fogalmazza meg a digitális biztonság megerősítését, különös tekintettel a gyermekek védelmére. A stratégia kulcspontjai között szerepel a társadalmi tudatosság növelése, az oktatás digitalizációs kockázatainak kezelése, valamint az online zaklatással és kizsákmányolással szembeni fellépés. A kiberbiztonság így már nemcsak technikai kérdés, hanem gyermekvédelmi ügy is. A gyermekekkel szembeni súlyos bántalmazások kezelésére nemzetközi szinten a Barnahus-modell kínál példaértékű választ. Az Izlandról származó, de immár több európai országban bevezetett rendszer lényege, hogy a gyermekeket egy gyermekbarát, több szakmát integráló közegben hallgatják meg, és biztosítanak számukra azonnali pszichológiai, jogi és egészségügyi segítséget. A Barnahus nem csupán egy intézményi modell, hanem szemlélet, a másodlagos áldozattá válás elkerülését, valamint a traumaérzékeny igazságszolgáltatás megvalósítását helyezi a középpontba.

FELHASZNÁLT IRODALOM

- Article – Ofcom Media Use & Attitudes Report 2025 – KIDSONLINEWORLD.COM.
- DOMOKOS ANDREA: Gyermekáldozatok védelme az online világban. In: HOMICSKÓ ÁRPÁD OLIVÉR (szerk.): *A technológia fejlődés társadalmi kihívásai és hatása a jogi szabályozásra*. Budapest, Patrocinium Kiadó, 2022. Gyermekáldozatok védelme az online világban.
- Európai Bizottság COM (2022) 212 final. Digitális évtized a gyermekek és az ifjúság számára: a gyermekbarát internetre (BIK+) vonatkozó új európai stratégia.
- MEGYESFALVI BOGLÁRKA: Kockázati tényezők a digitális térben. A gyerekek internet- és közösségi média használata és az online áldozattá válás. *Belügyi szemle*, 2023 (12).
- Kockázati tényezők a digitális térben megtekintése | Belügyi Szemle.
- Online safety rules: what you need to know – Ofcom.
- Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. COM/2022/209 final.