DOI: 10.38146/BSZ.2023.12.3

Kockázati tényezők a digitális térben

A gyerekek internet- és közösségi média használata és az online áldozattá válás

Risk factors in the digital space

Children's Internet and social media use and online victimization

Meggyesfalvi Boglárka
kriminológus
Eötvös Loránd Tudományegyetem,
Állam- és Jogtudományi Kar
meggyesfalvi.b@gmail.com

Absztrakt

Cél: A tanulmány célja, hogy átfogóan vizsgálja a gyermekek tevékenységeit, az áldozattá válás kockázati tényezőit és egyes hatásait a digitális világban, az internethasználati szokásaikat és a közösségi média releváns működési sajátosságait. Kriminológiai szempontból releváns befolyásoló tényezőket azonosít, amelyek megkönnyítik a gyermekek elleni bűnelkövetést a digitális térben, és segíti megérteni, hogy milyen megelőző vagy kockázatnövelő szerepe lehet a fejlődő digitális technológiáknak a gyermekek online térben való védelmében.
Módszertan: A kutatás – kriminológiai elméleti keretekben – főként áttekinti és elemzi a releváns tudományos szakirodalom, szakpolitikai dokumentumok, jogi források és statisztikai adatok részleteit.
Megállapítások: A tanulmány rámutat, hogy a gyermekek jelentős mennyiségű időt töltenek a digitális térben, és ennek előnyei mellett növekszik az áldozattá válás kockázata is. A gyermekek érzelmi sebezhetőségére és az online bántalmazás hatásaira való figyelemfelhívás kiemelten fontos a megelőzés és kezelés során. A szabályozás és az intézkedések folyamatos javítása, a nemzetközi jó gyakorlatok figyelemmel kísérése, a fejlődő technológiák és trendek megismerése és megfelelő kezelése, illetve a szereplők közötti együttműködés elősegíthetik a gyermekek hatékonyabb védelmét az online világban.
Érték: A tanulmány hozzájárul a gyermekek internethasználati szokásai és a velük járó kockázatok jobb megértéséhez, valamint az online áldozattá válásuk

folyamatainak és körülményeinek feltárásához. Emellett elősegíti a hatékony rendészeti és szabályozási gyakorlatok, a gyermekvédelmi protokollok és együttműködések kialakítását, kiemelten figyelembe véve az áldozatvédelmi és gyermekjogi szempontokat.

Kulcsszavak: online áldozattá válás, internethasználat, gyermekvédelem, online gyermekbántalmazás

Abstract

Aim: The aim of the study is to provide a comprehensive analysis of children's Internet usage and their activities in relation to the risk factors and some of the effects of victimisation in the digital world, besides looking at a few of the relevant functional characteristics of social media. By identifying pertinent criminological factors that contribute to harmful behaviours targeting children in the cyber domain, this research contributes understanding of the preventive measures or potential risks associated with online victimisation and the development of digital technologies in safeguarding children online.
Methodology: The research mainly reviews and analyses relevant data from academic literature, policy documents, legal sources and statistics in a criminological theoretical context.
Findings: The study highlights that children dedicate a substantial amount of time to the digital space, and alongside its advantages, the risk of becoming victims also escalates. Drawing attention to children's emotional vulnerability and the effects of online abuse is particularly crucial in terms of prevention and intervention. Constant enhancement of regulations and measures, diligent monitoring of international best practices, comprehending and effectively addressing emerging technologies and trends, as well as promoting collaboration among stakeholders, can facilitate a more effective safeguarding of children in cyberspace.
Value: The study facilitates a better comprehension of children's internet usage habits and the risks inherent in them, as well as the processes and circumstances leading to online victimisation, thereby promoting the development of law enforcement and regulatory practices that prioritise effective victim protection and the consideration of children's rights. Additionally, it aids in the establishment of child protection protocols and collaborations that take into account the aforementioned aspects.

Keywords: online victimisation, internet use, child protection, online child abuse

Bevezetés

A tanulmány kísérletet tesz arra, hogy friss kutatások alapján megvizsgálja, mit tudunk a gyermekek internethasználati szokásairól, tevékenységeikről a digitális világban, illetve azt is, hogy a közösségi média működési sajátosságai milyen hatással vannak a gyermekek online áldozattá válására. Körbejárja, hogy milyen – kriminológiai szempontból releváns – befolyásoló tényezők könnyítik meg a gyermekek ellen irányuló bűnelkövetést a digitális térben. Kitér az online behálózás (grooming) folyamatára és lehetséges hatásaira, kiemelve azokat a komplex érzelmi kihívásokat, amikkel az online bántalmazást túlélő gyerekek szembesülhetnek, illetve nemzetközi jó gyakorlatokat szemléltetve a bűncselekmények kezelését is bemutatja. Elemzi egyes fejlődő digitális technológiák szerepét a megelőzésben. Mindezt annak szem előtt tartásával, hogy a téma összetettségének megértése egyaránt előmozdíthatja az áldozattá vált kiskorúak szakmai megsegítését, a prevenciót, illetve a gyermekek jogainak tiszteletben tartását a digitális világban a nekik megfelelő felületek használata során, beleértve az olyan tevékenységek folytatását, mint a tartalomfogyasztás, a szórakozás, az ismerkedés, vagy az intim kapcsolatok kialakítása és fenntartása.

A gyerekek internethasználati szokásai

2021-ben majdnem minden 5–15 éves gyermek naponta töltött időt az interneten (Ofcom, 2021). Egy reprezentatív kutatás szerint (Childwise, 2021) a gyermekek internethasználata az életkor és az idő múlásával növekszik, és a COVID–19-járvány idején a 2021-es évben további, példátlan mértékű bővülés következett be: a internetezéssel töltött órák száma a gyermekek esetében 10%-kal, napi 3,8 órára emelkedett. A fiatalok 83%-a már a hálószobájából, magáncélra is hozzáfér az internethez, és a szülők az első járványügyi lezárások óta egyre nehezebbnek érezték gyermekeik online tevékenységeinek felügyeletét (Childwise, 2021). A Nemzeti Média- és Hírközlési Hatóság kutatása (NMHH, 2021) szerint 2017 óta jelentős növekedést láthatunk a saját mobiltelefonnal rendelkező magyar gyerekek arányában is, például a 7–8 évesek körében ez az arány 14%-ról 24%-ra nőtt, a 15–16 éveseknél 2020-ra pedig elérte a 96%-ot. A kutatás szerint a magyar gyermekek átlagosan tízéves korukban kaptak először saját mobiltelefont.

A fiatalok számos okból használják az internetet, többek között olyan pozitív és konstruktív tevékenységek folytatásához, mint a tanulás vagy a minőségi szórakozás; de ezen kívül az is fontos számukra, hogy az internethozzáférés 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 (Livingstone & Brake, 2010).

Gyakorlatilag minden gyermek használ olyan videómegosztó felületeket és alkalmazásokat, mint a YouTube vagy a TikTok. Jelentős többségük más közösségimédia-platformokat is, például a Facebookot vagy az Instagramot, és a 12–15 évesek 91%-a naponta használ olyan azonnali üzenetküldő alkalmazásokat, mint a Messenger vagy a WhatsApp (Ofcom, 2021). Az Európai Unióban élő 6–10 éves gyermekek 73%-a, a 11–14 éves gyermekek 84%-a játszik rendszeresen online videojátékokkal (Smahel et al., 2020).

Az internethasználat tekintetében a magyar gyermekek is egyre több időt töltenek online: 2020-ban a 9–10 évesek az iskolán kívül naponta átlagosan 1,5–2 órát, míg a 15–16 évesek napi 2,5–4 órát töltöttek az interneten (NMHH, 2021). Magyarországon is nőtt a gyermekkorúak jelenléte a regisztrációhoz kötött közösségimédia-oldalakon, különösen a 9–12 évesek körében: a legnépszerűbb közösségimédia-felület a Facebook, a YouTube, az Instagram és a TikTok volt, a regisztrált taggá válás korhatára lejjebb csúszott, 2020-ban már átlagosan 10–11 éves korra (NMHH, 2021). A gyermekek nagy része meg szokta adni az igazi nevét és fényképét a közösségi médiában, és minden ötödik gyermeknek volt olyan ismerőse, akit személyesen még sohasem látott (NMHH, 2021). A növekvő internethasználat ellenére a szülők több mint 20%-a egyáltalán nem aggódott, hogy a gyermeke idegenekkel állhat kapcsolatban online, vagy kéretlenül intim fotót kaphat, vagy intim fotót kérhetnek tőle, vagy szexuális tartalommal találkozhat (NMHH, 2021).

Egyrészt az online felületeknek a használata megkönnyíti a gyermekek számára az olyan jogok gyakorlását, mint az új ismeretekhez való hozzáférés, az érdeklődési körük, identitásuk felfedezése és az önkifejezés, a szórakozás, valamint a másokkal való kapcsolatteremtés és interakció. Másrészt kutatások alátámasztották, hogy az olyan nyíltan hozzáférhető, közvetlen kommunikációs csatornák használata, mint a Messenger és a Discord, az egyének láthatóságának fokozásával megnövelték az interperszonális viktimizáció lehetőségét az online térben (Holt et al., 2017). Ez azt jelenti, hogy a kibertérben töltött több idő potenciálisan megnövekedett kockázatnak és ártalomnak teheti ki a gyermekeket. Ennek megelőzése és hatékony kezelése érdekében érdemes a kriminológia elméleti kereteiben vizsgálni az internet néhány olyan egyedi jellemzőjét, amelyek befolyásolhatják a gyermekek online védelmét és biztonságát a világhálón, beleértve a közösségi média működési sajátosságait, illetve a dinamikusan fejlődő modern digitális technológiák hatását a kiskorúak online áldozattá válására.

A gyermekek online áldozattá válása rutintevékenység-elméleti megközelítésben

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. Az elmélet kidolgozói, Cohen és Felson (1979) azzal érveltek, hogy a „ragadozótípusú szabályszegések" akkor következnek be, ha három alkotóelem ugyanakkor van jelen, ugyanabban a térben, három olyan alkotóelem, amelyek a kriminológusok szerint a kibertérben is egyidejűleg jelen lehet: egy motivált és kompetens elkövető; egy megfelelő célpont, tehát például egy olyan potenciális áldozat, mint egy sebezhető, felnőtt felügyelet nélkül internetező gyermek; illetve egy alkalmas őrző hiánya, ami lehetne egy védelmező személy, vagy egy megfelelően beállított/beüzemelt biztonsági rendszer (Holt et al., 2017).

Ahogy Yar (2019) rámutat, további tényezők is befolyásolhatják, elősegíthetik az online térben megvalósuló kizsákmányolást. Az első ilyen tényező a téridő koncentráció, amely lehetővé teszi a fizikailag távoli helyeken élő felek azonnali kommunikációját, például az információk egy szempillantás alatt történő megosztásával. Ez alatt érthető az erőszakos, illegális tartalmak globális élő online „közvetítése", csakúgy mint annak a lehetősége, hogy az elkövetők egymást segítve online hozzáférést szerezhetnek rendőrségi tevékenységekhez, adatbázisokhoz, és megnehezíthetik a bűnüldözési tevékenységeket, mindezt távolról, akár anélkül, hogy „valós életbeli" kapcsolatuk lenne, és ismernék egymás valódi személyazonosságát.

A második tényező a multiplikátorhatás, mely lehetővé teszi a korlátozott erőforrásokkal rendelkező egyének számára, hogy akár rendkívül csekély ráfordítással olyan rendkívül káros és gyorsan terjeszthető digitális tartalmakat állítsanak elő, mint például a gyermekek otthoni környezetében megörökített szexuális bántalmazása. Ezt a bűncselekménytípust akár könnyen beszerezhető és eldobható, olcsó okostelefonok segítségével is meg lehet valósítani, majd a gyermekbántalmazást ábrázoló anyagokat könnyen elérhetővé tenni, és ingyen, akár profilért cserébe illegális online kereskedelmi felületeken keresztül terjeszteni.

A harmadik tényező az internet anonim jellege. Az anonimitás lehetőséget nyújt a bűnözőknek ahhoz, hogy beazonosíthatatlanok maradjanak, vagy inkognitóban tevékenykedjenek, elválasztva online személyiségüket valós

személyazonosságuktól, ami nagy mértékben megnehezíti, bonyolulttá és erőforrás-igényessé teszi a nyomozást és a büntetőeljárás sikeres lefolytatását (Europol, 2021). Az anonimitás ráadásul megkönnyítheti a bűnelkövetést azáltal, hogy az ezt erősítő titkosítási módszerek, alkalmas eszközök könnyen elérhetőek, megvásárolhatóak a világhálón, illetve a beazonosíthatatlanság érzése előidézheti a motivált elkövetőben a büntetlenség vagy büntethetetlenség érzését (Grund, 2021).

Online áldozattá válás és behálózás

A rutintevékenység-elmélet három alkotóeleme és az online kizsákmányolást befolyásoló további tényezők online térben való egyidejű érvényesülése, valamint a fentebb vázolt internethasználati statisztikák tükrében a gyermekek online áldozattá válása egyre valószínűbbé válik, főleg mivel a kutatások alapján folytatódik az a trend, hogy életük egyre nagyobb százalékát töltik felügyelet nélkül az interneten, ezzel megfelelő célpontokat kínálva az elkövetők számára. A brit állami kommunikációs hivatal, az Ofcom (2021) feltárta, hogy a gyermekek leggyakoribb negatív élményei az interneten ahhoz kötődtek, amikor ismeretlen személyek léptek kapcsolatba és próbáltak meg barátkozni velük. Ez a brit tinédzserek közel egyharmadával fordult már elő, míg egy magyar kutatás szerint a magyar gyerekek 28%-ánál volt megfigyelhető az online ismerkedés kapcsán kockázatos tevékenység (NMHH, 2021). A rosszindulatú ismeretlenekkel való kommunikáció különösen kockázatos lehet olyan kevés személyes kapcsolódásra lehetőséget nyújtó időszakokban, mint például a COVID–19-világjárvány körüli hónapok-évek, amikor a gyermekek közül aggasztóan sokan (62%-uk) érezték úgy, hogy magányosak (Childwise, 2021), ami potenciálisan kiszolgáltatottá tette őket az érzéseiket megértő, magukat barátságos ismerősöknek álcázó online elkövetők általi behálózásra és kizsákmányolásra.

Míg a gyerekek saját elmondásuk szerint arra használják az internetet és a közösségimédia-oldalakat, hogy valódi új barátokat szerezzenek (Livingstone & Brake, 2010), kutatási eredmények azt mutatják, hogy felnőtt bűnelkövetők a kibertérben új személyazonosságot vesznek fel, és szexuális és kereskedelmi kizsákmányolás céljából a közösségi oldalakon próbálják a kiskorúakat behálózni (Bryce et al., 2019). Gámez-Guadixet és munkatársai (2018) kutatásukban megállapították, hogy körülbelül minden második elkövető tévesztette meg sikeresen a gyerekeket a saját online identitásával kapcsolatban, tehát hazudott arról, hogy hány éves, hamis képeket osztott meg másokról az tettetve, mintha őt ábrázolnák, vagy digitálisan manipulálta a magáról megosztott képeket

azért, hogy szimpatikusabbnak vagy vonzóbbnak tűnjön. Magyarországon is több ilyen ügyet derített fel a rendőrség az elmúlt években, többek között egy esetet, amely során egy Zala vármegyei középkorú férfi népszerű internetes játékokon keresztül 9 és 17 év közötti kiskorúakat különböző profilokon keresztül próbált szexuális cselekményekre rávenni, magát konzekvensen hasonló korúnak hazudva (URL1), vagy amikor egy monori kamasz fiút tévesztettek meg fiú ismerősei, magukat lánynak hazudva, és csaltak ki tőle intim képeket, majd ezeket feltöltötték az internetre, és megosztották másokkal (URL2).

A behálózás az a folyamat, amikor az elkövető szándékosan olyan cselekményeket hajt végre, melyek célja, hogy közel kerüljön egy gyermekhez, és érzelmi kapcsolatot alakítson ki vele azért, hogy csökkentse az áldozat gátlásait a szexuális tevékenységre előkészítése érdekében (Bryce et al., 2019). Az egyik első nemzetközi figyelmet kapott online behálózás ügy a 15 éves Ryan Carly nevű lány esete volt, amelyről a The Carly Ryan Foundation (URL3) honlapja is hitelesen számol be. Carly volt az első olyan gyermek Ausztráliában, akiről kiderült, hogy egy online szexuális ragadozó áldozatává vált. A lány összebarátkozott „Brandonnal", egy fiktív fiatal amerikai zenésszel, aki a valóságban egy 50 éves férfi volt. Az online kapcsolat egyre romantikusabbá vált, és Carly részéről szerelemmé alakult. Anyja ellenérzéseit figyelmen kívül hagyva a tizenötödik születésnapja után elment otthonról, hogy találkozzon „Brandonnal", ekkor gyilkolta meg a férfi és egy társa. A rendőrség megállapította, hogy a férfi, aki az internet segítségével az utolsó pillanatig fenntartotta a szerető barát álcáját, egy jegyzetfüzetet tartott magánál, amely mintegy 200 online identitásának leírását tartalmazta, olyan profilok információit, amelyeken keresztül gyerekeket hálózott be és csábított el. A Carly halálát követő, törvénymódosítást indítványozó országos kampány hatására az ausztrál parlamentben előterjesztették és elfogadták az ausztrál büntető törvénykönyv kiskorúak online védelméről szóló törvényének módosításáról szóló 2017. évi törvényjavaslatot, amely minősített esetként szabályozta, és magasabb büntetési tételt szabott ki arra az elkövetőre, aki egy kiskorúnak kárt okozó, tervezett cselekmény részeként életkorát hamisan tünteti fel az interneten.

A behálózás bármely formája, beleértve az online behálózást is, a nyugati világ nagy részében illegális (Bryce et al., 2019), mivel súlyosan káros következményekkel jár az áldozatokra nézve. Az ilyen cselekményeket Magyarországon a 2012. évi C. törvény a Büntető Törvénykönyvről szankcionálja, adott esetek és magatartások függvényében például a gyermekpornográfia, a szexuális visszaélés vagy erőszak, a személyes adattal visszaélés, vagy más bűncselekmények körében. Az áldozatokkal való bizalmi kapcsolat kiépítésére és a viselkedésük manipulációjára irányuló behálózási technikák közé tartozik a kiszolgáltatott

gyerekekkel való szexuális érdekből történő barátkozás, a számukra értéket képviselő dolgok ajándékozása (beleértve a fizikai tárgyak mellett az olyan, gyermekek által gyűjtött online „javakat", mint például a digitális fizetőeszközök egy virtuális játékban/felületen), a megvesztegetés vagy a zsarolás, a pozitív családi vagy más bizalmi személyektől vagy szociális védőhálótól való célzott elszigetelés, valamint az, amikor az elkövető az áldozat védelmezőjének vagy segítőjének adja ki magát (Martellozo & Jane, 2017; Gámez-Guadixet et al., 2018). A korábban említett, Zala vármegyei férfi esetében például az ügyészségi vádirat szerint a férfi módszerei közé tartozott, hogy a gyerekek profiljaihoz megszerezte a jelszavakat és a hozzáférést azzal, hogy egy internetes játékon belül pénzt küldött és további segítséget ajánlott nekik, majd lerombolta az addig felépített virtuális városaikat, és megzsarolta őket profiljuk letiltásával, amennyiben nem küldenek neki szexuális tartalmú képeket (URL1).

Az is gyakran előfordul, hogy az elkövető meggyőzően használja a dicséreteket, vagy úgy tesz, mintha romantikus érzelmeket táplálna a kiszemelt gyermek iránt, elhitetve vele, hogy különleges és közös beleegyezésen alapuló intim kapcsolatban állnak egymással. Ez egyes serdülők esetében azzal a következménynyel járhat, hogy a fiatalban mély, valódi érzéseken alapuló hűség és szeretet alakul ki, ami miatt rendkívül nehéz lehet megérteniük, hogy félrevezették és becsapták őket; így előfordulhat, hogy nem ismerik fel, hogy áldozattá váltak, és nem hajlandóak feljelentést tenni vagy tanúskodni/terhelő vallomást tenni a bántalmazó ellen (Tener et al., 2015). A hosszú távú bántalmazás következtében a gyermekekben fokozatosan káros kötődés alakulhat ki a bántalmazó iránt, olyan Stockholm-szindrómához hasonló kapcsolat, melyben a túlélők önmagukat hibáztatják, és védik a szexuális gyermekbántalmazás elkövetőjét azáltal, hogy felelősséget vállalnak az ellenük elkövetett bűncselekményekért (Sanchez et al., 2019). Ez gyakran párhuzamos folyamat azzal, hogy a túlélő-áldozat a kényszerítő kapcsolat megszűnésekor bűntudatot és elhagyatottságot tapasztal, ami a környezetében élők számára hihetetlennek tűnhet (Sanchez et al., 2019). A túlélők sérülékeny lelki állapotára reflektál az a Magyarországon is hatályos szabályozás,[1] miszerint a gyermekek szándékos kizsákmányolásába való beleegyezése nem vehető enyhítő körülményként sem figyelembe.

Annak felismerése és feldolgozása, hogy a bántalmazóval való kapcsolat nem volt egészséges, és egy káros befolyású, bántalmazó emberben bízott meg az áldozat, egy sokrétű, fájdalmas és hosszú gyógyulási folyamat része lehet (Sanderson, 2013). A gyógyulási és feldolgozási folyamat járhat újratraumatizálódással,

1 2013. évi XVIII. törvény az Európa Tanács Emberkereskedelem Elleni Fellépésről szóló Egyezményének kihirdetéséről.

és olyan mentális problémák megjelenésével, mint a szorongás, a depresszió, szörnyű flashbackek átélése, kötődési problémák, az alacsony önértékelés, az addiktív viselkedés és az öngyilkossági hajlam; így az áldozat támogatása szakemberek tudását és segítségét igényli. Az online behálózást túlélő gyermekekkel foglalkozó szakembereknek, például a gyermekpszichológusoknak, gyakran kell foglalkozniuk a terápiás munka keretében az áldozatok veszteség- és gyászérzéseivel, mielőtt segíteni tudnának benne, hogy megkeressék, újra felállítsák érzelmi és pszichológiai határaikat, és újra tanulják az alapvető kapcsolatkezelési készségeket, beleértve az online térben történő kapcsolódást (Sanderson, 2013).

A kibertérben szexuális bántalmazás áldozattá vált gyermekekkel való bűnüldözői és segítői munka kapcsán is kiemelten fontos figyelni és megfelelően kezelni azt a jelenséget, hogy a gyermek esetleg (még) nem érzi magát készen arra, hogy a felderítő vagy vizsgálati folyamatok során beismerje a bántalmazó kapcsolat káros voltát és aszimmetrikus hatalmi jellegét, illetve hogy az elkövetők gyakran próbálják az önfelmentés és az áldozathibáztatás eszközeivel azt sugallni, hogy valójában a gyermekek voltak azok, akik „elcsábították" őket (Martellozzo & Jane, 2017). Az Egyesült Királyságban ezért a gyermekek szexuális kizsákmányolási formáit, köztük a behálózási tevékenységeket kriminalizáló, 2003-tól hatályos kommunikációs törvény nem követeli meg, hogy a gyermek az elkövetővel való kommunikációt kellemetlennek érzékelje (Pegg, 2017). Ehelyett a jogalkotó az elkövető viselkedésének szándékos jellegére összpontosított, tehát arra, hogy a gyermekkel való kommunikáció eredendően vagy objektíve szexuális jellegű volt-e, illetve hogy szexuális tartalmú válaszreakció kiváltása volt-e a célja (Pegg, 2017).

A fejlődő digitális technológiák és a közösségi média szerepe a gyermekek online áldozattá válásában

Az olyan gyorsan fejlődő új digitális technológiák, mint az élő online közvetítéseket (angolul live-streaming) lehetővé tevő szoftverek, a végpontok közötti titkosított (angolul end-to-end encryption) üzenetküldő szolgáltatások, vagy az olyan anonim fizetési módszerek, mint például a kriptovaluták elterjedése, mind megkönnyítették a gyermekek online behálózását, és a digitális szexuális gyermekbántalmazási tartalmak előállítását (Europol, 2021). Ezek a technológiák lehetővé teszik az elkövetők számára, hogy nehezen felderíthető és kinyomozható módokon működjenek, és segítségükre szolgálnak abban, hogy hálózatokat építsenek ki, információkat osszanak meg egymással, illetve bárhonnan és bármikor bűncselekményeket követhessenek el kiskorúak ellen, akár egyszerre

több áldozatot megcélozva. Bár a technológiai fejlődést és az új eredményeket lehetetlen lenne megállítani vagy visszafogni – sőt, a bűnüldöző szerveknek és az online biztonságtechnológiai vállalkozásoknak vitathatatlanul szükségük van arra, hogy a digitális fejlődés tekintetében megelőzzék a bűnözői hálózatokat, és proaktívan lépjenek fel az online bűncselekmények megelőzése és megakadályozása érdekében (Davidson et al., 2016) –, azonban azt szükséges gondosan szabályozni, hogy a közösségimédia-vállalatok milyen szabályozási környezetben és garanciák mellett alkalmazhatják ezeket a technológiákat. Jelenleg számos olyan nemzetközi irányelv és jogszabálytervezet van előkészítés alatt, amelyek célja a közösségimédia-platformok szabályozása, és ezáltal a sérülékenyebb csoportok, kiemelten a gyermekek védelme az online ártalmaktól.

Ezek közé tartozik az Egyesült Királyságban az online biztonságról szóló 2022-es évi törvényjavaslat (Online Safety Bill) és az Európai Unió digitális szolgáltatásokról szóló törvényjavaslata is; mindazonáltal úgy tűnik, hogy általánosságban továbbra is kihívást jelent az online biztonsággal kapcsolatos felelősségek egyértelmű kijelölése a különböző érdekelt felek között (Meggyesfalvi, 2021). Az Instagram, a Facebook, a TikTok és a többi, kiskorúak körében rendkívül népszerű közösségimédia-platform működési módja – például a moderálás formája, alaposssága 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",[2] illetve legújabb, a gyermekek online szexuális bántalmazásának megelőzése és az ellene folytatott küzdelem érdekében kidolgozott és előterjesztett uniós rendeletjavaslatát,[3] 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 szorgalmazzák továbbá egy európai központ létrehozását, melynek feladata lesz a gyermekek szexuális kizsákmányolásának megelőzésére és leküzdésére szolgáló szervezetek koordinációja, kapcsolódó kutatási és szakértői

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

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

tevékenységek, az áldozatok támogatása, valamint – megkönnyítve a nemzeti rendészeti szervek munkáját – a gyermekek online szexuális bántalmazásával összefüggő ügyek felderítésének, bejelentésének és kezelésének támogatása is.

Úgy tűnik azonban, hogy 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 biztonsági fejlesztésekre fordítani (Meggyesfalvi, 2021). Ennek aktuális példája, hogy 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 jótékonysági szervezetek, digitális technológiai szakértők, és áldozat-túlélők 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. 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 azáltal, hogy sem a moderátorok, sem a gépi algoritmusok nem lesznek képesek a gyanús vagy káros tartalmakat azonosítani (BBC, 2022). Állításuk szerint, ha a bevezetést tervező közösségimédia-vállalatok nem állítják le ennek a technológiának az alkalmazását, évente mintegy 14 millió feltételezett, gyermekekkel szembeni online szexuális kizsákmányolási esetet nem jelentenek majd be ezután.

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 (BBC, 2022).

A végpontok közötti titkosítás azonban nem az egyetlen olyan technológia, ami miatt a bűnüldöző szervek és a gyermekvédelmi szakemberek aggódnak a gyermekek és a bűnözők internethasználatával kapcsolatban. Az életkor-ellenőrzés a másik vitatott kérdés. Amikor a felhasználók regisztrálnak a közösségimédia-platformokra, adatokat kell megadniuk magukról, általában olyan információkat, mint a név, a lakcím, a nem és az életkor. A legtöbb közösségimédia-szolgáltató – különösen azok, amelyekről ismert, hogy kockázatosak

a felületeiket nagy arányban (ki)használó online szexuális bűnelkövetők miatt, mint például az Instagram, a Facebook és a Tiktok – a belépést életkorhoz kötő, korlátozó tagsági irányelvekkel rendelkeznek, amelyek célja elvileg az, hogy megakadályozza a fiatalabb gyermekek hozzáférését a szolgáltatásaikhoz. Egy 2020-as tanulmány (Pasquale & Zippo, 2020) a gyermekek által leggyakrabban használt tíz közösségimédia-alkalmazást vizsgálva megállapította, hogy három kivételével (Discord, Messenger és WhatsApp) mindegyik kért a felhasználó életkorára vonatkozó nyilatkozatot a regisztrációkor. A legtöbb esetben az olyan személyeket, akik 13 évesnél fiatalabbnak vallották magukat, nem engedték volna tovább. Amikor azonban valaki regisztrál az ilyen felületekre, a beírt adatokat automatizált, gépi technológiával ellenőrzik. Annak megítélése, hogy a potenciális jövendő felhasználó megfelelő-e életkorú-e egy profil létrehozásához általában emberi interakció nélkül történik, nagyrészt a potenciális felhasználó által megadott adatokra támaszkodva. Ez azt jelenti, hogy a fiatalabb és sérülékenyebb gyerekek különösebb erőfeszítés nélkül idősebbnek adhatják ki magukat, egyszerűen hozzáférhetnek ezekhez a felületekhez, ugyanúgy, ahogyan az online szexuális ragadozók is bármilyen személyazonosság-változást beállíthatnak a profiljukban, hazudva korukról, nemükről vagy fizikai megjelenésükről, akár hamis profilképek illusztratív felhasználásával *(*Bryce et al., 2019*)*. Egy kutatásban megállapították (Pasquale & Zippo, 2020), hogy a gyerekek valóban könnyedén megkerülhetik a legnépszerűbb közösségimédia-platformok összes életkor-ellenőrzési mechanizmusát a hamis életkor megadásával, és bizonyára a rosszindulatú felnőttek is ugyanilyen könnyen adnak meg hamis adatokat magukról ellenőrizhetetlenül.

Martellozzo és Bradbury kriminológusok (2021) azzal érveltek, hogy amíg a kockázatos és potenciálisan káros online felületeken és alkalmazásokban nem vezetnek be hatékonyabb életkor-ellenőrzési eszközöket és folyamatokat, addig nem lehet garantálni az ezeket előszeretettel használó gyermekek tényleges online védelmét és biztonságát. Amennyiben a felületeket üzemeltető vállalkozások valóban elkötelezik magukat amellett, hogy technológiai és folyamatfejlesztési szempontból is megerősítsék a gyermekek online védelmét, akkor a sebezhető, megfelelő digitális kompetenciák hiányában lévő gyerekek belépésének megakadályozását prioritásként kell kezelniük az általuk generálható profitszerzéssel szemben, amely profitba jelenleg beleértendőek azok az összegek is, melyeket a gyermekek online szexuális kizsákmányolásából eredő felhasználói tevékenység termel, például a bűnelkövetők aktivitása, termékhasználata után befolyó hirdetési jutalékok formájában. 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 (Meggyesfalvi, 2021).

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 (Davidson et al., 2017). Kutatások emellett arra is rámutattak, hogy a fiatal felhasználók nem használják ki a közösségimédia-platformok jelentési és egyéb biztonsági funkcióit, mivel bonyolultnak és nehezen érthetőnek tartják azokat (Davidson et al.,2017). Egy 2021-es kutatásban megállapították, hogy bár a gyerekek körében magas a bejelentési funkciók ismertsége (70% a 12–15 évesek körében), ennek ellenére csak kis százalékuk (a 12–15 évesek 14%-a) jelentett valaha káros tartalmakat vagy negatív online tapasztalatokat (Ofcom, 2021). Ezért megállapítható, hogy amíg a közösségimédia-vállalatok nem hoznak érdemi lépéseket, fejlesztve a gyermekek online védelmét biztosító technológiákat, és a felhasználókat érintő intézkedéseket implementálva – egyidejűleg visszaszorítva a motivált elkövetők bűnelkövetési lehetőségeit és ellehetetlenítve az áldozatok könnyű célponttá válását, továbbá csökkenteni próbálva a multiplikátorhatást és az online anonimitásban rejlő kockázatokat –, addig a gyermekek biztonsága az interneten valószínűleg továbbra is veszélyben marad, növekvő kihívásokat okozva a bűnüldöző és áldozatsegítő szervezetek számára.

Összefoglalás és következtetések

A tanulmány kísérletet tett arra, hogy kontextusba helyezze a gyerekek internethasználati szokásait, és bemutassa az ezzel kapcsolatos növekvő kockázatokat az áldozattá válás kapcsán. Bemutatta, hogy ma már gyakorlatilag minden kiskorú jelentős mennyiségű időt tölt a digitális térben, ahol veszélyeztetettségüket olyan tényezők növelik, mint az alkalmas védő személyek és technológiai biztonsági funkciók megfelelő rendelkezésre állásának és alkalmazásának hiánya, illetve a jelentős számú, a világ minden pontjáról bármikor becsatlakozni képes bűnelkövetők sokasága, beazonosíthatatlansága, és egyszerűen elérhető hatásossága a potenciális károkozásban. Az elemzés kitért a gyermekek érzelmi kitettségére és befolyásolhatóságára az online behálózásuk következtében, és a közösségimédia-platformok felelősségére a bűnmegelőzésben. Hangsúlyozta, hogy a kiskorúak érzelmi involváltságát az elkövetővel, a létrejövő kötődési nehézségeket és negatív pszichés hatásokat figyelembe kell venni az áldozattá

válás komplex, sokrétű jelenségének megelőzése és kezelése kapcsán, differenciált – és akár az idő elteltével változó – megoldásokat kínálva az áldozat adott érzelmi állapotától és helyzetétől függően. Bár Magyarországon is vannak már a jogszabályok által garantált áldozatvédelmi intézkedések a gyermekek vonatkozásában (például a rendőrség által akkreditált, gyermekbarát meghallgató helységek bevezetése, a különleges bánásmódot igénylő személyek kezelésével kapcsolatos szabályozások és utasítások, vagy az általános védelmi intézkedés kapcsán bevezetett eljárások), ezek gyakorlati megvalósulásáról fontos lenne pontosabb képet kapni, fejleszteni az ellátórendszert a digitális térben áldozattá váló gyermekekre (is) koncentrálva, illetve tudományos alapossággal vizsgálni hatásosságukat, és fokozottan ügyelni az eljárások gyermekjogi szemléletű megvalósulására.

Nem feledkezhetünk meg a szülői felelősségről sem. A digitális térben való kockázatkezelés és a gyermekvédelem terén a technológiai vállalatoktól vagy fejlesztésektől sem várható el, hogy teljes megoldást nyújtsanak. Hangsúlyozni kell, hogy a szülői felügyelet mellett az oktatás és a digitális higiénia fontossága alapvető szerepet játszik a gyermekek védelmében. Az internetes biztonsági intézkedések, a biztonságos online viselkedés és a digitális személyes adatvédelem ismeretei nélkülözhetetlenek a mai digitális világban. Az oktatási intézményeknek és a szülőknek egyaránt szembe kell nézni ezekkel a kihívásokkal, és a lehető legjobban megtanítani a gyermekeket az online kockázatok felismerésére, valamint azok kezelésére.

Bár számos fontos témakört, például a cyberbullying egyes fajtáit, a gyermekek online felületeken öngyilkosságra való rábírását vagy felbujtását, vagy a káros online kihívások témaköreit nem volt lehetőség ennek az írásnak a keretein belül vizsgálni, a tanulmányban felvetett, a gyermekek által a digitális világban megtapasztalt problémáknak csak egy szűkebb körét tárgyaló témák is világosan mutatják, számos megoldandó kihívással néz szembe a magyar és nemzetközi jogalkotási terület mellett a bűnmegelőzés és a bűnüldözés is. Ezek fel- és megismerése után kiemelten fontos, hogy a kiskorúak védelmében a gyermekeket érintő valós digitális tendenciákat és a nemzetközi jó gyakorlatokat megismerve, ezek tudatában születhessenek olyan stratégiák és akciótervek, melyek proaktívan és eredményesen tudják az őket érintő, növekvő kockázatokat kezelni, együttműködésre ösztönözve a piaci, állami és egyéb szereplőket az online áldozattá válás megelőzése és megfelelő kezelése érdekében.

Felhasznált irodalom

BBC (2022). 'New campaign aims to stop more encrypted apps'. *BBC News, 18 January*.

Bryce, I., Robinson, Y. & Petherick, W. (2019) *Child abuse and neglect: forensic issues in evidence, impact and management*. Academic Press.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Childwise (2021). *The Monitor Report 2021*. CHILDWISE Research.

Davidson, J., DeMarco, J., Bifulco, A., Bogaerts, S., Caretti, V., Aiken, M., Chevers, C., Corbari, E., Scally, M., Schimmenti, A. & Puccia, A. (2016). *Enhancing police and industry practice.* Middlesex University.

Europol (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Publications Office of the European Union. https://doi.org/10.1016/S1361-3723(21)00125-1

Gámez-Guadix, M., Almendros, C., Calvete, E. & De Santisteban, P. (2018). Persuasion strategies and sexual solicitations and interactions in online sexual grooming of adolescents: Modeling direct and indirect pathways. *Journal of Adolescence, 63*(1), 11–18. https://doi.org/10.1016/j.adolescence.2017.12.002

Grund B. (2021). A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. *MTA Law Working Papers, 8*(21), 2-34.

Holt, T. J., Bossler, A. M. & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction.* Routledge. https://doi.org/10.4324/9781315296975

Livingstone, S. & Brake, D. R. (2010). On the rapid rise of social networking sites: New findings and policy implications. *Children & Society, 24*(1), 75–83. https://doi.org/10.1111/j.1099-0860.2009.00243.x

Martellozzo, E. & Jane, E. A. (2017). *Cybercrime and its victims*. Routledge. https://doi.org/10.4324/9781315637198

Martellozzo, E. & Bradbury, P. (2021). How the pandemic has made young people more vulnerable to risky online sexual trade. *Blogs LSE*, 2 March.

Meggyesfalvi, B. (2021). Policing harmful content on social media platforms. *Belügyi Szemle*, *69*(6ksz), 26–38. https://doi.org/10.38146/BSZ.SPEC.2021.6.2

NMHH (2021). *Digital parenting kutatás 7–16 éves gyerekekkel és szüleikkel.* Psyma Hungary Kft.

Ofcom (2021). *Children and parents: media use and attitudes report 2020/2021.* Ofcom.

Pasquale, L. & Zippo, P. (2020). *A Review of Age Verification Mechanism for 10 Social Media Apps.* UCD Dublin.

Pegg, S. (2017). *Online grooming and the law.* The Law Society Gazette.

Sanchez, R. V., Speck, P. M. & Patrician, P. A. (2019). A concept analysis of trauma coercive bonding in the commercial sexual exploitation of children. *Journal of pediatric nursing*, *68*(3), 48–54. https://doi.org/10.1016/j.pedn.2019.02.030

Sanderson, C. (2013). *Counselling skills for working with trauma: Healing from child sexual abuse, sexual violence and domestic abuse.* Jessica Kingsley Publishers.

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.

Tener, D., Wolak, J. & Finkelhor, D. (2015). A Typology of Offenders Who Use Online Communications to Commit Sex Crimes Against Minors. *Journal of Aggression, Maltreatment & Trauma, 24*(3), 319–337. https://doi.org/10.1080/10926771.2015.1009602

Yar, M. & Steinmetz, K. F. (2019). *Cybercrime and society*. Sage Publications.

A cikkben található online hivatkozások

URL1: *Online játékok közben szedte kiskorú áldozatait*. http://ugyeszseg.hu/online-jatekok-kozben-szedte-kiskoru-aldozatait-fotokkal-a-bacs-kiskun-varmegyei-fougyeszseg-sajtokozlemenye/?fbclid=IwAR1-YbLJ6fHUhmcV0Dul9OZ_MRAP10adsaqImREc_FlVeYp43w4PkPsRadY

URL2: *Lezárt akta – Felelsz, vagy mersz*. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/lezart-akta-felelsz-vagy-mersz

URL3: *Carly's Story.* https://www.carlyryanfoundation.com/carlys-story

A cikk APA szabály szerinti hivatkozása

Meggyesfalvi B. (2023). Kockázati tényezők a digitális térben. A gyerekek internet- és közösségi média használata és az online áldozattá válás. *Belügyi Szemle*, *71*(12), 2163–2178. https://doi.org/10.38146/BSZ.2023.12.3