



Barabás A. Tünde

A DIGITÁLIS VIKTIMIZÁCIÓ KRIMINOLÓGIAI VIZSGÁLATA

Polt Péter professzor jogalkalmazói és gyetemi oktatói munkájával egy időben kezdte meg tudományos pályafutását. Kutatói munkássága kezdetekor, amely egyébként végigkísérte szakmai útját, már 1983-ban foglalkozott a számítógépes bűnözéssel és az ehhez köthető büntetőjogi szabályozás alakításával. Abban az időben mind a téma felvetése, mind az elkövetkezendőkre tett megállapításai, amelyek – mára nyugodtan kijelenthető – kiállták az idő próbáját, úttörő jellegűek voltak, hiszen a számítógépek használata hazánkban még gyerekcipőben járt. Ezzel a témával a későbbiek során is többször foglalkozott, ami jól mutatja tudományos gondolkodásának naprakészségét. Így, kapcsolódva ehhez a különösen aktuális témához, az alábbi tanulmányommal szeretném kifejezni jókívánságaimat a jeles alkalomból az ünnepeltnek, egykori tanáromnak.



1983-as tanulmányában Polt Péter a digitalizáció és a technikai fejlődés okozta változásokkal és azok következményeivel foglalkozott. Már ekkor világosan jelezte a mára már beigazolódtott folyamatot, nevezetesen, hogy a változások viharos gyorsasággal következnek be, és eddig nem látott széles rétegeket érintenek.¹ És ez valóban bekövetkezett, megtöbbszörözve a korábbiakhoz képest a hatóságok munkaterhét, a bűnüldözés és az igazságszolgáltatás résztvevőitől egyre speciálisabb ismereteket, készségeket igényelve eljárásuk során.

Hasonlóképpen alakult mindez a lakosság, a potenciális áldozatok oldalán is, hiszen a mindennapi élet egyre szélesebb spektrumát hálózza be a digitalizáció. Nemcsak a vásárlás, a játék vagy a közösségi élet, de a hivatalos ügyintézés (ügyfélkapu, eeszt, NAV stb.), a banki ügyintézés és a lehetőségek egyre bővülő

¹ POLT 1983.

köre kerül át az online térbe. Ezek alkalmazásához már nem szükséges számítógép, infrastruktúra, elég pusztán egy okostelefon és néhány kattintás. Ez a világ tehát gyakorlatilag mindenki számára elérhetővé válik, nem igényel speciális ismereteket és tudást, elérhető bárhol, bármikor, kitéve a használatát az internetes felületen jól mozgó bűnelkövetőknek, csalóknak, adatlopóknak, hackereknek, vírustámadóknak.

Az online térben zajló társas interakciók elterjedésével mindinkább növekszik az itt eltöltött idő is. A 2020-as Covid-19-járvány miatti lezárások ezt a folyamatot hihetetlenül felgyorsították világszerte, hiszen a személyes és szakmai élet is egyre inkább a virtuális térbe tevődött át. Ezzel párhuzamosan az online bűncselekmények és így az áldozatok száma is megugrott,² és a virtuális térben elkövetett átverések és adatlopások egyre változatosabb formái alakulnak ki.

A bűncselekmények és a bizonytalanságérzet csökkentését célzó stratégiák egyik legfontosabb kérdése, hogy *kik és hol válnak áldozattá*, vannak-e meghatározható demográfiai és szociokulturális jellemzőik, valamint van-e a helyszínek valamilyen jellegzetessége, amely a bűncselekmény elkövetését megkönnyíti, előidézi. Az online tér a bűncselekmények elkövetésének és elszენvedésének olyan, a korábban megismertekhez képest speciális területe, amely működéséből adódóan – de feltételezhetően más okokból is – meghatározó abban, hogy ki válik elkövetővé vagy áldozattá. Mindezek miatt nem véletlen, hogy a kiberbűnözés vizsgálata az elmúlt évtizedben egyre nagyobb teret nyert kriminológiai szempontból is.³

KUTATÁSOK ÉS ELMÉLETEK

Az online áldozattá válások gyakoriságának növekedésével a vizsgálatok fókuszába elsősorban az online zaklatás különböző formái, valamint az online csalások kerültek, amely utóbbi cselekmény változatos elkövetési módokkal és eszközökkel jellemezhető. Tematikájuk szerint a kutatások a következő módon csoportosíthatók:

1. *A nagy mintás prevalenciakutatások az egyes online cselekményekben való áldozattá válás gyakoriságát, valamint a feljelentések arányát vizsgálják a nagyobb*

² FBI 2021.

³ VARGA 2021.

populációban. A Nemzetközi Csalás Elleni Szövetség (Global Anti-Scam Alliance, GASA) 2023-as jelentése alapján a csalások okozta vagyoni hátrány elérte az egytrillió dollárt, ami a világ GDP-jének körülbelül 1%-a. A GASA 2023-as jelentése alapját képező kutatás eredményei szerint a résztvevők 78%-a áldozattá vált valamilyen csalási formában az elmúlt 12 hónapban.⁴

A bűnügyi adatgyűjtés kizárólag a hatóság tudomására jutott elkövetési és áldozattá válási adatokra terjed ki, a latencia miatt ennél jóval magasabb lehet az áldozattá válás aránya. Egy kutatás szerint az online csalás áldozatainak kevesebb mint 10%-a tett feljelentést a hatóság felé. A feljelentés megtételét pedig leginkább a pénzveszteség mértéke határozta meg.⁵

A kérdőíves viktimizációs kutatások alapján pontosabb képet kaphatunk az online viktimizációs tendenciákról. Mo Houtti és munkatársai⁶ 12 országban (köztük Magyarországon is) vizsgálták a különböző típusú offline és online csalásokban való áldozattá válás gyakoriságát. Az egyes csalástípusok közül az online vásárlásos csalás előfordulási aránya volt a legmagasabb, első helyen Szlovákia (35%), második helyen pedig Magyarország (34%) szerepelt. Nagy fokú változatosságot mutatott az offline és online csalási módok aránya a különböző országokban; Dél-Koreában például sokkal nagyobb arányban fordult elő az offline csalásnak az a formája, amikor az elkövető hivatalos személyként, közszolgáltató alkalmazottjaként vagy az áldozat hozzátartozójaként igyekszik pénzt kicsalni a sértettből, mint az online vásárlásos csalás (28% és 17%), míg Magyarországon a személyes csalás kevésbé volt jellemző (8%).

Az online zaklatás vagy *bullying* esetében szintén növekvő tendencia figyelhető meg az áldozattá válás gyakoriságát illetően, feltehetően a növekvő technológia-használat miatt,⁷ az előfordulás gyakorisága viszont nagy fokú változatosságot mutat az egyes országokban (5–24% között); leginkább az iskoláskorúak érintettek az áldozattá válás ezen formájában.⁸ Egy 2017-es magyar nagy mintás *cyberbullying*-kutatásban Zsila Ágnes és Demetrovics Zsolt azt találta, hogy a résztvevők 16,7%-a vált áldozattá a zaklatás valamilyen formájában (*flaming*, zaklatás, *flamebaiting*/befeketítés, kiközösítés, személyiséglopás, kibeszélés, trükközés, *sexting*), 3,4%-uk pedig elkövetett valamilyen egyéb zaklatási formát

⁴ JORIJ et al. 2023.

⁵ FONSECA-MOREIRA-GUEDES 2022.

⁶ HOUTTI et al. 2024.

⁷ JAIN et al. 2020.

⁸ BROCHADO-SOARES-FRAGA 2017.

a vizsgált egy évben.⁹ Ez a kutatás is megerősítette azt a korábbiakban alaposan alátámasztott kutatási megállapítást, miszerint az áldozatok gyakran maguk is elkövetői az online zaklatásnak; a magyar mintán 21-szer nagyobb eséllyel váltak áldozattá azok a fiatalok, akik maguk is elkövetők voltak, mint azok, akik nem. Glenn Walters metaanalízisében 22 hosszmetzeti kutatás adatainak elemzésével gyenge-közepes erejű korrelációt talált az elkövetés és az áldozattá válás között,¹⁰ amely összefüggést más metaanalízisek is megerősítettek.¹¹

2. Az online viktimizációs kutatások jelentős részénél az áldozattá válást bejósoló demográfiai, pszichológiai és társas tényezők, valamint az áldozattá válás pszichés és szociális következményei kerülnek a vizsgálat fókuszába. A *cyberbullying* esetében elmondható, hogy nagyobb valószínűséggel válnak áldozattá a lányok és az idősebb kamaszok,¹² valamint a lányok esetében a zaklatás hosszú távú érzelmi következményei is súlyosabbak.¹³

A *cyberbullying* áldozatai gyakrabban szenvednek szorongásos betegségektől, és iskolai teljesítményük is alacsonyabb,¹⁴ a depresszió valószínűsége esetükben háromszor nagyobb a kortársaikhoz képest,¹⁵ valamint jellemző rájuk az internalizáló személyiségstruktúra, a problémákból fakadó stressz önmaguk ellen fordítása, a depresszív és szorongásos hangulat mellett a pszichoszomatikus tünetképzés.¹⁶

Az online csalások esetében ellentmondásos eredmények születtek arra vonatkozóan, hogy a demográfiai tényezőknek mekkora szerepe van az áldozattá válásban. Egyes szerzők szerint a demográfiai változók – mint kor, nem és szocioökonomiai státusz – nem közvetlenül, hanem az ezekből fakadó életmód és online fogyasztási szokások mentén befolyásolja az áldozattá válás valószínűségét.¹⁷ Az online töltött idő mértéke egyaránt növelheti az online csalásokban,¹⁸

⁹ ZSILA–DEMETROVICS 2018.

¹⁰ WALTERS 2021.

¹¹ GUO 2016; KOWALSKI et al. 2014; MARCIANO–SCHULZ–CAMERINI 2020.

¹² ZSILA–DEMETROVICS 2018; LOZANO-BLASCO–QUÍLEZ ROBRES–LATORRE-COSCULLUELA 2023.

¹³ BROWN–DEMARAY–FREDICK 2014.

¹⁴ KOWALSKI–LIMBER 2013; MARCIANO–SCHULZ–CAMERINI 2020; SCHNEIDER et al. 2012.

¹⁵ TRAN et al. 2023.

¹⁶ CHRISTINA et al. 2021.

¹⁷ HOLTFRETER–REISIG–PRATT 2008.

¹⁸ GUERRA–INGRAM 2020.

személyazonosság-lopásban¹⁹ és romantikus csalásban való áldozattá válást.²⁰ Ezzel összefüggésben a negatív életesemények előfordulása egy személy életében további rizikófaktorként jelenik meg, mivel a társas támogatás csökkenése és az izoláció miatt növekszik az online aktivitás és a befolyásolhatóság mértéke is.²¹ Zhi Zhang és Zhi Ye kínai nagy mintás kutatásukban²² ezenfelül a demográfiai változók és az online csalásokban való áldozattá válás között is talált szignifikáns összefüggést; az áldozatok fiatalabbak és alacsonyabb iskolai végzettségűek voltak, magasabb szintű impulzivitás és bizalom jellemezte őket. Az online csalásban való áldozattá válás pszichológiai tényezői közül az impulzivitáson túl kiemelendők az alacsonyabb kognitív készségek, az alacsony önkontroll mint személyiségvonás és mint aktuális énállapot az áldozattá válás idején, a túlzott mértékű magabiztosság a csalások felismerésére vonatkozóan, az alacsony pszichológiai jóllét és az idealizációra való fokozott hajlam – utóbbinak a romantikus csalások esetében van magyarázó szerepe.²³

3. Az online áldozattá válás szociológiai magyarázóelméletei közül a rutintevékenységlelméletet (RAT) és az önkontroll szerepét hangsúlyozó értelmezési kereteket alkalmazzák a leggyakrabban a témában kutató szerzők.²⁴ Az internetezéssel töltött idő áldozattá válást bejósoló szerepén túl a RAT-elmélet mentén például azt is bebizonyították a kutatók, hogy a rendszerfeltörés és *malware*-fertőzés áldozatai később szignifikánsan nagyobb arányban használnak biztonsági eszközöket, és óvatosabbak az interneten szörfölés közben.²⁵ Az alacsony önkontroll szerepe az online áldozattá válásban a *cyberbullying* mellett az online hálózat segítségével elkövetett (*computer-assisted*) csalások esetében egyértelműen kimutatható,²⁶ míg a számítógépes rendszert célzó csalások (*computer focused*) esetében – mint például a rendszer feltörése, *hacking* – ellentmondásosak a kutatási eredmények az önkontroll szerepét illetően.²⁷

¹⁹ GUEDES–MARTINS–CARDOSO 2023.

²⁰ SNYDER–GOLLADAY 2024.

²¹ DELIEMA 2015; EMAMI–SMITH–JORNA 2019; ZHANG–YE 2022.

²² ZHANG–YE 2022.

²³ NORRIS–BROOKES–DOWELL 2019.

²⁴ WILSEM 2013.

²⁵ GUERRA–INGRAM 2020.

²⁶ NGO–PATERNOSTER 2011; VAZSONYI et al. 2012; WILSEM 2013.

²⁷ BOSSLER–HOLT 2010; NGO–PATERNOSTER 2011.

Az online csalásban való áldozattá válás pszichológiai elméleteiről Gareth Norris, Alexandra Brookes és David Dowell ad áttekintést online csalásról szóló metaanalízisükben.²⁸ Az *elaboráció valószínűségi modellje* (*Elaboration Likelihood Model*, ELM) alapján az áldozat motivációs szintje fordítottan arányos az áldozattá válás valószínűségével: a magasan motivált személyek esetében megvalósul a csaló üzenet kognitív szintű feldolgozása és felismerése, míg az alacsonyan motivált személyek az üzenet tartalma helyett a perifériás jelzésekre figyelnek, és különféle kerülőutakon (érzelmi érvekkel) meggyőződhetnek az üzenet tartalmának valóságosságáról. A *szignáldetektációs elmélet* mentén értelmezve azok a személyek válnak könnyebben offline vagy online csalás áldozatává, akik a csalóval folytatott kommunikáció során kevésbé képesek az üzenetet zavaró információkat, a „zajt” kiszűrni, amely információkat a csalók a potenciális áldozat megzavarására használnak az elkövetés során. Végül az *interperszonális megtévesztés elmélete* szerint a csalás nem egyirányú folyamat, hanem a csaló és az áldozat dinamikus kapcsolatban áll egymással a kommunikációs térben. A kidolgozott megtévesztés nagy fokú mentális erőfeszítést igényel a csaló részéről, aki emiatt akaratlanul is verbális és nonverbális nyomokat hagy (*leakage cues*) a kommunikáció során, amelyek felfedik a csalási szándékát. Az elmélet szerint azok válnak áldozattá, akik nem ismerik fel ezeket a nyomokat a csaló üzenetben.

4. Az online áldozattá válással kapcsolatos kutatások egy újabb irányát képezik a *mesterséges intelligencia segítségével elkövetett csalások*, amelyeket az MI és a virtuális környezetalkotás terén tapasztalható hatalmas mértékű fejlődés tett lehetővé az utóbbi években. Az online csaláshoz használt, MI segítségével létrehozott eszközök négy fő csoportja:²⁹

- *Szöveges és képi tartalmak*: személyre szabott csaló e-mailek, szöveges üzenetek és képek létrehozása személyek megtévesztése érdekében. Az MI által létrehozott csaló üzenetek már sokkal kevésbé tartalmaznak nyelvhelyességi hibákat, így nehezebben ismerhetők fel a potenciális áldozat által. A generált képi tartalmak pedig széles körben felhasználhatók a csalás különböző formáiban (például sérült gépjárműről készült kép a biztosítási csaláshoz).
- *MI által támogatott chatbotok*: a chatbotok sokkal kevesebb erőforrással több potenciális áldozatot érnek el, mint a klasszikus online csalásra specializálódott *call centerek*.

²⁸ NORRIS–BROOKES–DOWELL 2019.

²⁹ JAWARKAR–TIKEKAR 2024.

- ♦ „Deep fake” videótartalmak: egyre gyakoribb elkövetési forma az online csalások során, hogy az elkövetők az áldozat számára megbízható személyekről készült, MI által generált videófelvevételekkel igyekeztek megtéveszteni az áldozatot, illetve több esetben banki videós azonosítási rendszert próbáltak az elkövetők átverni az áldozatról készült hamis videófelvevételekkel.
- ♦ Hangklónozó átverések: a deep fake technológia segítségével az emberi hangszín egyre nagyobb pontossággal utánozható. Az elkövetők a potenciális áldozat számára fontos személynek adhatják ki magukat egy online vagy telefonos beszélgetésben.

Mindez csak a kezdet a MI területén, amely folyamatosan fejleszti önmagát, így ma még elképzelhetetlen módszerek és eszközök jönnek létre a bűnelkövetést, csalást, megtévesztést segítő, amelyekre felkészülni sincs még eszköz és lehetőség.

HAZAI EREDMÉNYEK EGY NEMZETKÖZI ONLINE VIKTIMIZÁCIÓS KUTATÁS TÜKRÉBEN

Az online és offline áldozattá válás és egyes kiberbűncselekmények elkövetésének témakörében végzett kutatás három ország részvételével zajlott.³⁰ Elméleti kiindulópontja az volt, hogy amennyiben érthetőbbé válnak a kiberbűncselekmények elkövetőinek motivációi, a deviáns viselkedésüket alakító tényezők, az online térben elkövetett bűncselekmények számának növekedő tendenciája is megfordítható.

A lekérdezés 2020 áprilisában zajlott az Egyesült Államokban, Magyarországon és Finnországban, reprezentatív mintán. A hiányos esetek kiszűrése után 4212 fő került a mintába.

Az áldozattá válási blokkban a megelőző 12 hónapra vonatkozóan kérdeztük meg a résztvevőket arról, hogy áldozattá váltak-e különféle online átverésekben és cselekményekben (e-mail-csalások, adatokkal visszaélés, ismeretlen számla-

³⁰ A kutatás a Jean Monnet Center of Excellence, Collage Center for European Union, Transatlantic, and Trans-European Space Studies (CEUTTSS) támogatásával valósult meg, a Virginia Tech College of Liberal Arts and Human Sciences (CLAHS), a University of Turku Faculty of Social Sciences, valamint a Nemzeti Közzolgálati Egyetem Rendészettudományi Kar Kriminológia Tanszéke részvételével.

tranzakciók, számítógépes vírusok, kéréslen online hozzászólások), illetve nem a kibertérben elkövetett cselekményekben (igazolvány, bankkártya ellopása, kéréslen személyes hozzászólások, személyes tulajdon rongálása).

Az online és offline áldozattá válási gyakoriságokat országonkénti bontásban vizsgálva azt találjuk, hogy minden cselekményforma szignifikánsan gyakrabban fordult elő az Egyesült Államokban a khi-négyzet-próba alapján ($p < 0,01$), a „nem kívánt jellegű szexuális hozzászólások online” kivételével, ahol nem volt számottevő különbség az országok szerint.

A magyar mintában az online áldozattá válás nagyobb gyakorisága figyelhető meg az offline cselekményekhez képest (30,7–21%). Ez összefüggésben lehet azzal, hogy maga a kérdés a Covid-19-járványt követően zajlott, és az előző év eseményeire kérdezett rá. Az online áldozattá válási formák közül a leggyakoribb cselekmény a nem kívánt jellegű szexuális hozzászólás volt (13,5%), ezt követi a számítógépes vírus vagy program (11,8%) és az e-mailes, webes csalások (8,8%). A magyar résztvevők körében az offline áldozattá válás formái közül a személyes sértő hozzászólások fordultak elő legnagyobb arányban (11,6%), valamint a személyes jellegű nem kívánt szexuális hozzászólások (8,4%) és a tulajdon megrongálása (5,9%).

Szignifikáns eltéréseket találtunk a magyar mintán az egyes online és offline áldozattá válási módok esetében az áldozat neme és életkora szerint. Az ismeretlen számlatranzakciók szignifikánsan nagyobb arányban fordultak elő az időskorú férfiak esetében, a férfiak továbbá gyakrabban estek áldozatul álcéges, álszolgáltató általi személyes adatlopási kísérletnek a nőkhöz képest. A férfiaknál azért lehet nagyobb a kitettség az online csalásoknak és adatlopásnak, mivel átlagosan több időt töltenek különböző tevékenységekkel az interneten. Az e-mailes/webes csalások áldozatai között nagyobb arányban voltak az időskorúak (60 éves vagy idősebb).

Az offline cselekmények esetében elmondható, hogy az offline vagy telefonos csalás áldozatai nagyobb arányban voltak férfiak, míg a nem kívánt jellegű személyes szexuális hozzászólások áldozatai nagyobb arányban nők. Ezen két cselekmény esetében a fiatal felnőtt korosztály a legveszélyeztetettebb. A személyes tulajdon megrongálása a felnőtt (26–59 éves) korcsoportot szignifikánsan nagyobb mértékben érintette a fiatal felnőtt és idős korcsoporthoz képest a magyar mintában.

Az eredmények azt mutatták, hogy az összes cselekmény esetében az *önkontroll mértéke* gyakorolta a legnagyobb hatást az áldozattá válásra. Az alacsonyabb

önkontrollal rendelkező személyek nagyobb valószínűséggel esnek áldozatul a különböző e-mailes, webes csalásoknak, adatlopási kísérleteknek, számítógépes vírusoknak. Az online töltött idő hatása több csalás esetében volt szignifikáns, de alacsony mértékű (β : 0,004–0,006). Az alacsonyabb szintű számítógépes ismeretek valószínűsíthetik az e-mailes vagy webes felületen történő áldozattá válást (β : –0,123), valamint a bankszámlán, online fizetési rendszeren tapasztalt ismeretlen tranzakciókat (β : –0,103). Egyes online csalástípusok viszont – távoli elérés, webes adatlopás – a számítógéphez jobban értők körében voltak jellemzők.

A sértő tartalom megjelenése, valamint a nem kívánt szexuális hozzászólások elsősorban a fiatalabb, alacsony önkontrollal rendelkező nőket érintették, akik több időt töltenek online felületeken. Ezzel szemben az online társskereső oldalon keresztül végrehajtott csalás áldozatai alacsonyabb önkontrollal rendelkező fiatalabb férfiak voltak.

Az online aktivitással töltött idő mellett a csalások és egyéb kibercselekmények megelőzésére szolgáló biztonsági intézkedések alkalmazását is vizsgáltuk. Az áldozattá válásban ugyanis jelentős szerepet játszik a megfelelő védelem, valamint a biztonsági ismeretek hiánya, ami mind technikai, mind pedig tudás-szinten megmutatkozik.

A személyazonosság ellopását monitorozó megoldást, valamint vírusirtó programot vagy tűzfalat szignifikánsan gyakrabban használtak (a lekérdezés idején) a férfiak a nőkhez képest. A webkamera eltakarása és a bankkártya befagyasztása esetében nem találunk jelentős különbséget a nemek között. A férfiak így részben elővigyázatosabbak, másrészt ezek az intézkedések csak bizonyos csalások, átverések és egyéb kiberbűncselekmények ellen jelentenek védelmet.

Kutatásunk során bebizonyosodott az is, hogy több tényező van, amelyek gyengítik az önkontroll és környezeti kontroll hatását az elkövetők, illetve az áldozatok esetében:³¹ az online tér távolító hatása, az alacsony felderítettség, az információ hiánya vagy az anonimitásba vetett hit egyes elemei. A férfiak nagyobb áldozati kitettsége összefügghet a nagyobb kockázatvállalási készséggel, ami az offline világban is nagyobb mértékű sértetté válást eredményez körükben.³²

Az online bűnözést és viktimizációt magyarázó tényezők azonosítása lehetővé teszi a megelőzés célcsoportokra, illetve konkrét felhasználói típusokra és magatartásformákra történő kidolgozását. Az esetszámok gyors növekedésében

³¹ VARGA 2021.

³² BARABÁS 2015.

szerepet játszó azonosított tényezők, a csekély elkövetői kockázat és az alacsony felderítettség pedig arra az ünnevelt által tett megállapításra hívja fel a figyelmet, amely szerint a jog alkalmazása ezen új jelenségek esetében csak akkor lehetséges, ha a jogalkalmazók a technológia jogi szempontból releváns működési elemeit megértik.³³ Azaz az edukáció nemcsak a felhasználó állampolgárok, hanem a büntetőügyekben eljáró hatóságok számára is elengedhetetlen, ami jelentős szerepet játszhat ezen a területen mind a bűnmegelőzés, mind pedig a büntetőeljárás eredményesebbé tételében.

IRODALOMJEGYZÉK

- BARABÁS Andrea Tünde (2015): *Áldozatok és igazságszolgáltatás*. Budapest: Országos Kriminológiai Intézet.
- BOSSLER, Adam M. – HOLT, Thomas J. (2010): The Effect of Self-Control on Victimization in the Cyberworld. *Journal of Criminal Justice*, 38(3), 227–236. Online: <https://doi.org/10.1016/j.jcrimjus.2010.03.001>
- BROCHADO, Sandra – SOARES, Sara – FRAGA, Sílvia (2017): A Scoping Review on Studies of Cyberbullying Prevalence Among Adolescents. *Trauma, Violence, & Abuse*, 18(5), 523–531. Online: <https://doi.org/10.1177/1524838016641668>
- BROWN, Christina F. – DEMARAY, Michelle K. – FREDICK, Stephanie S. (2014): Cyber Victimization in Middle School and Relations to Social Emotional Outcomes. *Computers in Human Behavior*, 35(6), 12–21. Online: <https://doi.org/10.1016/j.chb.2014.02.014>
- CHRISTINA, Stefanny et al. (2021): The Bidirectional Relationships Between Peer Victimization and Internalizing Problems in School-Aged Children. An Updated Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 85(2), 101979. Online: <https://doi.org/10.1016/j.cpr.2021.101979>
- DELIEMA, Marguerite (2015): *Using Mixed Methods to Identify the Characteristics of Older Fraud Victims*. PhD-disszertáció. Los Angeles: University of Southern California.
- EMAMI, Catherine – SMITH, Russel G. – JORNA, Penny (2019): *Online Fraud Victimization in Australia. Risks and Protective Factors*. Canberra: Australian Institute of Criminology. Online: <https://doi.org/10.52922/rr09319>
- FBI (2021): *Internet Crime Report 2021*. Washington, DC: Federal Bureau of Investigation Internet Crime Complaint Center. Online: www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
- FONSECA, Catarina – MOREIRA, Samuel – GUEDES, Inês (2022): Online Consumer Fraud Victimization and Reporting. A Quantitative Study of the Predictors and Motives. *Victims & Offenders*, 17(5), 756–780. Online: <https://doi.org/10.1080/15564886.2021.2015031>

³³ POLT 2022.

- GUEDES, Inês – MARTINS, Margarida – CARDOSO, Carla S. (2023): Exploring the Determinants of Victimization and Fear of Online Identity Theft. An Empirical Study. *Security Journal*, 36(3), 472–497. Online: <https://doi.org/10.1057/s41284-022-00350-5>
- GUERRA, Chris – INGRAM, Jason R. (2020): Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior*, 43(1), 44–60. Online: <https://doi.org/10.1080/01639625.2020.1774707>
- GUO, Siying (2016): A Meta-Analysis of the Predictors of Cyberbullying Perpetration and Victimization. *Psychology in the Schools*, 53(4), 432–453. Online: <https://doi.org/10.1002/pits.21914>
- HOLTFRETER, Kristy – REISIG, Michael D. – PRATT, Travis C. (2008): Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology*, 46(1), 189–220. Online: <https://doi.org/10.1111/j.1745-9125.2008.00101.x>
- HOUTTI, Mo et al. (2024): A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries. *Journal of Online Trust and Safety*, 2(4), 1–26. Online: <https://doi.org/10.54501/jots.v2i4.204>
- JAIN, Ojasvi et al. (2020): Has the COVID-19 Pandemic Affected the Susceptibility to Cyberbullying in India? *Computers in Human Behavior Reports*, 2(2), 100029. Online: <https://doi.org/10.1016/j.chbr.2020.100029>
- JAWARKAR, Rhutika V. – TIKEKAR, Priyanka C. (2024): An In-Depth Exploration of AI in the Digital Age-A Focus on Scams and Frauds in the Introduction Phase. In YENKAR, Pradnya S. (szerk.): *Recent Advancements in Science and Technology*. Vol. IV. *Electronics, Computer Science & Application*. Nagpur: Sai Jyoti Publication, 272–275. Online: www.vbm.v.org/pdf/4.pdf
- JORIJ, Abraham et al. (2023): *State of Scams Report 2023. Technical Report*. Den Haag: Global Anti-Scam Alliance.
- KOWALSKI, Robin M. – LIMBER, Susan P. (2013): Psychological, Physical, and Academic Correlates of Cyberbullying and Traditional Bullying. *Journal of Adolescent Health*, 53(1 Suppl.), S13–S20. Online: <https://doi.org/10.1016/j.jadohealth.2012.09.018>
- KOWALSKI, Robin M. et al. (2014): Bullying in the Digital Age. A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. *Psychological Bulletin*, 140(4), 1073–1137. Online: <https://doi.org/10.1037/a0035618>
- LOZANO-BLASCO, Raquel – QUILÉZ ROBRES, Alberto – LATORRE-COSCULLUELA, Cecilia (2023): Sex, Age and Cyber-Victimization. A Meta-Analysis. *Computers in Human Behavior*, 139(3), 107491. Online: <https://doi.org/10.1016/j.chb.2022.107491>
- MARCIANO, Laura – SCHULZ, Peter J. – CAMERINI, Anne-Linda (2020): Cyberbullying Perpetration and Victimization in Youth. A Meta-Analysis of Longitudinal Studies. *Journal of Computer-Mediated Communication*, 25(2), 163–181. Online: <https://doi.org/10.1093/jcmc/zmz031>
- NGO, Fawn T. – PATERNOSTER, Raymond (2011): Cybercrime Victimization. An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, 5(1), 773–793.

- NORRIS, Gareth – BROOKES, Alexandra – DOWELL, David (2019): The Psychology of Internet Fraud Victimization. A Systematic Review. *Journal of Police and Criminal Psychology*, 34(3), 231–245. Online: <https://doi.org/10.1007/s11896-019-09334-5>
- POLT Péter (1983): A számítógépes bűnözés. *Belügyi Szemle*, 21(6), 60–64.
- POLT Péter (2022): Digitális fejlődés és büntetőjog – akkor és most. *Belügyi Szemle*, 70(11), 2389–2393. Online: <https://doi.org/10.38146/bsz.2022.11.47>
- SCHNEIDER, Shari Kessel et al. (2012): Cyberbullying, School Bullying, and Psychological Distress. A Regional Census of High School Students. *American Journal of Public Health*, 102(1), 171–177. Online: <https://doi.org/10.2105/ajph.2011.300308>
- SNYDER, Jamie A. – GOLLADAY, Katelyn (2024): More Than Just a „Bad” Online Experience. Risk Factors and Characteristics of Catfishing Fraud Victimization. *Deviant Behavior*, 1–21. Online: <https://doi.org/10.1080/01639625.2024.2416071>
- TRAN, Huong Giang Nguyen et al. (2023): Cyber-Victimization and Its Effect on Depression in Adolescents. A Systematic Review and Meta-Analysis. *Trauma, Violence, & Abuse*, 24(2), 1124–1139. Online: <https://doi.org/10.1177/15248380211050597>
- VARGA Árpád (2021): Kriminológiai elméletek és informatikai bűnözés. In *Medias Res*, 10(1), 155–196. Online: <https://inmediasresfolyoirat.hu/imr/article/view/228>
- VAZSONYI, Alexander T. et al. (2012): Cyberbullying in Context. Direct and Indirect Effects by Low Self-Control Across 25 European Countries. *European Journal of Developmental Psychology*, 9(2), 210–227. Online: <https://doi.org/10.1080/17405629.2011.644919>
- WALTERS, Glenn D. (2021): School-Age Bullying Victimization and Perpetration. A Meta-Analysis of Prospective Studies and Research. *Trauma, Violence, & Abuse*, 22(5), 1129–1139. Online: <https://doi.org/10.1177/1524838020906513>
- WILSEM, Johan van (2013): Hacking and Harassment – Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, 29(4), 437–453. Online: <https://doi.org/10.1177/1043986213507402>
- ZHANG, Zhi – YE, Zhi (2022): The Role of Social-Psychological Factors of Victimity on Victimization of Online Fraud in China. *Frontiers in Psychology*, 13, 1030670. Online: <https://doi.org/10.3389/fpsyg.2022.1030670>
- ZSILA Ágnes – DEMETROVICS Zsolt (2018): Cyber-viktimizáció és cyber-agresszió. A közösségioldal-használat összefüggései az online bántalmazással. *Médiakutató*, 19(1), 21–33. Online: https://mediakutato.hu/cikk/2018_01_tavasz/02_cyber_viktimizacio_es_cyber_agresszio.pdf