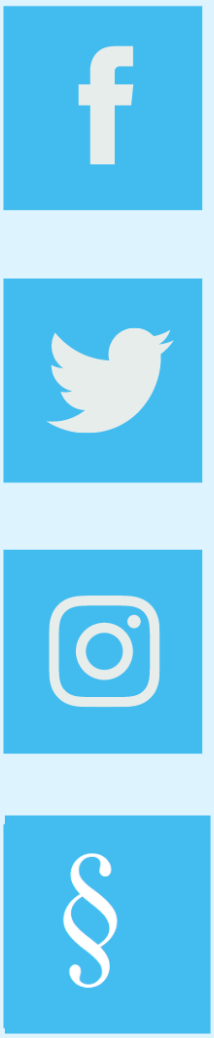
AZ INTERNET ÉS A KÖZÖSSÉGI MÉDIA JOGI KIHÍVÁSAI

Konferenciakötet

Szerkesztette:
Tóth Dávid



PTE-ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

Pécs, 2022.

Az internet és a közösségi média jogi kihívásai – Konferenciakötet

Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

Pécs, 2022.

Az internet és a közösségi média jogi kihívásai – Konferenciakötet

Szerkesztette:

dr. Tóth Dávid

Lektorálta:

Prof. dr. Kőhalmi László

Kiadja:
Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék
7622 Pécs, 48-as tér 1.

Felelős Kiadó: Prof. Dr. Fábián Adrián dékán

ISBN: 978-963-429-992-9

A konferenciakötet az Innovációs és Technológiai Minisztérium ÚNKP-21- 4-II-PTE-962 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Tartalomjegyzék

Előszó

A tematikus nemzetközi online konferenciára 2022. 04. 27.-én került sor, amely a „Teams” alkalmazáson keresztül valósult meg. A konferenciára 17 fő jelentkezett számos országból, akik között találkozhatunk professzorokkal, adjunktusukkal, doktoranduszokkal. Az előadók a kutatáshoz kapcsolódó előadásaikat magyar, angol és német nyelven adhatták elő. A prezentációkat követően a résztvevőknek lehetőségük volt kérdéseket és hozzászólásokat megfogalmazni. A konferencia teljes programjának a kötet végén található meg mellékletben.

Az *„Az internet és a közösségi média jogi kihívásai”* című konferenciának a célja az volt, hogy a témával foglalkozó kutatókat a jog minden területéről arra hívja, hogy bemutassák eredményeiket és a közös eszmecsere révén elősegítsék egymás kutatómunkáját. Az internet és közösségi média alapjaiban változtatta meg az emberek életét és ez új kihívásokat teremt a jog minden területén. A technológia fejlődése hatással van a közjogi és magánjogi jogágakra, új lehetőségeket és új problémákat teremtve. A konferencia résztvevőiből tizenegyen járultak hozzá közleményükkel e könyv megvalósulásához. A jövőben a téma iránt érdeklődő olvasók és kutatók számára egy hivatkozási mű lehet. Szerkesztőként ezúton is köszönöm az előadóknak és a szerzőknek a munkájukat.

A konferenciakötet az Innovációs és Technológiai Minisztérium ÚNKP-21- 4-II-PTE-962 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Dr. Tóth Dávid
Szerkesztő

D. Horváth Vanessza
PhD-hallgató (PTE-ÁJK)

Gyermekprostitúció a kibertérben

Absztrakt

Tanulmányom a gyermekprostitúció és a virtuális valóság kapcsolódási pontjait mutatja be. A gyermekekkel való bánásmód vizsgálata során nem hagyhatjuk figyelmen kívül az adott gyermeket körülvevő társadalmi környezetet. Elvégre az európai ember számára durva erőszakként értelmezhető az a Kínában egészen a XX. század elejéig élt szokás, miszerint a lányok lábfejét már kisgyermekkorban eltörte és elkötötte saját édesanyjuk annak érdekében, hogy megakadályozzák a láb növekedését, és így a férfiak számára később szexuálisan vonzóvá váljanak. [1] *A szexuális célú gyermekbántalmazás azonban Európa történelmét is végig kíséri, az online felületek egyre népszerűbbé válása által pedig új dimenzióba helyeződött. Ebből fakadóan tanulmányom első részében azt a folyamatot tekintem át, amely által a gyermekek szexuális kizsákmányolása elleni küzdelem fontos célkitűzéssé válhatott. A gyermekprostitúció fogalmának ismertetése után térek rá a jogalkotás dilemmáira, ezt követően pedig a gyermekek szexuális kizsákmányolásának online formái kerülnek ismertetésre.*

Kulcsszavak: gyermekprostitúció, child grooming, online bántalmazás, gyermek szexuális célú kizsákmányolása

1. Bevezető gondolatok

A gyermekjogok deklarálása és betartatása hosszú társadalmi fejlődés eredménye. Amint azt Lloyd deMause megfogalmazta: „*A gyermekkor története rémálom, amelyből csak mostanában kezdünk felébredni. Minél távolabb megyünk vissza a történelemben, annál alacsonyabb a gyermekről való gondoskodás színvonala, és annál nagyobb a valószínűsége, hogy a gyermeket megölték, kitették, testileg bántalmazták, terrorizálták, vagy szexuálisan zaklatták*."[2]
A Word Health Organization (továbbiakban WHO) által megalkotott definíció szerint a gyermekek bántalmazása és elhanyagolása a hanyag bánásmód,

[1] Babity Mária: A gyermekbántalmazás rizikótényezőinek vizsgálata (magas kockázatot képviselő gyermeknevelési attitűdök, a szülőkkel kapcsolatos gyermekkori emlékek és néhány lehetséges közvetítő tényező összefüggései). PhD értekezés, Pécs. 2013. p. 10.
[2] Idézi: Pukánszky Béla: A gyermekkor története. Műszaki Könyvkiadó, Budapest. 2001. p. 1.

illetve a fizikai, érzelmi és/vagy szexuális visszaélések mellett magában foglal minden olyan kizsákmányolási formát is, ami a gyermek egészségének, fejlődésének vagy méltóságának sérelmét eredményezi.[3]
A meghatározás további eleme, hogy a bántalmazás felelősségen, bizalmon vagy hatalmon alapuló kapcsolat keretében következik be, mindez azonban nem jelenti kizárólagosan azt, hogy a bántalmazó csak családtag, vagy a közvetlen környezetben hatalmi befolyással rendelkező személy lehet. Amennyiben figyelembe vesszük a WHO által kidolgozott fogalmi elemeket, a felelősség fordulatot kiterjesztően értelmezve aligha találhatunk olyan, gyermeket érintő szituációt, amelyben nem állapítható meg a felnőtt világ erkölcsi felelőssége. Abban az esetben, ha gyermekvédelmi paradigmában gondolkodunk, az online térben, gyermek sérelmére elkövetett bárminemű bántalmazás gyermekbántalmazásnak számít.[4]
Napjainkban a világhálón tömegesen jelennek meg a gyermekeket szexuális eszközként ábrázoló felvételek, amelyek bár törlésre kerülhetnek az illetékes hatóság által, az adott szexuális kizsákmányolást rögzítő anyaggal kapcsolatba került összes felhasználó gyakorlati azonosítása szinte lehetetlen, és az esetlegesen multiplikálódott felvételek a gyermek többszörös viktimizációját eredményezhetik. [5] Amellett azonban, hogy a felvétel terjesztése bűncselekményt valósít meg, nem feledkezhetünk meg annak vizsgálatáról sem, hogy miképp került a gyermek kiszolgáltatott helyzetbe.
Azon esetek, amelyek megvalósítják a prostitúciós célú kizsákmányolást, a legtöbb országhoz hasonlóan Magyarországon is gyakran rejtve maradnak a hatóságok előtt. Ez részben a bűncselekmény jellegéből fakadó látenciára vezethető vissza, [6] az online világ pedig újabb és újabb rejtőzködési lehetőségeket kínál.
Írásomban, gyermekvédelmi paradigmában gondolkodva, a Gyermekjogi Egyezményben foglaltaknak megfelelően[7], „gyermek” kifejezéssel illetek minden tizennyolcadik életévét be nem töltött jogalanyt.

[3] Pintér Ádám – Tóth Judit Nikoletta: A bántalmazott gyermekek – Gyermekjogok és gyermekbántalmazás. In: Statisztikai Szemle 2017/8-9. p. 849.
[4] Köllő Dávid: A gyermekek szexuális kizsákmányolása a kibertér felhasználásával. IN: Belügyi Szemle, 2020/2. p. 66.
[5] Parti Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó, Miskolc. 2009. p. 82.
[6] ECPAT Országjelentés – Magyarország. Jelentés a gyermekek szexuális kizsákmányolásának formáiról, jellemzőiről és méreteiről, 2021. február. p. 8.
[7] A Gyermek jogairól szóló, New Yorkban 1989. november 20-án kelt egyezmény 1. cikk.

2. Történeti visszatekintés

Tanulmányom e fejezetének célja az egyes korszakok feljegyzéseit alapul véve röviden áttekinteni, a gyermekek szexuális kizsákmányolása miképp kísérte végig a történelem idővonalát.

Az ókorban a gyermekek szexuális kizsákmányolása összefonódott a gyermekkereskedelemmel: míg a római korban a fiúgyermekek ára magasabb, a bizánci periódusban a hangsúly a lányokra helyeződött.[8] Az a tény, miszerint Justitianus 529-ben betiltotta a gyermekprostitúciót, olyan magas esetszámról árulkodik, amelyet nem hagyhatott figyelmen kívül az uralkodó a jogalkotási folyamatok során sem. Mindazonáltal a korszakban e tilalom áldozatvédelemmel nem párosult, ugyanis a korabeli feljegyzések[9] szerint Bíborbanszületett Konstantin idejében a 12 évesnél idősebb, megerőszakolt gyermekre életfogytig tartó kolostor várt.

A pedofília jelensége végigvonult az egész bizánci korszakon: a V-VII. században a szülők nem merték egyedül kiengedni gyermekeiket az utcára, és a kortársak feljegyzései szerint II. Theodosziosz, illetve V. Konsztantinosz hírhedt pedofilok hírében álltak.[10]

A középkor emberére nem volt jellemző a gyermeki sajátosságok iránt tanúsított érzékenység, és a gyermekkorral szembeni archaikus távolságtartás („a kicsi nem számít") az újkorban is megfigyelhető, azonban a 16.-17. századtól kezdve a gyermek a moralisták sugallatára egyre inkább ártatlan, törékeny teremtményként jelenik meg.[11]

Ami a 19. századot illeti, a vitathatatlan fejlődés mellett a korrekt társadalmi kép kialakítása érdekében fontos egy gondolat erejéig szót ejteni a szegény sorsú gyermekek helyzetével kapcsolatos visszaélésekről – ezek kívül a legkirívóbb, szépirodalmi alkotásokból is közismert jelenség a gyermekmunka gátlástalan alkalmazása volt, amely azonban hozzájárult a kapitalista fejlődés gazdasági alapjainak megteremtéséhez.[12] Annak ellenére azonban, hogy a gyermek alávetteti státuszát valló közfelfogás eljutott napjainkig Európában addig az álláspontig, mely szerint „gyermekeink jelentik számunkra a jelent és

[8] Józsa László: Prostitúció és pedofília a Bizánci Birodalomban (324-1453). In: Művelődés-, Tudomány –és Orvostörténeti Folyóirat. 2011/2. p. 42.

[9] Armenopoulos Hexabiblos. 349-350.o. Idézi: Józsa, (2011) p.44.

[10] Józsa (2011) p. 47.

[11] Pukánszky Béla: A gyermekkortörténet bölcsőjénél. https://eta.bibl.u-szeged.hu/1887/2. (2022.05.14.)

[12] Pukánszky Béla: A változások kora: a 19. század. https://eta.bibbl.u-szeged.hu/mentorhalo/tananyag. (2022.05.14.)

a jövőt”[13], a gyermekbántalmazás még mindig egy a megoldásra váró problémák közül.
A következőkben a nemzetközi dokumentumokban megfogalmazott gyermekvédelmi elvek közül azok kerülnek bemutatásra, amelyek kifejezetten a gyermekprostitúció kapcsán tartalmaznak releváns rendelkezéseket.

3. A gyermekprostitúció tilalma a nemzetközi dokumentumokban

A gyermekprostitúció tilalma számos nemzetközi dokumentumban[14] megfogalmazásra került.
A gyermekek jogairól szóló, New Yorkban, 1989. november 20-án kelt egyezmény (amelyet hazánkban az 1991. évi LXIV. törvény hirdetett ki) kötelezi az államokat arra, hogy megvédjék a gyermekeket a nemi kizsákmányolás minden formájától.[15]
Az Európai Szociális Karta rögzítette, hogy a gyermekek és fiatalkorúak védelmét biztosítani kell az elhanyagolással, az erőszakkal és a kizsákmányolással szemben.[16]
A Nemzetközi Munkaügyi Szervezet (továbbiakban ILO) 1990-ben a gyermekmunka legrosszabb formái között meghatározta a gyermekprostitúciót és a gyermekpornográf anyagok előállítása céljából történő foglalkoztatást.[17]
Az ILO álláspontja szerint tehát a gyermekprostitúció végső soron nem más, mint a gyermekmunka egyik legrosszabb formája.
A definiálás kérdésénél maradva, a Lanzarote Egyezmény – összhangban az ENSZ Gyermekjogi Egyezményének Fakultatív Jegyzőkönyvével – a következőket rögzíti: *„(…) a gyermekprostitúció kifejezés azt jelenti, amikor valaki egy gyermeket szexuális tevékenység céljára használ, és amelynek a során pénzt vagy valamilyen más jutalmat vagy ellenszolgáltatást adnak vagy ígérnek fizetségképpen, tekintet nélkül arra, hogy ezt a kifizetést, ígéretet vagy ellenértéket a gyermek kapja vagy egy harmadik személy*.”[18]

[13] Az Európai Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.24. o. https://data.consilium.europa.eu/doc./document/ST-9977. (2022.05.14.)
[14] ld. Gyermekjogi Egyezmény 34. cikk, Fakultatív Jegyzőkönyv 1. cikk, Lanzarote Egyezmény 19. cikkely (1) bekezdés.
[15] Parti (2009) p. 113.
[16] Európai Szociális Karta 7. cikk. 10. pont.
[17] ILO konvenció a gyermekmunka legrosszabb formáinak tilalmáról. 3. cikk b.) pont.
[18] Az Európa Tanács Egyezménye A gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen. 19. cikkely (2) bekezdés.

A gyermekprostitúció mibenlétének meghatározása mellett a nemzetközi jogforrások a gyermekprostitúció tilalma, prevenciója és az áldozatvédelem hármas pillérére támaszkodnak az állami kötelezettségek meghatározásakor.[19]

4.A gyermekprostitúció szabályozásának dilemmái

4.1.A gyermek, mint elkövető?

Számos esetben a prostitúcióra kényszerített gyermek akkor kerül a hatóságok látóterébe, amikor már megtörtént a kriminalizálódása – ez esetben ellenben a vele szemben megindult büntetőeljárás már kevésbé foglalkozik az előzményekkel, így a prostitúciós út, a gyermek korábbi vagy azonos idejű státusza nem kerül figyelembevételre.[20]
Bár napjainkra feloldásra került, a problematika kapcsán érdemes röviden kitérni arra az anomáliára, miszerint 2020 nyaráig – szemben a Btk. szabályrendszerével – életkorra tekintet nélkül indult eljárás azzal a prostituálttal szemben, aki A szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvényben (továbbiakban Szabs.tv.) meghatározott, prostitúciós tevékenység végzésével kapcsolatos tilalmakat megsértette.
A Szabs.tv. vonatkozó, tiltott prostitúció szabálysértésének törvényi tényállását érő kritikai észrevételek kiemelték, hogy a nemzetközi gyakorlattal szemben a 14-18 év közötti gyermek prostituált szankcionálható, ahelyett, hogy a hatóság vélelmezné esetében a kényszerítést. Mindez az Alaptörvény szellemiségével is nehezen volt összeegyeztethető, példának okáért felmerül a gyermek testi, szellemi és erkölcsi fejlődésének védelme[21], illetve a fentebb bemutatásra került egyezmények fényében a magyar és nemzetközi jog összhangjának biztosítása [22] is problematikus lehet. Erre tekintettel az Alkotmánybíróság megállapította a 172.§ alaptörvény-ellenességét,[23] azonban az alkotmányjogi panasz benyújtása és a határozathozatal között bekövetkezett törvénymódosítás okán csupán elvi jelentősége miatt fontos mérföldkő az alaptörvény-ellenesség utólagos kimondása.

---

[19] Varga-Sabján Dóra – Sebhelyi Viktória: Gyermekprostitúció – magyarországi helyzetkép emberi jogi és pszichológiai nézőpontból. In: Fundamentum 2018/1. p. 44.
[20] Gyermekprostitúció visszaszorítása, gyermekkereskedelem. Szociális és Gyermekvédelmi Főigazgatóság, Budapest 2018. 70. o.
[21] Alaptörvény XVI. cikk (1) bekezdés.
[22] Alaptörvény Q,¸cikk (2) bekezdés.
[23] 18/2020. (VII.21.) AB határozat a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény 121-122- §-aival kapcsolatos mulasztásban megnyilvánuló alaptörvény-ellenesség megállapításáról, valamint a korábban hatályban volt 172. § alaptörvény-ellenességének megállapításáról és a 32.Szef.66/2017/2. számú szabálysértési eljárás felülvizsgálatának elrendeléséről.

A Szabs.tv. 172.§ hatályos formája rögzíti, hogy a törvényben, vagy törvény felhatalmazása alapján hozott önkormányzati rendeletben meghatározott szexuális szolgáltatással összefüggő korlátozást megszegő prostituált nem büntethető, amennyiben a cselekmény elkövetésekor még nem töltötte be tizennyolcadik életévét. A 172.§ (5) bekezdése által újabb előrelépés történt a gyermekvédelem terén, deklarálásra került ugyanis, hogy a gyermek prostituált védelme érdekében a rendőrség azonnal végrehajtható általános védelmi intézkedést hozhat.

4.2. Az önkéntesség kérdése

Számos bűnözési forma, így az ember-, és fegyverkereskedelem, a pénzmosás mind-mind ezernyi szállal kötődhet a prostitúcióhoz. [24] A bűncselekményekhez való kapcsolódás azonban nem evidens, mindemellett pedig számos más szempont is megnehezíti, hogy állást lehessen foglalni akár a kriminalizálás, akár a legalizálás mellett. A megítélés dilemmáit álláspontom szerint leginkább az a két végpont szemlélteti, amely a feminista elméletek körében alakult ki.

Egyrészt, a prostitúció felfogható akképp is, mint a nők saját testük feletti önrendelkezési jogának kifejeződése,[25] míg a másik feminista irány híveinek véleménye szerint a prostitúció csak egy férfiak által uralt társadalomban lehet elfogadott, ahol természetes, hogy a férfiak szexuális igényeire a megfelelő intézményt a pénzért hozzáférhető nők jelentik.[26]

Amennyiben a jogalkotó szabályozza a prostitúciót, mindez nem oldható meg anélkül, hogy valamilyen mértékben ne foglaljon állást abban a kérdésben, hogy elfogadhatónak tarja-e létét a társadalomban, és amennyiben igen, milyen keretek között.[27]

Ami a magyar szabályozást illeti, napjainkban a prostitúció, bizonyos kritériumok fennállta esetén, nem jogellenes tevékenység. Ugyan a Btk. büntetni rendel egyes magatartásokat, példának okáért kerítés, kitartottság, illetve témánk szempontjából elengedhetetlen a gyermekprostitúció kihasználása bűncselekmény említése, és a Szabs.tv. is meghatároz bizonyos keretfeltételeket, elmondható, hogy a vonatkozó közegészségügyi,

[24] Janó Márk: A prostitúcióval kapcsolatos jogi szabályozás. IN: Ékes Ilona (szerk.) : Nyitott szemmel az ifjúság védelmében. ERGO Európai Regionális Szervezet, Budapest, 2014. p. 20.
[25] Podoletz Léna: A prostitúció szabályozásának lehetséges megoldásai és főbb problémai. In: Belügyi Szemle 2015/3. p. 100.
[26] Carole Pateman: What's Wrong with Prostitution?In: Womaen's Studies Quarterly 1999/27. p.57. Idézi Podoletz (2015) p. 100.
[27] Podoletz (2015) p. 97.

közrendvédelmi és gazdasági kritériumoknak való megfelelés esetén a prostituált nem követ el jogsértést.[28]
Amint arra a feminista irányzat is utalt, a prostitúció megítélése nagyban függ attól, miképp vélekedünk az egyén saját teste feletti önrendelkezési jogáról. A legalizálás fontos kritériuma, hogy adott személy azon döntése, melyből következően áruba bocsátja önmagát – vagy legalábbis, amennyiben a szerződéses elmélet [29] nézeteit vesszük alapul, egy önnön testéhez elválaszthatatlanul kötődő szolgáltatást – kényszermentes elhatározás nyomán szülessen meg. Mindebből azonban következik a kérdés: mi is tekinthető kényszernek valójában? Amennyiben filozófiai síkra helyezkedünk, felmerül a következő dilemma: mi történik, ha elvesszük egy gyermektől, akár akaratlanul is a jövőt úgy, hogy felé ártalmakat közvetítve torzítjuk a személyiségét, belekényszerítve őt ekképp az önsorsrontósba?
Különösen érdekes ennek vizsgálata, amennyiben figyelembe vesszük, hogy „*a prostituálttá válás okai között első helyen a gyermek-és fiatalkorban elszenvedett visszatérő szexuális, illetve fizikai visszaéléseket kell megemlíteni. (…) Megtanulja, hogy teste nem csupán saját énjének egy aspektusa, hanem egyben más személyek az övéitől független, nemegyszer számára kellemetlen céljainak szolgálatában is állhat. A verés, az éheztetés, a gondoskodás és a gyöngédség hiánya sajátos hasadást (szkízist) idézhet elő: az intimitás és a test egymástól elkülönülő entitássá válik szét.”*[30]
Az általánosítás kerülendő ugyan, és nem lehet kijelenteni, hogy minden szexmunkás mögött hányattatott gyermekkor áll, ám az idézett problematikának újabb vetülete vezet el, és mutat rá azon esetek szomorú hatásira, amikor a gyermek nem az őt ért bántalmazás hatására dönt később a prostitúció mellett, hanem már gyermekként prostituálódik. Felmerül a kérdés: beszélhetünk-e önkéntességről gyermekek esetén? Jelentheti-e a belegyezési korhatár elérése a teljes szexuális önrendelkezést, és ily formában a prostituálttá válást?
Nem lehet kérdés, hogy a gyermekprostitúcióra csak kizsákmányolásként lehet tekinteni, aminek hátterében súlyos kényszerítő tényezők állhatnak. [31] Egyrészt, a gyermek prostitúció világába történő bekerülése átlagosan 13 éves korára tehető, amely életszakaszban a kognitív struktúrák éretlenségére visszavezethetően nem várható el átgondolt döntések meghozatala.[32]

[28] Kovács István: TEÁOR 9604, avagy a prostitúció legalitásának gazdasági kritériuma. p. 102. https://real.mtak.hu/105884. (2022.05.14.)
[29] A szerződéses elmélet lényege, hogy nem saját magát adja el, hanem csak bizonyos szolgáltatást. Podoletz (2015) p. 99.
[30] Betlen Anna: A képmutatás törvényi útja, avagy egy lépés a prostitúció legalizálása felé. In: Fundamentum 1998/4. p. 162.
[31] Varga-Sabján – Sebhelyi (218) p. 52.
[32] [32] Gyermekprostitúció visszaszorítása, gyermekkereskedelem. Szociális és Gyermekvédelmi Főigazgatóság, Budapest 2018. p. 42.

A választás szabadságát makro- és mikroszociális okok is behatárolják.[33] Mikroszinten említhető az elhanyagolás, a bántalmazás, családi funkciók szétesése, makroszinten pedig, hogy a média és a patriarchális berendezkedés aláássa a prostitúció iránti társadalmi figyelem igényét.[34]
Az önkéntesség kérdése az online szexuális abúzusok során új köntösbe bújtatva, ugyanakkor sokkal konkrétabban jelenik meg, hiszen a gyermek számos esetben nem is tudhatja, példának okáért a róla készített intim felvételeket kihez juttatják el az általa esetlegesen engedélyezett személyeken kívül.

5. Gyermekprostitúció online környezetben

5.1. Online szexuális kizsákmányolás

Jelentős probléma, hogy a gyermekprostitúció szinte láthatatlan. Túlnyomórészt nem az utcán, és még csak nem is azokon a helyeken történik, amelyet az emberek a prostitúcióval azonosítanak. Az online világ a szexuális szolgáltatások hirdetésének kulcsfontosságú színtere, hiszen a szolgáltatást igénybe vevők számára előnyös az anonimitás, a fiatalok pedig számos színtéren könnyen és gyorsan elérhetők.[35]
A szakemberek, akadémikusok és az áldozatok a szexuális erőszak alatt olyan cselekményt is értenek, amely a fizikai sérelem okozása mellett/helyett pszichés traumát is okoz, így a kibertérben elkövetett szexuális erőszakot, mint olyan cselekményt azonosíthatjuk, amelyet számítástechnikai eszköz felhasználásával követnek el.[36] Nem szükséges tehát a személyes jelenlét ahhoz, hogy a bántalmazás megtörténjen.
A gyermekek online szexuális kizsákmányolásának öt típusát különböztethetjük meg: gyermek szexuális kizsákmányolását rögzítő anyag, onine grooming, sexting, sexortion és a gyermek szexuális bántalmazásnak online közvetítése.[37]
Az alábbiakban a gyermekek online szexuális kizsákmányolásának azon formáit tekintem át, amelyek megvalósítják a Lanzarote Egyezményben meghatározott gyermekprostitúciót, majd ezt követően térek rá a grooming

[33] [33] Gyermekprostitúció visszaszorítása, gyermekkereskedelem. Szociális és Gyermekvédelmi Főigazgatóság, Budapest 2018. p. 43.
[34] Uo.
[35] The role of the Internet in prostitution as a phenomenon among minors. https://gov.il/en/departments/giudes/online_teen_prostitution. (2022.05.14.)
[36] Köllő (2020) p. 65.
[37] Merli Pullerits: Online Child Sexual Exploitation: A Common Understanding. https://childhub.org/en/child-protection. (2022.05.14.)

cselekmények elemzésére, amelyek alkalmasak arra, hogy a gyermeket a későbbiekben prostitúció folytatásra vegyék rá.

5.2. Élő online szexuális bántalmazás

Az úgynevezett „szexturizmus" egy aspektusa a gyermekek szexuális kizsákmányolása az utazás és a turizmus kontextusában.[38]
Általánosságban elmondható, hogy egy szegényebbnek tekinthető országban az idegenforgalom fejlődése szinte óhatatlanul a gyermekprostitúció terjedéséhez vezet. [39] A téma kapcsán bizonyára legtöbben Ázsiára asszociálunk, azonban a szexturizmus Magyarországot is érinti: statisztikák szerint az emberkereskedelem magyar gyermek áldozatait külföldön szexuális célra használják.[40]
A gyermekek elleni szexuális visszaélések a legtöbb államban napjainkra tiltott cselekménnyé váltak, ám a számítógépes szexturizmus kialakulásával nemcsak, hogy az országhatár átlépésének kényelmetlensége szűnt meg, hanem speciális technikák segítségével a lelepleződés kockázata is csökkenthető.
A Terre des Homes svájci gyermekvédő szervezet megfogalmazásában az ilyesfajta esetek során felnőttek fizetnek, vagy más ellenszolgáltatást nyújtanak azért, hogy megtekinthessék a más országban élő, szexuális visszaélést elkövető által közvetített élő videofelvételeket. [41]
Amennyiben egységes terminológia alá kívánjuk vonni a hasonló ügyeket, a gyermekvédelmi szakemberek álláspontja alapján megállapíthatjuk, hogy a „webkamerás gyermek szexturizmus" elnevezés helyett a „webkamerás gyermek szexuális bántalmazása" kifejezés a megfelelő, tekintettel arra, hogy jelen esetben egy speciális technológiai eszközről van szó, továbbá az élő online szexuális bántalmazás kifejezés sokkal szélesebb fogalmat takar.[42]
A szexuális zaklatásban részt vevők lehetnek passzívak – azaz fizetnek, hogy nézzék az online közvetítést, de lehetőség van arra is, hogy a különböző kommunikációs alkalmazások video csevegés funkciói által kommunikáljanak a gyermekkel, a szexuális bántalmazóval vagy az őt segítő személlyel, és konkrét fizikai cselekményeket hajtassanak végre.[43]

---

[38] Hegyaljai Mátyás: Nemzetközi rendvédelmi lehetőségek az idegenforgalomban megjelenő szexuális kizsákmányolás ellen. In: Németh Kornél (szerk): I. Turizmus és biztonság nemzetközi tudományos konferencia konferenciakötete. Pannon Egyetem, Nagykanizsa, 2016. p. 25.
[39] Hegyaljai, (2016) p. 26.
[40] A szexturizmus nem bocsánatos bűn – Dr. Gyurkó Szilvia a Thaiföldre utazó harcostársról, a homoszexualitás és a pedofília összemosásáról. https://wmn.hu/ugy/54099. (2022.05.14.)
[41] Köllő (2020) p. 72.
[42] Hegyaljai, (2016) p. 28.
[43] E4J University Modul Series: Cybercrime. https://unodc.org/e4j.hu. (2022.05.14.)

Amennyiben a streaming során felvételek is készülnek, a gyermek szexuális kizsákmányolását rögzítő anyag birtoklása amellett, hogy a legtöbb állam büntetőjogában tiltott,[44] a gyermekre nézve további ártalmakat okozhat. Abban az esetben, ha a felvételt megosztják az interneten, hatására a traumatizáló faktor is megváltozik: a viktimizáció örökké tart, és a felvételek újbóli megtekintésével megy végbe.[45] A gyermekpornográf tartalmak készítése, illetve az azzal való kereskedés jövedelmező voltát a szervezett bűnözői csoportok is felismerték és kihasználják.[46]

6. A child grooming szerepe a prostitúcióban

6.1. A „loverboy jelenség" online aspektusai

Az utóbbi időkben a klasszikus értelemben vett futtatók helyét úgynevezett „loverboyok" vették át, akik általában a hátrányos helyzetű, érzelmileg és fizikailag kiszolgáltatott gyermekeket hálózzák be.[47] Az online világ térhódításából fakadóan pedig a behálózásnak is új dimenzióival kell szembenéznünk.
Müller-Güldermeister megfogalmazásában a loverboy olyan személy, aki elcsábítás, ígéret, zsarolás, akár erőszak útján prostitúcióra bírja rá áldozatait anyagi előny szerzése céljából. Áldozatai túlnyomórészt kiskorú lányok, akiket személyesen, vagy online ismer meg.[48] Az áldozatokkal történők kapcsolatfelvétel taktikái tehát a grooming fizikai és online formái körébe sorolhatók.
A grooming, vagy más néven luring magyarra fordítva leginkább a behálózás, becserkészés szavakkal írható le. A „groomer" olyan személy, aki érzelmi kapcsolatot alakít ki a gyermekkel annak érdekében, hogy rávegye őt szexuális tartalmú beszélgetések folytatására, intim képek küldésére (sexting), a fentebb említett élőben közvetített szexuális cselekmények folytatására, valamint a személyes találkozóra.[49] A fiatalok körében oly népszerű Tinder, Snapchat, Tiktok és Instagram direct alkalmazások mind alkalmas felületek az online

[44] A magyar büntetőjog a Btk. 204. §-a alatt szabályozza a gyermekpornográfia tényállását.
[45] E.J. Klain: The Global Victimization of Children: Problems and Solutions. Idézi Köllő (2020) p. 69.
[46] Mezei Kitti: A kiberbűnözés aktuális kihívásai a büntetőjogban. Társadalomtudományi Kutatóközpont Jogtudományi Intézet – L'Harmattan, Budapest. 2020. p. 171.
[47] Hatvani Erzsébet – Sebhelyi Viktória – Vaskuti Gyergely: Gyermekprostitúció visszaszorítása, gyermekkereskedelem. p. 42. https://prekogalfa.hu/documents/efop/tf-_gyvgy_pdf.pdf. (2022.05.14).
[48] Christina Sarah Wuff-Besold: Wenn aus Liebe Prostituton wird – die Opfer der Loverboy-Methode. Bachelor Thesis zum Erwerb des Bachelor-Diploms in Sozialer Arbeit, Bern, 2020. p. 8.
[49] https://childline.org.uk. (2022.05.14.)

grooming megvalósítására. A leginkább veszélyeztetettek az érzelmileg elhanyagolt, emellett pedig alacsony média- és adattudatossággal rendelkező gyermekek, hiszen a közösségi média világában akár már egy poszt alapján is rendkívül pontosan fel lehet mérni a megosztó önbecsülését, könnyű szerrel kiválasztva így a megerősítésre vágyó áldozatokat.

6.2. Az online csevegéstől a prostitúció felé vezető út állomásai

Az online grooming problematika jelentőségét szemlélteti, hogy a Lanzarote Bizottság 2015-ben kiadott álláfoglalása szerint a jelenlegi és jövőbeli technológiai fejlettség mellett a szerződő feleknek meg kell fontolniuk a kriminalizáció kiterjesztését azon esetekre is, amikor a szexuális célú kapcsolatfelvétel csak a virtuális valóságban következik be[50].
A grooming folyamata során a behálózó személyek a gyermek bizalmi körébe férkőznek, majd manipulálják őt: fokozatosan elhitetik vele, hogy a felnőttel való fizikai kapcsolat elfogadható, kellő bizalom után pedig ráveszik, hogy hajtsa végre a kívánt szexuális tevékenységet.[51] A tapasztalatlan fiatalok számára normalizálódik, hogy idegen személyekkel, például a loverboy barátaival kell nemi kapcsolatot létesíteniük szerelmük megsegítése érdekében.[52]
Ellenállás esetén az érzelmi zsarolás („más megtenné értem”), anyagi függőség és ebből adódóan a menekülési lehetőségek csökkentése, valamint drogfüggőség kialakítása mellett a nyomásgyakorlás fontos eszköze az áldozatok tudatos kriminalizálása azáltal, hogy kényszerítik őket bűncselekmények elkövetésére, például lopásra, kábítószerkereskedelemre vagy pornográf tartalmakon való szereplésre.[53]
Ebből fakadóan kiemelten fontos a prostitúció és a gyermekbántalmazás közötti összefüggések felismerése, annak az evidenciának a minél szélesebb jogalkalmazói körben történő nyomatékosítása, hogy amint azt Székely László megfogalmazta: a gyermekprostituált mindig csak áldozat lehet[54].

[50] Mezei Kitti: Az online gyermekpornográgia és a büntetőjog. In: Ügyészek Lapja 2021/4. p. 22.
[51] Alin Teodorus Dragan: Child pornography and child abuse in cyberspace. In: Journal of Legal Studies 2018/28. p. 52.
[52] Wuff-Besold, (2020) p. 16.
[53] Wuff-Besold, (2020) p. 17-18.
[54] A prostitúció áldozatává váló gyermek jogainak védelme és a megelőzés lehetséges eszközei- az alapvető jogok biztosának utóvizsgálata. https://ajb.hu/a-prostitucio. (2022.05.14.)

7. Értékelő megállapítások

A vonatkozó uniós egyezményeknek megfelelően a gyermekek szexuális kizsákmányolása minden tagállamban büntetőjogilag tilalmazott, a technológiai fejlődés azonban számos szürke zónát eredményezett. Így példának okáért nem egységes a grooming cselekmények szabályozása sem.
A Lanzarote Egyezmény rögzíti, hogy a szerződő feleknek meg kell tenniük minden szükséges jogalkotási intézkedést annak érdekében, hogy büntethető legyen az, aki informatikai vagy kommunikációs technológiák alkalmazása útján grooming körébe tartozó cselekményeket követ el.[55]
Példával szemléltetve az eltérő megközelítési módokat, a becserkészés a magyar jogban előkészületi cselekményt jelent, ebből fakadóan a gyermekpornográfia tényállásába a „rábírni törekszik" fordulat útján került be[56], míg az osztrák büntetőjog[57] önálló törvényi tényállás alatt szabályozza a cybergrooming fordulatait.
Az áldozatok számos esetben nem mernek a hatóságtól segítséget kérni, holott, amint arra Jessica Taylor rámutat: nem csak a szexuális bűnözők tudnak manipulálni, rávenni valakit valamire: a legtöbben minden nap – még ha csekély szinten is, de – szembesülünk a behálózás formáival. Ebből fakadóan fontos tudatosítani az áldozatban, hogy grooming elszenvedése esetén nincs egyedül[58], így elkerülhető, hogy hiszékenysége táplálta szégyenérzetéből fakadóan magába zárkózzon traumáival. Az elzárkózás kapcsán említésre érdemes, hogy kvantitatív kutatások alapján a prostitúciós iparban a nők sorstársaik előtt is titkolják félelmeiket, amely számos esetben kizárhatja a külső segítség kérése mellett egymás támogatását is a veszélyes helyzetekben.[59]

---

[55] Az Európa Tanács Egyezménye A gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen. 23. cikkely.
[56] Krasznay Csaba: Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése.In: Külügyi Szemle 2021/1. p. 203.
[57] *„(1) Wer in einer unmündigen Person in der Absicht, an ihr eine strafbare Handlung nach den §§ 201 bis 207a Abs. zu begehen,*

1. im Wege einer Telekommunikation, unter Verwendung eines Computersystems oder

2. auf sonstige Art unter Tä,uschung über seine Absicht

ein persönliches Treffen vorschlägt oder ein solches mit ihr vereinbart und eine konkrete Vorbereitungshandlung zur Durchführung des persönlichen Treffens mit dieser Person setzt, ist mit Freihetitsstrafe bis zu zwei Jahren zu bestrafen." § 208a StGB Anbahnung von Sexualkontakten zu Unmündingen.
[58] Jessica Taylor: Why grooming is so hard to spot:The truth. https://prostitutionresearch.com/why-grooming-is. (2022.05.14.)
[59] Dés Fanni: A patriarchátus elbeszélhetetlensége. A távolság szerepe a prostitúciós iparban használt és a prostitúciós iparból kiszállt nők traumanarratíváiban. In: Replika 200/117-118. p. 14.

Az Alkotmánybíróság 18/2020.(VII.21.) határozatában kiemelte, hogy a gyermekek megfelelő fejlődését hátrányosan érinti a prostitúciós tevékenységgel való közvetlen kapcsolatba kerülés, ebből következően az állam intézményvédelmi kötelezettsége rendkívül fontos a gyermekek prostitúciós célú kizsákmányolásának kérdésében. [60]

A védőfaktorok között számon tarthatjuk a harmonikus családban felnevelkedést, érzelmi biztonság meglétét [61], ebből következően pedig a gyermekprostitúcióba való bevonódás elleni küzdelemben jelentős szerephez kell, hogy jusson a gyermekvédelem intézményrendszerének fejlesztése, a gyermekvédelmi paradigmában gondolkodás kiterjesztése. Az online világ térhódítására tekintettel, a gyermek minél fiatalabb korban történő média-és adattudatosságra nevelése sem hanyagolható el.

Megkerülhetetlen továbbá a média szerepe a prostitúcióról alkotott kép megformálásában – problematikus azonban, hogy az érintett fiatalok a vonatkozó hírekben nem gyermekként, hanem „éjszakai pillangó", „örömlány" szalagcímek alatt szerepelnek.[62]

A koronavírus-járvány negatív hatásai a gyermekvédelem területén is érzékelhetők. Az EUROPOL statisztikái szerint a pandémia alatt megszaporodtak az online felületeken a gyermekek sérelmére elkövetett szexuális erőszakot ábrázoló felvételek. [63] A gyermekek szexuális kizsákmányolása, mint a cyberbűnözés egy formája elleni küzdelem az EU egyik prioritása lesz a 2022-2025 közötti időszakban.[64]

Más szemszögből megközelítve a kérdést, az által, hogy életük a közelmúltban egyre inkább a virtuális valóságba helyeződött, a gyermekek is egyre merészebb, aktívabb, az idősebb generáció által pedig egyre kevésbé követhető módon vesznek részt a cybertársadalomban. Gyermekprostitúció esetében azonban nem beszélhetünk önkéntességről, még ha az adott gyermek el is érte a beleegyezési korhatárt, az esetleges szabálysértések elkövetése esetén is csupán, mint áldozat kerülhet a hatóság fókuszába.

A gyermekprostitúció és a virtuális valóság összefonódásai pedig rávilágítottak arra is, hogy a gyermek szexuális bántalmazása a technológiai fejlettség jelenlegi fokán akár az áldozat és az elkövető fizikai érintkezése nélkül is megvalósulhat.

---

[60] ECPAT Országjelentés: Jelentés a gyermekek szexuális kizsákmányolásának formáiról, jellemzőiről és méretéről- Magyarország, 2021. február. p. 22. https://tinyurl.com/2p99sc4x. (2022.05.14.)

[61] Kugler Gyönygi: Gyermekprostitúció megelőzése. Gyökerek-megelőzés- jelzőrendszer szerepe. IN: Ékes Ilona (szerk.) : Nyitott szemmel az ifjúság védelmében. ERGO Európai Regionális Szervezet, Budapest, 2012. p. 20.

[62] Hatvani Erzsébet – Sebhelyi Viktória – Vaskuti Gyergely, (2018) p.82.

[63] Why Children are at Risk of Sexual Exploitation during COVID-19. https://ecpat.org.

[64] https://europol.europa.eu/c rime-areas-and-statistics/crime-areas/child-sexual-exploitation.

Irodalomjegyzék

- Babity Mária: A gyermekbántalmazás rizikótényezőinek vizsgálata (magas kockázatot képviselő gyermeknevelési attitűdök, a szülőkkel kapcsolatos gyermekkori emlékek és néhány lehetséges közvetítő tényező összefüggései). PhD értekezés, Pécs, 2013.
- Betlen Anna: A képmutatás törvényi útja, avagy egy lépés a prostitúció legalizálása felé. In: Fundamentum 1998/4. pp. 159-166.
- Dés Fanni: A patriarchátus elbeszélhetetlensége. A távolság szerepe a prostitúciós iparban használt és a prostitúciós iparból kiszállt nők traumanarratíváiban. In: Replika 2000/117-118. pp. 127-148.
- Dragan, Alin: Child pornography and child abuse in cyberspace.In: Journal of Legal Studies 2018/28. pp. 52- 60.
- Hatvani Erzsébet – Sebhelyi Viktória – Vaskuti Gyergely: Gyermekprostitúció visszaszorítása, gyermekkereskedelem. Szociális és Gyermekvédelmi Főigazgatóság, Budapest, 2018.
- Hegyaljai Mátyás: Nemzetközi rendvédelmi lehetőségek az idegenforgalomban megjelenő szexuális kizsákmányolás ellen. In: Németh Kornél (szerk): I. Turizmus és biztonság nemzetközi tudományos konferencia konferenciakötete. Pannon Egyetem, Nagykanizsa, 2016. pp. 25-32.
- Janó Márk: A prostitúcióval kapcsolatos jogi szabályozás. IN: Ékes Ilona (szerk.) : Nyitott szemmel az ifjúság védelmében. A gyermekbántalmazás és a gyermekprostitúció ellen. ERGO Európai Regionális Szervezet, Budapest, 2014. pp.11-33.
- Józsa László: Prostitúció és pedofília a Bizánci Birodalomban (324-1453). In: Művelődés, Tudomány –és Orvostörténeti Folyóirat. 2011/2. pp. 35-52.
- Köllő Dávid: A gyermekek szexuális kizsákmányolása a kibertér felhasználásával. IN: Belügyi Szemle, 2020/2. pp. 59-87.
- Kugler Gyöngyi: Gyermekprostitúció megelőzése. Gyökerek-megelőzés-jelzőrendszer szerepe. IN: Ékes Ilona (szerk.) : Nyitott szemmel az ifjúság védelmében. ERGO Európai Regionális Szervezet, Budapest, 2012. pp. 79-89.
- Mezei Kitti: A kiberbűnözés aktuális kihívásai a büntetőjogban. Társadalomtudományi Kutatóközpont Jogtudományi Intézet – L'Harmattan, Budapest, 2020.
- Mezei Kitti: Az online gyermekpornográgia és a büntetőjog. In: Ügyészek Lapja 2021/4. pp. 19-31.
- Parti Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó, Miskolc. 2009.

- Pintér Ádám – Tóth Judit Nikoletta: A bántalmazott gyermekek – Gyermekjogok és gyermekbántalmazás. In: Statisztikai Szemle 2017/8-9. pp. 847-872.
- Podoletz Léna: A prostitúció szabályozásának lehetséges megoldásai és főbb problémai. In: Belügyi Szemle 2015/3.pp. 97- 122.
- Pukánszky Béla: A gyermekkor története. Műszaki Könyvkiadó, Budapest. 2001.
- Varga-Sabján Dóra – Sebhelyi Viktória: Gyermekprostitúció – magyarországi helyzetkép emberi jogi és pszichológiai nézőpontból. In: Fundamentum 2018/1. pp. 41.-57.
- Wuff-Besold - Christina Sarah: Wenn aus Liebe Prostituton wird – die Opfer der Loverboy-Methode. Bachelor Thesis zum Erwerb des Bachelor-Diploms in Sozialer Arbeit, Bern, 2020.

Gáti Balázs
PhD-hallgató (PTE-ÁJK)

A Schrems II ítélet lehetséges hatásai a nemzetközi jogalkotásra

Absztrakt

A Schrems I ítélet során az Ír Legfelsőbb Bíróság által megállapításra került, hogy a Facebook Ireland hatályos adatkezelési gyakorlata az EU állampolgárok személyes adatainak harmadik országba történő továbbítása vonatkozásában ellentétes az Alapjogi Charta-ban foglaltakkal. A Schrems II ítélet kapcsán az Európai Unió Bírósága szintén, immár az Általános Adatvédelmi Rendelet hatályba lépése után, de a 95/46 EK irányelv alapján úgy ítélte meg, hogy az EU-USA Adatvédelmi Pajzs nem nyújt megfelelő szintű védelmet a személyes adatok továbbítása tekintetében, így érvénytelenítette a megállapodást.
A fenti ítéletben az Európai Uniós Bírósága által megfogalmazott ajánlásokat az Európai Adatvédelmi Testület először 2020. novemberében az ítélet meghozatala után véleményezte, majd 2021. június 21-én hagyta jóvá azok végleges változatát a kiegészítő intézkedések kapcsán.
Tanulmányomban elemzem az EDPB által is elfogadott lehetséges gyakorlati megoldások, valamint az aktuális jogpolitikai folyamatok várható hatásait a személyes adatok nemzetközi továbbítására, különös tekintettel a közösségi média kapcsán előtérbe kerülő személyes- és gazdasági érdekekre.

Kulcsszavak: közösségi média, Schrems II, Privacy Shield, adatvédelem, adattovábbítás

1. Bevezetés

Az adattovábbítás a közösségi média vonatkozásában az Általános Adatvédelmi Rendelet[1] (továbbiak: „GDPR" vagy „Rendelet") szabályozása által kerül meghatározásra. A Rendelet szerint a tagállami szabályozás csak olyan harmadik országokba történő adattovábbítást tesz lehetővé, amelyek a személyes adatok kezelését tekintetében megfelelő szintű védelmet biztosítanak. A megfelelőséget az Európai Bizottság állapíthatja meg az

[1]Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) *Hivatalos Lap, L 119., 2016.5.4.,p.1- 88.*

GDPR-ban meghatározott előírások alapján az egyes országok adatvédelmi szintje tekintetében. Ha az adott ország által meghatározott adatkezelési szabályok nem felelnek meg az abban meghatározott követelményeknek, az adattovábbítás csak az Általános Adatvédelmi rendeletben meghatározott megfelelő jogalapok alkalmazásával lehetséges.[2] A GDPR viszonylag részletes szabályokat tartalmaz arra vonatkozóan, hogy milyen feltételek mellett továbbíthatók az adatok harmadik országokba (vagy nemzetközi szervezetek részére), hiszen ahogy a GDPR preambuluma is rögzíti (101): „*A nemzetközi kereskedelem és a nemzetközi együttműködés bővítéséhez szükség van a személyes adatoknak az Unión kívüli országok és a nemzetközi szervezetek viszonylatában megvalósuló forgalmára.*" A GDPR harmadik országokba történő adattovábbítására vonatkozó szabályai[3] lépcsőzetesen egymásra épülnek, ezek a megfelelőségi határozat, a megfelelő garanciák,[4] ennek hiányában a különleges helyzetek.[5] A GDPR 46. cikke további lehetőségeket biztosít az egyes adatkezelők számára az adattovábbítás jogszerűségének biztosítására. Ezek alapján az adatkezelők bevezethetnek úgynevezett kötelező érvényű vállalati szabályokat (Binding Corporate Rules, BCR), szerződéseikbe belefoglalhatják a Bizottság által elfogadott általános adatvédelmi záradékokat, tevékenységüket magatartási kódexnek vagy tanúsítási mechanizmusok szerint határozhatják meg. Fontos hangsúlyozni, hogy ilyen körülmények között adatkezelési szempontból nem a harmadik ország tekinthető a GDPR szabályai szerint megfelelőnek, hanem kizárólag az adott adattovábbítás, illetve ez utóbbi esetben az maga az adatkezelő, aki a meghatározott garancia alapján végzi az adatkezelési tevékenységet.

---

[2] Adatvédelmi irányelv, 25. cikk (1), 25. cikk (6), 26. cikk (1), 25. cikk (4)–(5)

[3] GDPR 44. cikk

[4] GDPR 45-46. cikk

[5] Különleges helyzetek esetében az adatok akkor továbbíthatók, ha - az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő esetleges kockázatokról, az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges, az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;az adattovábbítás fontos közérdekből szükséges; az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

A Schrems ítéletek az egyik legnagyobb közösségi háló adattovábbításával kapcsolatosak, ez pedig a Facebook, valamint a hozzá kapcsolt közösségi hálók.

Az Oxford Dictionaries a közösségi médiát weboldalak és alkalmazások összességeként írja le, amelynek során a felhasználók tartalmat készíthetnek és oszthatnak meg a közösségi hálózatokon.[6] Kaplan és Haenlein meghatározása szerint a közösségi média „*internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom*".[7] Bányász kiegészíti ezt a definíciót, mely szerint „*közösségi média alatt olyan internetes oldalak és alkalmazások összességét értem, amelyben a felhasználók állítják elő a tartalmat, a szolgálatók csupán a keretet biztosítják. Ebből következik, hogy a közösségi média a felhasználói interakcióból alakul ki, azonban ez a tartalom állandóan változhat a többi felhasználó interakciója révén.*"[8]

A piacvezető Facebook volt az első közösségi hálózat, amely meghaladta az egymilliárd regisztrált fiókot. A 2022-es januári Statista.com által közzé tett adatok alapján jelenleg több mint 2,9 milliárd havi aktív felhasználóval rendelkezik. 2022-ben, a közösségi oldalak a becslések szerint elérik a 3,96 milliárd felhasználót, és ezek a számok továbbra is növekedni fognak, mivel a mobileszközök használata és a mobil közösségi hálózatok egyre nagyobb teret hódítanak[9,10].

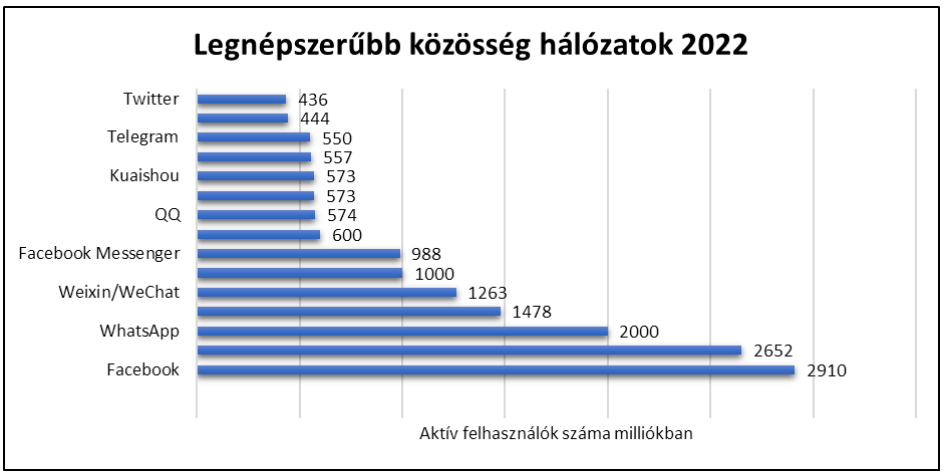
[6] Definition of social media in English, In: Oxford Dictionaries. URL: http://www .oxforddictionaries.com/definition/english/social-media

[7] Andreas Kaplan - Michael Haenlein: Users of the world, unite! The challenges and opportunities of Social Media. In: Business Horizons, 2010/1. p. 59.

[8] Bányász Péter: Közösségi média és közszolgálat. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet Kiadása, Budapest, 2020. p. 9.

[9] Ahmet Efe - Hamed Suliman: How Privacy is threatened from Social Media communication? In: Anatolian Journal Of Computer Sciences, 2021/6. p. 32.

[10] Andrea Kraut - László Kőhalmi - Dávid Tóth: Digital Dangers of Smartphones. In: Journal Of Eastern-European Criminal Law, 2020/1. p. 36.



1. ábra: A legnépszerűbb közösségi hálózatok világszerte 2022 januárjában, a havi aktív felhasználók száma szerint rangsorolva (milliókban). Saját szerkesztés Forrás: Statista.com

A Facebook adattovábbítása kapcsán születtek meg a Schrems I és II ítéletek, melyek felhívták a figyelmet a harmadik országokba való adattovábbítási gyakorlatok problémáira, a közösségi oldalak helytelen gyakorlatára az érvényben lévő adatvédelmi szabályozások tükrében. Tanulmányomban elemezni kívánom az EDPB által elfogadott lehetséges gyakorlati megoldások, valamint az aktuális jogpolitikai folyamatok várható hatásait a személyes adatok nemzetközi továbbítására, különös tekintettel a közösségi média kapcsán előtérbe kerülő személyes- és gazdasági érdekekre.

2. Előzmények – A Biztonságos kikötő és a Schrems I ítélet

Az osztrák állampolgárságú Maximillian Schrems 2013-ban panaszt nyújtott be az ír felügyeleti hatósághoz, melyben kérte a hatóságot, hogy tiltsa meg a Facebook Ireland számára a személyes adatainak az Egyesült Államokban letelepedett leányvállalata, a Facebook Inc[11]. számára történő továbbítását. Arra hivatkozott, hogy az Egyesült Államokban hatályban lévő jog a hatóságok

[11]A Meta Platforms, Inc. Meta néven, korábban Facebook, Inc. és TheFacebook Inc.néven egy amerikai multinacionális technológiai konglomerátum, amelynek székhelye a kaliforniai Menlo Parkban található. A cég a Facebook, az Instagram és a WhatsApp anyaszervezete, más leányvállalatok mellett. A Meta a világ egyik legértékesebb vállalata. A Meta termékek és szolgáltatások közé tartozik a Facebook, a Messenger, a Facebook Watch és a Facebook Portal. Felvásárolta az Oculust, a Giphyt, a Mapillaryt, a Kustomer-t, a Presize-t is, és 9,99%-os részesedéssel rendelkezik a Jio Platforms-ban. 2021-ben a cég bevételének 97,5%-át a marketingesek számára értékesített reklámelhelyezésekből érte el.

által folytatott megfigyelési tevékenységekkel [12] szemben nem biztosít a területén tárolt személyes adatok számára elégséges védelmet. Panaszát a Bizottság 2000/520 határozatára[13] hivatkozással utasították el, megállapítva, hogy az Egyesült Államok a *„Safe Harbour"* rendszere keretében megfelelő védelmi szintet biztosít, így lehetővé teszi a személyes adatok továbbítását részükre.

Az Európai Unió Bíróságának ítélete a Schrems I C-362/14. No. Maximillian Schrems kontra Adatvédelmi Biztos ügy kapcsán ezt a határozatot érvénytelennek nyilvánította. Megállapította a 2000. július 26-i 2000/520/EK határozat érvénytelenségét előzetes döntéshozatali eljárás keretében.[14] Ezen ítélet értelmében az ír felügyeleti hatóság köteles volt kivizsgálni Maximilian Schrems panaszát, és a vizsgálat végén döntenie kellett arról, hogy az irányelv alapján felfüggeszti-e az európai Facebook-felhasználók adatainak az Egyesült Államokba történő továbbítását azon az alapon, hogy a személyes adatok megfelelő szintű védelme nem biztosított az EU-s standardok szerint. A Schrems I ítéletben az Ír Legfelsőbb Bíróság megállapította, hogy a Facebook Ireland hatályos adatkezelési gyakorlata az EU állampolgárok személyes adatainak harmadik országba történő továbbítása vonatkozásában ellentétes az Alapjogi Charta-ban foglaltakkal.

2015. október 6-án az Európai Unió Bírósága kimondta a Bizottság „Safe Harbor" határozatának érvénytelenségét[15].

Schubauer a Safe Harbor érvénytelenítésének általános adatvédelmi gyakorlatra vonatkozó hatásait részletesen elemezte[16]. Kiemelte, hogy a „*Safe Harbor határozat érvénytelenítésével az eddig kialakult adatvédelmi gyakorlat megroppant, bizonytalanságban hagyva a piaci szereplőket és néha még magukat a tagállami adatvédelmi hatóságokat is*". Kis Kelemen és Hohman megállapítja, hogy mindez komoly kihívás az adatkezelők számára, „*hogy más, az EU adatvédelmi irányelvének megfelelő jogalapot biztosítsanak a transzatlanti adattovábbításra*." Közleményükben elemzik, az Adatvédelmi

[12]Edward Snowden, aki az amerikai Nemzetbiztonsági Ügynökségnél (NSA) dolgozott, 2013-ban információt szivárogtatott ki a szervezet által végzett tömeges adatgyűjtésről újságíróknak.

[13]A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről, *Hivatalos Lap L 215, 25/08/2000. p. 0007 – 0047.*

[14] Yves Bot Főtanácsnok Indítványa, C-362/14. sz. ügy Maximillian Schrems kontra Data Protection Commissioner https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62014CC0362&from=HU

[15] A Bíróság (nagytanács) 2015. október 6-i ítélete (a High Court [Írország] előzetes döntéshozatal iránti kérelme) – Maximillian Schrems kontra Data Protection Commissioner (C-362/14. sz. ügy), Hivatalos Lap, C 398, 2015.11.30. p. 6.

[16] Schubauer Petra: A Safe Harbor határozat érvénytelenítésének hatása az európai adatvédelmi gyakorlatra. In: Belügyi Szemle, 2017/2. p. 88.

Irányelv adattovábbítási szabályozása mellett különösen az érintett hozzájárulásán alapuló adattovábbítási gyakorlatot, részletesen kiemelve a fogalmi meghatározások jelentőségét, és a Facebook adattovábbítási gyakorlatát is, valamint M. Schrems újabb beadványai kapcsán, az adattovábbítási gyakorlat lehetséges megítélését is[17].

A Schrems I ítélet nyomán és azt követően, hogy az ír bíróság ez alapján megsemmisítette az e panaszt elutasító határozatot, az ír felügyeleti hatóság felhívta M. Schremset, hogy fogalmazza újra a panaszát figyelemmel arra, hogy a Bíróság érvénytelennek nyilvánította a 2000/520 határozatot. Schrems továbbra is fenntartotta, hogy az USA nem nyújt megfelelő védelmet az oda továbbított adatok vonatkozásában és ismét kérte, hogy a hatóság tiltsa meg vagy függessze fel személyes adatainak a Facebook Inc. részére történő továbbítását, amelyet a Facebook Ireland immár a 2010/87 határozat [18] mellékletében szereplő általános adatvédelmi kikötések alapján végez.

A kialakult helyzet nyomán az Európai Bizottság 2015. november 6-án iránymutatást[19] nyújtott a tagállami adatvédelmi hatóságoknak, hogy hogyan járjanak el az Egyesült Államokba történő adattovábbításokkal kapcsolatos ügyekben. Ezen felül tájékoztatót adott ki a transzatlanti adattovábbítások jogi alapját megteremtő alternatív megoldásokhoz a piaci szereplők számára, valamint megkezdődött a Safe Harbor program újra tárgyalása az Egyesült Államokkal. Az Egyesült Államok és az EU között a személyes adatok áramlásának új keretrendszeréről 2016 februárjában született megállapodás eredményeként az Európai Unió Bizottsága 2016. július 12-én fogadta el az EU-USA Adatvédelmi Pajzsot. [20] Az Európai Bizottság 2016. júliusában igazolta is az ez által biztosított védelem megfelelőségét. Az Adatvédelmi Pajzs egyrészt már valódi védelmet[21] kíván biztosítani azon európai polgárok

[17] Kis Kelemen Bence - Hohmann Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. In: Infokommunikáció és Jog, 2016/2-3. p. 66.

[18]A 2016. december 16-i (EU) 2016/2297 bizottsági végrehajtási határozattal módosított, a 95/46 irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i 2010/87/EU bizottsági határozat Hivatalos Lap 2010. L 39. p. 5.

[19]A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK a 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-)ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról, Brüsszel, 2015.11.6. COM(2015) 566 final

[20] A BIZOTTSÁG VÉGREHAJTÁSI HATÁROZATA (2016.7.12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről. Brüsszel, 2016.07.12. C(2016) 4176 final

[21] A szabályozás szerint az USA Kereskedelmi Minisztériuma közzéteszi az adatvédelmi pajzsban részt vevő szervezetek listáját és a szervezeteknek évente újra kell tanúsítaniuk magukat, ennek hiányában nem kezelhetnek jogszerűen az EU-ból származó személyes adatokat. A Pajzs – elviekben – biztosítékokat nyújt az USA kormányzata általi adathozzáférésekkel szemben és jogorvoslati lehetőségeket teremt az EU-s polgárok számára.

számára, akiknek a személyes adatai továbbításra kerülnek az USA-ba, másrészt tiszta jogi helyzetet kíván teremteni azon vállalatok részére, akik számára mindennapos az ilyen adattovábbítás.
Az előzetes döntéshozatal iránti kérelmében az előterjesztő bíróság a GDPR-nak a 2010/87 határozatban szereplő általános adatvédelmi kikötéseken alapuló személyesadat-továbbításra való alkalmazhatóságáról, az ilyen továbbítás keretében az e rendelet által megkövetelt védelmi szintről és az ebben az összefüggésben a felügyeleti hatóságokra háruló kötelezettségekről kérdezte a Bíróságot. Továbbá felvetette mind a 2010/87 határozat[22], mind pedig a 2016/1250 határozat érvényességének kérdését.

3. A Schrems II. ítélet[23] és az Adatvédelmi Pajzs érvénytelenítése

A Bíróság - az Ír Legfelsőbb Bíróság beterjesztése alapján – 2020. július 16.-án hozott ítéletében érvénytelennek nyilvánította a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot. Ugyanakkor a Bíróság megállapította, hogy a személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló 2010/87 bizottsági határozat érvényes.
A Bíróság vizsgálta a GDPR által megkövetelt védelmi szintet is, mind az ÁSZF-határozat, mind pedig a Privacy Shield érvényessége tekintetében megvalósuló adattovábbítások esetén.
A Bíróság megállapította, hogy az uniós jog, valamint a GDPR alkalmazandó a személyes adatoknak EU tagállami gazdasági szereplő által harmadik országban letelepedett másik gazdasági szereplő részére kereskedelmi célból végzett továbbítására. Az uniós jog és a GDPR alkalmazandó abban az esetben is, ha ezeket az adatokat az érintett harmadik ország hatóságai közbiztonsági, honvédelmi és nemzetbiztonsági célból kezelhetik. A Bíróság kiemelte, hogy valamely harmadik ország hatóságai általi ezen adatkezelések nem zárhatják ki az ilyen továbbítást a rendelet hatálya alól. A Bíróság megállapította, hogy a Safe Harbour-hoz hasonlóan a Privacy Shield határozat is a nemzetbiztonság, a közérdek és a bűnüldözés követelményeinek elsőbbségét fejezi ki. Ez

[22] 2010/87/: A Bizottság határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről (az értesítés a C(2010) 593. számú dokumentummal történt) (EGT-vonatkozású szöveg), *Hivatalos Lap 39, 12.2.2010, p. 5–18*
[23] A Bíróság (nagytanács) 2020. július 16-i ítélete (a High Court (Ireland) [Írország] előzetes döntéshozatal iránti kérelme) – Data Protection Commissioner kontra Facebook Ireland Limited, Maximillian Schrems
(C-311/18. sz. ügy), Hivatalos Lap C 297., 2020.9.7. p.4-5

azonban beavatkozást tesz lehetővé azon érintettek alapvető jogaiba, akiknek az adatait az Unióból az Egyesült Államokba továbbítják.
A Bíróság vizsgálta az amerikai jogrendszerben biztosított jogorvoslati lehetőségeket is. Kiemelte, hogy az Egyesült Államok állami szabályozásából nem következik sem az, hogy létezne az ilyen megfigyelési programok végrehajtására vonatkozó felhatalmazás tekintetében korlátozás, sem az, hogy léteznek az esetlegesen érintett, nem egyesült államokbeli személyek számára szóló megfelelő garanciák. Vannak bizonyos követelmények, amelyeket az amerikai hatóságoknak ezen megfigyelési programok során be kell tartaniuk, a szabályozás azonban nem biztosít az érintett személyek számára az amerikai hatóságokkal szemben a bíróságok előtt érvényesíthető jogokat.
A Bíróság álláspontja szerint a Bizottság által az Adatvédelmi Pajzs határozatban történt megállapítás, mely szerint az USA megfelelő szintű védelmet biztosít az Unióból az ahhoz csatlakozott USA-beli szervezetek részére továbbított személyes adatok tekintetében, megsértette az Európai Unió Alapjogi Chartájának összefüggésben értelmezett GDPR 45. cikkének (1) bekezdéséből eredő követelményeket[24].
A Bíróság érvénytelennek nyilvánította az Adatvédelmi Pajzsot, így ezen megfelelőségi határozat alapján személyes adatok az USA-ba nem továbbíthatóak. A 2010/87 bizottsági határozat érvényességével kapcsolatban a Bíróság megállapította annak érvényességét. Ugyanakkor kikötéseket tett. Az érvényesség attól függ, hogy az említett határozat „*tartalmaz-e olyan hatékony mechanizmusokat, amelyek a gyakorlatban lehetővé teszik annak biztosítását, hogy az uniós jog által megkövetelt védelmi szintet tiszteletben tartsák, és hogy a személyes adatok ilyen kikötéseken alapuló továbbítását az e kikötések megsértése, illetve tiszteletben tartásuk lehetetlensége esetén felfüggesszék vagy megtiltsák*.” [25] Ezek alapján az általános adatvédelmi kikötésen alapuló adattovábbítást meg kell, hogy előzze a védelmi szint megfelelőségének ellenőrzése.
A Schrems II ítéletben foglalt kiegészítő intézkedések értékelésével kapcsolatban megállapítható, hogy a nem megfelelő adatvédelmi szintet garantáló harmadik országba - mint pl. az USA - történő adattovábbítás esetén az adatkezelőknek (úgynevezett „adatexportőrként”) előzetesen meg kell vizsgálniuk az adatvédelmi szint megfelelőségét. Az USA egyes hatóságai adathozzáférési lehetőségei miatt az adattovábbítást megelőzően az adatkezelőknek az adattovábbítás címzettjével - az úgynevezett „adatimportőrrel”- szemben a Standard Contractual Clauses (SCC) azaz

[24] GDPR 45. cikk.
[25] C-311/18. sz., Ítélet, 137. pont.

általános szerződési feltételek megkötésén[26], illetve elfogadásán túl további szerződéses, szervezési és technikai intézkedéseket kell biztosítaniuk.

3.1. Az Európai Adatvédelmi Testület állásfoglalása

Az Európai Adatvédelmi Testület a 2020. július 17-i 34. plenáris ülésén megvitatta a Bíróság ítéletét, és nyilatkozatot fogadott el.[27] Az EDPB kiemeli a magánélethez való alapvető jog szerepét a személyes adatok harmadik országokba történő továbbítása során. Az Európai Adatvédelmi Testület (EDPB) tudomásul vette, hogy a Bíróság érvényteleníti az EU-USA Privacy Shield által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot, valamint azt, hogy úgy ítéli meg, hogy a Bizottság 2010/87 számú - A személyes adatok harmadik országokban letelepedett adatfeldolgozóknak történő továbbítására vonatkozó általános szerződési feltételekről szóló - rendeletét érvényesnek találta. Ami az adatvédelmi pajzsot illeti, az EDPB rámutat, hogy az EU-nak és az Egyesült Államoknak teljes és hatékony keretet kell elérnie, amely garantálja, hogy a személyes adatoknak az Egyesült Államokban biztosított védelmi szintje lényegében megegyezzen az EU-n belül garantált szinttel.
Az európai adatvédelmi hatóság utal a korábbi állásfoglalásaira az adatvédelmi pajzs kapcsán, és arra, hogy a Privacy Shield éves közös felülvizsgálatairól szóló jelentéseiben megkérdőjelezte a szükségesség és az arányosság adatvédelmi elveinek való megfelelést az Egyesült Államok jogának alkalmazása során.[28,29]
A GDPR értelmében személyes adat harmadik országba vagy nemzetközi szervezetnek csak abban az esetben továbbítható, ha az adattovábbítást követően is az Európai Unión belüli védelemmel azonos szintű a személyes adatok védelme.
Amíg az általános szerződési feltételek érvényben maradnak, az Európai Unió Bírósága (EUB) hangsúlyozta, hogy az ezek által biztosított védelmi szint a

[26] Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to regulation (eu) 2016/679 of the european parliament and of the council. European Comission, Brussels, 4.6.2021 C(2021) 3972 final.
[27] Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems,17 July 2020, https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en
[28] EU - U.S. Privacy Shield - Second Annual Joint Review report – 22/01/2019, https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-privacy-shield-second-annual-joint-review-report_en
[29] EU - U.S. Privacy Shield - Third Annual Joint Review report – 12/11/2019, https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en

gyakorlatban az EU Chartája fényében lényegében meg kell, hogy egyezzen a GDPR által garantált szinttel. Annak értékelése, hogy azon országok, amelyekbe az adatokat küldik, megfelelő védelmet nyújtanak-e, elsősorban az exportőr és az importőr felelőssége. Az exportőr az előzetes értékelés elvégzésekor (szükség esetén az importőr közreműködésével) figyelembe veszi az általános szerződési feltételek tartalmát, az adattovábbítás konkrét körülményeit, valamint az importőr országában érvényes jogi szabályozást. Ez utóbbi vizsgálatát a GDPR 45. cikkének (2) bekezdésében meghatározott tényezők figyelembevételével kell elvégezni. Ha az importőr országa nem biztosít lényegében egyenértékű védelmet, az exportőrnek fontolóra kell vennie további intézkedések bevezetését. Az európai adatvédelmi testület tovább vizsgálja, hogy ezek a kiegészítő intézkedések mit tartalmazhatnak. Az általános szerződési feltételek alapján figyelemmel kell lenni az importőr országában bekövetkezett jogszabályváltozásokkal kapcsolatos tájékoztatási kötelezettségekre. Ha ezek a szerződéses kötelezettségek nem teljesíthetők, az exportőr az általános szerződési feltételek értelmében köteles felfüggeszteni az átadást vagy megszüntetni azokat, illetve értesíteni az illetékes felügyeleti hatóságát, amennyiben folytatni kívánja az adattovábbítást.

Az EDPB felhívta a figyelmet a GDPR 49. cikke szerinti kivételekre[30] a harmadik országba való adattovábbítással kapcsolatban, valamint arra, hogy az ilyen eltéréseket eseti alapon kell alkalmazni.

Az EDPB 2020.novemberében, a Schrems II ítélettel kapcsolatban ajánlásokat fogalmazott meg az Európai Unióból harmadik országba történő adattovábbításra vonatkozóan: *„A „Schrems II" ítéletében (C-311/18) az Európai Unió Bírósága (EUB) arra emlékeztet bennünket, hogy a személyes adatok Európai Gazdasági Térségben (EGT) biztosított védelmét az adatok helyétől függetlenül biztosítani kell. (…)A Bíróság ezt annak egyértelművé tételével is megerősíti, hogy a harmadik országokban biztosított védelmi szintnek nem azonosnak, hanem lényegében azonosnak kell lennie az EGT-ben biztosított védelmi szinttel"*[31].

[30] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

[31] 01/2020. számú ajánlás az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében kiegészítő intézkedésekről, EDPB, 2020. november 10. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_hu.pdf

3.2. A Schrems II ítélet alapján az USA-ba történő adattovábbítás problémaköre

A határozat nem zárja ki az adatok Egyesült Államokba történő továbbítását. Az Adatvédelmi Pajzson alapuló megfelelőségi határozat érvénytelenség miatt a továbbiakban nem szolgál megfelelő jogalapként az adattovábbításra. Az általános szerződési feltételekkel kapcsolatban a védelmi szint megfelelőségének ellenőrzése gyakorlati nehézséget jelenthet azokban az esetekben, amikor az állami felügyeletet lehetővé tevő jogszabályok hatálya alá tartozó jogalanyok számára továbbítanak adatot: a védelmi szint valószínűleg az általános adatvédelmi kikötések alapján sem elégséges. Az EDBP állásfoglalás alapján a GDPR vonatkozó cikkeit már idéztem, az adattovábbítás kivételeit is beleértve.
Az Európai Parlament 2021. május 20-i állásfoglalást tett közzé az Európai Bíróság 2020. július 16-i ítéletéről[32]. A Schrems-ügy Európai Bírósági ítéletével kapcsolatban fogalmazta meg állásfoglalását 34 pontban. Észrevételeket tett többek között az ítéletben megfogalmazott „Általános szerződési feltételek", valamint az „Adatvédelmi Pajzs" vonatkozásában, illetve kifejtette álláspontját a „Tömeges megfigyelés és jogi keret" és a „Megfelelőségi határozatok" tekintetében.
A Schrems II. ítélet nemcsak az USA, hanem valamennyi harmadik országba irányuló adattovábbítással kapcsolatos, így az Európai Parlament a vonatkozó elveket a Brexit utáni Egyesült Királysággal kapcsolatban is megfogalmazta.[33]
Az Európai Bizottság 2021. június 4-én két általános szerződési feltételt fogadott el, egyet az adatkezelők és adatfeldolgozók közötti használatra, egyet pedig a személyes adatok harmadik országokba történő továbbítására. Ezen rendelkezések összhangban vannak a GDPR szabályaival és figyelembe veszik a Bíróság Schrems II. ítéletét[34],[35]. A feltételek nagyobb jogi kiszámíthatóságot

[32] Az adatvédelmi biztos kontra Facebook Ireland Limited, Maximillian Schrems (Schrems II) – C311/18. sz. ügy Az Európai Parlament 2021. május 20-i állásfoglalása az Európai Bíróság 2020. július 16-i ítéletéről – Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems („Schrems II") – C-311/18. sz. ügy (2020/2789 (RSP)), P9_TA (2021)0256

[33] A személyes adatok Egyesült Királyság általi megfelelő védelme Az Európai Parlament 2021. május 21-i állásfoglalása a személyes adatok Egyesült Királyság általi megfelelő védelméről (2021/2594 (RSP)) Hivatalos Lap, C 15. p. 218.

[34] A Bizottság (EU) 2021/915 végrehajtási határozata (2021. június 4.) az adatkezelők és az adatfeldolgozók közötti, az (EU) 2016/679 európai parlamenti és tanácsi rendelet 28. cikkének (7) bekezdése és az (EU) 2018/1725 európai parlamenti és tanácsi rendelet 29. cikkének (7) bekezdése szerinti általános szerződési feltételekről (EGT-vonatkozású szöveg) C/2021/3701, Hivatalos Lap L199, 7.6.2021, p. 18 -30

[35] A Bizottság (EU) 2021/914 végrehajtási határozata (2021. június 4.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerinti, harmadik országok részére történő

biztosítanak az európai vállalkozások számára, és különösen a kkv-kat segítik a biztonságos adattovábbításra vonatkozó követelmények betartásában, miközben lehetővé teszik az adatok szabad, határokon átnyúló, jogi akadályok nélküli áramlását. Az új általános szerződési feltételek figyelembe veszik az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos közös véleményét, a széles körű nyilvános konzultáció során az érdekelt felek visszajelzéseit, valamint a tagállamok képviselőinek véleményét.
Az új általános szerződési feltételek főbb újításai: frissítés az általános adatvédelmi rendelettel (GDPR) összhangban, egyetlen belépési pont, amely az adatátviteli forgatókönyvek széles skáláját fedi le külön záradékcsoportok helyett, nagyobb rugalmasság az összetett feldolgozási láncok számára a „moduláris megközelítés" révén, valamint azáltal, hogy kettőnél több fél csatlakozhat és használhatja a záradékokat, gyakorlati eszköztár a Schrems II ítéletnek való megfeleléshez - azaz a különböző lépések áttekintése, amelyeket a vállalatoknak meg kell tenniük, hogy megfeleljenek a Schrems II ítéletnek, valamint példák a lehetséges „kiegészítő intézkedésekre", mint például a titkosítás, amelyeket a vállalatok szükség esetén szintén megtehetnek.

A Bizottság (Eu) 2021/914 végrehajtási határozat (2021. Június 4.) felépítése a GDPR szerinti, harmadik országok részére történő személyesadat-továbbításra vonatkozó általános szerződési feltételekről (SSC)	
I szakasz	Cél és alkalmazási kör A feltételek megváltoztathatatlansága Értelmezés Hierarchia
Fakultatív	Dokkolási feltétel
II. SZAKASZ *A FELEK KÖTELEZETTSÉGEI*	Az adatkezelés(ek) leírása A Felek kötelezettségei Segítségnyújtás az adatkezelőnek Adatvédelmi incidensről szóló értesítés
III. SZAKASZ *ZÁRÓ RENDELKEZÉSEK*	A feltételeknek való meg nem felelés és a szerződés felmondása

2. ábra Az (Eu) 2021/914 határozat részeként az egyes feltételek szakaszonként, a táblázatban ábrázolt felosztás szerint kerültek elfogadásra. Saját szerkesztés

személyesadat-továbbításra vonatkozó általános szerződési feltételekről (EGT-vonatkozású szöveg) C/2021/3972, Hivatalos Lap L 199., 2021.6.7. p. 31- 61.

A harmadik országba való történő adattovábbítás az (EU) 2021/914 végrehajtási határozata alapján lehetséges, amely a GDPR-nak megfelelő védelmi szintet kívánja biztosítani. A jogszabály 18 feltételt állapított meg, amelyeket „… *az (EU) 2016/679 rendelet 46. cikkének (1) bekezdése és 46. cikke (2) bekezdésének c) pontja értelmében megfelelő garanciákat – többek között érvényesíthető jogokat és hatékony jogorvoslati lehetőségeket, továbbá az adatkezelők által az adatfeldolgozók részére és/vagy az adatfeldolgozók által az adatfeldolgozók részére történő adattovábbítás tekintetében az (EU) 2016/679 rendelet 28. cikkének (7) bekezdése szerinti általános szerződési feltételeket határoznak meg*…”. A célok és az alkalmazási kör tekintetében meghatározásra kerül a felek szerepe a személyes adatok továbbítása és a harmadik országok viszonylatában.[36] Részletesen tárgyalja a feltételeket, az adattovábbítást modulokba osztva részletezi, amelyek a következők: adatkezelők közötti adattovábbítás, adattovábbítás az adatkezelőtől az adatfeldolgozó részére, adattovábbítás adatfeldolgozók között, adattovábbítás az adatfeldolgozótól az adatkezelő részére. Ezek részletes szabályait, az egyes különbözőségek esetében külön ismerteti, mint például további adatfeldolgozók alkalmazása esetében.[37] Ezek a szabályok az adatkezelés biztonságát hivatottak garantálni, azaz az adatvédelmi garanciákat és 9 elv mentén kerülnek meghatározásra: célhoz kötöttség, átláthatóság, pontosság és adattakarékosság, a tárolás korlátozása, az adatkezelés biztonsága, különleges adatok, adattovábbítás harmadik fél részére, az adatátvevő irányítása alatt végzett adatkezelés, dokumentáció és megfelelés. A dokumentáció egyben hivatalos igazolás a felügyeleti hatóság részére. A hazai szabályozást is az EDBP állásfoglalása határozza meg. Az EU-s nemzeti adatvédelmi hatóságok döntései is befolyásolják 2022-ben a hazai adatvédelmi joggyakorlatot, legyen az a Schrems II ítélet miatti változások következménye, vagy a szinte valamennyi vállalat által használt Google Analytics-szel kapcsolatos osztrák döntés.[38]

---

[36] (EU) 2021/914 1. szakasz 1.(b) „A Felek: i.az I. melléklet A. részében felsorolt, személyes adatokat továbbító természetes vagy jogi személy(ek), közigazgatási szerv(ek), ügynökség(ek) vagy egyéb szerv(ek) (a továbbiakban: az adatátadó); valamint harmadik országbeli jogalany(ok), amely(ek) az I. melléklet A. részében felsoroltak szerint az adatátadótól közvetlenül vagy közvetve más, szintén e szerződési feltételekben részes jogalanyon keresztül átveszi(k) a személyes adatokat (a továbbiakban külön-külön: az adatátvevő), elfogadták ezeket az általános szerződési feltételeket (a továbbiakban: „feltételek”).” elfogadták ezeket az általános szerződési feltételeket (a továbbiakban: „feltételek”).”

[37] (EU) 2021/914, II. szakasz, 9. feltétel

[38] Vass Enikő: Az IP cím is személyes adatnak számít in: IT Business 2022.06.02-03.
„ha az EU-n kívülre továbbítunk adatokat, akkor az Európai Bizottság által előírt mintaszerződés megléte mellett a vállalatoknak fel is kell mérniük, hogy az ország mennyire kockázatos”. A kockázatelemzés költséges és nehézkes faladatára mutat rá, mely további mérlegelést igényelne. A blog kiemeli az IP-adatok személyes adatokként történő kezelésének a problémáját, valamint a Google Analytics használatával járó körülményes adatvédelmet.”

3.3 A közösségi média adatkezelési gyakorlata

A közösségi média felelősségére hívja fel a figyelmet több kirobbant botrány. 2018 október 25-én ötszáz ezer dollárra bírságolták meg Nagy-Brittanniában a Facebook-ot, mivel az a felhasználók tudta nélkül továbbította az érintettek adatait harmadik személy részére. A Cambridge Analytica (a cég, amely megszerezte az adatokat) botrány felelősei a Facebook 87 millió felhasználójának adataival élhettek vissza, ebből 2,7 millió volt uniós állampolgár. A Cambridge Analytica az amerikai választásokat is befolyásolta.[39] 2019. január 21-én a francia adatvédelmi hatóság, a CNIL 50 millió euróra bírságolta a Google-t azért, mert nem felelt meg a GDPR előírásainak, adatvédelmi tájékoztatása túlzottan általános volt, valamint jogszerűtlenül használt fel felhasználói adatokat a személyre szabott hirdetések közléséhez

Az GDPR meghatározza az adatkezelés tárgyi és területi hatályát, ez utóbbi érdekes a harmadik országokba való továbbítás szempontjából, és amelyben például a Facebook is érintett, hiszen a korábban már említett Meta központja az Egyesült Államokban van.

A közösségi média működésével, és adatkezeléseivel kapcsolatosan Szőke részletesen elemezte a Google, a Facebook adatkezelési gyakorlatát[40], a profilalkotást[41] és a Facebook adatvédelmi tájékoztatója kapcsán a közösségi oldalak működését.[42] Az általa vizsgáltak alapján a Facebook működése megfelel ugyan a GDPR feltételeinek, de a Google több hiányosságot mutat.

Azonban, mint írja a Facebook adatkezelési tájékoztatója kapcsán: „*Számos ponton ezzel együtt nem igazán átlátható, a részletesnek ható szövegezés ellenére szembetűnő a külső partnerekkel történő adatmegosztásokkal*

---

[39] Donald Trump kampányüzeneteit pontosabban tudták becélozni a megfelelő felhasználóknak, de hatása volt a Brexit kampányra is[39].A botrányról 2018 április 18-án tartottak vitát a Parlamentben, a képviselők arra kérték a Facebookot, hogy tisztázza az adatkezelési gyakorlatát és azt, hogyan fog eleget tenni a május 25-én életbe lépő Általános Adatvédelmi Rendelet (GDPR) feltételeinek. Ebben a tekintetben a felügyeleti hatóságok szerepét emeli ki, tisztázásra szorul azonban, hogy milyen módon lehet az érintetti jogokat ebben a kontextusban a mindennapi életben gyakorolni.

[40] Pataki Gábor - Szőke Gergely László: A Google és a Facebook adatvédelmi tájékoztatási gyakorlata a GDPR szabályozásának tükrében. In: Polyák Gábor (Szerk.): Algoritmusok, Keresők, Közösségi Oldalak és a Jog: A forgalomirányító szolgáltatások szabályozása., HVG-ORAC, Budapest, 2020. p. 89.

[41] Pataki Gábor - Szőke Gergely László: Az online személyiségprofilok jelentősége. In: Polyák Gábor (Szerk.): Algoritmusok, keresők, közösségi oldalak és a jog: A forgalomirányító szolgáltatások szabályozása, HVG-ORAC, Budapest, 2020. p. 74.

[42] Szőke Gergely László: A közösségi oldalak működése az európai adatvédelmi szabályozás tükrében. In: Barzó Tímea - Czékmann Zsolt - Csák Csilla (Szerk.): "Gondolatok Köztere" A közösségi média személyiségvédelemmel összefüggő kihívásai és szabályozása az egyes államokban. Miskolci Egyetemi Kiadó, Miskolc, 2021. p. 118.

kapcsolatos, valamint a profilozással és automatizált, algoritmusokon alapuló döntéshozatallal kapcsolatos hiányérzet: végső soron ezekről akkor sem tud meg érdemi részleteket a felhasználó, ha valóban végig olvassa a rendelkezésre álló tájékoztatókat."
Érdemi kérdés a felhasználók részére, hogy a részletes adatvédelmi tájékoztatókat mennyire értik, és tudják a jogaikat gyakorolni. Egyetértve ezzel kijelenthető, hogy ez nemcsak a közösségi média felületein érhető tetten.
A NAIH álláspontja alapján[43] az Infotv. 2. § (1) bekezdése szerint az Infotv. hatálya a Magyarország területén folytatott adatkezelésre terjed ki. Az állásfoglalás szerint „(…) *Bár a Facebook tevékenysége magyarországi felhasználókra (is) irányul, és a közösségi oldalnak van magyar nyelvű változata, tekintettel arra, hogy a Facebooknak, mint adatkezelőnek nincs magyarországi tevékenységi helye és képviselője, a közösségi oldalra nem irányadó az Infotv., következésképpen a Hatóság nem rendelkezik joghatósággal, így vizsgálatot sem tud indítani a Facebookkal szemben*."
Ugyanakkor a GDPR által bevezetett „érintett felügyeleti hatóság" fogalmára tekintettel „(…) *amennyiben magyarországi lakóhellyel rendelkező érintettek (vagyis nem csak magyar állampolgárok) panaszt nyújtanak be a Hatósághoz a Facebookkal szemben, a Hatóság érintett felügyeleti hatóságnak fog minősülni, azonban a Facebook által végzett határon átnyúló adatkezelés tekintetében változatlanul az ír adatvédelmi hatóság, mint fő felügyeleti hatóság lesz jogosult eljárni*."

3.4. Privacy Shield 2.0

Az Európai Bizottság elnöke és az Egyesült Államok elnöke 2022 március 26-án bejelentette, hogy az Egyesült Államok és az EU elvi megállapodást kötött a transzatlanti adatáramlás új keretrendszeréről, amely felváltja az érvénytelenített eredeti Privacy Shield Framework keretrendszert.
A régi Privacy Shield több részének átvétele mellett a 2.0-s verzió új intézkedéseket fog hozni a hírszerzési adatok gyűjtésének korlátozására a „jogos nemzetbiztonsági célok előmozdítása érdekében", és további felügyeletet telepít az amerikai hírszerző ügynökségek számára a magánélet és a polgári szabadságjogok védelme érdekében. Miben lesz új a Privacy Shield 2.0? A régi Privacy Shield több részének átvétele mellett a 2.0-s verzió új intézkedéseket fog hozni a hírszerzési adatok gyűjtésének korlátozására a „jogos nemzetbiztonsági célok előmozdítása érdekében", és további felügyeletet telepít az Egyesült Államok hírszerző ügynökségei számára a magánélet és a polgári szabadságjogok védelme érdekében. Az új adatvédelmi

[43] NAIH/2018/2198/2/V, https://www.naih.hu/files/Adatved_allasfoglalas_2018_2198-2_V_Facebook_old.pdf

pajzsnak megoldást kell kínálnia a személyes adatoknak az Unióból (EGT) az Egyesült Államokba történő továbbítására. A GDPR-nak megfelelően az EGT-ben tartózkodó egyének személyes adatait nem lehet az EGT-n kívülre a megfelelő biztosítékok nélkül továbbítani. Az új Privacy Shield[44],[45]jelenleg még „politikai bejelentés" mivel a Privacy Shield 2.0 részletei még mindig ismeretlenek, és az „elvi megállapodás" kifejezés azt sugallja, hogy a végleges szöveg és a megoldás még kidolgozásra vár[46].

4. Összefoglalás

A tanulmány a Schrems II ítélet utáni nemzetközi jogalkotási folyamatokba nyújt betekintést, különösen azok harmadik országokba történő adattovábbítási szabályozásába. A Schrems II ítélet az EU-USA közötti Adatvédelmi Pajzsot hatályon kívül helyezte, ez sürgető megoldást kívánt az USA- ba irányuló adattovábbítások miatt. Megelőzte ezt a Schrems I ítélet, mely ugyancsak a Facebook adattovábbításait érintette, egyben érvénytelenítette az EU-USA Biztonságos Kikötő Egyezményét, amely alapján az adattovábbítás történt. Az ítéletek alapvetően a Facebook adattovábbítási gyakorlata kapcsán keletkeztek, tekintettel arra, hogy bár a Facebook európai központja Írországban található, azonban a Meta, az anyavállalat Kaliforniában van. A Facebook Ireland az uniós adatvédelmi jogi szabályozásnak megfelel, azonban a továbbított adatok védelme az amerikai Kereskedelmi Központ gyakorlatában nem biztosította az uniós jognak megfelelő szintű védelmet. A megoldást nemcsak a közösségi hálók, de a gazdasági szereplők és valamennyi érdekelt számára kellett megtalálni. Az érvénytelenítéssel kapcsolatosan meg kell jegyezni, hogy előzetes döntéshozatali eljárás keretében történtek. Erre vonatkozóan az uniós szabályozás úgy rendelkezik, hogy az előzetes döntéshozatali eljárás lehetővé teszi a tagállami bíróságok számára, hogy az előttük folyamatban lévő jogvita keretében az uniós jog értelmezésére vagy valamely uniós jogi aktus érvényességére vonatkozó kérdést terjesszenek a Bíróság elé. A Bíróság nem dönti el a tagállami bíróság előtti jogvitát. A nemzeti bíróság feladata, hogy az ügyet a Bíróság határozata alapján elbírálja. Tehát a Schrems határozatok a tartalmilag hasonló kérdésben eljáró más nemzeti bíróságokat is kötik.
A Bíróság ítéletében megállapította, hogy 2010/87 határozatnak az Alapjogi Chartára tekintettel történő vizsgálata nem tárt fel olyan tényezőt, amely e

[44] Trans-atlantic data privacy framework, European Comission, March, 2022. https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100
[45] New EU – U.S. Privacy Shield 2.0 26/03/2022 in Blog, Data Privacy, https://dataprivacymanager.net/new-eu-u-s-privacy-shield-2-0/
[46] Pók László: Adatvédelmi hírek. 2022/12. in: GDPR/Adatvédelem mindenkinek,https://gdpr.blog.hu

határozat érvényességét érintené, így az (EU) 2016/2297 bizottsági végrehajtási határozattal módosított, a 95/46 irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010/87/EU bizottsági határozat érvényes. Az Európai Bizottság 2021. június 4-én két általános szerződési záradékot fogadott el, egyet az adatkezelők és adatfeldolgozók közötti használatra, egyet pedig a személyes adatok harmadik országokba történő továbbítására. Az első az (EU) 2016/679 rendelet 28. cikkének (7) bekezdése és az (EU) 2018/1725 rendelet 29. cikkének (7) bekezdése szerinti, az adatkezelők és adatfeldolgozók közötti általános szerződési feltételeket szabályozza, melyek figyelembe veszik az Európai Adatvédelmi Testület és az Európai Adatvédelmi Biztos közös véleményét, és nagyobb jogi kiszámíthatóságot biztosítanak az európai vállalkozások számára, és különösen a kkv-kat segítik a biztonságos adattovábbításra vonatkozó követelmények betartásában. A második a személyes adatok harmadik országokba történő továbbítására vonatkozó általános szerződési feltételekről az (EU) 2016/679 rendelet értelmében részletes szabályozást tartalmaz. A közösségi média újabb adattovábbítási botrányai arra utalnak, hogy ez a megoldás korántsem biztosítja a személyes adatok uniós jogi szintű védelmét. Komplikálja a megoldást, hogy a közösségi oldalak, nem csak adatkezelők - és feldolgozók önállóan, hanem lehetnek együttesen is, valamint, hogy ezeken az oldalakon az érintettek is adatkezelőként szerepelhetnek.
Tehát az EU- USA, és más kétoldalú adattovábbítási keretmegállapodásokon kívül is vannak még kihívások a jogalkotás számára, ezekre kívánta a közlemény felhívni a figyelmet.

Irodalomjegyzék

- Ahmet Efe - Hamed Suliman: How Privacy is threatened from Social Media communication? In: Anatolian Journal Of Computer Sciences, 2021/6. pp. 32-45.
- Andrea Kraut - László Kőhalmi - Dávid Tóth: Digital Dangers of Smartphones Journal Of Eastern-European Criminal Law, 2020/1. pp. 36-49.
- Andreas Kaplan - Michael Haenlein: Users of the world, unite! The challenges and opportunities of Social Media. In: Business Horizons, 2010/1. pp. 59-68.
- Bányász Péter: Közösségi média és közszolgálat. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet Kiadása, Budapest, 2020.
- Kis Kelemen Bence - Hohmann Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. In: Infokommunikáció és Jog, 2016/2-3. pp. 64-69.
- Pataki Gábor - Szőke Gergely László: A Google és a Facebook adatvédelmi tájékoztatási gyakorlata a GDPR szabályozásának tükrében. In: Polyák Gábor (Szerk.): Algoritmusok, Keresők, Közösségi Oldalak és a Jog: A forgalomirányító szolgáltatások szabályozása., HVG-ORAC, Budapest, 2020. pp. 89-107.
- Pataki Gábor - Szőke Gergely László: Az online személyiségprofilok jelentősége. In: Polyák Gábor (Szerk.): Algoritmusok, keresők, közösségi oldalak és a jog: A forgalomirányító szolgáltatások szabályozása, HVG-ORAC, Budapest, 2020. pp. 74-88.
- Schubauer Petra: A Safe Harbor határozat érvénytelenítésének hatása az európai adatvédelmi gyakorlatra. In: Belügyi Szemle, 2017/2. pp. 88-99.
- Szőke Gergely László: A közösségi oldalak működése az európai adatvédelmi szabályozás tükrében. In: Barzó Tímea - Czékmann Zsolt - Csák Csilla (Szerk.): "Gondolatok Köztere" A közösségi média személyiségvédelemmel összefüggő kihívásai és szabályozása az egyes államokban. Miskolci Egyetemi Kiadó, Miskolc, 2021. pp. 118-134.

Kőhalmi László
tanszékvezető egyetemi tanár (Kriminológiai és Büntetés-végrehajtási Jogi Tanszék PTE-ÁJK)

Nyilvánosság és büntetőeljárás

Absztrakt

A tanulmány a nyilvánosság garanciális intézményét vizsgálja a büntetőeljáráson belül. A nyilvánosság elve szorosan összefügg az ártatlanság vélelméhez és a tisztességes eljáráshoz való joggal, hiszen e nélkül a fair eljárás nem valósulhat meg.
A tanulmány 4 részre tagozódik. A bevezető részben kontextusba kerül a nyilvánosság intézménye. A második rész a jogtörténeti aspektusait vizsgálja az 1800-as évektől napjainkig. Az ezt követő részben a sajtónyilvánosság kérdéskörei kerülnek analízisre külön kitérve a közösségi médiára. A záró részben az összegző gondolatok kerülnek megfogalmazásra.

Kulcsszavak: nyilvánosság, büntetőeljárás, sajtó, közösségi média.

1.Bevezető gondolatok

Az Európai Unió Alapjogi Chartájának 47. és 48. cikke, az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény 6. cikke, a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 14. cikke és az Emberi Jogok Egyetemes Nyilatkozatának 11. cikke rögzítik az ártatlanság vélelmét és a tisztességes eljáráshoz való jogot.
A fair eljárás követelménye akkor valósulhat meg, ha olyan büntetőeljárási garanciamechanizmus-rendszer működik, mely a vádlotti jogok tényleges perfektuálódását szavatolja. Több feltételt említhetnék, de ehelyütt az előadás címében jelzett nyilvánosság érvényesülésének fontosságra szeretném a T.Hallgatóság figyelmét felhívni.
Magyarország Alaptörvényének XXVIII. cikke rögzíti a tárgyalás nyilvánosságának alapelvét, mely kimondja: mindenkinek joga van ahhoz, hogy az ellene emelt bármely vádat vagy valamely perben a jogait és kötelezettségeit törvény által felállított, független és pártatlan bíróság tisztességes és nyilvános tárgyaláson, ésszerű határidőn belül bírálja el.
A nyilvánosság követelménye garanciális jelentőségű alapelv: biztosítja az igazságszolgáltatás működésének átláthatóságát, ellenőrizhetőségét.

Az alapelvek jelentőségére nem térek ki, hiszen a Pécsi Büntetőeljárásjogi Műhely professzorai (Tremmel Flórián, Fenyvesi Csaba, Herke Csongor) több munkájukban[1] foglalkoztak a kérdéskörrel.

2. A nyilvánosság joghistóriai aspektusai

A nyilvánosság az 1800-as évek közepétől lényegében alapelvi szinten funkcionál a bírósági szakban, sőt a büntető perrendtartásról szóló 1896.évi XXXIII. törvénycikkben már jogszabályszövegként is megjelent.[2]
Finkey Ferencz értelmezésében a nyilvánosság a büntető eljárásban kétféle jelentéstartalmat hordoz: egyrészt a bírói tárgyalások a közönség előtt nincsenek elzárva, hanem azokon bárki akadály nélkül megjelenhet, mint hallgató és szemlélő[3]; másrészt az ún. ügyfélnyilvánosságot, mely szerint az eljárási cselekményeknél a felek és képviselőik jelen lehetnek.[4]
Angyal Pál szerint a nyilvánosság nagy általánosságban azt jelenti, hogy a büntető eljárás során végzett különböző bírósági és hatósági cselekményeknél minden korlátozástól menten bárki jelen lehet.[5]
Vargha Ferencz megközelítésében a nyilvánosság a szabad és biztosított bemenete a nagy közönségnek a főtárgyalás termébe. Azt ellenben nem tekinti a nyilvánoság megvalósulása szükségszerű elemének, hogy a közönség közül valaki ténylegesen, fizikai valóságában is jelen legyen a tárgyaláson.[6]

---

[1] Herke Csongor – Fenyvesi Csaba – Tremmel Flórián: A büntető eljárásjog elmélete. Dialóg Campus Kiadó. Budapest-Pécs, 2012. pp. 47-86.

[2] *Bp. „293. § A főtárgyalás rendszerint nyilvános. A főtárgyaláson hozott birói határozatok, kivéve a nyilvánosság kizárásával tartott főtárgyalás során hozott határozatokat, mindig nyilvánosan hirdetendők ki. A tanácskozásnál és a szavazásnál csak az itélőbiróság tagjai és jegyzője lehetnek jelen. A bíróság a nyilvánosság kizárását az egész főtárgyalásra, vagy egy részére nézve bármikor elrendelheti, ha a tárgyalás nyilvánossága a közrendet vagy a közerkölcsiséget veszélyeztetné. E kérdésben a törvényszék a feleknek a közönség kizárásával történt meghallgatása után határoz. Ha a határozat a nyilvánosság kizárását rendeli el, ennek nyilvános kihirdetése után a hallgatóságnak el kell távoznia.*
294. § A nyilvánosság kizárása esetében is a főtárgyaláson mindenik vádlott és sértett részéről kijelölt két-két bizalmi férfi lehet jelen.
295. § Fel nem nőttek és oly egyének, kik nem a hely méltóságának megfelelően jelennek meg, a hallgatók közül kizárandók. Bottal senki sem, fegyverrel pedig csak azok bocsáthatók a tárgyaló terembe, a kik azt hivatalos vagy szolgálati állásuknál fogva viselik."

[3] Finkey ez alatt értette a teljes, általános vagy népnyilvánosságot.

[4] Finkey Ferenc: A magyar büntető eljárás tankönyve. Harmadik kiadás, Politzer-féle Könyvkiadóvállalat, Budapest, 1908. p. 226.

[5] Angyal Pál: A magyar büntetőeljárásjog tankönyve I.kötet. Atheneum Irodalmi és Nyomdai R.-T. kiadás, Budapest, 1915. p. 273.

[6] Vargha Ferencz: Főtárgyalás a törvényszék előtt. In: Balogh Jenő – Edvi Illés Károly – Vargha Ferencz: A bűnvádi perrendtartás magyarázata. Harmadik kötet. Grill Károly, Cs. és Kir. Udvari Könyvkereskedése, Budapest, 1899. p. 287.

Fayer László a nyilvánosságot a reformált bűnvádi eljárás szükségszerű járulékának tekinti. *„Fogalmilag a bizonyítékok szabad mérlegelése és a szóbeliség csak azt követelik meg, hogy a felek a tárgyaláson jelen legyenek; de igen nagy súlyt kell helyezni arra, hogy a tárgyalás mindenkire nézve nyilvános legyen s egyszersmind oly módon rendeztessék be, miszerint vonzerővel bírjon a közönségre s a nyilvánosság elve tényleg is érvényesüljön."* [7] Teljes mértékben egyetértek FAYER László véleményével, miszerint a nyilvánosság szinte fontosabb, mint a többi szervezeti elv együttvéve.

Az első szocialista eljárási kódex a büntető perrendtartásról szóló 1951. évi III. törvény[8] természetesen szovjet szabályozási mintán alapult.[9] A hivatkozott büntető eljárási kódex légkörét az alábbi rövid idézettel szeretném szemléltetni: *„A szocialista büntetőeljárás gyökeresen és minőségileg különbözik a burzsoá eljárástól. A szocialista büntetőeljárás célja, hogy – mint a Büntető Perrendtartásról szóló 1951:III. tv. is kifejezi – a szocialista állam állami, társadalmi és gazdasági rendjének és intézményének, valamint a dolgozók jogainak védelmében 1. biztosítsa a bűncselekmények üldözését, 2. a dolgozó nép ellenségeinek a megbüntetését, s 3. a dolgozóknak a szocialista társadalmi együttélés szabályaira való nevelését."*[10] Elképzelhetőjük, hogy az 1950-es években milyen „jelentőséggel" rendelkezett a nyilvánosság.

A büntető eljárásról szóló 1962. évi 8. törvényerejű rendelet szabályai[11] nem hoztak érdemi változást a nyilvánosság szabályozását illetően.

---

[7] Fayer László: A bűnvádi perrendtartás vezérfonala. Teljesen átalakított negyedik kiadás. Franklin-Társulat Magyar Irod. Intézet és Könyvnyomda, Budapest, 1905. p. 26.

[8] 1951.évi III. törvény *„7.§ (1) A bíróságok tárgyalásai nyilvánosak. (2) A bíróság a nyilvánosságot indokolt határozatával az egész tárgyalásról vagy annak egy részéről bármikor kizárhatja, ha az államtitok, katonai titok vagy hivatali titok megőrzése végett vagy erkölcsiokokból feltétlenül szükséges. A bíróság egyes hivatalos személyeknek ebben az esetben is megengedheti, hogy a tárgyaláson jelen lehessenek. (3) A bíróság a tárgyalás során hozott határozatait általában nyilvánosan hirdeti ki."*

[9] Kovács Judit – Nagy Zsolt: A társadalmi változások hatása a büntető eljárási szabályokra a rendszerváltozás után. Jogelméleti Szemle 2001/2. A szerzők szerint: „*Ezt a törvényt módosításokkal továbbfejlesztették, így – a szocialista alapelvek figyelembe vétele mellett – egyre nagyobb teret kapott a törvényesség tiszteletben tartása. Az 1940-es évek végén és az 50-es évek elején ártatlan emberek ellen folytatott törvénytelen perek tragikus következményei miatt szükségesnek tartották a törvényességi garanciák fokozását, ami főleg az 1954. évi V. törvényben – a Bp. novellájában – jutott kifejezésre."* Mindehhez annyit fűznék hozzá, hogy a „törvényesség tiszteletben tartása" ennél jóval összetettebb problematika volt, de a szerzők színvonalas tanulmánya nem kifejezetten erre a kérdéskörre fókuszált, így nem is várható el ebben a tekintetben terjedelmesebb elemzés.

[10] Olti Vilmos. A védő szerepe a burzsoa és a szocialista büntető eljárásban (III.). Jogtudományi Közlöny 1954. január-február. hó. 51.o.

[11] 1962.évi 8. tvr. „10.§ (1) A bírósági tárgyalások nyilvánosak. (2) Ha államtitok vagy szolgálati titok megőrzése végett vagy erkölcsi okból szükséges, a bíróság a nyilvánosságot indokolással ellátott határozatával az egész tárgyalásról vagy annak egy részéről bármikor

A büntetőeljárásról szóló 1973.évi. I. törvény (Be.) szabályrendszere – szocialista viszonyok között – némi előbbre lépést jelentett. Ugyanakkor mértékadó szocialista ideológusai nem említették a nyilvánosság jelentőségét, mégis akadtak olyan bátor teoretikusok, akik a hivatkozott elvárást alapelvnek tekintették.[12]

A büntetőeljárásól szóló 1998.évi XIX. törvény a tárgyalás nyilvánosságát tekinti „főszabálynak", s a tanács elnökének kezébe adja a nyilvánosságát korlátozásának jogkörét.[13]

---

kizárhatja. A bíróság egyes hivatalos személyeknek ebben az esetben is megengedheti, hogy a tárgyaláson jelen lehessenek. (3) A bíróság a tárgyalás során hozott határozatait általában nyilvánosan hirdeti ki."

[12] Makója Imre: Az új büntető eljárási törvényről. In: Belügyi Szemle 1973/5. pp. 7-9. A kommunista politikus nem sorolta fel tanulmányában az alapelvek között a nyilvánosságot, de nyilván egy pártállami funkcionáriustól ilyet nem is várhatunk el.; Szabóné Nagy Teréz: Az alapelvek rendszere az új büntetőeljárási törvényben. Belügyi Szemle XI. évfolyam 1973/6. 14-19.o. Az már inkább elszomorítóbb, hogy az ELTE néhai egyetemi docensének opusában sem kerül említésre a nyilvánosság fontos szerepe. A szerző védelmében ugyanakkor elmondható, hogy vélhetően a tanulmány terjedelmi korlátai miatt nem tért ki a nyilvánosság elemzésére, hiszen itt egy informatív, figyelemfelhívó kéziratról van szó.

[13] „*Be. 237. § (1) A bíróság tárgyalása nyilvános. A tanács elnöke a tárgyalás szabályszerű lefolytatása, méltóságának és biztonságának megőrzése érdekében, helyszűke esetén meghatározhatja a hallgatóság létszámát. (2) A tárgyaláson hallgatóként a tizennegyedik életévét be nem töltött személy nem vehet részt, a tizennyolcadik életévét be nem töltött személyt a tanács elnöke a hallgatóság köréből kizárhatja. (3) A bíróság hivatalból vagy az ügyész, a vádlott, a védő, a sértett, illetőleg a tanú indítványára a nyilvánosságot az egész tárgyalásról vagy annak egy részéről indokolt határozattal kizárhatja (zárt tárgyalás) a) erkölcsi okból, b) az eljárásban részt vevő kiskorú védelme érdekében, c) az eljárásban részt vevő személyek (V. Fejezet) vagy a tanú magánéletének védelme érdekében, d) az államtitok vagy szolgálati titok megőrzése végett. (4) A nyilvánosság kizárása az eljárás bármely szakaszában indítványozható. 238. § (1) A nyilvánosság kizárásáról szóló határozatot a bíróság nyilvános tárgyaláson hirdeti ki. A nyilvánosság kizárása ellen külön fellebbezésnek nincs helye, azt az ügydöntő határozattal szemben bejelentett fellebbezésben lehet sérelmezni. (2) A bíróság a nyilvánosság kizárása esetén is engedélyezheti, hogy az igazságszolgáltatással összefüggő feladatokat ellátó hivatalos személyek a tárgyaláson jelen legyenek. (3) A nyilvánosság kizárása esetén a sértett és - ha nincs védője - a vádlott indítványozhatja, hogy a tárgyalás helyszínén tartózkodó, általa megnevezett személy legyen jelen. Az indítvány elutasítása ellen nincs helye fellebbezésnek. (4) Ha a bíróság zárt tárgyalást rendel el, szükség esetén figyelmezteti a résztvevőket arra, hogy a tárgyaláson elhangzottakról tájékoztatást nem adhatnak, figyelmezteti őket az államtitoksértés, a szolgálati titoksértés következményeire. A figyelmeztetést a jegyzőkönyvben fel kell tüntetni. 239. § (1) A tárgyalást nyilvánosan kell folytatni, ha a zárt tárgyalás indoka megszűnt. (2) A bíróság a tárgyaláson hozott határozatát akkor is nyilvánosan hirdeti ki, ha a tárgyalásról a nyilvánosságot kizárta."*

Farkas Ákos tankönyvében emlékeztet arra, hogy az EEJK 6. cikk 1. bekezdése is követelményként fogalmazza meg a független és pártatlan bíróság nyilvános tárgyalását.[14]
Hatályos büntető eljárási alapnormánk, a büntetőeljárásról szóló 2017.évi XC. törvény 436. § (1) bekezdése világosan fogalmaz: a bírósági tárgyalás nyilvános!
Fantoly Zsanett felhívja a figyelmet arra, hogy a Be.-ben a nyilvánosság az egyetlen nevesített processzuális alapelv.[15]

3. A nyilvánosság speciális alakzata: a sajtónyilvánosság

A nyilvánosságról Háger Tamás kifejti, hogy az *„egyik olyan alapelv a büntetőeljárásban, mely a tisztességes eljárás (fair trial) jogcsokrának (bundle of rights) igen fontos eleme. Biztosítja az igazságszolgáltatás átláthatóságát, ellenőrizhetővé téve a bírói hatalom működését, egyben jogosultságot teremt a vád alá helyezett személynek, hogy ügyét pártatlanul, jól kontrollálhatóan bírálják el."*[16]
Érdemes továbbá felidézni Navratil Szonja releváns kutatási eredményeit is, miszerint annak *„eldöntésére tehát, hogy az igazságszolgáltatás valóban függetlenül, a törvényeknek alárendelten végzi-e a tevékenységét a nyilvánosság bevonásával van lehetőség."*[17]
Tóth Mihály szerint a nyilvánosság nem abszolút és korlátozhatatlan elv.[18] Kiss Anna[19] és Háger Tamás helyesen látják, hogy a tanács elnöke a tárgyalóterem méreteire tekintettel meghatározhatja a hallgatóság létszámát, eldöntve, hogy mekkora létszámú hallgatóság befogadására alkalmas a terem.

---

[14] Farkas Ákos: Alkotmányosság és büntetőeljárás. In. Farkas Ákos – Róth Erika: A büntetőeljárás. Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2012. p. 70.
[15] Fantoly Zsanett: A büntetőeljárás alapelvei. In: Fantoly Zsanett – Budaházi Árpád: Büntető eljárásjogi ismeretek. I. Statikus rész. Dialóg Campus Kiadó, Budapest, 2019. p. 37.
[16] Háger Tamás: A nyilvánosság mint a tisztességes eljárás egyik garanciája a büntetőperben. In: Pro Futuro 2014/1. p. 46.
[17] Navratil Szonja: A tárgyalás nyilvánossága. In: Nagy, Marianna (szerk.): Jogi tanulmányok 2010: Ünnepi konferencia az ELTE megalakulásának 375. évfordulója alkalmából 2010. április 23. ELTE Eötvös Kiadó, Budapest, 2010. p. 108.: *„A tárgyalás nyilvánosságának legjelentősebb funkciója a társadalmi ellenőrzés, amely így lehetőséget biztosít arra, hogy az igazságszolgáltatás működése és tevékenysége átlátható, és ebből következően ellenőrizhető is legyen. A társadalmi ellenőrzés mellett a pártatlan eljárás biztosítása és a társadalom alakítása is a tárgyalások nyilvánosságának funkciói közé sorolható."*
[18] Tóth Mihály: A magyar büntetőeljárás az Alkotmánybíróság és az európai emberi jogi ítélkezés tükrében. KJK-Kerszöv Kiadó, Budapest, 2001. p. 147.
[19] Kiss Anna: Média és büntetőeljárás. Kriminológiai Tanulmányok 41. Országos Kriminológiai Intézet, Budapest, 2004. pp. 316-332.

Mindez azt jelenti, hogy a nyilvánosság nem korlátlan, tömegméretű, hanem más kizáró okok hiányában is „tárgyalóterem-méretű" nyilvánosságot jelent.[20] Németh Kata rendkívül érdekes és előremutató megállapításokat tesz a társadalmi nyilvánosság, a tárgyalótermi nyilvánosság és az ügyfélnyilvánosság témaköreiben.[21]

Háger Tamás a nyilvánosság korlátozásnak esetköreit két típusba sorolja.

- Az első csoportba a tárgyalás rendjének fenntartása, a bizonyítás zavartalan lefolytatása érdekében, vagy az eljárásban részt vevőként nem szereplő kiskorú személyek jelenlétének tilalmával kapcsolatban vezethetnek a nyilvánosság korlátozásához vagy kizárásához.
- A másikba – Háger Tamás szerint – olyan esetek tartoznak, amikor erkölcsi okból, titokvédelmi-vagy tanúvédelmi érdek miatt kerül a nyilvánosság korlátozásra.[22]

A titokvédelemi okból történő korlátozás sajátos válfaját, az orvosi titok, mint ágazati titok problematikáját színvonalas tanulmányban mutatja be Németh Kata.[23]

A tanúvédelmi okból történő nyilvánosság korlátozás bár valóban elfogadható kiemelt tárgyi súlyú deliktumok (pl.: terrorcselekmény) esetén, mégis egyes alapelvek (pl.: közvetlenség) ilyenkor sérülnek.[24]

A modern digitális világ azonban új kiívások elé állítja az igazságszolgáltatást is, hiszen a sajtónyilvánosság a technikai nóvumok megjelenésével teljesen más perspektívába került.

A „Medienjustiz" jelentősége kiszámíthatatlan folyamatokat indíthat el és kétségeket ébreszthet, hogy tud-e, képes-e a büntető igazságszolgáltatás a tömegtájékoztatásban megjelenő hírekkel nem foglalkozva pártatlan és igazságos döntést hozni. MÁRKI Dávid az igazságszolgálatás mediatizálódásával foglalkozó tanulmányában már felhívja a figyelmet az új „sajtótermékek", a közösségi médiák veszélyfaktoraira. [25] A közösségi platform (pl.: Facebook, Instagram), a blogok – részben – egy jogi szabályozási *terra incognita*, s így nagyon nehéz egyrészt a normatív, másrészt az erkölcsi elvárások betartatása. Egy kamuprofilú blogger pillanatok alatt karaktergyilkosságot képes elkövetni, s az anyagilag és szociális kapcsolatilag

[20] Háger, (2014) p. 52.
[21] Németh Kata: A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre. Debreceni Jogi Műhely 2019/1-2. pp. 58-61.
[22] Háger, (2014) p. 51.
[23] Németh (2019)
[24] Hesz Tibor – Kőhalmi László: A tanúvédelem a terhelt védőjének aspektusából. In: Mészáros Bence (szerk.): A tanú védelmének elméleti és gyakorlati kérdései. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2009. pp. 103-105.
[25] Márki Dávid: Az igazságszolgáltatás nyilvánossága, különös tekintettel a büntetőeljárás sajtónyilvánosságára. Doktori Műhelytanulmányok 2017. pp. 156-158.

tönkrement terheltnek sovány vígaszt jelent, hogy az öt évig elhúzódó büntetőeljárás végén büntetőjogi felelősség vele szemben nem kerül megállapításra.
Ehhez kapcsolódóan érdemes Szabó Andrásnak a tömegtájékoztatásban előforduló hamis bűnözőképet kialakító és szelektáló tevékenységét is megemlíteni.[26]
Teljesen új, kitaposatlan jogi területet jelentett a nyilvánosság biztosítása a koronavírus járvány körülményei között.[27] A fogvatartottak minden bizonnyal előnyben részesítik a jelenléti tárgyalásokra történő visszatérést, s nem örülnek a büntetés-végrehajtási intézeti kamerarendszer segítségével megvalósuló tárgyalásoknak.
Németh János külföldi – kanadai és amerikai – szabályozási megoldásokra hívja fel a figyelmet, melyek irányt mutathatnak a médiaszolgáltatók tárgyalási közvetítési módszereire. Németh szerint a tárgyaláson „történtek rögzítése és közzététele a médiaszolgáltatók közvetítése útján – a nyilvánosság tájékoztatására vonatkozó szabályokra is figyelemmel – eddig is megvalósulhatott, a vádlott vagy védője általi rögzítés mégis új megoldás, s nem szorítkozik csak olyan esetekre, amit előbbiek is hírértékűnek minősítenek. Az azonban kétségtelen, hogy a valós időben jelenlevő nyilvánosságot ez sem képes pótolni. A kérdés így az lehet, hogy van-e más reális megoldási lehetőség? A nemzetközi gyakorlatot figyelembe véve erre a kérdésre igenlő válasz adható: a nyilvánosság digitális biztosítására (távmeghallgatás igénybevételével tartott eljárási cselekmények esetén) ugyanis egyre több külföldi példa áll rendelkezésére.” [28] NÉMETH János ugyancsak Cristin Schmitz munkásságát idézve említi meg a Zoom platform nyújtotta médianyilvánosságban rejlő lehetőségeket. [29]
Szintén NÉMETH publikált az interneten közzétett tárgyalási anyagokkal (képernyő-vagy hangfelvételekkel) történő visszaélési lehetőségekről.[30]
Ezt a jogos kritikát el kell ismerni, ugyanakkor az online nyilvánosság jelentős mértékben hozzájárulhatna a bírósági működés kontrolljához is.

[26] Szabó András: A nyilvánosság és az adatvédelem egyes kérdéseiről a büntetőeljárások sroán. Erdélyi Jogélet 2021/4. pp. 62-63.
[27] Németh János: Nyilvánosság a büntetőeljárásban: a járványhelyzet egy újabb kérdéses pontja. Mesterséges Intelligencia 2021/1. pp. 61-70.
[28] Németh (2019) p. 67.
[29] Schmitz, Cristin: SCC poised for first virtual appeal hearing; Zoom ‘observers’ to see novel contract, criminal cases. The Lawyer’s Daily Friday, June 05/2020. (https://www.thelawyersdaily.ca/articles/19410/scc-poised-for-first-virtualappeal-hearing-zoom-observers-tosee-novel-contract-criminalcases? category=news)
[30] Németh (2019) p. 67

Végül érdemes a NÉMETH János munkájába hivatkozott, Richard SUSSKIND által jegyzett tanulmányt felidézni, mely a digitalizáció és a bírósági tárgyalás jövőjének kérdéseit tárgyalja.[31]

4. Zárógondolatok

A társadalmi ellenőrzés lehetősége hozzájárul ahhoz, hogy a bíróságok és az eljárásban részt vevő más hivatalos személyek valóban függetlenül és pártatlanul, kizárólag a törvényeknek alárendelten járjanak el. Ez pedig nem csupán az adott eljárásban részt vevő felek, hanem az egész társadalom érdeke.[32]
Király Tibor intelmeit komolyan kell venni: „A büntetőeljárás gyorsítása és egyszerűsítése sohasem juthat odáig, hogy egyeduralkodóvá tegye a nyilvános, kontradiktórius tárgyalás nélküli eljárást, mert az igazság megállapításának és a törvényesség megvalósításának ez a legfőbb eljárási eszköze."[33]

[31] Susskind, Richard: The Future of Courts. In: Remote Courts 2020/5.
[32] https://kuria-birosag.hu/hu/3-targyalas-nyilvanossaga
[33] Király Tibor: Büntetőeljárási jog. Osiris Kiadó, Budapest, 2000. p. 389.

Irodalomjegyzék

- Angyal Pál: A magyar büntetőeljárásjog tankönyve I.kötet. Atheneum Irodalmi és Nyomdai R.-T. kiadás, Budapest, 1915. p. 273.
- Fantoly Zsanett: A büntetőeljárás alapelvei. In: Fantoly Zsanett – Budaházi Árpád: Büntető eljárásjogi ismeretek. I. Statikus rész. Dialóg Campus Kiadó, Budapest, 2019. p. 37.
- Farkas Ákos: Alkotmányosság és büntetőeljárás. In. Farkas Ákos – Róth Erika: A büntetőeljárás. Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2012. p. 70.
- Fayer László: A bűnvádi perrendtartás vezérfonala. Teljesen átalakított negyedik kiadás. Franklin-Társulat Magyar Irod. Intézet és Könyvnyomda, Budapest, 1905. p. 26.
- Finkey Ferenc: A magyar büntető eljárás tankönyve. Harmadik kiadás, Politzer-féle Könyvkiadóvállalat, Budapest, 1908. p. 226.
- Háger Tamás: A nyilvánosság mint a tisztességes eljárás egyik garanciája a büntetőperben. In: Pro Futuro 2014/1. p. 46.
- Herke Csongor – Fenyvesi Csaba – Tremmel Flórián: A büntető eljárásjog elmélete. Dialóg Campus Kiadó. Budapest-Pécs, 2012. pp. 47-86.
- Hesz Tibor – Kőhalmi László: A tanúvédelem a terhelt védőjének aspektusából. In: Mészáros Bence (szerk.): A tanú védelmének elméleti és gyakorlati kérdései. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2009. pp. 103-105.
- Király Tibor: Büntetőeljárási jog. Osiris Kiadó, Budapest, 2000. p. 389.
- Kiss Anna: Média és büntetőeljárás. Kriminológiai Tanulmányok 41. Országos Kriminológiai Intézet, Budapest, 2004. pp. 316-332.
- Kovács Judit – Nagy Zsolt: A társadalmi változások hatása a büntető eljárási szabályokra a rendszerváltozás után. Jogelméleti Szemle 2001/2.
- Makója Imre: Az új büntető eljárási törvényről. In: Belügyi Szemle 1973/5. pp. 7-9. A kommunista politikus nem sorolta fel tanulmányában az alapelvek között a nyilvánosságot, de nyilván egy pártállami funkcionáriustól ilyet nem is várhatunk el.; Szabóné Nagy Teréz: Az alapelvek rendszere az új büntetőeljárási törvényben. Belügyi Szemle XI. évfolyam 1973/6. 14-19.o. Az már inkább elszomorítóbb, hogy az ELTE néhai egyetemi docensének opusában sem kerül említésre a nyilvánosság fontos szerepe. A szerző

védelmében ugyanakkor elmondható, hogy vélhetően a tanulmány terjedelmi korlátai miatt nem tért ki a nyilvánosság elemzésére, hiszen itt egy informatív, figyelemfelhívó kéziratról van szó.

- Márki Dávid: Az igazságszolgáltatás nyilvánossága, különös tekintettel a büntetőeljárás sajtónyilvánosságára. Doktori Műhelytanulmányok 2017. pp. 156-158.
- Navratil Szonja: A tárgyalás nyilvánossága. In: Nagy, Marianna (szerk.): Jogi tanulmányok 2010: Ünnepi konferencia az ELTE megalakulásának 375. évfordulója alkalmából 2010. április 23. ELTE Eötvös Kiadó, Budapest, 2010. p. 108.: „A tárgyalás nyilvánosságának legjelentősebb funkciója a társadalmi ellenőrzés, amely így lehetőséget biztosít arra, hogy az igazságszolgáltatás működése és tevékenysége átlátható, és ebből következően ellenőrizhető is legyen. A társadalmi ellenőrzés mellett a pártatlan eljárás biztosítása és a társadalom alakítása is a tárgyalások nyilvánosságának funkciói közé sorolható."
- Németh János: Nyilvánosság a büntetőeljárásban: a járványhelyzet egy újabb kérdéses pontja. Mesterséges Intelligencia 2021/1. pp. 61-70.
- Németh Kata: A büntetőeljárás nyilvánosságának jogszabályi hátterében húzódó alapjogi kollíziók feltárása, különös tekintettel az ágazati titokvédelemre. Debreceni Jogi Műhely 2019/1-2. pp. 58-61.
- Olti Vilmos. A védő szerepe a burzsoa és a szocialista büntető eljárásban (III.). Jogtudományi Közlöny 1954. január-február. hó. 51.o.
- Schmitz, Cristin: SCC poised for first virtual appeal hearing; Zoom 'observers' to see novel contract, criminal cases. The Lawyer's Daily Friday, June 05/2020. (https://www.thelawyersdaily.ca/articles/19410/scc-poised-for-first-virtualappeal-hearing-zoom-observers-tosee-novel-contract-criminalcases? category=news)
- Susskind, Richard: The Future of Courts. In: Remote Courts 2020/5.
- Szabó András: A nyilvánosság és az adatvédelem egyes kérdéseiről a büntetőeljárások sroán. Erdélyi Jogélet 2021/4. pp. 62-63.
- Tóth Mihály: A magyar büntetőeljárás az Alkotmánybíróság és az európai emberi jogi ítélkezés tükrében. KJK-Kerszöv Kiadó, Budapest, 2001. p. 147.
- Vargha Ferencz: Főtárgyalás a törvényszék előtt. In: Balogh Jenő – Edvi Illés Károly – Vargha Ferencz: A bűnvádi perrendtartás magyarázata. Harmadik kötet. Grill Károly, Cs. és Kir. Udvari Könyvkereskedése, Budapest, 1899. p. 287

Mitrovics Zoltán
PhD-hallgató (PTE-ÁJK)

Skype-alapú kapcsolattartás a hazai börtönökben

Absztrakt

A 2020-ban megjelent COVID-19 világjárvány a magyarországi büntetés-végrehajtási szervezetet is számos kihívás elé állította. A járványhelyzet okán elrendelt veszélyhelyzetben számos jogszabály született, melyek érintették a büntetés-végrehajtási szabályokat, többek közt a fogvatartottak kapcsolattartására vonatkozó rendelkezéseket is. Az egészség megóvása, a vírus terjedésének megakadályozása érdekében a büntetés végrehajtás 2020. március 7. napjával felfüggesztette az ideiglenes intézet elhagyások engedélyezését a fogvatartottak számára, valamint a látogatások is megszűntek. A személyes látogatófogadás megszüntetésének ellensúlyozására széles körben elérhetővé váltak a fogvatartotti internetalapú videó hívások (Skype). Tanulmányomban a kapcsolattartás és a sikeres társadalmi reintegráció viszonyának elemzésére, valamint ehhez kapcsolódóan a Skype térnyerésének lehetséges okainak vizsgálatára törekszem.

Kulcsszavak: COVID-19, fogvatartotti jogok és kötelezettségek, látogatófogadás, Skype alapú kapcsolattartás

1. Bevezetés

A büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról szóló 2013. évi CCXL. törvényben (továbbiakban: Bv. tv.) a szabadságvesztés végrehajtásának feladataként és a speciális prevencióhoz köthető célként – az ítéletben meghatározott joghátrány érvényesítése mellett – jelenik meg, hogy az elítélt szabadulása után a társadalomba sikeresen visszailleszkedjen és a társadalom jogkövető tagjává váljon. A sikeres társadalmi reintegrációt a büntetés-végrehajtási intézeteken (továbbiakban: bv. intézet) belül számos intézkedés, szakember segíti, ezek között szerepel többek közt a fogvatartottak munkáltatása, oktatása, részükre különböző programok szervezése, illetve a családi és társadalmi kapcsolatok fenntartásának biztosítása. A sikeres társadalmi reintegráció sikerességének szempontjából kiemelkedő jelentőségű lehet a kapcsolattartás. Számos hazai és nemzetközi kutatás, mely a családi, társas kapcsolatok hatásait vizsgálta a fogvatartottak esetében azon eredményekről számol be, melyek azt támasztják

alá, hogy a bűnismétlés csökkenése tekintetében a kapcsolattartás meghatározó szerepet tölthet be.

A hazai kutatások közül Albert Fruzsina és Bíró Emese egy 2012 és 2015 között zajló, „Szubjektív reszocializációs esélyek" elnevezésű OTKA kutatás keretében vizsgálták többek közt a családi kapcsolatok szerepét a reintegrációban. A kutatás eredményeképpen megállapították, hogy a proszociális családi kapcsolatok a kapcsolattartás útján fejtik ki pozitív hatásukat, társas támogatást nyújtanak és ezáltal hozzájárulnak a bűnismétlés csökkenéséhez. A támogatás mellett egyfajta kontrollt is jelentenek a fogvatartott számára, mely által motiváltabbá válik a normakövetésre, a szabadságvesztés alatt a szabályok betartására. Ugyanakkor a kutatásuk során a deviáns családi kapcsolatokat is vizsgálták. A deviáns családi kapcsolatok hatással lehettek a bűnelkövetésre, közvetve vagy közvetlenül szerepet játszhattak a bűncselekmény elkövetésében. Az eredményeik alapján még a deviáns családi kapcsolatok is nyújthatnak társas támogatást, ugyanakkor a kontroll funkciót nem töltik be, így a bűnismétlés tekintetében nem hatnak visszatartó erővel.[1]

Borbíró Andrea és Szabó Judit 2011. évben induló kutatásának célja a hazai bv. intézetek társadalmi reintegrációt elősegítő programjainak és tevékenységének a vizsgálata volt, elsősorban a harmadlagos prevenció érvényesítésével, eredményességével összefüggő kérdéseket vizsgálták, illetve a dezisztencia és a sikeres reintegráció összefüggéseit. A kutatás során komplex módszertant alkalmaztak, jogszabályelemzést, dokumentumelemzést, fókuszcsoportos és félig strukturált interjúkat is készítettek. Az ő kutatási eredményeik is arra engedtek következtetni többek közt, hogy a család, a külső társas kapcsolatok a reintegráció szempontjából nagyon fontos tényezők, ezért ezek fenntartásának támogatására kiemelt feladatként kell tekintenie a hazai büntetés-végrehajtásnak.[2]

A fentiek alapján elmondható, hogy a kapcsolattartás, a támogató családi és baráti kapcsolatok megléte a sikeres reintegráció szempontjából kiemelt jelentőségű. A hazai büntetés-végrehajtás a kapcsolattartás számos módját biztosítja a fogvatartottak részére, ilyenek a levelezés, telefonbeszélgetés a bv. intézet által biztosított telefonnal és telekommunikációs eszköz útján történő

[1] Bíró Emese: A fogvatartottak családi kapcsolatainak szerepe a bűnelkövetésben, a börtönélményben és a reintegrációban. In Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek. MTA Társadalomtudományi Kutatóközpont. 2015. (Szociológiai Intézet). Forrás: real.mtak.hu/31000/1/albert_biro_sikeres%20reintegracio_bortonon%20innen%20es%20tul.pdf (letöltés ideje: 2021.12.30.)

[2] Borbíró Andrea – Szabó Judit: Harmadlagos megelőzés a magyar büntetés-végrehajtási intézetekben a nemzetközi kutatások fényében. In: Vókó Gy. (szerk.): Kriminológiai Tanulmányok 49. OKRI, Budapest. 2012.

kapcsolattartás, csomag küldése és fogadása, látogató fogadása, látogató bv. intézeten kívüli fogadása, kimaradás, eltávozás. [Bv.tv. 173. § (1)]

2. Koronavírus hatása a kapcsolattartásra

A SARS-CoV-2 néven (koronavírus) azonosított vírus 2020. évben történő megjelenése kihívás elé állította a büntetés-végrehajtás szerveit. A büntetés-végrehajtási jogviszonyból következő egyik felelőssége a bv. szervezeteknek, hogy megóvják a fogvatartottak egészségét, ugyanakkor a fogvatartottaknak joguk van a kapcsolattartásra. A fennálló helyzet megoldására a bv. szervezet nagy szakmai érzékenységgel reagált, az elrendelt intézkedések során megfelelően sikerült kialakítani a fogvatartottak jogai és a közérdek védelme közötti arányokat. [3] A vírus zárt térben történő gyors terjedésének megakadályozása érdekében a Büntetés-végrehajtás Országos Parancsnoksága különböző intézkedések bevezetésével reagált. Az intézkedések elsősorban a személyes kontaktussal járó kapcsolattartási formákat érintették, de módosultak a levelezés, csomag küldés és fogadás szabályai is. A személyes kontaktussal járó kapcsolattartási formák közül első körben a fogvatartottak egészségének megőrzése érdekében 2020. március 7. napjától a bv. intézetek felfüggesztették az ideiglenes intézetelhagyások (látogató bv. intézeten kívüli fogadása, kimaradás, eltávozás) engedélyezését a fogvatartottak számára.

Ezt követően a látogatófogadás felfüggesztésére került sor, mely intézkedés összhangban volt a Kormány 2020.03.28. napjától bevezetett kijárási korlátozásával. Ezen intézkedések hatására a személyes kapcsolattartás lehetősége a fogvatartottak számára tulajdonképpen megszűnt. A személyes kapcsolattartási formák korlátozásának ellensúlyozására a BVOP elsősorban a személyes kontaktussal nem járó kapcsolattartási formák bővítésével, illetve a Skype alapú kapcsolattartási lehetőség kiterjesztésével kompenzálta a fogvatartottakat.

3. A Skype alapú kapcsolattartás

Az elektronikus kapcsolattartási forma igénybevételére már a koronavírus megjelenése előtt lehetőségük volt a fogvatartottaknak. A Bv.tv. 173.§ (2) bekezdésében a jogalkotó, már a jogszabály megalkotásakor rendelkezett róla.[4] Az elektronikus kapcsolattartás igénybevételének részletszabályait a szabadságvesztés, az elzárás, az előzetes letartóztatás és a rendbírság helyébe lépő elzárás végrehajtásának részletes szabályairól szóló 16/2014. (XII. 19.) IM rendelet tartalmazza. Ezen szabályok szerint az ilyen típusú

[3] Forgács Judit: Kapcsolattartás járvány idején. In.: Börtönügyi Szemle, 2021/1.

[4] Fehér Szilárd: Kihívások a büntetés-végrehajtásban a koronavírus-járvány alatt. In: Börtönügyi Szemle, 2021/2.

kapcsolattartásra csak a fogvatartottak egy bizonyos részének volt lehetősége (a szigorúbb rezsimbe sorolt fogvatartottak nem vehették igénybe). Az egészségügyi válsághelyzetre tekintettel azonban a veszélyhelyzet kihirdetésével összefüggésben egyes büntetés-végrehajtási szabályok módosításáról szóló 90/2020. (IV. 5.) Korm. rendelet rendelkezései alapján az elektronikus kapcsolattartás a rezsimszabályokra tekintett nélkül alkalmazhatóvá vált, ezzel megteremtve a lehetőséget a kapcsolattartási forma igénybevételi körének szélesítésére, illetve a Skype alapú kapcsolattartás térnyerésére.
Ezt követően a bv. intézetek a helyzetre gyorsan reagálva, nagyon rövid idő alatt megteremtették annak lehetőségét, hogy a fogvatartottak Skype alapú hívásokon keresztül tudják tartani a kapcsolatot a rögzített kapcsolattartóikkal. A Skype használatára vonatkozó szabályok folyamatosan változtak, de ezek a változások a fogvatartottak oldaláról tekintve elsősorban pozitív irányba történtek. A változások eredményeképpen növekedett egyrészt az egyes Skype hívások időtartama, másrészt a Skype kapcsolattartás havi gyakorisága is.

IDŐSZAK	GYAKORISÁG	IDŐTARTAM	IGÉNYBE VEHETI
2017.07.10. – 2020.04. 21.	Heti 1x	10 perc	Enyhébb rezsimben és HSR részlegen elhelyezettek részére
2020.04.21 – 2020.08.02.	Heti 1x	15-60 perc	Rezsimszabályoktól függetlenül
2020.08.02. – 2020.11.01.	Heti 2x	15-60 perc	Rezsimszabályoktól függetlenül
2020.11.01. – 2021.03.05.	Heti 2x	30-60 perc	Rezsimszabályoktól függetlenül
2021.03.05. - visszavonásig	Heti 2x	45-120 perc	Rezsimszabályoktól függetlenül

1. számú táblázat: Az internet alapú Skype-telefonálás fokozatos bevezetése[5]

A Skype alapú kapcsolattartás elemzése kapcsán Forgács Judit arra a megállapításra jutott, hogy egyrészt azon fogvatartottak esetében, akik rendelkeztek ugyan rögzített kapcsolattartóval, de aktív kapcsolattartásuk nem volt, esetükben a Skype kapcsolattartás igénybevételi lehetősége ismét

[5] Forrás: Forgács Judit (2021): Kapcsolattartás járvány idején. In.: Börtönügyi Szemle, 2021/1., p. 61.

lehetővé tette az aktív kapcsolattartást a hozzátartozókkal. Másrészt vizsgálta az aktív kapcsolattartással rendelkező, de látogatót nem fogadók körében a Skype használatának alakulását. Az eredmények alapján ezen fogvatartottak esetében is megállapítható, hogy egyre többen kapcsolódtak be a Skype alapú kapcsolattartás használatába.[6]
Hasonló eredményre jutott Somogyvári Mihály is. A Skype kapcsolattartás kérdéskörében végzett vizsgálatuk során arra a megállapításra jutottak, hogy 2020. márciusát követően robbanásszerűen megnőtt a fogvatartottak körében a Skype alapú kapcsolattartás. A vizsgálat felvételekor a teljes fogvatartotti populáció 56,76%-a élt a Skype kapcsolattartással. A vizsgált fogvatartotti körben a fogvatartottak több mint 46%-a a Skype használatának köszönhetően tudott kapcsolatot tartani családtagjaival, hozzátartozóival, ennyi volt ugyanis azon fogvatartottak aránya, akiknek a Skype lehetősége előtt nem volt személyes kapcsolattartásuk. A vizsgálatuk egy további nagyon fontos megállapítása, hogy a Skype alapú kapcsolattartás leginkább a letartóztatott és fiatalkorú kapcsolattartás nélküli fogvatartottak körében javította a kapcsolattartást, márpedig a fiatalkorú fogvatartottak esetében a családi kötelékek megléte, a rendszeres kapcsolattartás kiemelt fontosságú a sikeres társadalmi reintegrációjuk, a bűnismétlés elkerülése érdekében.[7]
Összegezve elmondható, hogy a Skype alapú kapcsolattartás a fogvatartottak és rögzített hozzátartozóik közötti interakciókat növelték, a fogvatartottak nagyobb arányban tartottak kapcsolatot hozzátartozóikkal és hosszabb időtartamban volt lehetőségük ezt megtenni.

4. Skype használat tapasztalatai a Baranya Megyei Büntetés-végrehajtási Intézetben

Jelen tanulmányomban a reintegrációs tisztek és a fogvatartottak szubjektív megítélését vizsgálom a Skype használatával kapcsolatosan a Baranya Megyei Büntetés-végrehajtási Intézetben. A vizsgálatba csak azon fogvatartottak kerültek be, akik rendszeresen használják a Skype alkalmazást, közülük a megkérdezettek véletlen mintavételi eljárással kerültek kiválasztásra.
Első körben a 2022. április hónapban érvényben lévő Skype használati szabályokat vizsgáltam meg. Az országos szabályozáshoz hasonlóan a Baranya Megyei Bv. Intézetben is csak azon hozzátartozókkal lehetséges a Skype-on keresztüli kapcsolattartás, akik kapcsolattartóként szerepelnek a nyilvántartásban és nyilatkoztak Skype elérhetőségükről. Az Intézetben a Skype minden fogvatartott számára egységesen heti egy alkalommal vehető

[6] Forgács (2021)
[7] Somogyvári Mihály: A koronavírus hatása a fogvatartotti kapcsolattartásra – Kihívások és szervezeti válaszok: A fogvatartotti videóhívások alkalmazásának empirikus vizsgálata. In: Belügyi Szemle 2021/5 különszám. pp. 109-143.

igénybe, alkalmanként maximum 45 perc időtartamban. A kapcsolattartás során egyidejűleg maximum 4 fő lehet jelen a hozzátartozói oldalon. A beszélgetés alatt kép és/vagy hangrögzítés tilos, illetve nem lehet sértő, megalázó módon viselkedni, nem lehet levetkőzni, írásos dokumentációt bemutatni. A reintegrációs tisztek elmondásai alapján a szabályokat az esetek nagy részében a fogvatartottak betartják, amennyiben erre vonatkozóan szabályszegést tapasztalnak a „Skype beszélőt" azonnal megszakítják.

4.1.Skype előnyei-hátrányai a fogvatartottak szemszögéből

Ezt követően a Skype-ot használó fogvatartottak körében a „Skype beszélő" előnyeit és hátrányait vizsgáltam a személyes látogatófogadáshoz viszonyítva. A fogvatartottak válaszait az alábbi táblázatban összegeztem.

ELŐNYÖK	HÁTRÁNYOK
• A hozzátartozónak nem kell utaznia • Egy helyen 4-en lehetnek • „Kényelmesebb" • Otthonát is láthatja • Ingyenes • Hetente elérhető	• Hiányzik a személyesség • Nem lehet megosztani a 45 percet • Előfordulnak technikai nehézségek

2. sz. táblázat: Skype előnyei-hátrányai (fogvatartottak)[8]

A fogvatartottak előnyként emelték ki, hogy a hozzátartozónak nem szükséges utaznia a kapcsolattartás érdekében, így a család jelentős költséget tud megtakarítani. A jelentős anyagi kiadáson túl, előfordulhat olyan eset is, amikor a hozzátartozónak több száz kilométert szükséges utaznia a kapcsolattartás érdekében. Különös nehézséget okoz a nagy távolság abban az esetben, ha kisgyermek vagy csecsemő is utazna a családdal. Ezek a nehézségek a Skype segítségével kiküszöbölhetők, így a kapcsolttartás ezen formája kevesebb kiadással jár és „kényelmesebb" is.
A fogvatartottak pozitívumként emelték ki egyrészt, hogy a kapcsolattartás során otthonukat is láthatják, mely egyfajta nyugalmat ad nekik. Másrészt, hogy akár négy családtaggal is tudnak egyszerre kapcsolatot tartani. A kapcsolattartó családtagok különböző településeken élnek, így a „Skype beszélő", vagyis a kapcsolattartás céljából akár egymáshoz utazhatnak, mely lényegesen kisebb távolságot jelent, mint a fogvatartó bv. intézetbe történő eljutás.

[8] Forrás: Saját szerkesztés, 2022.

Mindezeken túl a fogvatartottak pozitívan értékelték, hogy míg a látogatófogadásra havonta maximum 2 alkalommal volt lehetőségük, addig a Skype kapcsolattartás hetente megvalósulhat. Nem utolsó sorban említették a Skype ingyenességét. Egyrészről a családtagoknak sem szükséges külön anyagi ráfordítás, internet hozzáférés, okos mobiltelefon már majdnem minden családban elérhető. Másrészről a fogvatartottaknak nem szükséges a bv. intézeti mobiltelefonálás magas percdíjait fizetni.
A hátrányok közt említették a fogvatartottak, hogy hiányzik a személyesség. Még abban az esetben is igényelnék a személyes találkozást, ha a látogatófogadás során egy „plexi fal" választja el a családtagokat egymástól. Hátrányként jelent meg, hogy a 45 percet nem lehet megosztani a kapcsolattartók között. Előfordulhat, hogy a fogvatartott a rendelkezésre álló idejét megosztva szeretné felhasználni (pl: 25 percet beszélne családtagjaival és a fennmaradó 20 percet a barátaival vagy leendő munkáltatójával használná fel) erre azonban nincs lehetőség, egy alkalommal csak egy hívást lehetséges indítani és amennyiben ennek keretében a kapcsolattartást befejezték annak ellenére, hogy esetlegesen van további fennmaradó időkeret nem lehetséges újabb hívás indítása.

4.2. Skype előnyei-hátrányai a reintegrációs tisztek szemszögéből

A Skype használati tapasztalatok vizsgálata keretében a reintegrációs tisztek álláspontjára is rákérdeztem, a fogvatartotti vizsgálathoz hasonlóan. A reintegrációs tisztek véleményét is abból a szempontból vizsgáltam, hogy mit gondolnak a „Skype beszélő" előnyeiről és hátrányairól a személyes látogatófogadáshoz viszonyítva.

ELŐNYÖK	HÁTRÁNYOK
• Nincs ki-be léptetés • Tiltott tárgyak bekerülése elkerülhető • Gyakoribb a tényleges megvalósulás (beszélő havi 1-2-szer volt) • Ingyenes • Nem magyar állampolgárságú fogvatartottak részére is elérhető	• Biztosítani kell • Technikai eszközöket gyakran cserélni szükséges • Külön adminisztrációt igényel

3. számú táblázat: Skype előnyei-hátrányai (reintegrációs tisztek)[9]

[9] Forrás: saját szerkesztés, 2022.

A reintegrációs tisztek a „Skype beszélő” előnyei közt említették, – a fogvatartottakhoz hasonlóan – annak ingyenességét. A reintegrációs tisztek is főként arról számoltak be, hogy a fogvatartottak többségének családtagjai rendelkeznek internet hozzáféréssel, így tulajdonképpen külön anyagi megterhelést a Skype alapú kapcsolattartás nem jelent számukra. Elmondták továbbá, hogy amennyiben mégis valamely hozzátartozó anyagi vagy más okok (pl.: idős kora miatt nem tudja használni a technikát) miatt nem tudná tartani a kapcsolatot Skype-on keresztül otthonról, akkor lehetősége van a Digitális Jóléti Program keretében létrehozott Digitális Jóléti Pontok valamelyikén is kapcsolatot tartani a fogvatartottal. A Digitális Jóléti Program egy 2015 végén indult kormányzati program, melynek célja az internet mindenki számára történő hozzáférhetővé tétele. A program keretében digitális jóléti pontokat hoztak létre, jelenleg az országban több mint 1 500 helyen érhetőek el a digitális jóléti pontok többnyire önkormányzati fenntartású épületekben, főként könyvtárakban. [10] A Büntetés-végrehajtás Országos Parancsnoksága együttműködési megállapodást kötött a Program vezetőivel, melynek értelmében a hozzátartozóknak 2021. decembere óta itt is lehetőségük van a skype használatára. Technikai és egyéb nehézségek esetén a digitális jóléti pontokon dolgozó mentorok segítséget tudnak nyújtani.

Az előnyök közt említették továbbá, hogy a Skype beszélő esetén nincs az intézetbe történő be és kiléptetés. A bv. intézetbe történő belépés és kilépés hosszabb időt vesz igénybe. A látogatókat tájékoztatják a szabályokról, fémkereső kapun kell áthaladniuk stb. A szabályok maximális betartása mellett is előfordult azonban, hogy az intézetbe tiltott tárgy került be. A „Skype beszélő” bevezetése óta erre nincs lehetőség, így az intézet biztonságára is pozitív hatással van.

További előnye a „Skype beszélőnek” a személyes látogatófogadáshoz képest, hogy a látogatófogadás különböző okok miatti elmaradása sokkal gyakoribb volt, mint a „Skype beszélő” elmaradása, valamint a Skype heti rendszerességgel is megtartható, míg a személyes látogatófogadásra maximum kéthetente volt csak lehetőség. Nem utolsó sorban pozitívum, hogy a nem magyar állampolgárságú fogvatartottak esetében is megnövekedett a kapcsolattartás a családtagokkal. A külföldi fogvatartottak esetében gyakran egyáltalán nem volt személyes kapcsolattartás az utazás, a költségek miatt, a Skype azonban ezeket a nehézségeket is áthidalhatja.

A reintegrációs tisztek a hátrányok közt említették, hogy a „Skype beszélőt” is biztosítani kell, a szabályok betartását folyamatosan monitorozni szükséges. Mivel a Skype kapcsolattartás több alkalommal kerül lebonyolításra, ezért ennek biztosítása is sokkal több időt vesz igénybe, így az amúgy is leterhelt

[10] Digitális Jólét Program: www.digitalisjoletprogram.hu

reintegrációs tisztek munkaterhe növekedett. Ráadásul a „Skype beszélő” adminisztrációja külön eljárás szerint történik, mely még inkább tovább növeli a munkaterhet, adminisztrációs kötelezettséget.
Végül a hátrányok között került említésre a technikai eszközök gyakori amortizációja. A „Skype beszélő” alkalmával egy teremben a kialakított végpontoknak megfelelő számú fogvatartott részére biztosított egyidőben a kapcsolattartás lehetősége. Annak érdekében, hogy a beszélgetés intimitása biztosított legyen és megfelelően tudjanak egymással kommunikálni, a „Skype beszélő” során a fogvatartott mikrofont és fülhallgatót használ. Ezen eszközök azonban gyakran meghibásodnak és cseréjük válik szükségessé.
Összességében a „Skype beszélő” gyakorlati tapasztalataival kapcsolatban, mind a fogvatartottaknak, mind a reintegrációs tiszteknek pozitív a véleményük.

5. Összegzés

A 2020. évben megjelenő koronavírus járvány komplex probléma elé állította a büntetés-végrehajtás szervezetét, melyet adekvát intézkedésekkel sikerült úgy megoldani, hogy közben a szabadságvesztés büntetés végrehajtásának biztonsága nem sérült, valamint a fogvatartotti jogok biztosítása is megvalósult. Az elektronikus kapcsolattartás hátrányait és előnyeit latba véve összességében mind a szakemberek, mind a fogvatartottak pozitívan értékelték annak bevezetését. Számos fogvatartott esetében a „Skype beszélő” nyitotta meg annak lehetőségét, hogy családtagjaival felvegye és rendszeresen tartsa a kapcsolatot. Az egészségügyi veszélyhelyzet megszűnésével a magyarországi büntetés-végrehajtási intézetekben 2022. május hónaptól ismételten lehetőség lesz a személyes látogatófogadásra. Első körben havonta maximum egy alkalommal, két fő, látogató fogadható 1 óra időtartamban. Személyes látogatófogadás igénylése esetén a „Skype beszélő” az eddigi havi 4 lehetőségről lecsökken havi egy lehetőségre. A fogvatartottak az egyik legnagyobb hátárnyként a személyesség hiányát említették a Skype beszélő esetén, ezért feltételezhető, hogy az első hónapokban sokan szeretnének szeretteikkel, hozzátartozóikkal személyesen találkozni. Ugyanakkor a Skype előnyei nem elhanyagolhatók, ezért az is feltételezhető, hogy az első hónapok magas személyes látogatófogadásai idővel lecsökkennek és azon hónapok esetén amikor nem lesz lehetőség bármilyen okból kifolyólag a személyes kapcsolattartásra a Skype beszélő továbbra is népszerű lesz a fogvatartottak körében.

Irodalomjegyzék

- Bíró Emese: A fogvatartottak családi kapcsolatainak szerepe a bűnelkövetésben, a börtönélményben és a reintegrációban. In Albert Fruzsina szerk.: Életkeretek a börtönön innen és túl. Szubjektív reszocializációs esélyek. MTA Társadalomtudományi Kutatóközpont. 2015. (Szociológiai Intézet). Forrás: real.mtak.hu/31000/1/albert_biro_sikeres%20reintegracio_bortonon%20innen%20es%20tul.pdf (letöltés ideje: 2021.12.30.) pp. 73-112.
- Borbíró Andrea – Szabó Judit: Harmadlagos megelőzés a magyar büntetés-végrehajtási intézetekben a nemzetközi kutatások fényében. In: Vókó Gy. (szerk.): Kriminológiai Tanulmányok 49. OKRI, Budapest, 2012. pp. 158–192.
- Fehér Szilárd: Kihívások a büntetés-végrehajtásban a koronavírus-járvány alatt. In.: Börtönügyi Szemle, Büntetés-végrehajtás Országos Parancsnoksága, 2021/2., pp. 67-82.
- Forgács Judit: Kapcsolattartás járvány idején. In.: Börtönügyi Szemle, Büntetés-végrehajtás Országos Parancsnoksága, 2021/1., pp. 51-68.
- Somogyvári Mihály: A koronavírus hatása a fogvatartotti kapcsolattartásra – Kihívások és szervezeti válaszok: A fogvatartotti videóhívások alkalmazásának empirikus vizsgálata. Belügyi Szemle 2021/5. különszám pp.110-144.

Projics Nárcisz
PhD-hallgató (PTE-ÁJK)

Valótlan médiatartalommal kapcsolatos különleges személyiségvédelmi eszköz

Absztrakt

A mai digitális korban egyre gyakrabban fordul elő a személyiségi jog megsértése valótlan médiatartalommal online környezetben, hírportálokon. A sajtó-helyreigazítás különleges személyiségvédelmi eszköz. Ha valakiről meghatározott médiatartalomban valótlan tényt állítanak, híresztelnek vagy valós tényt hamis színben tüntetnek fel, az érintett helyreigazító közlemény közzétételét kérheti a sajtószervtől. Amennyiben a sajtószerv a helyreigazítás közzétételére irányuló kötelezettségének határidőben nem tesz eleget, a helyreigazítást igénylő pert indíthat a közlemény közzététele iránt. A sajtó-helyreigazítási per a helyreigazító közlemény közzétételére irányul. Az eljárás anyagi jogi alapját a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény és a Polgári Törvénykönyvről szóló 2013. évi V. törvény adja. Az igényérvényesítés két szakaszra osztható. A peres eljárást megelőzően kell sor kerülnie a sajtószerv előtti kötelező előzetes eljárásra és csak ennek sikertelensége esetén kezdeményezhető eredményesen a peres eljárás. A médiatartalomban megjelenő tényállítást sérelmező személy nem fordulhat közvetlenül a bírósághoz. A sajtószerv előtti eljárás kötelező és mellőzhetetlen előzménye a perindításnak. A peres eljárás során speciális szabályok érvényesülnek, amelyek a per hatékony és gyors lefolytatását segítik elő. A tanulmányban a sajtó-helyreigazítás egyes attribútumaira és néhány jogalkalmazásban felmerülő kérdésre kívánok rávilágítani.

Kulcsszavak: sajtó-helyreigazítás, sajtószerv, médiatartalom, helyreigazító közlemény

1. Bevezető gondolatok

A tömegtájékoztatási eszközök az emberek életében fontos szerepet töltenek be. A sajtó az emberek információhoz jutását és tájékozódását segíti elő. Napjainkban egyre elterjedtebbek a napilapok, folyóiratok online elérhető, elektronikus változatai. A közelmúltban készült egy felmérés, amely azt vizsgálja, hogy „*Honnan tájékozódunk?*”. Az adatokból egyértelműen megfigyelhető az internet szerepének növekedése, ezen belül is az internetes hírportálokról történő információszerzés, ugyanakkor egyre jelentősebb a

közösségi média hatása is. Annak ellenére, hogy még mindig alacsony azok aránya, akik a közösségi médiát tekintik elsődleges hírforrásnak, a korábbi adatokhoz képest növekedést mutat. A kutatás során a megkérdezettek öt médiumból hármat választhattak, ahonnan leggyakrabban tájékozódnak. A televízió végzett az első helyen, a tévé hírműsoraiból a megkérdezettek háromnegyede tájékozódik, azonban ezt követően a második legfontosabb tájékozódási forrásnak az interneten elérhető hírportálok számítanak. Eközben a nyomtatott napilapok nemcsak, hogy elmaradnak a két vezető médiumtól, hanem szerepük csökkent, egyre inkább veszítenek súlyukból. Az is megfigyelhető, hogy az internetes hírportálokról, illetve közösségi médiából tájékozódok életkora nőtt. Itt azonban nem elöregedésről beszélhetünk, hanem ez azt jelenti, hogy korábban csak a fiatalabb korosztály tájékozódott ezekből a forrásokból, ma már viszont az idősebbek közül egyre többen szereznek a világhálóról információt, ahogy egyre nő körükben az internethasználók, Facebookon regisztráltak száma is. Egyre inkább megfigyelhető a közösségi média térnyerése.[1]

A Nemzeti Média- és Hírközlési Hatóság 2019 novembere és decembere között készített kutatást az internetezők körében, amely azt vizsgálta, hogy a legalább hetente internetező népesség honnan tájékozódik, mit néz, valamint hogyan kommunikál. A tájékozódás esetében a kutatás eredményei alapján kijelenthetjük, hogy a tájékozódási források között az internet teret nyert minden korosztály körében, a hagyományos sajtó pedig háttérbe szorult.[2]

A fentiekben röviden vázolt kutatások és az azok során nyert adatok is mutatják, hogy a médiatartalmaknak a tájékozódásban, illetve az információszerzésben nagy jelentőségük van, rövid idő alatt rengeteg emberhez jut el a közzétett tartalom. Ha a médiatartalom valótlan tényt tartalmaz és ezzel személyiségi jogsértés valósul meg, akkor ennek orvoslására a sajtó-helyreigazítás mint a polgári jog különleges személyiségvédelmi eszköze áll az érintett rendelkezésére.

2. Jogszabályi környezet

Magyarország Alaptörvénye a IX. cikkben kimondja, hogy mindenkinek joga van a véleménynyilvánítás szabadságához, valamint Magyarország elismeri és védi a sajtó szabadságát és sokszínűségét. Azonban a véleménynyilvánítás szabadságának is van korlátja, nem irányulhat mások emberi méltóságának a megsértésére.[3] Jobbágyi Gábor ezt így foglalta össze: „*Egy nyílt, demokratikus társadalomban a sajtó és a véleménynyilvánítás szabadsága alapvető emberi*

[1] https://www.forsense.hu/honnan-tajekozodunk-2/ (2022. 04. 20.)
[2] https://nmhh.hu/cikk/213676/NMHHfelmeres_csokken_a_hagyomanyos_media_fogyasztoinak_aranya_az_internethez_kepest (2022. 04. 20.)
[3] Alaptörvény IX. cikk (1) és (4) bek.

és politikai jog. Így a sajtónak kettős követelménynek kell megfelelnie: a sajtó és véleménynyilvánítás szabadsága mellett gondosan őrizkednie kell a személyiségi jogok megsértésétől." [4]

A sajtótól elvárt feladat a valósághű tájékoztatás adása. A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (a továbbiakban: Smtv.) 4. § (1) bekezdése rögzíti, hogy Magyarország elismeri és védi a sajtó szabadságát és sokszínűségét. Azonban az Smtv. a sajtóval szemben támasztott fontos követelményként mondja ki, hogy tiszteletben kell tartania az emberi méltóságot.[5] A felelősségi kérdések körében az Smtv. a médiatartalom-szolgáltatót nevesíti, amely szerint a médiatartalom-szolgáltató a jogszabályok keretei között önállóan dönt a médiatartalom közzétételéről, és felelősséggel tartozik e törvényben foglaltak megtartásáért.[6]

A Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) a személyiséget, a személyiségi jogokat általános jelleggel védi, valamennyi személyiségi jogvédelem alatt áll, azok is, amelyek nem kerültek külön nevesítésre. A személyiségi jogokat mindenki köteles tiszteletben tartani.[7] A személyiséget sajtóközlemény útján ért sérelem orvoslásának sajátos szabályai vannak. A sajtó-helyreigazítás intézménye a személyiség védelme mellett segít megőrizni a sajtó hitelét. A sajtó-helyreigazítási jogot az Smtv. rögzíti.[8] A valósághű tájékoztatás elvárásának történő megfelelés miatt a sajtószervnek is érdeke a valótlan tények kiigazítása. Emellett az Smtv. kimondja, hogy mindenkinek joga van, hogy megfelelően tájékoztassák a helyi, az országos, az európai közélet ügyeiről, valamint Magyarország polgárai és a magyar nemzet tagjai számára jelentőséggel bíró eseményekről. Ezen ügyekről és eseményekről hiteles, gyors, pontos tájékoztatást kell adnia a médiarendszernek.[9]

A polgári perrendtartásról szóló 2016. évi CXXX. törvény (a továbbiakban: Pp.) határozza meg a sajtó-helyreigazítás iránt indított per eljárási szabályait, illetve részben tartalmazza a sajtószerv előtti előzetes eljárásra vonatkozó szabályokat. [10] A jogvita természete megköveteli a jogalkalmazó szerv gyorsaságát, az eljárás gyorsaságának irányába hat, hogy a bíróságnak soron kívül kell eljárnia a per minden szakaszában, így a fellebbezési és

[4] Jobbágyi Gábor: Személyi és családi jog. Szent István Társulat, Budapest, 2000. p. 76.
[5] Smtv. 14. § (1) bek.
[6] Smtv. 21. § (1) bek.
[7] Ptk. 2:42. § (1) – (2) bek.
[8] Smtv. 12. §
[9] Smtv. 10. §
[10] Pp. 495. § - 501. §

felülvizsgálati eljárás során is. A soronkívüliséget a Pp. rövid határidőkkel[11], valamint egyes eljárási cselekmények kizárásával[12] igyekszik biztosítani.

3. A sajtószerv előtti kötelező előzetes eljárás kezdeményezésére jogosultak

A sajtó-helyreigazítás iránti igény polgári peres eljárásban történő érvényesítése esetén az igényérvényesítés két szakaszból áll. Először a sajtószerv előtti kötelező eljárást kell kezdeményezni és csak ezen eljárás sikertelensége esetén kerülhet sor eredményesen a perindításra.
A sajtószerv előtti kötelező előzetes (megelőző) eljárás kezdeményezésére a Pp. 495. § (1) bekezdése alapján az érintett jogosult. Azonban az érintett fogalmát a Pp. nem határozza meg. Az Smtv. 12. § (1) bekezdése szerint, ha valakiről bármely médiatartalomban valótlan tényt állítanak, híresztelnek vagy vele kapcsolatban való tényeket hamis színben tüntetnek fel, követelheti olyan helyreigazító közlemény közzétételét, amelyből kitűnik, hogy a közlés mely tényállítása valótlan, illetve megalapozatlan, mely tényeket tüntet fel hamis színben és ehhez képest melyek a való tények. A Kúria Polgári Kollégiumának 13. számú állásfoglalása a sajtó-helyreigazítási per indításának feltételeit elemzi. E szerint az kérheti a sajtó-helyreigazítást, akire a közlemény nevének megjelölésével vagy más módon utal, vagy akinek a személye felismerhető a sajtóközleményből. Sajtó-helyreigazítási igényt az érvényesíthet, akinek a személyhez fűződő jogait megsértették. Itt a jogsértés valótlan tények állításával vagy való tények hamis színben történő feltüntetésével valósul meg. Ez a jogvédelem nemcsak a magánszemélyekre korlátozódik, hanem jogi személyekre is kiterjed. Azonban, ha a közlemény kizárólag a jogi személy valamely alkalmazottját, tagját, tisztségviselőjét sérti, nem kérhet helyreigazítást nevükben a jogi személy. A személyhez fűződő jogokat csak személyesen lehet érvényesíteni, így az alkalmazottat megillető helyreigazítási igényt a munkáltató nem érvényesítheti. Amennyiben a közlemény a jogi személy munkáltatót is sérti, akkor a munkáltató saját nevében helyreigazítást kérhet. [13] A sajtó-helyreigazítási pert kezdeményező fél érintettsége kereshetőségi jogot megalapozó anyagi jogi kérdés. Amennyiben a kifogásolt

[11] Pp. 497. § (1) „*Ha a keresetlevél perfelvételre alkalmas a bíróság legkésőbb a keresetlevél előterjesztésétől számított tizenötödik napra kitűzi a perfelvételi tárgyalást, amelyre a feleket idézi. Ha a keresetlevél csak a bíróság intézkedését követően válik tárgyalásra alkalmassá, a tárgyalás kitűzésére előírt határidő kezdő időpontját ettől az időponttól kell számítani. A tárgyalási időköz legalább három nap.*"
Pp. 498. § (1) „*A bíróság a perfelvételt lezáró végzés meghozatalát követően nyomban megtartja az érdemi tárgyalást.*"
[12] A perben nincs helye például felfüggesztésnek, keresetkiterjesztésnek, kereset- és ellenkérelem-változtatásnak, beavatkozásnak. (Pp. 500. §)
[13] PK 13. számú kollégiumi állásfoglalás

közlemény név szerint megnevezi a sérelmet szenvedett felet, egyszerűbb az érintettség megítélése. Az eljárás kezdeményezéséhez szükséges érintettségnek objektív, mások által is felismerhető körülményeken kell alapulnia, tehát nem elegendő a személyes érintettség szubjektív érzete.[14]
A Ptk. 2:54. § (1) bekezdése szerint a személyiségi jogokat személyesen lehet érvényesíteni, ez a sajtó által megsértett fél részére biztosított speciális jogvédelmi eszközre is vonatkozik. A sajtó-helyreigazítás jellegénél fogva a jogi személy is érvényesíthet ilyen jellegű igényt. A jogi személy az általános szabályok alapján a sajtó-helyreigazítás érdekében is képviselője útján járhat el. A jogi személy képviselője saját nevében akkor léphet fel, ha a közlemény őt magát is személyében érinti. Jogi személy képviselője érintettség és közvetlen jogi érdekeltség hiányában saját nevében nem terjeszthet elő eredményesen helyreigazítási kérelmet akkor sem, ha feltünteti képviselői minőségét a keresetlevélben.[15]
A sajtó-helyreigazítási igény, mint speciális személyiségvédelmi eszköz személyesen érvényesíthető. Jogutódlásnak nincs helye a személyes igényérvényesítés miatt. Ezért a jogutód által benyújtott kereset esetén azt kell vizsgálni, hogy a kifogásolt kijelentések vonatkoztathatók-e a jogutódra. Így a jogutód akkor indíthat eredményesen pert a jogelőd személyét érintő valótlan tényállítások miatt, ha ezek a tényállítások rá is vonatkoztathatók és így a személyes érintettség megállapítható. Önmagában a jogutódlás nem alapozza meg az igényérvényesítési jogosultságot.[16]
A kérelemmel szemben támasztott tartalmi követelmény, hogy abban meg kell jelölni a sérelmezett közleményt, a valótlan, illetve hamis színben feltüntetett tényállításokat és a valós tényeket, amennyiben az érintett ezek közzétételét is igényli.[17]

4. A sajtószerv

A helyreigazítás iránti kérelmet a sajtószervnél kell előterjeszteni, amelynek törvény szerint a médiaszolgáltató, a sajtótermék szerkesztősége és a hírügynökség tekintendő. A felperes kötelezettsége felderíteni az anyagi és eljárásjogi szabályok által meghatározott médiaszolgáltatót vagy

[14] Pribula László: Egyes személyiségi jogok érvényesítése iránt indított perek. In: Wopera Zsuzsa (Szerk.): Kommentár a polgári perrendtartáshoz. Kommentár a polgári perrendtartásról szóló 2016. évi CXXX. törvényhez. Wolters Kluwer Hungary Kft., Budapest, 2019. pp. 1195-1196.
Böszörményiné Kovács Katalin: Egyes személyiségi jogok érvényesítése iránt indított perek. In: Varga István (Szerk.): A polgári perrendtartás és a kapcsolódó jogszabályok kommentárja II/III. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2018. p. 1882.
[15] Pécsi Ítélőtábla Pf.III.20. 098/2014/4
[16] Fővárosi Ítélőtábla 2.Pf.20. 721/2013/3
[17] Pp. 495. § (1) bek.

szerkesztőséget. Ennek kiemelt jelentősége van, mivel ellenkező esetben a keresetlevél elutasításra kerül. Például, ha a pert megelőző helyreigazítási kérelem a sajtótermék kiadójánál, de a kereset a jogszabályi rendelkezések szerint a szerkesztőség ellen kerül előterjesztésre, akkor a keresetlevél elutasításra kerül. A tényállás szerint[18] felperes 2014. augusztus 14-én a ….hu weboldalon megjelent, általa sérelmezett tartalom miatt 2014. szeptember 2-án sajtó-helyreigazítás iránti kérelmet adott postára „….hu weboldal tulajdonosai, működtetője és Szerkesztősége illetékesek, szerkesztők részére" címzett borítékban. A posta a levelet „cím nem azonosítható" jelzéssel visszaküldte. Majd felperes 2014. szeptember 22-én keresetet terjesztett elő, amelyben alperest helyreigazító közlemény közzétételére kérte kötelezni. Az alperes nem terjesztett elő ellenkérelmet. Az elsőfokú bíróság ítéletével elutasította a keresetet, indokolásában a Pp. szabályaira hivatkozott, amelyek szerint a felperes azoknak a tényállításoknak a helyreigazítását kérheti, amelyeket a sajtószervhez a vitatott közlemény közzétételétől 30 napos jogvesztő, anyagi jogi határidőn belül megérkezett írásbeli kérelmében megjelölt. A sajtószerv részére feladott, azonban kézbesítetlenül visszaérkezett kérelemről a sajtószerv nem tudott dönteni. A felperes fellebbezést terjesztett elő, amelyben kérte az elsőfokú ítélet megváltoztatását és az elsőfokú bíróságnak az eljárás folytatására kötelezését. Ezen kérelmét azzal indokolta, hogy a weboldal impresszumában megjelölt szerkesztőség címére határidőben küldte meg a helyreigazítás iránti kérelmet, amelyet a posta „cím nem azonosítható" jelzéssel küldött vissza. Továbbá arra hivatkozott, hogy a szerkesztőség impresszumban feltüntetett hibás adatai miatt nem szenvedhet hátrányt. Az ítélőtábla az elsőfokú bíróság döntésével és indokolásával egyetértett. Az indokolást kiegészítette a fellebbezésben foglaltak értékelésével, amely szerint az Smtv. 1. §-ának 6. pontja alapján az internetes újság vagy hírportál sajtótermék, annak tartalmáért valamely természetes vagy jogi személy viseli a szerkesztői felelősséget, így a perbeli internetes sajtótermék esetében a sajtó-helyreigazítási perben a szerkesztőség perelhető, a pert megelőző igény címzettje is csak a szerkesztőség lehet. A felperesnek a keresetlevélben igazolnia kell, hogy határidőben igényelte a helyreigazító közlemény közzétételét és a kérelem a címzetthez meg is érkezett. E két feltétel bármelyikének hiánya esetén nem szerez anyagi jogosultságot az igény peres úton történő érvényesítésére. Ezért az ilyen keresetet tartalmi vizsgálat nélkül el kell utasítani. A felperes által a keresetleveléhez csatolt „cím nem azonosítható" jelzéssel visszaküldött boríték e feltételek teljesülését nem igazolja. Az ítélőtábla rámutatott arra, hogy a posta nem kísérelte meg a küldemény kézbesítését, így az alperes erről nem értesült. A kézbesíthetetlenség okát a postai szolgáltatások nyújtásának és a hivatalos

[18] BDT2015. 3372.

iratokkal kapcsolatos postai szolgáltatás részletes szabályairól, valamint a postai szolgáltatók általános szerződési feltételeiről és a postai szolgáltatásból kizárt vagy feltételesen szállítható küldeményekről szóló 335/2012. (XII. 4.) Korm. rendelet 25. § (2) bekezdése értelmében a postai szolgáltató köteles a kézbesíthetetlenség okát a küldeményen feltüntetni és a küldeményt a feladónak visszakézbesíteni. A 335/2012. (XII. 4.) Korm. rendelet 25. § (1) bekezdése tartalmazza a postai küldemény kézbesíthetetlenségének okait, e bekezdés a) pontja szerint a postai szolgáltatón kívül álló okból kézbesíthetetlen a postai küldemény a címzett részére, ha a küldemény címzése vagy címe nem megfelelő, vagy a cím nem létező, továbbá, ha a címhely azonosításra nem alkalmas, vagy az nem egyértelmű (jelzése: cím nem azonosítható). A kézbesítés elmaradásának az okát maga a felperes idézte elő. Ennek azért van kiemelt jelentősége, mert így nem kért határidőben helyreigazítást. Ezért a felperesnek határidőben ismételten meg kellett volna küldenie a kérelmet az internetes újság impresszumában a szerkesztésért felelősként feltüntetett részére ahhoz, hogy az igény perbeli úton érvényesíthető legyen. Fentiekre tekintettel az ítélőtábla az elsőfokú bíróság érdemben és indokaiban helyes ítéletét helybenhagyta.

A Pp. 496. § (2) bekezdése alapján a sajtó-helyreigazítási perben félként jár el a sajtószerv akkor is, ha egyébként nincs perbeli jogképessége. A Pp. 33. §-a alapján a perben félként járhat el az, akit a polgári jog szabályai szerint jogok illethetnek és kötelezettségek terhelhetnek. Az anyagi jogi szabályok szerint a médiaszolgáltató és a hírügynökség jogi személy, azonban a szerkesztőség nem. Így e feljogosító szabály alapján a sajtótermék szerkesztősége is félként járhat el, tehát ellene is indítható eljárás.[19]

A keresetlevél előterjesztésekor a személyi és tartalmi változtatás a helyreigazító kérelemhez képest nem megengedett. Ugyanazon sajtószervvel szemben kell előterjeszteni az előzetes eljárásban a helyreigazítás iránti kérelmet és perindítás esetén a keresetlevelet. A kereset tartalmát tekintve nem terjeszkedhet túl a helyreigazítási kérelmen. Ugyanannak a személynek kell előterjesztenie a helyreigazítás iránti kérelmet és a keresetet. Ha nem az a személy nyújtja be a keresetet, aki a helyreigazítási kérelmet előterjesztette, akkor a keresetet el kell utasítani.[20]

A jogalkalmazás állást foglalt abban, hogy az internetes blogok és közösségi oldalak által megjelentetett tartalom magánközleménynek minősül, szerkesztői felelősség hiányában a sajtótermékkel szembeni hiteles tájékoztatás követelménye a speciális helyreigazításra irányuló perben nem érvényesíthető. Az internetes blog nem minősül sajtóterméknek, annak szerzője nem visel szerkesztői felelősséget.[21]Az Alkotmánybíróság 165/2011.

[19] Pribula, (2019) p. 1200.
[20] Pribula, (2019) p. 1199.
[21] Kúria Pfv.IV.20.642/2014/6

(XII. 20.) AB határozatában kifejtette, hogy a sajtószabadság kiterjed az internetes sajtó tevékenységére is, a tömegkommunikációs formákhoz hasonlóan az internetes sajtó is szabályozás alá vonható. Azonban a magáncélú közlések (blog, közösségi portál) nem kezelhetők együtt a tömegek tájékoztatását vagy szórakoztatását célzó internetes újságokkal, hírportálokkal. Ezek nem sorolhatók be a tömegkommunikáció körébe, így ezekre nem irányadóak a sajtó szabályozásánál meghatározó szempontok. Az Alkotmánybíróság 19/2014. (V. 30.) AB határozata szerint jelentős különbség van az internetes oldal üzemeltetője által szerkesztett és ekként tartalmi egységet alkotó szolgáltatás és a közösségi oldalak, valamint tisztán véleményoldalak között. Utóbbiaknak nincs szerkesztőjük, ezért nem is lépnek fel tájékoztatási igénnyel, céljuk a közösségbe tartozók közötti eszmecsere. Tulajdonképpen az ezekben foglalt közlésekhez csak a közlő által meghatározott felhasználó jut hozzá, akinek ő megengedi, ezért ezek közel állnak az Alaptörvény VI. cikkében védett magánközlésekhez.

5. Az előzetes eljárás kezdeményezése

A vitatott közlemény közzétételétől 30 napon belül írásban terjeszthet elő az érintett helyreigazítás iránti kérelmet. Megtartottnak kell tekinteni a határidőt, ha a kérelmet a határidő utolsó napján a sajtószerv címére ajánlott küldeményként postára adják. A Pp. 495. § (1) bekezdése a kötelező előzetes eljárás kezdeményezésének határidejéről 2020. december 31-ig a következőképp rendelkezett: „*A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény szerinti helyreigazító közlemény közzétételét az érintett személy vagy szervezet az általa vitatott közlemény közzétételétől számított harminc napos jogvesztő határidőn belül írásban kérheti a médiaszolgáltatótól, a sajtótermék szerkesztőségétől vagy a hírügynökségtől (a továbbiakban együtt: sajtószerv). A kérelemben meg kell jelölni a sérelmezett közleményt, a valótlan, illetve hamis színben feltüntetett tényállításokat és - feltéve, hogy ezek közzétételét is igényli - a valós tényeket.*” A sajtószerv előtti kötelező előzetes eljárásra vonatkozó rendelkezést a polgári perrendtartásról szóló 2016. évi CXXX. törvény módosításáról szóló 2020. évi CXIX. törvény[22] (a továbbiakban: I. Pp. Novella) 2021. január 1. napjától a következőképp módosította: „*A sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény szerinti helyreigazító közlemény közzétételét az érintett személy vagy szervezet az általa vitatott közlemény közzétételétől számított harminc napon belül írásban kérheti a médiaszolgáltatótól, a sajtótermék szerkesztőségétől vagy a hírügynökségtől (a továbbiakban együtt: sajtószerv). A határidőt megtartottnak kell tekinteni,*

[22] I. Pp. Novella 68. §

ha a helyreigazítás iránti kérelmet legkésőbb e határidő utolsó napján a sajtószerv címére ajánlott küldeményként postára adták. E határidő elmulasztása esetén igazolásnak nincs helye. A kérelemben meg kell jelölni a sérelmezett közleményt, a valótlan, illetve hamis színben feltüntetett tényállításokat és - feltéve, hogy ezek közzétételét is igényli - a valós tényeket."
Az I. Pp. Novella indokolása szerint „*Nem indokolt ebben az esetben a kézbesítés tényleges megvalósulásához szükséges időtartam hosszától vagy a kézbesítés sikerességétől függővé tenni a későbbi bíróság előtti jogérvényesítés lehetőségét.*"[23]
Tehát az I. Pp. Novella által bevezetett módosítás előtt 30 napos határidőben meg kellett érkeznie a kérelemnek a sajtószervhez, míg a jelenleg hatályos rendelkezés alapján az igényérvényesítéshez elegendő e határidő utolsó napján ajánlott küldeményként postára adni. A határidő a közlemény megjelenésétől számít és nem az arról történő tudomásszerzéstől. E határidő elmulasztása nem menthető ki igazolással. Ez a határidő anyagi jogi jellegű, ezért ennek elmulasztása esetén nincs helye a keresetlevél visszautasításának a Pp. 176. § (1) bekezdés i) pontja alapján (a felperes a perindításra jogszabályban megállapított határidőt elmulasztja), ennek vizsgálatára az ítéletben kerülhet sor.
Internetes sajtótermék esetén nem lehet azonosnak tekinteni a közzétételt és a hozzáférhetőséget. Az internetes közlemény közzétételétől kell számítani a 30 napot akkor is, ha ezt követően továbbra is hozzáférhető volt az adott tartalom. Ez felel meg annak a jogalkotói célnak, hogy a lehető legrövidebb időn belül kell biztosítani a hatékony jogvédelmet.[24]

6. A kereset előterjesztése

A felperesnek a keresetlevelet a közlési kötelezettség [25] utolsó napjától számított tizenöt napon belül kell előterjesztenie. Az előzetes eljárás

[23] I. Pp. Novella Indokolása 68. §-hoz
[24] Pécsi Ítélőtábla Pf.III.20. 816/2012/4
[25] Az Smtv. 12. § (2) bekezdése alapján a helyreigazító közleményt

- napilap, internetes sajtótermék és hírügynökség esetében az erre irányuló igény kézhezvételét követő öt napon belül a közlemény sérelmezett részéhez hasonló módon és terjedelemben,
- lekérhető médiaszolgáltatás esetében az erre irányuló igény kézhezvételét követő nyolc napon belül a közlemény sérelmezett részéhez hasonló módon és terjedelemben,
- más időszaki lap esetében az igény kézhezvételétől számított nyolc napot követően a legközelebbi számban a közlemény sérelmezett részéhez hasonló módon és terjedelemben,
- lineáris médiaszolgáltatás esetében pedig ugyancsak nyolc napon belül, a közlemény sérelmezett részéhez hasonló módon és azzal azonos napszakban kell közölni.

kezdeményezésére nyitva álló határidő anyagi jogi jellegű, ezért annak elmulasztása esetén nincs helye igazolásnak. Azonban a kereset előterjesztésére rendelkezésre álló határidő eljárásjogi jellegű, amelynek elmulasztása esetén van helye igazolásnak, ha a felperes a mulasztás okát és vétlenségét megfelelően valószínűsíteni tudja.[26]
A BDT.2019. 4053. számú döntés rámutatott arra, hogy az elsőfokú ítélet hatályon kívül helyezésének és az elsőfokú bíróság új eljárásra és új határozat hozatalára utasításának van helye, ha sajtó-helyreigazítási perben a bíróság azért szünteti meg az eljárást, mert a felperes elmulasztotta a perindítást megelőzően a helyreigazításnak sajtószervnél előterjesztésére előírt 30 napos határidőt. Ebben a kérdésben a bíróságnak érdemben, tárgyalás alapján kell állást foglalnia, mert az anyagi jog érvényesítésének feltételéről kell dönteni. A sajtó-helyreigazítás iránt indított per megszüntetésének van helye, ha a perindítást nem előzte meg a sajtószerv előtti kötelező előzetes eljárás. A tényállás szerint az alperes által szerkesztett ….hu weboldalon 2018. december 2-án megjelent írás miatt felperes 2018. december 27-én kelt helyreigazítási kérelmet juttatott el postán az alpereshez, amelyet alperes 2019. január 8-án vett kézhez. A felperes 2019. január 23-án keresetlevelet terjesztett elő a helyreigazítás iránt. Alperes ellenkérelmében az eljárás megszüntetését kérte elsődlegesen, másodlagosan pedig a kereset elutasítását. Az elsőfokú bíróság végzéssel megszüntette az eljárást. Az elsőfokú bíróság elfogadta az alperes azon érvelését, amely szerint a helyreigazítási kérelem előterjesztésére előírt határidő anyagi jogi határidő, ezért a kérelemnek 30 napon belül meg kell érkeznie a sajtószervhez.[27] Ebben az esetben a kérelem határidőn túl érkezett, így nem előzte meg a sajtószerv előtti kötelező előzetes eljárás. A felperes fellebbezést terjesztett elő, amelyben kérte a sérelmezett végzés hatályon kívül helyezését és az elsőfokú bíróság új eljárásra és új határozat hozatalára utasítását. Álláspontja szerint a hivatkozott visszautasítási ok nem áll fenn, a sajtószerv előtti eljárás kezdeményezésére szabott határidő eljárásjogi határidő. Az alperes az ellenkérelmében az elsőfokú végzés helybenhagyását kérte. A Pp. 495. § (1) bekezdése szerint helyreigazító közlemény közzétételét 30 napon belül kell kérni a sajtószervtől. A Pp. 496. § (1) bekezdése alapján sajtó-helyreigazítás iránt pert indítani akkor lehet, ha a sajtószerv a törvényi határidőben nem vagy nem a kérelemnek megfelelően tesz eleget helyreigazítási kötelezettségének. A peres eljárást megelőző igényérvényesítés anyagi jogi előfeltétel, így a kötelezett önként eleget tud tenni a helyreigazításnak. Az előzetes eljárás kezdeményezésére vonatkozó 30 napos határidő anyagi jogi jellegű, elmulasztása jogvesztő. Az ítélőtábla

[26] Pp. 496. § (3) bek., Pribula, (2019) p. 1200.
[27] 2021. január 1. napjától a Pp. 495. § (1) bekezdése kiegészült azzal, hogy a határidőt megtartottnak kell tekinteni, ha a helyreigazítás iránti kérelmet legkésőbb e határidő utolsó napján a sajtószerv címére ajánlott küldeményként postára adták.

megállapítása szerint a keresetlevél visszautasítására abban az esetben kerülhet sor, ha a felperes egyáltalán nem terjesztett elő helyreigazítási kérelmet sajtószervhez. Ez következik a Pp. 496. § (1) bekezdésének azon rendelkezéséből, amely szerint tájékoztatni kell a felperest a visszautasító végzésben az előzetes eljárás lefolytatásának szükségességéről. Ezzel a Pp. azt a korábbi bírói gyakorlatot emelte jogszabályi szintre, hogy az előzetes eljárás hiányosságainak értékelésére a perbíróság ítélete ad választ. Ha a felperes határidőn túl terjeszt elő helyreigazítási kérelmet, a bíróságnak ítélettel kell elutasítania a keresetet. A helyreigazítás iránti kérelem előterjesztésére nyitva álló határidő elmulasztása miatt nem lehetett a keresetlevelet visszautasítani. Az ítélőtábla az elsőfokú bíróság végzését hatályon kívül helyezte és új eljárásra és új határozat hozatalára utasította. Az elsőfokú bíróságnak érdemi döntést kell hoznia, az előzetes eljárás szabályszerűsége és a kérelem előterjesztésének körülményeire vonatkozóan kell érdemben állást foglalnia.[28]

7. A jogsértés elbírálása és az ítélet

A jogsértés elbírálásánál a sajtóközleményt a maga egészében kell vizsgálni, az egymással összetartozó részeket összefüggésükben kell értékelni és tekintettel kell lenni a társadalmilag kialakult közfelfogásra.[29] A jogsértő közlés történhet közvetetten, célzásokkal, utalásokkal, egyes tényálláselemek elhagyásával, ha alkalmas valótlan tényállítás kifejezésére vagy valós tények hamis színben történő feltüntetésére. Nem lehet helyreigazítás alapja önmagában véleménynyilvánítás, értékelés, bírálat, valamint társadalmi, politikai, tudományos és művészeti vita, mivel a sajtó-helyreigazítás a tényállításokra korlátozódik.[30]
A sajtóközlemény kifogásolt tényállításainak valóságát a sajtószerv köteles bizonyítani.[31] A sajtó-helyreigazítási perben a bizonyítás korlátozott keretek között folytatható le. Csak olyan bizonyítékokra van helye bizonyításfelvételnek, amelyek a tárgyaláson rendelkezésre állnak, vagy amelyeket a felek legkésőbb a perfelvételt lezáró végzés meghozataláig felajánlottak.[32] Ez a korlátozás is azt célozza, hogy az eljárás mihamarabb lefolytatható legyen és az érintett jogvédelemben részesüljön.
A sajtóperben hozott ítélet tartalmát tekintve helyt adó vagy elutasító lehet. Abban az esetben, ha a bíróság a keresetnek helyt ad, megállapítja a helyreigazítás szövegét és az alperest ennek közzétételére kötelezi. A Pp. nem

[28] BDT2019. 4053.
[29] BDT2020. 4224.
[30] PK 12. számú kollégiumi állásfoglalás
[31] PK 14. számú kollégiumi állásfoglalás
[32] Pp. 498. § (1) bek.

határozza meg részletesen a helyreigazító közlemény alakját és tartalmát.[33] Arra vonatkozóan nincs törvényi szabályozás, hogy internetes sajtótermékben mennyi ideig kötelező a közzététel, ennek az internetes közlés sajátosságaihoz kell igazodnia.[34] A helyreigazító közlemény akkor tölti be rendeltetését, ha szükséges mértékben tartalmazza a valóságot sértő és való tényeket.
A tényállás szerint felperes korábban polgármester volt, az alperes a városban hírportálként működő internetes újság kiadója. A hírportálon megjelent cikk miatt felperes helyreigazítási kérelemmel fordult az alperes címén megtalálható szerkesztőséghez a közlemény közzétételének napján. Ezt követően a cikkben kisebb javításokat eszközöltek, de a helyreigazítási kérelemnek nem tett eleget a szerkesztőség. A felperes keresetében az alperes helyreigazító közlemény közzétételére kötelezését kérte, mivel a cikk több állítása valótlan, valamint hamis színben tünteti fel a valóságot. Az alperes ellenkérelmében elsődlegesen az eljárás megszüntetését kérte, mivel a felperes nem a helyreigazítási kérelmet nem megfelelően teljesítő sajtószerv ellen indította meg a pert. Alperes másodlagosan a kereset elutasítását kérte, arra hivatkozva, hogy a cikk sérelmezett része véleménynyilvánítást tartalmaz. Az elsőfokú bíróság ítéletével helyreigazító közlemény közzétételére kötelezte alperest, valamint alperes eljárás megszüntetése iránti kérelmét végzéssel elutasította. A bíróság döntése szerint az alperes médiaszolgáltatónak minősül, így passzív perbeli legitimációval rendelkezik. Az alperes fellebbezett az ítélettel szemben, az elsőfokú ítélet megváltoztatásával kérte elsődlegesen az eljárás megszüntetését, másodlagosan a kereset egészének elutasítását. Fenntartotta, hogy alperes nem sajtószerv, ezért az eljárást meg kellett volna szüntetni. A Pp. 495. § (1) bekezdése és 496. § (1) bekezdése értelmében a pert azzal szemben lehet megindítani, aki a kérelmet nem vagy nem megfelelően teljesítette, azaz akihez a kérelmet intézték. Jelen eljárásban a helyreigazítási kérelem címzettje a főszerkesztő volt. A pert a szerkesztőség ellen kellett volna megindítani. Az alperes helytállóan hivatkozott arra, hogy felperes nem a jogszabályban megjelölt személy ellen indította meg a pert, azonban ennek nem az eljárás automatikus megszüntetése a jogkövetkezménye. Ha a keresetlevél csak meghatározott személlyel szemben terjeszthető elő és a felperes nem ezt a személyt nevezi meg alperesnek, akkor a bíróságnak hiánypótlási felhívást kell tenni a megfelelő alperes perbe vonása érdekében és csak ennek sikertelensége esetén utasítja vissza a keresetlevelet, illetve, amennyiben a kereset közlésére sor került megszünteti az eljárást. Jelen esetben az elsőfokú bíróság nem hívta fel felperest e hiány pótlására, hogy a sajtó szerkesztőségét vonja perbe alperesként, ezzel az elsőfokú eljárás szabályait az ügy érdemére kiható módon megsértette. Ez a szabálysértés a

[33] Pp. 499. § (1) bek., PK 15. számú kollégiumi állásfoglalás
[34] Fővárosi Ítélőtábla 2.Pf.21.780/2012/4.

másodfokú eljárásban nem orvosolható. Az ítélőtábla hatályon kívül helyezte az elsőfokú bíróság ítéletét és utasította, hogy az eljárást a perfelvételi szaktól folytassa le, előírta az elsőfokú bíróság számára, hogy hívja fel a felperes figyelmét a keresetlevél hiányosságaira akként, hogy alperesként a sajtó szerkesztőségét vonja perbe.[35]

8. Összegzés

A sajtó-helyreigazítási per a különleges perként szabályozott személyiségi jogi perek közé tartozik. Az eljárás során az általánostól eltérő speciális szabályok érvényesülnek, hogy be tudja tölteni rendeltetését, a gyors jogvédelmet. A sajtó-helyreigazítási igény érvényesítésének két szakasza van, az első a sajtószerv előtti kötelező előzetes eljárás és csak ennek sikertelensége esetén kerülhet sor eredményesen a sajtó-helyreigazítási per megindítására. Az előzetes eljárás hiánya a keresetlevél visszautasítását vonja maga után. Az érintettnek körültekintően kell eljárni, hogy az előzetes eljárást és a pert ugyanazon sajtószerv ellen indítsa meg. Míg a Pp. azt rögzíti, hogy a helyreigazítás kérhető a médiaszolgáltatótól, a sajtótermék szerkesztőségétől vagy a hírügynökségtől, adott esetben kiemelten fontos annak megválasztása, akihez az érintett helyreigazítás iránti kérelemmel fordul. Az igényérvényesítés perbeli szakaszában a kereset elutasítását vonja maga után, ha nem ugyanattól igényli a helyreigazítást a perindításkor és az előzetes eljárásban. Az igény természetéből adódóan csak személyesen érvényesíthető, ezért a jogutódlás kizárt. E jogvédelmi eszköz nem korlátozódik a természetes személyekre, hanem a jogi személyt is megilleti. Az előzetes eljárás kezdeményezésekor a kérelem tartalmát úgy kell meghatároznia az érintettnek, hogy azt a peres eljárás kezdeményezésekor a keresetlevélben nem bővítheti, tehát a túlterjeszkedés tilalma érvényesül. Amennyiben a bíróság marasztaló ítéletet hoz, alperest helyreigazító közlemény közzétételére kötelezi.

[35] BDT2021. 4380.

Irodalomjegyzék

- Böszörményiné Kovács Katalin: Egyes személyiségi jogok érvényesítése iránt indított perek. In: Varga István (Szerk.): A polgári perrendtartás és a kapcsolódó jogszabályok kommentárja II/III. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2018. pp. 1880-1907.
- Jobbágyi Gábor: Személyi és családi jog. Szent István Társulat, Budapest, 2000.
- Pribula László: Egyes személyiségi jogok érvényesítése iránt indított perek. In: Wopera Zsuzsa (Szerk.): Kommentár a polgári perrendtartáshoz. Kommentár a polgári perrendtartásról szóló 2016. évi CXXX. törvényhez. Wolters Kluwer Hungary Kft., Budapest, 2019. pp.1193-1215.

Ripszám Dóra
PhD-hallgató (PTE-ÁJK)

A közösségi média szerepe a gyermekkereskedelemben

Absztrakt

Számos elkövető használja ki a közösségi médiát annak érdekében, hogy elrejtse, eltitkolja személyazonosságát, és így bűncselekményeket kövessen el. Ilyen bűncselekmény lehet többek között az internetes zaklatás, a kiberterrorizmus, az emberkereskedelem, és a kábítószer-kereskedelem.[1]
A National Human Trafficking Hotline toborzást regisztrált mind a szexuális, mind a munkaerőkizsákmányolás céljából elkövetett emberkereskedelem valamennyi típusában a közösségi média általános platformjain, többek között, de nem kizárólagosan a Facebookon, az Instagramon, a WhatsApp-on, a Snapchaten, a Kik-en, a Meetme.com-on és a társkereső oldalakon/alkalmazásokon (például Tinder).[2]
A közösségi média térnyerésével a gyermekkereskedelem toborzásának módjai is jelentős változáson, fejlődésen mentek keresztül. Az áldozattá válás ezen formája elsősorban a 6-18 év közötti gyermekeket érinti.

Kulcsszavak: gyermekkereskedelem, közösségi média, toborzás, applikáció

1. Bevezetés

Az Internet alapvetően a kommunikáció szükséglete hívta életre a hidegháború éveiben és a kommunikáció lehetősége azóta is meghatározó funkciója. Az ezredfordulót követően a technikai, illetve technológiai fejlődéssel, a felhasználók tartalomfogyasztóból tartalomkészítőkké váltak, egyúttal megjelentk különböző közösségi oldalak, a web2 nyilvánossága a hivatalostól eltérő, számos esetben azzal szembemenő véleménynyilvánítás és privát kommunikáció lehetősége bővült. Számtalan kommunikációs platform

[1] Wingyan Chung - Elizabeth Mustaine - Daniel Zeng: Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking (Bűnügyi hírszerzés megfigyelése és nyomon követése a közösségi médiában: Kiberkereskedelem esetei). In: IEEE: IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, Peking, 2017. pp. 191-193.
[2] Polaris: On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking (Felhajtók, kereszteződések és kivezető utak: Útiterv a rendszerek és az iparágak számára az emberkereskedelem megelőzésére és megakadályozására). Social Media, na., 2018. p. 43.

(chatszobák, Skype, Viber, Signal, WhatsApp, WeChat stb.) és technika létezik.[3]

Számos elkövető használta ki a közösségi médiát annak érdekében, hogy elrejtse, eltitkolja személyazonosságát[4], és így bűncselekményeket kövessen el, mint például internetes zaklatás, kiberterrorizmus, [5] kábítószer-kereskedelem, vagy akár az emberkereskedelem.[6]

A közösségi média alig egy évtizedes múltja jelentős mértékben átformálta a társadalmakat, és a társadalmi jelenségeken belül hatással van a bűnözésre is[7]. A közösségi média Andreas Kaplan - Michael Haenlein definíciója alapján nem más, mint az „internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom."[8] Bányász Péter szerint ha a legegyszerűbb megközelítést választjuk, a közösségi média olyan oldalak és alkalmazások összessége, amelyben a tartalmat a felhasználók állítják elő (legyen szó videóról, bejegyzésről stb.), a szolgáltató csupán a keretet biztosítja.[9]

A Z generáció tagjait gyakran nevezik C generációnak, ami az angol connection szó után kapta a nevét, illetve D-nek, ami a digitális szóra utal, de R-nek is, ami az angol responsibiliy vagyis felelősség kifejezésből származik [10], azonban a C-generáció (szemben az "X" vagy "Y" vagy „Z"generációkkal) nem szigorúan demográfiai, születési évek alapján képzett csoport, hanem egyéletmód csoport. Számukra a közösségi média,

---

[3] Nagy Zoltán András: A gyermekekre leselkedő veszélyek az Interneten. In: Nagy, Melánia (szerk.): Gyermekekre fókuszálva. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 202. pp. 5-10.

[4] Lásd még a személyazonosság-lopásról: Tóth Dávid: Személyiséglopás az interneten. In: Büntetőjogi Szemle 9. évf. 2020/1. pp. 113-119.

[5] Tóth Dávid: A terrorizmus típusai és a kiberterrorizmus In: Rab Virág (szerk.) XII. Országos Grastyán Konferencia előadásai.PTE Grastyán Endre Szakkollégium, Pécs. 2014. pp. 286-296.

[6] Wingyan Chung - Elizabeth Mustaine - Daniel Zeng: Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking (Bűnügyi hírszerzés megfigyelése és nyomon követése a közösségi médiában: Kiberkereskedelem esetei). In: IEEE: IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, Peking, 2017. pp. 191-193.

[7] Tóth Dávid: A közösségi média és a bűnözés összefüggései. In: Bujtár, Zsolt et. al. (Szerk.) Fintech – DEFI - Kriptoeszközök Gazdasági és jogi lehetőségei és kockázatai: konferenciakötet – válogatott tanulmányok. PTE-ÁJK, Pécs pp. 133-141.

[8] Andreas Kaplan - Michael Haenlein: Users of the world, unite! The challenges and opportunities of Social Media (A világ felhasználói, egyesüljetek! A közösségi média kihívásai és lehetőségei). Business Horizons, Párizs, pp 59-68. Idézi: Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. In: Nemzetbiztonsági Szemle 2015/2. p. 22.

[9] Bányász (2015) p. 22.

[10] Pais Ella Regina: Alapvetések a Z generáció tudomány-kommunikációjához – tanulmány. Pécsi Tudományegyetem, Pécs, 2013. p. 11.

és elsősorban az okostelefonok használata [11] már-már a Maslow-féle szükséglet hierarchia legalsó szintjén, a fiziológiai szükségletek szintén jelentkezik. A C-generációra jellemző, hogy napjaik nagy részét online töltik, a tartalomfogyasztást, a kapcsolattartást elsődlegesen ezeken az eszközökön végzik, illetve elvárják, hogy az élet minden területén érvényesüljenek a közösségi alapelvek, mint a transzparencia, a hozzáférés, a megoszthatóság, a bevonás, a kommentelhetőség.[12]

2. Érintkezési pontok a közösségi média és az emberkereskedelem kapcsán

Egy nemzetközi tanulmány feltárta azokat az érintkezési pontokat a közösségi médiával, amelyek az emberkereskedelem életciklusa során felmerülnek, ideértve a toborzást is, a reklámozás megkönnyítését, a visszaéléseket vagy az általános üzleti műveleteket, továbbá a túlélők támogatását az emberkereskedelemmel kapcsolatos tapasztalataik kapcsán, mely alapján megállapítható, hogy a közösségi médiában a legnagyobb szerepet a Facebook, az Instagram, valamint a chat applikációk játszák.[13]
Az emberkereskedelem áldozatainak 2015-re számos esetben volt internet-hozzáférése, és sokan aktívan részt is vettek a közösségi médiában, ami először tette lehetővé közvetlen tranzakció lehetőségét közvetítő nélkül.[14]
Az emberkereskedelem áldozatait nem ritkán hirdetik internetes felületen, mind munkavégzés, mind szexuális kizsákmányolás, mind pedig az emberi test tiltott felhasználása céljából.
A Polaris adatai szerint a 2015. január és 2017. december közötti időszakban mintegy 845 internetes platformon toborzott potenciális áldozatot azonosítottak, mely a következők szerint alakult:

- 250 lehetséges áldozat toborzása Facebookon
- 120 toborzási eset egy társkereső oldalon
- 78 főt toboroztak az Instagramon

11 Az okostelefonok használata általánosságban is számos kriminalitási veszélyt hordoz. Lásd bővebben: Kraut Andrea – Kőhalmi László – Tóth Dávid: Digital Dangers of Smartphones. In: Journal of Eastern-European Criminal law. 2020/1. pp. 36-49.
12 Bányász (2015) p. 23.
13 Polaris: On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking (Felhajtók, kereszteződések és kivezető utak: Útiterv a rendszerek és az iparágak számára az emberkereskedelem megelőzésére és megakadályozására). Social Media, na., 2018. p. 43.
14 Campbell Fraser: An analysis of the emerging role of social media in human trafficking. Examples from labour and human organ trading (A közösségi média emberkereskedelemben betöltött szerepének elemzése. Példák a munkaerő- és emberi szervkereskedelemből). In: na.: International Journal of Development Issues, Emerald Group Publishing, Bingley, 2016. pp. 98 – 112.

– 489-et más típusú internetes platformon, például Craigslisten, chatszobákon vagy olyan webhelyen, amelyet nem lehetett azonosítani.[15]

A National Human Trafficking Hotline toborzást regisztrált mind a szexuális, mind a munkaerőkizsákmányolás céljából elkövetett emberkereskedelem valamennyi típusában a közösségi média általános platformjain, elsősorban a Facebookon, az Instagramon, a Snapchaten, a Kik-en, a Meetme.com-on, a WhatsApp-on és a társkereső oldalakon/alkalmazásokon, mint például a Tinder.[16]

3. A közösségi média formáló ereje a gyermekkereskedelemben

Az internetnek köszönhetően a bűnözés új ága jelent meg, mely sokkal védtelenebbé teszi az embereket, gazdálkodó szervezeteket; gyermekek, személyes adatok, üzleti, szolgálati és államtitkok kerülnek veszélybe.[17]
A gyermekkereskedelem toborzásának módjai a közösségi média térnyerésével párhuzamosan jelentős fejlődésen mentek keresztül.
A gyermekek internet - és elsősorban közösségi média - használatát az online tudatosság igen csekély mértékben jellemzi. A gyermekkereskedők számára könnyen megismerhetővé válik a gyermek napi rutinja, tartózkodási helye, szokásai, kedvelt dolgai.
A közösségi médiában a gyermekkereskedelem vonatkozásában kiemelkedő szerepe van többek között a Facebooknak, az Instagramnak, Snapchat-nek, valamint a TikTok-nak. A gyermekek figyelemre, népszerűségre vágynak, így a követési kéréseket arra tekintetet nélkül hagyják jóvá, hogy az adott személyt valóban ismernék, a közösségi médiában használt fiókjukat nyíltra állítják. A Snapchat Snap Map alkalmazásával - az alkalmazás beállításainak függvényében - a gyermek bármely követője számára hozzáférhetővé válik a gyermek aktuális tartózkodási helye, mely ismételten megkönnyítheti az elkövető dolgát.
Említést kell tenni továbbá arról a jelenségről is miszerint nem a gyermek a közösségi média aktív résztvevője, hanem példának okáért a szülő, illetve a nagyobb testvér és annak felelőtlen, könnyelmű magtartása biztosítja az elkövetők számára a gyermekkel kapcsolatos értékes információkat.
Az online toborzás mindaddig létező jelenség, amíg széles körben elterjedt az internetes platformokhoz való hozzáférés.[18] Annak ellenére, hogy a fiatalok a társadalom talán legtapasztaltabb felhasználói a közösségi médiában, mégis ők

[15] Polaris, (2018) p. 43.
[16] Polaris, (2018) p. 43.
[17] Szegediné Lengyel Piroska: Számítógépes bűnözés avagy fiatalok a cyber-térben. Hadmárnök 2010/2. pp. 366-379.
[18] Polaris, (2018) p. 43.

a legsebezhetőbbek az online kizsákmányolók és emberkereskedők által alkalmazott taktikákkal szemben.[19]
Fentiekre tekintettel fontosnak tartom az online tudatosság növelését Magyarországon mind a gyermekek, mind a hozzátartozóik körében, hiszen a Nemzetközi Migrációs Szervezet (IOM) az Országos Rendőr-főkapitánysággal partnerségben a Belső Biztonsági Alap és a Belügyminisztérium finanszírozásában megvalósuló a BBA-5.4.4.-16-2016-0001 azonosítószámú - Tudj róla! - Kampány az emberkereskedelem visszaszorítása keretében végzett kutatás eredményeként megállapította, hogy a nagymintás kutatás online tudatosságot érintő kérdéseire adott válaszok vegyes visszajelzéseket mutatnak.[20]

4. A közösségi média pozitív jelenléte a gyermekkereskedelemben

A közösségi média a gyermekkereskedelem kapcsán nem kizárólag az emberkereskedők számára nyújthat segítséget.
A „BBA-5.4.4 Tudj róla! Kampány az emberkereskedelem visszaszorítása érdekében" projekt 2017. április 1-jén indult és 2018. december 31-én ért véget, és a projekt felismerve a közösségi média lehetőségét többféle kommunikációs eszközt használva, online, közösségi média- és offline platformokon egyaránt felhívta a lakosság figyelmét az emberkereskedelem elleni küzdelemre. A kampány a weboldalán, a Facebook oldalán, az Instagram oldalán, plakátokon, nyomtatott és elektronikus tájékoztató anyagokon, a szexuális, illetve a munkacélú kizsákmányolás veszélyeire figyelmeztető kisfilmeken keresztül, valamint vidéki nagyvárosokban helyszíni lakossági tájékoztatókon kaphattak információt az érdeklődők.[21]
Fontos kitérni arra is, hogy léteznek olyan applikációk, melyek a megelőzést, a hatékony segítségnyújtást szolgálják, ilyen például a HelpAPP, a YounGo és a Kapcsolj Egyből.
A Kapcsolj Egyből applikáció a kapcsolati erőszak és az emberkereskedelem áldozatainak hatékonyabb segítését szolgálja, további célja a súlyos krízishelyzetek kialakulásának megakadályozása, segítség nyújtás a gyermekbántalmazás, a prostitúció- és emberkereskedelem áldozatainak azáltal, hogy szükség esetén gondoskodik az azonnali összeköttetésről a

[19] Online Safety (n. a.): Social Media and Exploitation (Közösségi média és kizsákmányolás), https://ocfs.ny.gov/programs/youth/online-safety/exploitation.php (letöltve: 2022. január 7.)
[20] Nemzetközi Migrációs Szervezet: Az emberkereskedelemmel kapcsolatos online tudatosságról szóló jelentés BBA-5.4.4.-16-2016-0001 Tudj róla! - Kampány az emberkereskedelem visszaszorítása érdekébe. Nemzetközi Migrációs Szervezet, Budapest, 2018. p. 37.
[21] Belügyminisztérium: Kampány az emberkereskedelem visszaszorítása érdekében. https://emberkereskedelem.kormany.hu/kampany-az-emberkereskedelem-visszaszoritasa-erdekeben (letöltve: 2022. május 15.)

megfelelő szakemberekkel. A gyorshívó gombok segítségével, az akut krízisbe került személy azonnal kapcsolatba tud lépni segítő szakemberrel, akár az egységes lelki segélyhívószámon, a 116-123 számon, akár a bántalmazottak segélyhívószámán, a 0680-20-55-20 számon keresztül.[22]
Ha a gyermeket bántják, vagy veszélyben van az UNICEF Magyarország HelpAPP nevű alkalmazásának használatával egyetlen gombnyomással segítséget hívhat, vagy elküldheti GPS koordinátáit, ezen túlmenően pedig a fiatal választ kaphat a bántalmazással kapcsolatos kérdéseire is. Az UNICEF Magyarország azért fejlesztette ki a HelpAPP-ot, mert a 21. század gyermekei a digitális világ gyermekei, és a legnagyobb természetességgel használják a mobiltelefonokat, számítógépeket, internetet, így ha segíteni akarunk nekik, azt a nyelvet kell megtanulnunk, amit ők beszélnek és azokat az eszközöket kell használnunk, amelyeket ők használnak.[23]
A YounGo App egy olyan alkalmazás, mely elsősorban a gyermekvédelemben élő gyermekek és fiatalok számára készült; mindenekelőtt az iskolai élettel összefüggő kérdésekben, a pénzkezelésben, a pályaválasztásban, vagy akár a gyermekvállalás/szexualitás kérdéskörében fogalmaz meg kérdéseket és válaszokat, mellyel végső soron az alkalmazás segíti a kiskorúak kiszolgáltatottá válásának megelőzését, így többek között az emberkereskedelemnek, illetve általában a kizsákmányolásnak való kitettségüket is mérsékli, hiszen az élet számos területét átfogó támogató információival sikeresebb tájékozódáshoz és magabiztosabb helyzetkezeléshez segíti hozzá a fiatalokat, ezzel egyúttal általános védettségüket is növelve.[24]

5. Összegzés

Az emberkereskedők módszerei változnak, sőt számos esetben már a végbement változás is nyomon követhető, melyet az internet és a közösségi média eszközei és széleskörű használata biztosít számukra. Az online tér a szervezett láncolat működtetésében és a megszerzett haszon befektetésében, hatóságok elől történő „elrejtésében" is megfelelő helyszínnek minősül, melyet rendkívül ügyesen és tapasztalt módon használnak ki. Fenteikre

[22] Kapcsolj Egyből!: Mobilalkalmazás. https://www.kapcsoljegybol.hu/mobilalkalmazas (letöltve: 2022. május 15.)
[23] UNICEF: Az UNICEF Magyarország HelpAPP nevű telefonos alkalmazása a kezedbe adja a segítséget, ha bántanak vagy támogatásra van szükséged. https://unicef.hu/ezt-tesszuk-itthon/segitunk/helpapp (letöltve: 2022. január 8.)
[24] Belügyminisztérium: YounGo App mobiltelefonos alkalmazás a gyermekvédelemben élő gyermekek és fiatalok számára - YounGo – egy mindig ráérő segítő a zsebedben. https://emberkereskedelem.kormany.hu/youngo-app-mobiltelefonos-alkalmazas-a-gyermekvedelemben-elo-gyermekek-es-fiatalok-szamara-youngo-egy-mindig-raero-segito-a-zsebedben (letöltve: 2022. január 8.)

tekinttel a bűnüldöző szerveket is külön fel kell készíteni ezen eszközök és online tér kiváló ismeretére, információk egyszerű és hatékony módon történő megszerzésére.[25]

A közösségi média térnyerésével a gyermekkereskedelem toborzásának módjai is jelentős változáson, fejlődésen mentek keresztül. Az áldozattá válás ezen formája elsősorban a 6-18 év közötti gyermekeket érinti.

A közösségi médiában a gyermekkereskedelem vonatkozásában kiemelkedő szerepe van többek között a Facebooknak, az Instagramnak, Snapchat-nek, valamint a TikTok-nak, hiszen a gyermekek figyelemre, népszerűségre vágynak, így a követési kéréseket arra tekintetet nélkül hagyják jóvá, hogy az adott személyt valóban ismernék, a közösségi médiában használt fiókjukat nyíltra állítják.

A közösségi média használatát illetően véleményem szerint szükséges az online tudatosság növelése mind a gyermekek, mind hozzátartozóik körében.

[25] Pocsai Tamás: Emberkereskedelem a bírói gyakorlatban. In: Miskolci Jogi Szemle 2021/4. pp. 96-97.

Irodalomjegyzék

- Andreas Kaplan - Michael Haenlein: Users of the world, unite! The challenges and opportunities of Social Media (A világ felhasználói, egyesüljetek! A közösségi média kihívásai és lehetőségei). Business Horizons, Párizs, pp 59-68. Idézi: Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. In: Nemzetbiztonsági Szemle 2015/2. p. 22.
- Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. In: Nemzetbiztonsági Szemle 2015/2. p. 22.
- Campbell Fraser: An analysis of the emerging role of social media in human trafficking. Examples from labour and human organ trading (A közösségi média emberkereskedelemben betöltött szerepének elemzése. Példák a munkaerő- és emberi szervkereskedelemből). In: na.: International Journal of Development Issues, Emerald Group Publishing, Bingley, 2016. pp. 98 – 112.
- Kraut Andrea – Kőhalmi László – Tóth Dávid: Digital Dangers of Smartphones. In: Journal of Eastern-European Criminal law. 2020/1. pp. 36-49.
- Nagy Zoltán András: A gyermekekre leselkedő veszélyek az Interneten. In: Nagy, Melánia (szerk.): Gyermekekre fókuszálva. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 202. pp. 5-10.
- Pais Ella Regina: Alapvetések a Z generáció tudomány-kommunikációjához – tanulmány. Pécsi Tudományegyetem, Pécs, 2013. p. 11.
- Pocsai Tamás: Emberkereskedelem a bírói gyakorlatban. In: Miskolci Jogi Szemle 2021/4. pp. 96-97.
- Szegediné Lengyel Piroska: Számítógépes bűnözés avagy fiatalok a cyber-térben. Hadmárnök 2010/2. pp. 366-379.
- Tóth Dávid: A közösségi média és a bűnözés összefüggései. In: Bujtár, Zsolt et. al. (Szerk.) Fintech – DEFI - Kriptoeszközök Gazdasági és jogi lehetőségei és kockázatai: konferenciakötet – válogatott tanulmányok. PTE-ÁJK, Pécs pp. 133-141.
- Tóth Dávid: A terrorizmus típusai és a kiberterrorizmus In: Rab Virág (szerk.) XII. Országos Grastyán Konferencia előadásai.PTE Grastyán Endre Szakkollégium, Pécs. 2014. pp. 286-296.
- Tóth Dávid: Személyiséglopás az interneten. In: Büntetőjogi Szemle 9. évf. 2020/1. pp. 113-119.
- Wingyan Chung - Elizabeth Mustaine - Daniel Zeng: Criminal intelligence surveillance and monitoring on social media: Cases of

cyber-trafficking (Bűnügyi hírszerzés megfigyelése és nyomon követése a közösségi médiában: Kiberkereskedelem esetei). In: IEEE: IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, Peking, 2017. pp. 191-193.

Idegen nyelvű tanulmányok

Barbara Szabó
PhD Student (University of Pécs, Faculty of Law)

Crimes committed on online surfaces

Abstract

In the 21st century, the fight against crime on the internet is increasing due to the development of information technology. The anonymity of the perpetrators and the revolutionary, yet newer, means and methods of committing crime make it easy to fall victim to Internet crime.

Keywords: cybercrime, crimes on the internet, cyberbullying.

1. Introduction

The number of unexplored online crimes is increasing every day, year after year. If we are physically the victim of a crime, we have the opportunity to identify the perpetrator. The essential aspect of identification lies in the fact that objective reality becomes the subject of investigation.[1] Minden must take place by the method of logic, which, more broadly, deals with forms of thought as permanently unchanged, solid and not only isolated, independent, self-existing formations.[2]
From this, we can argue that formal logic, with its rigid concepts, is by its very nature incapable of revealing the multifaceted, complicated connections of reality. However, I do not fully agree with this definition, since reality can be revealed and reached findings that – in the Code of Hungarian Criminal Law, the main conceptual elements of the general part are examined extensively, for example, guilt, danger to society – when analysing concepts, in the case of appropriate evaluation, with the questions asked, reality can be formed, the facts can be accepted and sanctioned accordingly.
However, the precise design and definition of reality, especially concerning virtual reality, sometimes carries many obstacles in itself, which are manifested in the scope of the criminalisation of the act, the complications arising from the detection of the offender, and the difficulties of proving it.

[1] Lenin's Works Volume 32 Budapest, 1953, p. 86.
[2] Fogarasi: Logic, Budapest, 16.16.1955.

2. “Reality” as the greatest power

Sina Aral claims that the greatest power in the world is to dictate reality.[3] I must agree with the professor's statement, and I think it is important to point out that the objective determination of reality can no longer be analyzed only in a physical sense.
In the 21st century, objective reality should be much more of an account of the formation of two main groups, which, on the one hand, are physical, that is offline reality, on the other hand, and online reality, which is made up of our various information and digital tools.
Among the many reasons for this, I would like to point out that by the fact that Nick Routley, one of the authors of visual capitalist, in the article Visualizing the social media Universe in 2018, shows that more than half of the world's population, which in 2018 was approximately 7.592 billion people, can be found on social platforms.[4]

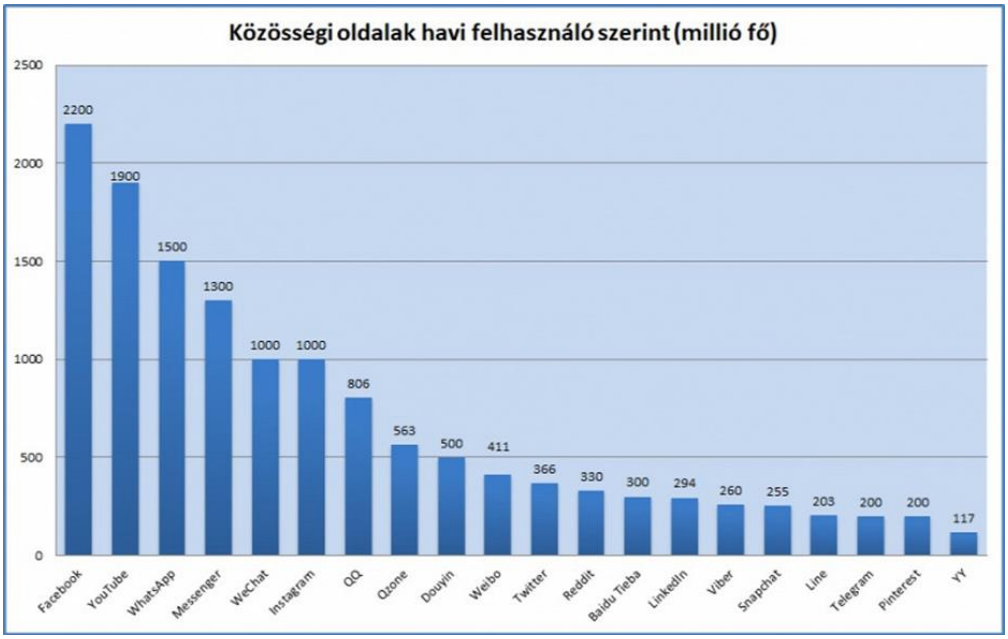


figure No. 1. by monthly user of social media sources: origo, visual kapitalist

A quarter of this is mainly interested in or using social content as a "user", in this respect it can be stated with certainty that masses of people can be reached in the online environment, whereas in the past written media, such as

[3] https://index.hu/gazdaság/2018/06/26/sinan_aral_interju/ (Download time: 11.04.2022.)
[4] https://www.visualcapitalist.com/social-media-universe/ (Download time: 11.04.2022.)

newspapers or radio for communications, was considered the media that had an extraordinary impact on society and individuals with posts now posted on the Internet, videos, messages and comments can influence the thinking and behaviour of individuals who use the Internet in society, both offline and online.
In the longer term, internet sites can be seen as a major influencer. The problem arises from the fact that when the online space and the real world and life become completely blurred and inseparable in a psychological sense.

3. Crimes committed on the Internet

The fact that the rise of the Internet means that we can fall victim to crimes committed on the Internet from anywhere in the world, in an even greater case, affects the fact that it becomes more difficult to detect crimes, which also increases the number of unexplored crimes.
The number of crimes committed on the Internet has increased radically today. In countless cases, the perpetrators gain access to our technical and electronic devices used in everyday life undetected. The average user can show activity through multiple media platforms, which can be filtered out very easily by generating the constant availability of these devices.
The main problem with constant availability is that an individual is in a compulsion situation that if they do not participate or put these platforms such as Facebook, Instagram, Twitter, Tik-Tok, and WhatsApp in the background, an internal urge may develop in which they feel that their exclusionary may be excluded from a certain part of society or may miss out on "news" (however, there is no adequate guarantee for most of this news, that they have real news value, or they are just "fake news".) It can also affect an individual's private life.
What are these effects? In my research by the European Parliamentary Research Service, I examined the thesis of Gianluca Quaglio and Sophie Millar, entitled In-depth analysis, published in May 2020 by the Panel for the Future of Science and Technology, published in May 2020. The Scientific Foresight Unit is called the Scientific Forecasting Unit (STOA), which conducts mainly interdisciplinary research while providing strategic advice in the areas of science and technology opportunity assessment and scientific forecasting.[5]
Breakthrough studies and workshops on developments in these areas are organised and the European Science and Media Centre (ESMH), a platform for promoting networking, training and knowledge sharing between the European

[5] Gianluca Quaglio – Sophie Millar: In-depth analysis Panel for the Future of Science and Technology PE 641.540. 2020. p. 15.

Parliamentary, the scientific community and the media. All this work is carried out under the direction of the Science and Technology Futures Board (STOA), which is made up of 25 MEPs appointed by nine European Parliamentary committees. The Science and Technology Futures Board Panel is an integral part of the structure of the European Parliamentary.
In the In-depth analysis report, the researchers analysed five main categories. Internet addiction and problematic internet use, negative effects on cognitive development, overloading of information, boundaries of public and private spheres, and damage to social relations and communities.
The study was particularly negative about the results of individuals using electronic devices or the Internet. It can be said unanimously that damage could be established for all five categories, but it was also shown that when internet consumption among participants was reduced or eliminated in the experiment, as a result of which, in many cases, the deterioration of physical and psychological well-being in individuals could be established in the short term.
Negative emotions were amplified, such as anger, sadness and confusion, loneliness, social and social anxiety, memory impairment, cognitive impairment, loss of motivation, isolation, overload, attention deficit, and blurring of the boundaries of public and private life in the study subjects.

4. Cyberbullying as a concept primarily means harassment in cyberspace

In 2004, researchers and research groups began to actively engage in "cyberbullying",[6] which was then a new phenomenon. At the same time, it is important to point out that due to the rise of the Internet, the first atrocity committed by cyberbullying concerning crimes committed by electronic devices arose in the United States of America, but among others, it reached the United Kingdom, Australia and Europe, among others, Hungary. [7]
Cyberbullying as a concept primarily means harassment in cyberspace, which can mainly be described as a negative act that publishes the false claims of the anonymous or known perpetrator in a negative tone that appears in a negative tone on the Internet or on internet platforms, in many cases deeply offensive, generate hatred for the individual or a part of society, or merely the anonymous or known perpetrator, the false statement, it disseminates it [8] (including defamation or defamation) possibly publishing images or videos of the

[6] Katalin Domonkos: Cyberbullying: Harassment using electronic devices. Applied psychological 2014/1. p. 59.
[7] Thomas Pongó: Cyberbullying, az ellenség, amely köztünk él. Jogászvilág, 2015. https://jogaszvilag.hu/cegvilag/cyberbullying-az-ellenseg-amely-koztunk-el/
[8] Borgen, N. T. – Olweus, D et. al.: The potential of anti-bullying efforts to prevent academic failure and youth crime. a case using the Olweus Bullying Prevention Program (OBPP). Prevention science. 2021/8. pp. 1147-1158.

individual that it can be concluded that for the victim this can result in psychological, emotional strain, confusion, shame, grief, anxiety or, in more serious cases, deep depression in circles.
Dan Olweus, a Swedish psychologist and Norwegian psychologist who is a former professor of psychological research at the University of Norway, said that cyberbullying can be established if repetition can be established behind the act, or that this act seeks to be aware and the intention to reinforce the offensive. In addition, in my opinion, groups of forces, which are not equal or behind deviant behaviour, can determine personal circumstances (personal, family circumstances, material circumstances) or external – internal characteristics such as appearance (the person's clothing, grooming), manifestation (style, personality) also play a major role in the choice of the victim.
By obtaining information electronically, we have the opportunity to take part in the workings of our world. We can monitor our activities, set agendas, contribute to decision making, and through the internet with the access of the world wide web can fully participate as citizens in the various institutions of social engagement.[9] The location of the crime is mostly pages created on the Internet, which can be implemented either through social media sites, messaging and receiving applications or even through the chat service of social networks.
In many cases, the identity of the perpetrator is realized by creating and operating anonymous or not real so-called fake profiles, therefore it is very difficult to discover exactly who is behind the implementation and cause of cyberbullying.
Many positive features of the Internet are in addition to the fact that with our electronic devices we can reach any continent with immediate internet proximity. This factor is precisely why the offender can be given such an advantage that the perpetrator can be carried out in public at any time of the day, on any continent, in any time slot, in a particularly favourable way concerning social media. For this reason, I believe that bullying and abuse in schools among children and young people who do not use the internet are quite different. Furthermore, this widely known school bullying or abuse can form another dimension by the fact that, in addition to committing it in the real world, the online and internet space can be considered another place of committing it. This poses the greatest danger to the victim since the victim cannot find a way from the atrocities, and the harassment becomes fully continuous and, in many cases, permanent via the Internet, resulting in a

[9] Aichholzer, G StrauB Experience with Digital Tools in Different Types of e-Participation p. 93

potentially vulnerable state, often causing greater psychological harm than if the victim were physically abused.

5. Summation

The regulation of harassment under the Penal Code in force today does not include electronic or telecommunications devices using the Internet as a way of carrying out harassment. In my opinion, in our modern world, it is impossible to go along with the fact that almost a quarter of the world's population is an integral part of the online world, an online society and is an active user. Human coexistence with the Internet should not be without the right in this area either. The application of the law should cover electronic and internet devices developed for everyday use as a result of criminal assessment as a result of technology and the digital revolution.

However, I feel the need for young people and the children to receive training already during general education, during which they can nevertheless acquire general knowledge so that they can be fully prepared and actively combat these crimes against atrocities carried out through these internet-receiving devices. At the same time, it would be an excellent deterrent from committing the crime if the legislator not only evaluated harassment or online harassment from a criminal point of view, but it would also be useful if, in this case, in the school institution, the identity of the offender is revealed, and the student of the given educational institution is reprimanded, suspended or banned from playing sports provided by the school or sports clubs for educational purposes. activities or transfer from the institution to another educational institution.

In many cases, recovery from trauma after harassment is impossible because they do not dare or their circumstances do not allow victims to seek help. To alleviate or eliminate the serious psychological disorders caused by harassment, I would consider the statutory therapeutic professional assistance justified to alleviate or eliminate the serious psychological disorders caused by harassment.

To prevent cyberbullying (as a concept primarily means harassment in cyberspace) in state (and I would suggest in private) schools as well, I would recommend expanding the scholastic job of a computer science instructor within an institution or employing a suitable computer specialist to connect students only to a school wireless network with a certain VPN (as Virtual Private Network) number, through which the availability of different social platforms can be thwarted, thereby eliminating the possibility that these platforms this crime can be committed. The main reason for this would be that the third parties or anonymous users, hackers can trace your device connected to the Internet based on your IP address (IP as a word means International Protection Marking it is an International Protection Mark) and even track it in

real life. By the ability to hire a scholastic computer science instructor within an institution or an employing a suitable computer specialist the children and the juvenile are in safe in this way.

The legislator could expand the range of classified cases by allowing the offender to be of adult age and committing the crime to the detriment of a minor or child, then the legislator could classify the abuse as a crime, thereby also protecting the physical integrity, health and life of children and minors.

To alleviate or eliminate the serious psychological disorders caused by harassment, I would consider the statutory therapeutic professional assistance justified to alleviate or eliminate the serious psychological disorders caused by harassment.

In conclusion, I believe that by using the positive features of the internet, especially the advantages of its proliferation, it is possible to reduce the number of cases of online bullying and to take steps to use the internet consciously to eliminate online bullying of children and minors

Bibliography

- Aichholzer, Georg, and Gloria Rose. "Experience with digital tools in different types of e-participation." European E-democracy in practice. Springer, Cham, 2020. pp. 93-140.
- Borgen, N. T. – Olweus, D et. al.: The potential of anti-bullying efforts to prevent academic failure and youth crime. a case using the Olweus Bullying Prevention Program (OBPP). Prevention science. 2021/8. pp. 1147-1158.
- Fogarasi: Logic, Budapest, 16.16.1955.
- Gianluca Quaglio – Sophie Millar: In-depth analysis Panel for the Future of Science and Technology PE 641.540. 2020.
- Katalin Domonkos: Cyberbullying: Harassment using electronic devices. Applied psychological 2014/1.
- Lenin's Works Volume 32 Budapest, 1953.
- Thomas Pongó: Cyberbullying, az ellenség, amely köztünk él. Jogászvilág, 2015. https://jogaszvilag.hu/cegvilag/cyberbullying-az-ellenseg-amely-koztunk-el/

Dávid Tóth
Adjunct professor (University of Pécs, Faculty of Law Criminology and Penal Execution Law Department)

Theories on the connection between social media and crime

Abstract

As a result of the technological achievements of the 21st century, we now live in a digital world. Digitization trends have only intensified in recent years. Just like the media in the last century, social media are currently shaping social phenomena, including crime. In my research, I examine what theories explain the connections between social media and crime.

Key Words: social media, crime, crime theories.

1. Introduction

The Internet and inside it social media play an increasingly important role in people's lives every day. It has an impact on people's news consumption habits, relationships, communication, leisure activities and crime. In my present study, I examine the connections between crime and social media with a theoretical approach.

2. The rise of social media

A joint digital report by DataReportal, We Are Social and Hootsuite shows that digitization continues to gain momentum worldwide.[1]
Over the past year, hundreds of millions of people have become Internet users, and a significant number of them have registered also on social media.
The main findings of the report are illustrated in the figure below.

[1] https://datareportal.com/reports/digital-2022-july-global-statshot (2022. 07. 25.)

No. 1 Figure: Digital report 2022 July.

Based on the figure, the total world population will soon (expectedly by end of 2022) reach 8 billion people. 66.9 percent of the population have a smartphone[2] and 63.1 percent have Internet connection. The number of active social media users is 4.7 billion, which is 59 percent of the world's total population. In one year, 178 million new Internet users were registered, which means an increase of 3.7 percent. This increase can be seen even more in the number of people registering on social media, where the increase was 5.1 percent, and 227 million new users joined them. The population spent an average of 6 hours and 49 minutes on the Internet and within that 2 hours and 29 minutes on social media platforms, which was an increase of 6 and 5 minutes compared to the previous year.
If we look at the population over the age of 13, the proportion of social media users is even higher, 75.5% of the world's population. percent registered at least on one site. The proportion of women and men is 45.7 and 54.3 percent, respectively.

[2] There are several dangers of criminality are associated with the use of smartphones., Kraut Andrea; Kőhalmi László Tóth Dávid: Digital Dangers of Smartphones. In: Journal of Eastern-European criminal law 2020/1 pp. 36-49.

Figure No. 2. The percentage of the registered users on social media compared to the total population

The figure above shows the percentage of social media users compared to the total population on different continents. In the Western world, a higher proportion of the population is registered (between 78-83%), but in Eastern societies they are present in larger numbers, for example in India in the summer of 2021 there were 416,600,000 registered Facebook users.[3] In Hungary, there are approximately 7 million registered people on Facebook alone.
It can be seen that nowadays social media has a decisive role in current societies both from a static side (how many people are registered on the pages) and a dynamic side (to what extent, manner and quantity people use these interfaces on a daily basis), and this has an impact on crime too.

3. Theories examining the relationship between the media and crime

In the science of criminology, possible connections between the media, violence and crime have been investigated for a long time. There are several theories that tried to explore these correlations. In my study I will examine three theories:

- the moral panic theory,
- the fear of crime theory,
- and the web. 2.0. theory.

[3] https://worldpopulationreview.com/country-rankings/facebook-users-by-country

3.1. The theory of moral panic

3.1.1. On the theory of moral panic in general

Thanks to the appearance and spread of the media, we acquire a significant part of our knowledge from non-direct sources. Nowadays, the media has become one of our most important sources of indirect knowledge. The media contributes to the definition of social reality.[4]
These statements were already true for traditional or old media (also called as legacy media in the legal literature) but even more so for social media. Algorithms created with artificial intelligence determine what kind of news and information reaches certain people, and this has a great influence on society as a whole. In addition, a kind of diversification can be observed, as each person receives different news and information based on their interests every day, thereby creating a so-called bubble, a specific and unique informational reality that no other human has at best only similar.
In all forms of the media, the distribution or promotion of sensational, scandalous, or high-interest news can be observed, which promotes the viewership of traditional media and the reach of social media (hunting for clicks). Thus, for the audience, a significant part of the news will be related to deviant behavior, and these can easily be personified to social problems and the language of popular morality. As Kitzinger puts it*, „the pioneers of the theory of moral panic investigated the processes of control over consensual reality in a plural social environment heavily imbued with media production."*[5]
The crime theory of moral panic was developed along with sociological and criminological research. The basis of moral panic is how society focuses and reacts (or even panics) to a certain behavior, problems and how they can demonize certain social groups as responsible for these problems.[6]
The term moral panic was first used by Jock Young in 1971 in his study on drug use, but Stanley Cohen's research on the construction of deviance in 1972 made it widely known. Originally, this theory was written and applied primarily to deviant youth subcultures, such as juvenile delinquents, children who watch violent videos, etc.[7]

[4] Kitzinger Dávid: A morális pánik elmélete. In: Replika 2000/40. p 23.
[5] Ibidem.
[6] Hayes, Rebecca – M.; Luther, Kate: #Crime. Palgrave Studies in Crime, Media and Culture. Springer International Publishing. 2018. p. 15.
[7] Ibidem.

According to Cohen's definition, we can talk about moral panic when *„a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests.*" [8]
The process begins with the appearance of a social problem. In essence, this phenomenon threatens the idealized order of society, and the media and society see a group as the cause of the problem, the scapegoat, or as Cohen puts it, the folk devil. Folk devils serve as a kind of visual reminder of what not to be. [9]
The media presents the problem in a sensationalistic and simplistic way, pointing the finger at the social group declared as the scapegoat. This activity of the media creates a public mood, to which the legislator reacts with legislative strictures. Due to the changes in the law, the law enforcement bodies also pay close attention to or observe these standards, and in the case of criminalization, the number of registered crimes may increase, thus imitating the steps taken to restore order. As a result, moral panic affects society's legal system, social order, authorities, institutions, and public perception. Members of society develop a simplified reality view of the problem through the media. In the jargon the word moral refers to *„the threat to interests, traditions and lifestyle is expressed through social morality as a symbolic system."* [10] The technical term, panic illustrates the intensity and spread of the phenomenon.[11]
According to Jewkes, moral panics have five important characteristics:

- Moral panic can occur when the media presents an ordinary event as a sensation.
- With this activity, the media starts a deviancy-reinforcing spiral. Within this, a moral discourse is created by journalists and other authorities, opinion leaders and moral actors, who collectively demonize the perceived wrongdoers, thus increasing the moral decline.
- It makes clear the moral boundaries in society, and thus creates consensus and concern.
- Moral panics tend to appear in times of rapid social change.
- Moral panics tend to target young people as they are a metaphor for the future and their behavior is seen as a barometer to test the health or sickness of a society.

According to Jewkes, the media is the main driver of moral panics, but with social media, the control tilts towards younger generations (and especially young adults within it), which was not present in the old media. [12]

---

[8] Cohen, Stanley: Folk devils and moral panics. Third edition Routledge, London-New York. 2002. p. 1.
[9] Cohen (2002) p. 2.
[10] Kitzinger (2000) p. 24
[11] Ibidem.
[12] Hayes, Rebecca – M.; Luther, (2004) p. 19

3.1.2. How does moral panic appear on social media?

According to Milton Mueller, social media makes interactions between people hyper-transparent, and, in many cases, perpetrators blame the platforms that make them available. This hyper-transparency promotes a moral panic in public media. Just like in the case of the old media, there are accusations that social media promotes terrorism and extremism, can contribute to ethnic cleansing, influence elections, and destroy democracy. And the moral panic places social media as the source of the problem. From a criminal aspect, he highlights the following problems:

- Fake news
- Promoting extremism and terrorism,
- Increasing racism and promoting verbal and violent actions against different ethnicities.[13]

Mueller therefore, points out that moral panic also appears around social media, but it is also one of its tools, just like the old media. [14]

Because of the instant nature of the internet and social media the triggering awareness of danger is more relevant nowadays (this also connects to the fear of crime theory in the next chapter). The users are under heavy influence from different cultural beliefs and therefore the social values of society can loosen up. Belief in the breakdown of the social order grows stronger, and tempers the political power offers solutions to alleviate it: the legislator typically responds with creating more strict statutes more instantly.[15]

According to Garland, there is a significant shift from moral panics to culture wars (or symbolic politicization). According to his view, nowadays the meaning and evaluation of a behaviour will become more and more controversial and the balance of power between competing groups will become less asymmetric. Examples of this are the challenges observed in recent years in connection with illegal migration[16] and legal reform, or the issue of Muslim women wearing the hijab in schools, which initially appeared as a moral panic and eventually became a politically disputed culture war.[17]

By the way, in one of his studies in 2011, Cohen also predicted that the refugee and migrant problem would end up in the narrative of moral panic. This has all

---

[13] Mueller, Milton: Challenging the social media moral panic: preserving free expression under Hypertransparency Cato Institute Policy Analysis 876 2019.

[14] Ibidem.

[15] Parti Katalin - Kiss Tibor: 18. Informatikai bűnözés. In Borbíró et. al. (Eds.) Kriminológia. Wolters Kluwer, Budapest, 2016. p. 492.

[16] See further about illegal migration: Kőhalmi, László: A migráció néhány biztonságpolitikai összefüggése. In Szakmai Szemle 2016/4. pp. 81-100.
Kőhalmi, László: A migráció és a kriminalitás néhány összefüggése. In Jura 2016/1 pp. 94-99.

[17] Martin, Greg: Crime, media and culture. Kindle edition. Routledge, New York. 2019. p. 68.

been seen in action in Europe and the United States in recent years. In this view, Muslim immigrants are the new folk devils.[18]

According to Garland, there are two reasons for the culture war. On the one hand, a fragmentation and heterogeneity can be observed in the current society, and on the other hand, the media has also proliferated, which includes dissemination through social media, which now allows the creation of many more alternative sites of resistance to question the dominant definitions of the situation. Here is the "citizen journalism" highlighted above. emergence and the growing use of social media increase the possibilities of protest and resistance: it expands the means of hearing and spreading the messages of alternative collective voices. [19]

In their study, Giulliani, Garraio and Santos examined the role of digital media in amplifying the "sexual moral panic" about migration. Through an analysis of studies in Italy and Germany, they came to the conclusion that digital media contributed greatly to the creation and spread of fears of invasion and sexual crimes, and that they gave birth to new racist crimes. In one legal case, in January 2018, Pamela Mastropietro, an 18-year-old woman, was raped and killed by three Nigerian migrants in the city of Macerata. The victim's body parts were also dismembered and tried to disappear outside of Macerata in bags. All three perpetrators were arrested and sentenced to life imprisonment in May 2019.

The horrific crimes were used by far-right groups to incite hatred. The moral panic appearing on social media is well illustrated by Salvini's Facebook post, in which he demanded the mass expulsion and chemical castration of illegal migrants, which reached more than 34,000 likes and almost 3,700 shares on Facebook. A significant number of the more than 4,500 commenters demanded the death penalty for the perpetrators. Then, in February 2018, Luca Traini, a far-right perpetrator, shot and killed six black people from his car, shouting Viva l'Italia (long live Italy). According to Traini, his actions were motivated by revenge for the crime committed against Mastropietro.[20]

3.2. Fear of crime theory

László Korinek found in his study that the fear of crime is increasing in the age of mass media. The media's inadequate portrayal of crime affects the way of life of the population, social insecurity and the lack of trust in public

[18] Cohen, Stanley: Whose side were we on? The undeclared politics of moral panic theory. Crime, Media, Culture: An International Journal, 2011/3. pp. 237–243.

[19] Martin (2019) p. 74.

[20] Santos, Sofia José – Júlia Garraio – Gaia Giuliani: Online social media and the construction of sexual moral panic around migrants in Europe. In: Socioscapes. International Journal of Societies, Politics and Cultures 2019/1: pp. 155-174.

institutions increase. Another negative consequence is social disintegration and the disintegration of the community.[21] Research in Western democracies shows that people fear crime and that this negatively affects their sense of security and well-being. Based on the studies, the fear of crime is not proportional to the true level of crime. The aforementioned moral panic processes further weaken people's sense of security and increase their anxiety. This is especially true if a terrorist attack occurs in the country. Fear of crime in relation to old media was measured by television viewing habits. Those who watched more TV had a greater fear of crime.[22]
According to Frank Füredi, a culture of fear prevails in postmodern societies, which is only aggravated by the presence of the Internet.[23] Regarding new media, Intravia et al [24] conducted research. The phenomenon of fear of crime was investigated in relation to the use of the internet by young adults. The anonymous questionnaire survey was conducted on three university campuses between autumn 2016 and spring 2017. Fear of crime was measured by asking respondents to indicate their level of fear (from 0 = not at all afraid, to 10 = very afraid) for the following six crime-related events:

- someone breaks into your home,
- being robbed on the street,
- sexual harassment / violence happens to him
- your car or bicycle is stolen
- been beaten or attacked by strangers,
- or be murdered.

Regarding their data, it is important to note that the relationship between media consumption and fear of crime may be reciprocal in nature. That is, individuals who fear more crime and violence may be more motivated to turn to media content to learn, process, and understand crime-related issues. Based on their results, they concluded that regular use of social media is significantly related to crime.

3.2. A new theory - the Web. Theory 2.0.

Yar dealt with a new theory called With Web 2.0. He pointed out that the ever-changing nature of the internet is likely to have an impact on crime and

[21] Korinek, László, A bűnözéstől való félelem és a tömegtájékoztatás. In: Belügyi Szemle 1989/4. pp. 31-38. p. 37.
[22] Hale, Chris: Fear of crime: A review of the literature. In: International Review of Victimology 1996/2. pp. 79–150.
[23] Parti – Kiss (2016.) p. 492.
[24] Intravia, J. – Wolff, K. T. – Paez, R., – Gibbs, B. R.: Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. In: Computers in Human Behavior. 2017. pp. 158-168.

victimization. According to Yar the Internet should be understood as a technologically supported social practice. [25] People use the Internet to function in society, so practice is one part of the social construction. The Web 2.0 theory also points out that the Internet creates new social and criminal problems.
For example, the Internet and social media make it easier for sexual predators and paedophiles to target their minor victims. Yar examines the issue from the perspective of victimology, in his view that young people can be easily manipulated through social media platforms and expose information about themselves that increases their vulnerability.[26]
In accordance with the theory, I also pointed out in a previous study that new forms of crime can appear on social media.[27]

4. Summary

Based on the research, it can be concluded that the influence of social media on social life conditions is significant. The relationship between social media and crime can be investigated using old media theoretical approaches such as moral panic theory or fear of crime research. Compared to the old media, the new media is a more global, more accessible, faster, and interactive form of communication. Theoretical approaches also emphasize that new crimes appear on social media (e.g., cyberbullying).[28] On the other hand, criminals can more easily find a motive and incitement to commit traditional crimes.
In my opinion, the research conducted with the theory of moral panic effectively demonstrates that a kind of scapegoating mechanism has always been present in society. This appears even more on social media than we saw through the Italian legal case. In contrast to traditional media, it is more difficult to fight such inflammatory narratives in new media, as it is a much more decentralized phenomenon. Service providers have and will continue to have a responsibility to remove these types of groups, comments, and people

[25] Yar, Majid: E-Crime 2.0: the criminological landscape of new social media. In: Information & Communications Technology Law 2012/3. p. 207.
[26] Yar (2012) p. 210.
[27] Tóth Dávid: The correlations between social media and crime. In: Garayová, Lilla Budúcnosť práva – Právo budúcnosti II. Zborník príspevkov z online vedeckej konferencie - The Law of the Future – The Future of Law II. Conference Proceedings. Paneurópska vysoká škola, Fakulta práva, Bratislava. 2022. pp. 149-164. ,
[28] Barbara A. Spears and Mike Zeederberg: 13. Emerging Methodological Strategies to Address Cyherballying Online Social Marketing and Young People as Co-Researchers. In: Bauman S. - Cross - Walker (Eds): Principles of cyberbullying Research. Routledge, London-New York 2013. p. 166.
Horowitz, M., – Bollinger, D: (Eds): Cyberbullying in social media within educational institutions: Featuring student, employee, and parent information. Rowman & Littlefield, Lanham-Boulder-New York-London 2014.

from their platforms. With the development of artificial intelligence and algorithms, we can trust that the number of such phenomena will decrease in the future. Though we must mention that these algorithms in their early stage usually don't value or measure the content on social media correctly and in occasions may contribute to the moral panic phenomenon.[29]

[29] Wood, Mark A. Antisocial media: Crime-watching in the internet age. Palgrave Studies in Crime, Media and Culture, Springer, Cham. 2018. p. 100.

Bibliography

- Barbara A. Spears – Mike Zeederberg: 13. Emerging Methodological Strategies to Address Cyherballying Online Social Marketing and Young People as Co-Researchers. In: Bauman S. - Cross - Walker (Eds): Principles of cyberbullying Research. Routledge, London-New York 2013. p. 166.
- Cohen, Stanley: Whose side were we on? The undeclared politics of moral panic theory. In: Crime, media, culture. 2011/3. pp. 237-243.
- Cohen, Stanley: Folk devils and moral panics. Third edition Routledge, London-New York. 2002. p. 1.
- Hale, Chris: Fear of crime: A review of the literature. In: International Review of Victimology 1996/2. pp. 79–150.
- Hayes, Rebecca – M.; Luther, Kate: #Crime. Palgrave Studies in Crime, Media and Culture. Springer International Publishing. 2018. p. 15.
- Horowitz, M., – Bollinger, D: (Eds): Cyberbullying in social media within educational institutions: Featuring student, employee, and parent information. Rowman & Littlefield, Lanham-Boulder-New York-London 2014.
- Intravia, J. – Wolff, K. T. – Paez, R., – Gibbs, B. R.: Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. In: Computers in Human Behavior. 2017. pp. 158-168.
- Kitzinger Dávid: A morális pánik elmélete. In: Replika 2000/40. p 23.
- Kőhalmi, László: A migráció és a kriminalitás néhány összefüggése. In Jura 2016/1 pp. 94-99.
- Kőhalmi, László: A migráció néhány biztonságpolitikai összefüggése. In Szakmai Szemle 2016/4. pp. 81-100.
- Korinek, László: A bűnözéstől való félelem és a tömegtájékoztatás. In: Belügyi Szemle 1989/4. pp. 31-38. p. 37.
- Kraut Andrea – Kőhalmi László –Tóth Dávid: Digital Dangers of Smartphones. In: Journal of Eastern-European criminal law 2020/1 pp. 36-49.
- Martin, Greg: Crime, media and culture. Kindle edition. Routledge, New York. 2019. p. 68.
- Mueller, Milton: Challenging the social media moral panic: preserving free expression under Hypertransparency Cato Institute Policy

Analysis 876 2019. panic theory. Crime, Media, Culture: An International Journal, 2011/3. pp. 237–243.

- Parti Katalin – Kiss Tibor: 18. Informatikai bűnözés. In Borbíró et. al. (Eds.) Kriminológia. Wolters Kluwer, Budapest, 2016. p. 492.
- Santos, Sofia José – Júlia Garraio – Gaia Giuliani: Online social media and the construction of sexual moral panic around migrants in Europe. In: Socioscapes. International Journal of Societies, Politics and Cultures 2019/1: pp. 155-174.
- Tóth Dávid: The correlations between social media and crime. In: Garayová, Lilla Budúcnosť práva – Právo budúcnosti II. Zborník príspevkov z online vedeckej konferencie - The Law of the Future – The Future of Law II. Conference Proceedings. Paneurópska vysoká škola, Fakulta práva, Bratislava. 2022. pp. 149-164. ,
- Yar, Majid: E-Crime 2.0: the criminological landscape of new social media. In: Information & Communications Technology Law 2012/3. p. 207.

Henrietta Németh
PhD Student (University of Pécs, Faculty of Law)

Verbreitung von Drogen im Darknet

Abstract:

Die vorliegende Studie untersucht die illegalen Drogenmärkte im Internet. Das Hauptziel meiner Forschung war es, Motivationsfaktoren zu analysieren, die zur Entscheidung neben der online Drogenbestellung gegenüber dem materiellen Drogenhandel beitragen. Um darüber einen Überblick zu geben, werden vor allem einige relevante Begriffe der digitalen Welt geklärt und das Geschäftsmodell der anonymen Drogenmärkte dargestellt. Die Methode meiner Untersuchung war die Verarbeitung der ungarischen und ausländischen Fachliteratur.
Durch die Verbreitung digitaler Technologien zeigt sich eine Änderung der Drogenkriminalität. Die von dem Darknet ermöglichte Anonymität spielt eine relevante Rolle bei der Verbreitung des online Drogenhandels. Außerdem können die bessere Verfügbarkeit, die günstige Preise, die höhere Qualität der online bestellbaren Drogen und die Gewaltlosigkeit als grundlegende Aspekte bezeichnet werden.

Schlüsselwörter: Darknet, Drogenhandel, Kryptomarkt, digitale Technologie. illegale Plattform

1. Einleitung

Die Entwicklung der Technologie, die Informationsverbreitung im Internet und die Vielfalt von sozialen Medien vereinfachen nicht nur unseren Alltag, sondern sie dienen auch zur neuen Plattform für die Kriminellen. Die durch die digitale Welt ermöglichte Kriminalität bedeutet eine große Herausforderung sowohl für die Strafbehörde, als auch für den Gesetzgeber und die Rechtsprechung. Die Anonymität des Darkwebs bietet Kriminellen einen Bereich, mit illegalen Waren zu handeln und verbotene Inhalte zu teilen. Waffen- und Drogenhandel, Kinderpornographie, Betrug, *Identitätsdiebstahl*[1] – nur einige Beispiele für die in den Online-Plattformen begangenen Straftaten. Im Darknet kann man sich unter anderem folgende Waren besorgen: *Drogen, Waffen, rezeptpflichtige Medikamente, Falschgeld, gestohlene*

[1] Dávid Tóth: Identity crimes on the darknet and the social media. In: Büntetőjogi Szemle 2021/1. p. 85. https://ujbtk.hu/david-toth-identity-crimes-on-the-darknet-and-the-social-media/ heruntergeladet am 18.03.2022

Kreditkartendaten, gehackte Bankkontodaten, Herstellungseinleitungen für psychoaktiven Substanzen.[2]
Außerdem muss darauf hingewiesen werden, dass Darknet nicht nur zu illegalen Zwecken verwendet wird, viele nutzen die Anonymität für den Schutz ihres Privatlebens (z.B. *Journalisten, Polizei, Militär*).[3] Die empirische Studie der britischen Sicherheitsfirma Intelliagg gibt einen Überblick über den Inhalt des Tor-Netzwerkes. Die Firma hat cirka 13.000 Internetseiten im Tor-Netzwerk untersucht. Die Studie zeigt, dass etwa die Hälfte von den Webseiten nach dem britischen oder US-Recht über einen legalen Inhalt verfügen. Die Wissenschaftler haben allerdings die strafrechtlich relevanten Webseiten folgendermaßen kategorisiert: 29 Prozent gehören der Gruppe „*Filesharing-Dienste*“, 28 Prozent der Kategorie „*geleakte Daten*“ und 12 Prozent der untersuchten Webseiten zählen zu der Kategorie „*Finanzbetrug*“. 4 Prozent der Internetseiten stehen im Zusammenhang mit Drogenhandel und 0,3 Prozent mit Waffen.[4]
Laut Weltdrogenbericht 2021 von UNODC haben die illegalen Drogenmärkte im Darknet einen Umsatz von ca. 315 Millionen Dollar pro Jahr.[5] Die Drogentransaktionen im Darknet machen jedoch nur einen Bruchteil des materiellen Drogenhandels aus. Dennoch sind sie eine neue Form des Drogenhandels in dem Sinne, dass sie die lokale „offline“ Märkte umstrukturieren, sie funktionieren als neuer Kanal im Drogenfluss.[6] Der Handel mit illegalen Waren im Darknet zeigt eine riesige Entwicklung in den letzten Jahren: *es hat sich eine globale Industrie ausgebaut, von der die Strukturen der legalen Plattformen wie ebay oder Amazon übernommen wird, die Produkte werden mit Fotos und Beschreibung aufgelistet, die*

[2] Meropi Tzanetakis: Drogenhandel im Darknet. Gesellschaftliche Auswirkungen von Kryptomärkten. In: Aus Politik und Zeitgeschichte. Darknet 46–47/2017. p. 41. https://www.bpb.de/system/files/dokument_pdf/APuZ_2017-46-47_online.pdf heruntergeladet am 30.03.2022
[3] Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. In: Büntetőjogi Szemle 2020/1. p. 91. https://ujbtk.hu/dr-serbakov-marton-tibor-kriminalitas-a-dark-weben-illegalis-piacok-pedofil-oldalak-terroristak-es-az-ellenuk-valo-kuzdelem/ heruntergeladet am 13.03.2022
[4] Tzanetakis (2017) p. 42.
[5] UNODC: World Drug Report 2021 (United Nations publication, Sales No. E.21.XI.8). p. 2. https://www.unodc.org/res/wdr2021/field/WDR21_Booklet_2.pdf heruntergeladet am 04.05.2022
[6] Judith Aldridge, David Décary-Hétu: Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. In: International Journal of Drug Policy. 2016. https://www.sciencedirect.com/science/article/pii/S0955395916301335#bbib0015. heruntergeladet am 10.04.2022

Gemeinschaft diskutiert sehr intensiv über die Vertrauenswürdigkeit von Händlern und es gibt einen 24/7 Kundensupport.[7]
Im Folgenden werden zunächst einige Begriffe geklärt: das Clearnet, das Deep Web und das Darknet.

2. Begriffserklärung

In der Regel differenziert man zwischen folgenden Bereichen des Internets: das *Clearnet*, das *Deep Web* und das *Darknet*. Der offen zugängliche Bereich des Internets heißt *Clearnet* (klares Netz), wird auch als *Surface Web* (*Oberflächennetz*) bezeichnet. Die Webseiten im *Clearnet*, beziehungsweise deren Inhalte sind von üblichen Browsern – wie Google Chrome oder Internet Explorer - erfassbar. Für diese Internetseiten ist charakteristisch, dass sie die typischen Domainendungen, wie .hu oder .com haben.[8] Drogentransaktionen finden auch im Clear Web statt, unter anderem mit der Hilfe von verschlüsselten Kommunikationsmitteln, oder durch Applikationen, die von den sozialen Medien bereitgestellt werden. Während sich aber die Vermarktung von traditionellen Drogen – wie Heroin oder Cannabis - auf das Darknet beschränkt, wird im Clearweb mit Substanzen gehandelt, die zur Verbreitung des Marktes der synthetischen Drogen beitragen.[9]
Ein anderer Bereich des Internets wird *Deep Web* (*tiefes Netzt*) genannt, was theoretisch mit jedem Internetbrowser aufgerufen werden kann, seine Inhalte können aber trotzdem nicht von Suchmaschinen erfasst und dadurch auch kaum von Benutzern besucht werden. Das kann z.B. darin liegen, dass es sich um Intranets für geschlossene Benutzergruppen oder Inhalte von Paywalls handelt.[10]
Die Definition von Darknet wird in der öffentlichen Debatte oft mit Kriminalität verbunden, aus diesem Grund wird von den Forschern eher eine neutrale Definition verwendet: *Darknet bezeichnet lediglich die Art und Weise des Zugangs (über eine Anonymisierungssoftware) und sagt nichts über den*

[7] Sabine Vogt: Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen? In: Die Kriminalpolizei. 2/2017. file:///C:/Users/Heni/Downloads/vogtArtikelDarknet%20(1).pdf heruntergeladet am 03.05.2022
[8] Stefan May: „Tor" in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets. In: Aus Politik und Zeitgeschichte. Darknet. 46–47/2017 p. 4. https://www.bpb.de/system/files/dokument_pdf/APuZ_2017-46-47_online.pdf heruntergeladet am 30.03.2022
[9] UNODC (2021) p. 66.
[10] May (2017) p. 4.

rechtlichen Status der Inhalte aus.[11] Das Darknet kann als ein kleiner Teil des Deep Webs verstanden werden, der die Lokation und die Identität des Users verbergt und dadurch eine Anonymität beim Surfen versichert. Zum Aufrufen der Internetseiten im Darknet benötigt man eine spezielle Software, wie der Tor-Browser und die entsprechenden Einstellungen.[12] Der Tor-Browser ist also eine Anonymisierungssoftware, von der die IP-Adressen oder Domainnamen verbergt werden und dadurch kann die Kommunikation auf die Parteien nicht zurückgeführt werden.[13] Tor ist die gekürzte Form von „The Onion Router". Der Entwickler hat den Aufbau der Tor-Technologie mit einem Zwiebeln dargestellt: der Kern der Zwiebel verbergt sich unter viele Schalen, genauso ist es bei Tor bemerkbar: *der Kern aus Identität und Aktivität der jeweiligen Internetnutzer versteckt sich unter mehreren Anonymisierungsschichten*. [14] Außer Tor-Browser stehen auch andere Verschlüsselungssoftware zur Verfügung – wie I2P und Freenet-, aktuell ist aber die Tor-Software die größte und beliebteste Anonymisierungssoftware.[15] Nach der Installierung der Tor-Software und nach den üblichen Einstellungen verbindet sich der Tor-Browser mit dem Tor-Netzwerk, der das anonyme Surfen ermöglicht. Für die Suche im Darknet sind die herkömmlichen Browser – wie Google – nicht geeignet, es ist eine spezielle Darknet Suchmaschine nötig. Ihre Spezialität liegt darin, dass diese Suchmaschinen speziell für die Darknet Seiten angelegt sind und sie finden auch die versteckten Inhalte des Internets, die z.B. von Google nicht erreicht werden können. Die meistgenutzte Darknet Suchmaschinen sind z.B. Torch, DuckDuckGo und HiddenWiki. [16]
Das nächste Kapitel gibt einen Überblick über den Aufbau und die Merkmale der anonymen Drogenmärkte.

---

[11] Meropi Tzanetakis: Digitalisierung von illegalen Märkten. Folgen, Grenzen und Perspektiven. In: Handbuch Drogen in sozial- und kulturwissenschaftlicher Perspekt. 2019. p. 479.
https://www.researchgate.net/publication/327966303_Digitalisierung_von_illegalen_Markten_Folgen_Grenzen_und_Perspektiven heruntergeladet am 20.03.2022

[12] Ines Maria Eckerman: Was ist das Darknet? 2017. https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet heruntergeladet am 16.03.2022

[13] Meropi Tzanetakis: Zur globalen Ökonomie von digitalen Drogenmärkten. In: Rausch. Wiener Zeitschrift für
Suchttherapie. 2017. p. 192.
https://www.researchgate.net/publication/323430078_Zur_globalen_Okonomie_von_digitalen_Drogenmarkten heruntergeladet am 17.03.2022

[14] May (2017) p. 5.

[15] Serbakov (2020)

[16] Jana Bergmann: Darknet Suchmaschinen. 2021. https://digital-hacks.de/darknet-suchmaschinen/ heruntergeladet am 20.05.2022

3. Merkmale der online Drogenmärkte

Im Oktober 2013 wurde Silk Road - der größte und meistgenutzte Kryptomarkt für Drogen - von dem FBI geschlossen. Silk Road hatte eine große Auswahl an Drogen, man konnte sich auf der digitalen Plattform verschiedene Typen von Substanzen und rezeptpflichtige Medikamente bestellen. Laut einer Studie waren MDMA, Cannabis und LSD die häufigsten gekauften Drogen in den USA, Großbritannien und Australien.[17] Auf der Plattform wurden nicht nur Drogen vertrieben: Hacker-Software und gefälschte Ausweisdokumente waren unter anderem auch verfügbar. Nach seinem 2,5-jährigen Betrieb wurde der online Drogenmarkt geschlossen und sein Gründer wurde zur lebenslangen Freiheitstrafe verurteilt.[18] Dream Market war auch ein relativ große Drogenmarktplatz im Darknet, welcher 2013 gegründet wurde. Im März 2019 hat der Betreiber die Abschaltung des Marktes angekündigt und mitgeteilt, dass die Services von einem Partnerunternehmen übernommen werden.[19] Mit seinen ca. 17 Millionen Kunden ist der russische Hydra Market im Jahr 2020 Marktführer geworden, aber auch diese illegale Plattform wurde im April 2022 gesperrt.[20] Laut der Generalstaatsanwaltschaft Frankfurt am Main und des Bundeskriminalamtes (BKA) wurden *Bitcoins in Höhe von ca. 23 Millionen EUR sichergestellt, welche dem Marktplatz zugerechnet werden*.[21] Zu den größten Darknet-Drogenmärkte zählt auch der auf Cannabis spezialisierte Cannazon Market. Die Mehrheit des Drogenhandels im Darknet betrifft das Cannabis, es gibt aber eine große Auswahl an Drogen: man kann sich unter anderem Amphetamin, Methamphetamin, Ecstasy, Kokain und Heroin bestellen.[22]

---

[17] Monica Barrat – Jason Ferris – Adam Winstock: Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. 2014. file:///C:/Users/Heni/Downloads/1652550929685_2006095374.pdf heruntergeladet am 02.04.2022

[18] Frankfurter Allgemeine Zeitung: Höchststrafe für den „Silk Road"-Gründer. 2015. https://www.faz.net/aktuell/gesellschaft/kriminalitaet/lebenslange-haft-hoechststrafe-fuer-den-silk-road-gruender-13620148.html heruntergeladet am 16.03.2022

[19] Olivia von Westernhagen: Seltsame Vorgänge bei Dream Market: Darknet-Marktplatz kündigt Schließung an. 2019.
https://www.heise.de/newsticker/meldung/Seltsame-Vorgaenge-bei-Dream-Market-Darknet-Marktplatz-kuendigt-Schliessung-an-4355932.html heruntergeladet am 16.03.2022

[20] Ruth Fulterer: Hydra ist tot: Deutschland sperrt den grössten Darknet-Marktplatz der Welt. 2022.
https://www.nzz.ch/technologie/deutsche-ermittler-schliessen-hydra-den-groessten-darknet-marktplatz-der-welt-ld.1678073?reduced=true heruntergeladet am 10.04.2022

[21] Bundeskriminalamt: Illegaler Darknet-Marktplatz „Hydra Market" abgeschaltet. 2022. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html heruntergeladet am 10.04.2022

[22] UNODC (2021) p. 79.

Obwohl die genannten Drogenmarktplätze – Silk Road, Dream Market und Hydra Market - mehrere Jahre betrieben wurden, haben die illegalen Darknet Seiten meist eine kurze Lebensspanne. Sie sind meistens in einem relativ kurzen Zeitraum (ca. 8 Monaten) aktiv.[23] Die Schließung des Marktes kann auf verschiedene Weise erfolgen: der häufigste Grund der Abschaltung ist der Betrug der Verbraucher: der Betreiber schließt den Markt plötzlich, ohne Erfüllung der Transaktionen und behält das eingezahlte Geld. Es kommt aber auch vor, dass die Seite mit Ankündigung und ohne Beschädigung der Kunden gesperrt wird. Außerdem können die Intervention der Strafbehörde und Hackerangriffe zur Schließung des Marktes führen.[24]

Die Zulassung neuer Darknetnutzer kann mit Voraussetzungen verbunden werden: bei einigen Plattformen erfolgt die Aufnahme als neuer Händler erst, wenn der neue Nutzer von den bereits aktiven Händlern als „verlässlich" bezeichnet wird. Auch die Käufer müssen in einigen Fällen von dem Betreiber zugelassen werden und einen Betrag für die Mitgliedschaft leisten.[25]

Um das entsprechende Angebot und den Händler auszuwählen, hilft den Käufern das Bewertungssystem. In der Darknet-Welt wurde ein Feedbacksystem ausgebaut, wo die Käufer die Zuverlässigkeit der Verkäufer bewerten können; man kann eine Rückmeldung unter anderem über die Qualität und Quantität der bestellten Drogen, über die Kundenbetreuung und auch über die Kommunikation des Verkäufers geben.[26]

Für die Waren bezahlt man in den Darknetmärkten mit virtuellen Währungen. Die Kunden haben die Möglichkeit, zwischen drei unterschiedlichen Bezahlsysteme zu wählen. Eine Bezahlvariante ist das sogenannte Treuhandverfahren, bei dem die Kryptowährung erst auf ein Depot eingezahlt wird und die Auszahlung an den Verkäufer wird erst freigegeben, wenn der Käufer über den Erhalt der Wahre eine Bestätigung gibt. Der Vorteil dieser Bezahlvariante ist, dass die Kunden vor einem möglichen Betrug geschützt sind, sie bringt aber das Risiko, dass der Treuhändler die Verwaltung des Kaufpreises missbraucht. Bei Finalized early wird der Geldbetrag dahingegen vor der Auslieferung der Ware an den Verkäufer überwiesen. Eine offenbare Gefahr dieses Bezahlsystems ist, dass die Ware nach dem Erhalt des Kaufpreises nicht versendet wird. Die sicherste Variante – die technisch gesehen ziemlich anspruchsvoll ist und aus diesem Grund wird sie auch nicht häufig verwendet – ist *Multi-signature:* hierbei müssen zwei von den drei

[23] UNODC (2021) p. 75.

[24] EUROPOL: Drugs and the darknet Perspectives for enforcement, research and policy. 2017. p. 16. https://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf heruntergeladet am 13.03.2022

[25] Eckerman (2017)

[26] EUROPOL (2017) p. 27.

Teilnehmern (Betreiber des Marktes, Verkäufer, Käufer) die Transaktion bestätigen, in dem sie *die Zahlungsfreigabe signieren.*[27]
Die Lieferung der Drogen wird durch die ahnungslosen Postdienstleister veranlasst. Um den Eingriff der Strafbehörde zu vermeiden, ist es besonders relevant, dass die Drogen „sicher und sauber" verpackt werden. Aus diesem Grund haben viele Händler einen separaten Raum zwecks Verpackung der Drogen, damit können sie es vermeiden, dass auf der Packung DNS-Spuren oder Drogenrückstände bleiben. Die Zustellung des Pakets erfolgt auf verschiedene Weise: es gibt Käufer, die für den Empfang einen Briefkasten mieten, es gibt Käufer, die auf die Postadresse von anderen Personen mit der Verwendung falscher Daten zugreifen und es gibt solche, die als Lieferanschrift ihren wahren Namen und Adresse angeben. In den verschiedenen Darknet-Foren stehen auch Anweisungen zur Verfügung, die Informationen über die sichere Zustellung für den Kunden enthalten. [28]

4. Motivationsfaktoren für die Entscheidung der online Drogenbestellung

Das Ziel des vorliegenden Kapitels ist, Faktoren zu analysieren, die zur Verbreitung der anonymen Drogenmärkte beitragen. Hierbei muss zunächst die Anonymität der Transaktionen erwähnt werden. Mit der Hilfe von verschiedenen Verschlüsselungssoftware und Kryptowährungen sind die Identität und Lokation der Händler und Käufer nicht auf die Teilnehmer zurückführbar. Die durch das Darknet ermöglichte Anonymität hat einen doppelten Zweck: zum einen sind Users vor den Strafverfolgungsbehörden geschützt, zum anderen bleibt die Identität des einen Teilnehmers vor dem anderen geheim. Aus diesem Grund haben die Nutzer des Darknets ein viel größeres Sicherheitsgefühl im Vergleich zum materiellen Drogenhandel. [29] Zwischen dem Verkäufer und Käufer ist die Möglichkeit der Identifizierung anhand des Gesichtes oder eines persönlichen Objektes völlig ausgeschlossen, sie kennen nur den Benutzernamen des anderen. [30]

---

[27]Tzanetakis (2019) p. 485.
[28] Alois Afilipoaie Patrick Shortis: From Dealer to Doorstep – How Drugs Are Sold On the Dark Net. 2015. p. 4. https://www.swansea.ac.uk/media/From-Dealer-to-Doorstep-%C3%A2%C2%80%C2%93-How-Drugs-Are-Sold-On-the-Dark-Net.pdf heruntergeladet am 02.04.2022
[29] Kiss Tibor: Miért népszerű a darknetes kábítószer-kereskedelem? In: Ünnepi tanulmányok a 75 éves NÉMETH ZSOLT tiszteletére. Navigare necesse est. 2021. p. 270. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/16609/web_PDF_NZs75.pdf?sequence=1 heruntergeladet am 20.03.2022
[30] Vári Vince: A bűnüldözés aktuális kihívása: az online kábítószerpiac. 2022. p. 145. https://drogkutato.hu/wp-content/uploads/2022/01/01-162_IDSZ-teljes_NET-139-161-1.pdf heruntergeladet am 17.03.2022

Barrat, Ferris und Winstock haben in Ihrer Studie unter anderem Gründe der Wahl von Drogenbestellung auf Silk Road untersucht. In der Analyse wurden die Antworten von Teilnehmer aus Australien, UK und aus den USA berücksichtigt. Die ersten vier Hauptgründe waren in identischer Reihenfolge in den untersuchten Ländern gleich: große Auswahl an Drogen, höhere Qualität, Bequemheit des online Kaufes – wie auch im Fall von üblichen online Bestellungen – und die hohe Bewertung des Verkäufers. Relevante Aspekte waren noch die günstige Preise, die Vermeidung des physischen Treffens mit den Dealern, die fehlenden Kontakte und die Anonymität.[31]
Drogenhändler im Einzelhandelsbereich verkaufen die illegalen Waren mit geographischer Beschränkung. Die Drogen werden über mehreren Stationen, bzw. Ländern zu den Konsumenten transportiert. Aus dem Aspekt des Händlers hat das einerseits den Nachteil, dass die Aktivitäten von den weit entfernten Mitarbeitern nur schwierig kontrollierbar sind. Andererseits erscheint mit der Lieferung über längere Distanzen ein höheres Risiko der Entdeckung von Strafverfolgungsbehörden. Außerdem sind Käufer auf Händler vor Ort beschränkt und auch die Verfügbarkeit von Drogen und psychoaktiven Substanzen ist unterschiedlich. Es kann vorkommen, dass der gewünschte Drogentyp aufgebraucht ist, in diesem Fall sind Käufer gezwungen, entweder die neue Lieferung abzuwarten, oder einen anderen Händler aufzusuchen. Demgegenüber kennt das Vertreiben von illegalen Drogen auf anonymen Drogenmärkte keine geographischen Grenzen.[32]
Der niedrige Preis der online bestellten Drogen ist ein weiterer mit der Distanz zusammenhängender Aspekt. Beim traditionellen Drogenhandel erhöht sich der Preis von Substanzen je nach Stationen, allen weiteren Tätigkeiten (*z.B. Schmuggel, Lagerung*) ergeben die Steigerung des Verbraucherpreises. Dahingegen überspannen die anonymen Plattformen den großen Teil dieser Stationen, und dadurch erreichen die Verbraucher die Drogen billiger.[33]
Die Vermeidung des physischen Kontaktes zieht einen weiteren Faktor nach sich: die Gewaltlosigkeit. Bei dem offline Drogenhandel können verschiedene Konflikte entstehen: vor allem *Probleme mit der Ware, Betreibung von Schulden, Konkurrenz mit anderen Verkäufern, Diebstahl oder Bedrohung der Informatoren*. Die Lösung dieser Konflikte bringen bei dem Drogenerwerb auf der Straße leicht Gewalt mit sich. Natürlich entstehen auch in den anonymen Drogenmärkte Konflikte: z.B. wenn der Käufer nicht die erwartete Qualität ausgeliefert bekommt, wenn er nicht die bestellte Menge erhält, oder wegen fehlender Lieferung.[34] Auf Grund des fehlenden Treffens wird aber die Wahrscheinlichkeit der Gewalttaten gering. Für die Konfliktverwaltung im

[31] Barrat, Ferris, Winstock (2014)
[32] Tzanetakis (2019) p. 484.
[33] Kiss (2021) p. 272.
[34]Tzanetakis (2017) p. 193.

Kryptomarkt stehen allerdings vier Wege der Parteien zur Verfügung: die Teilnehmer können sich den Kontakt durch das Marktplatz-Messaging System miteinander aufnehmen. Eine andere Lösung – die nicht von jedem Kryptomarkt angeboten wird – ist das Support-Ticket System: in diesem Fall wird der Konflikt mit der Hilfe des Administrators geklärt. Außerdem haben die Parteien die Möglichkeit, den Konflikt in verschiedenen Foren veröffentlichen und darüber mit den anderen Benutzern diskutieren. Als vierter Kanal steht der Teilnehmer das automatische Feedback-System zur Verfügung. [35]

Obwohl die *Qualität* der auf Kryptomärkten verkauften Drogen nicht garantiert ist, gibt es bestimmte Merkmale der online Marktplätze, die die Wahrscheinlichkeit der Qualität erhöhen. Das bereits erwähnte Treuhandsystem von Kryptomärkten ist ein Faktor, der den Verkäufer motiviert, die bestmögliche Ware zu liefern. Eine andere Erklärung für die bessere Qualität kann das Feedbacksystem sein: die Kundenzufriedenheit und die abgegebene positive Bewertung des Verkäufers sind wichtige Motivationsfaktoren, zukünftige Kunden zu erwerben und aus diesem Aspekt hat das Niveau der erhaltenen Drogen eine relevante Bedeutung.[36] Die höhere Qualität der online bestellten Drogen gegenüber den „auf der Straße" gekauften Substanzen wurde durch eine anonyme Umfrage bestätigt: 72 bis 77 Prozent der 9.470 Befragten gaben an, dass Substanzen, die auf Silk Road bestellt wurden, höherwertig waren, als die ansonsten zugänglichen Drogen.[37] Anonyme Drogenmärkte schaffen eine direkte Verbindung zwischen den Händlern und Käufern. Bei dem materiellen Drogenmarkt hängt die Verfügbarkeit der Drogen stark mit dem Kontaktkreis des potentiellen Kunden zusammen. Wenn der Käufer keinen Kontakt zu Dealern hat, kommt die Transaktion gar nicht oder nur schwierig zustande. Demgegenüber ermöglichen online Drogenmärkte dem Käufer, ohne persönliche Kontakte erdenkliche Drogen zu erwerben. [38]

---

[35] Carlo Morselli, David Décary-Hétu, Masarah Paquet-Clouston, Judith Aldridge: Conflict Management in Illicit Drug Cryptomarkets. In: International Criminal Justice Review. 2017. p. 7. https://www.researchgate.net/publication/317242036_Conflict_Management_in_Illicit_Drug_Cryptomarkets heruntergeladet am 12.05.2022

[36] Judith Aldridge – David Décary-Hétu: Cryptomarkets: The Darknet As An Online Drug Market Innovation. Final report to NESTA. 2015. p. 22. https://daviddhetu.openum.ca/files/sites/39/2017/04/Nesta-Final-Report.pdf heruntergeladet am 14.04.2022

[37] Tzanetakis (2017) p. 193.

[38] Dési Ádám: A digitális bennszülött generáció és a kábítószer tudatosság. In: Válogatás a kriminológia és bűnügyi tudományok PhD szekció „MÉDIA ÉS ERŐSZAK" címmel rendezett konferenciáján elhangzott előadásokból. 2018. p. 96. https://www.kriminologia.hu/files/kiadvany/2018/krim78szamdr_desi_adam_a_digitalis_bennszulott_generacio_es_a_kabitoszer_tudatossag.pdf heruntergeladet am 21.03.2022

5. Zusammenfassung

Infolge der technologischen Innovationen, der von dem Internet ermöglichte Informationsverbreitung und der Vielfalt von sozialen Medien steht eine neue Plattform für Kriminellen zur Verfügung. Die Anonymität des Darkwebs bietet den Verbrechern einen Bereich, mit illegalen Waren und Dienstleistungen zu handeln und verbotene Inhalte zu teilen.
Das Darknet wird in der Fachliteratur als ein kleiner Teil des Deep Webs verstanden, der die Lokation und die Identität des Users verbergt und dadurch eine Anonymität beim Surfen versichert. Laut dem neutralen Begriff bezeichnet das Darknet *lediglich die Art und Weise des Zugangs (über eine Anonymisierungssoftware) und sagt nichts über den rechtlichen Status der Inhalte aus.* [39] Die verschiedenen Verschlüsselungssoftware und Kryptowährungen ermöglichen, dass die Kommunikation, bzw. Transaktionen zwischen dem Händler und Käufer nicht auf die Teilnehmer zurückführbar sind.
Zusammenfassend kann festgehalten werden, dass die anonymen Drogenmärkte gegenüber dem materiellen Drogenhandel viele Vorteile aufweisen. Ein wichtiger Aspekt ist unter anderem, dass die anonymen Plattformen den großen Teil der Stationen des traditionellen Drogentransportes überspannen, und dadurch erreichen die Verbraucher die Drogen billiger. Im Vergleich zum offline Drogenhandel kennt das Vertreiben von illegalen Drogen auf anonymen Drogenmärkte keine geographischen Grenzen. Ein weiterer bei der Verbreitung des online Drogenhandels spielende Faktor ist die Gewaltlosigkeit. Außerdem können die Käufer die Drogen im Darknet zu einem günstigeren Preis erwerben. Anschließend kann erwähnt werden, dass die anonymen Drogenmärkte einen direkten Kontakt zwischen den Händler und Käufer schaffen.

[39]Tzanetakis (2019) p. 479.

Literatur

- Afilipoaie, Alois - Patrick Shortis: From Dealer to Doorstep – How Drugs Are Sold On the Dark Net. https://www.swansea.ac.uk/media/From-Dealer-to-Doorstep-%C3%A2%C2%80%C2%93-How-Drugs-Are-Sold-On-the-Dark-Net.pdf heruntergeladet am 02.04.2022
- Aldridge, Judith – David Décary-Hétu: Cryptomarkets: The Darknet As An Online Drug Market Innovation. https://daviddhetu.openum.ca/files/sites/39/2017/04/Nesta-Final-Report.pdf heruntergeladet am 14.04.2022
- Aldridge, Judith – David Décary-Hétu: Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets" https://www.sciencedirect.com/science/article/pii/S0955395916301335#bbib0015. heruntergeladet am 10.04.2022
- Barrat, Monica – Jason Ferris – Adam Winstock: „Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States" file:///C:/Users/Heni/Downloads/1652550929685_2006095374.pdf heruntergeladet am 02.04.2022
- Bergmann, Jana: „Darknet Suchmaschinen" https://digital-hacks.de/darknet-suchmaschinen/ heruntergeladet am 20.05.2022
- Dési, Ádám: „A digitális bennszülött generáció és a kábítószer tudatosság" https://www.kriminologia.hu/files/kiadvany/2018/krim78szamdr_desi_adam_a_digitalis_bennszulott_generacio_es_a_kabitoszer_tudatossag.pdf heruntergeladet am 21.03.2022
- Eckerman, Ines Maria: „Was ist das Darknet?" https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet heruntergeladet am 16.03.2022
- Fulterer, Ruth: Hydra ist tot: Deutschland sperrt den grössten Darknet-Marktplatz der Welt. https://www.nzz.ch/technologie/deutsche-ermittler-schliessen-hydra-den-groessten-darknet-marktplatz-der-welt-ld.1678073?reduced=true heruntergeladet am 10.04.2022
- Kiss, Tibor: Miért népszerű a darknetes kábítószer-kereskedelem? https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/16609/web_PDF_NZs75.pdf?sequence=1 heruntergeladet am 20.03.2022
- May, Stefan: „Tor" in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets"

https://www.bpb.de/system/files/dokument_pdf/APuZ_2017-46-47_online.pdf heruntergeladet am 30.03.2022

- Morselli, Carlo – David Décary-Hétu – Masarah Paquet-Clouston – Judith Aldridge: „Conflict Management in Illicit Drug Cryptomarkets" https://www.researchgate.net/publication/317242036_Conflict_Management_in_Illicit_Drug_Cryptomarkets heruntergeladet am 12.05.2022
- Serbakov, Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. https://ujbtk.hu/dr-serbakov-marton-tibor-kriminalitas-a-dark-weben-illegalis-piacok-pedofil-oldalak-terroristak-es-az-ellenuk-valo-kuzdelem/ heruntergeladet am 13.03.2022
- Tóth, Dávid: Identity crimes on the darknet and the social media. https://ujbtk.hu/david-toth-identity-crimes-on-the-darknet-and-the-social-media/ heruntergeladet am 18.03.2022
- Tzanetakis, Meropi: „Drogenhandel im Darknet. Gesellschaftliche Auswirkungen von Kryptomärkten" https://www.bpb.de/system/files/dokument_pdf/APuZ_2017-46-47_online.pdf heruntergeladet am 30.03.2022
- Tzanetakis, Meropi: „Zur globalen Ökonomie von digitalen Drogenmärkten" https://www.researchgate.net/publication/323430078_Zur_globalen_Okonomie_von_digitalen_Drogenmarkten heruntergeladet am 17.03.2022
- Tzanetakis, Meropi: „Digitalisierung von illegalen Märkten. Folgen, Grenzen und Perspektiven" https://www.researchgate.net/publication/327966303_Digitalisierung_von_illegalen_Markten_Folgen_Grenzen_und_Perspektiven heruntergeladet am 20.03.2022
- Vári Vince: A bűnüldözés aktuális kihívása: az online kábítószerpiac https://drogkutato.hu/wp-content/uploads/2022/01/01-162_IDSZ-teljes_NET-139-161-1.pdf 17.03.2022
- Vogt, Sabine: „Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen?"
- Von Westernhagen, Olivia: „Seltsame Vorgänge bei Dream Market: Darknet-Marktplatz kündigt Schließung an" https://www.heise.de/newsticker/meldung/Seltsame-Vorgaenge-bei-Dream-Market-Darknet-Marktplatz-kuendigt-Schliessung-an-4355932.html heruntergeladet am 16.03.2022

Rohail Kasi
PhD Student (University of Pécs, Faculty of Law)

Right of Privacy Invasion by Social Media Applications

Abstract

My presentation would be about how various social media platforms such as facebook, instagram etc invade the right to privacy of its users by giving away the user information to various advertisement, government agencies without seeking consent.
Moreover my presentation would highlight how such data is used by Government agencies in keeping a close supervision on certain people, in shaping people's political opinions and in brainwashing users of such social media platforms.
Similarly by taking huge amounts of money from advertisements agencies, the social media platforms sells information about likes and dislikes of its users and such information is used by big companies to target such users to buy their products. Moreover, there is also high occurrence of highly sensitive data of users such as bank details and highly confidential data of users which is also leaked out.

1. Introduction

Social media has taken the center stage in everyday communication in this digital age. Social media platforms are becoming critical for every activity from business to entertainment and politics to economics. In the last two decades, these technologies have changed the world unprecedentedly, with billions of users across these platforms. Crucially, these platforms have enabled the democratization of knowledge, empowering individuals in ways previously unavailable. The expansion of broadband connectivity has increased internet users, providing opportunities for people to connect across the globe with their friends and family, even strangers in the world of dating apps, to share their lives. These social media platforms allow people to share their personal lives, associations, opinions, etc. With people sharing their lives through photos, videos, and opinions, these social networking platforms have access to huge amounts of sensitive information that would be regarded as private and not accessible to third parties. Hence, people trust these platforms that they will respect and protect their privacy.
However, this multi-dimensional use of these networking sites has also placed the privacy of users at risk, with the potential of data leaking to third parties.

The increase in users across these platforms has turned these sites into a medium with great business potential. Consequently, marketers use these platforms for advertising their products to their potential customers and expand their businesses. This could include these social media platforms selling their users' data to third parties to develop their business and target a potential customer segment. It could also include government access to individual data for surveillance, potentially undermining civil rights and liberties individuals enjoy. The breach of data privacy puts individuals at most risk when attackers with malicious intentions get access to sensitive data, such as private photos and videos, for illegitimate purposes. Therefore, these social media sites potentially make its users vulnerable to wide-ranging threats, which severely undermines the promise of empowerment these platforms provide.
The Right to Privacy is a fundamental human right. Despite the existence of international and national laws regulating digital media privacy, the privacy of individuals on the internet is breached continuously. The culprits include governments, law enforcement agencies, social media companies, data mining companies, corporations, marketing agencies, and cybercriminals. Therefore, the challenge of protecting individual's right to privacy, particularly on social media, is immense since it is under threat from all quarters. The most important role in this aspect is of civil society, which has to restrict all these actors from breaching individual privacy while also ensuring that social media continues with its promise of empowering people.

2. What is Social Media:

Social Media, in the simplest of terms, is an internet-based form of communication that allows people to connect across the globe to share information, communicate with friends and family, and forge new relationships, both personal and professional. The development of the internet has been a vital stage whereby ways of communication changed[1]. Traditional media such as newspapers, radio, and television were one-way communication channels. Two-way communication channels such as the telephone facilitated dyadic communication, i.e., interpersonal communication between two people[2].
The emergence of social media changed the entire spectrum of communication, enabling two-way communication between wider audiences, facilitating larger groups of people to “associate with each other to form social relations and

[1] Miller, Daniel, et al: What Is Social Media? In: How the World Changed Social Media: 1st ed., vol. 1, UCL Press, 2016, p. 2. JSTOR, https://doi.org/10.2307/j.ctt1g69z35.8. Accessed 31 May 2022.
[2] Miller, et al, (2016) p. 2

societies", a concept called "sociality"[3]. The remarkable aspect of social media is that it has added multimodality to sociability through the addition of images and videos, along with the text, creating a more connected world[4]. Thus, social networking sites have become integrated into our lives, without which we feel lost, and through smartphones, they are our constant companions[5]. Hence according to Schroeder, "our sociability is always on"[6].

There are numerous social media platforms, but the most prominent applications for sociability include Facebook, WhatsApp, WeChat, Instagram, Twitter, Snapchat, Tinder, YouTube, TikTok, and LinkedIn. Since the inception of the very first social media sites, there has been a proliferation of social media sites with differentiated content, targeting different segments of the population (Schroeder 2018, p. 86). Currently, there are more than 4.6 billion users across social media sites, representing a more than three times increase in the number of users in the last decade, i.e., from 2012[7]. There was a 10.1% year-on-year increase in social media users in 2021[8]. Jain et al. divide the social media sites into four broad categories: the first includes social connection site such as Facebook and Twitter to connect with people and brands; the second category include multimedia such as YouTube, Instagram, and Snapchat, where people and brands get a chance to share multimedia such as pictures and videos; third include professional social networking sites such as LinkedIn to facilitate connections between professionals; the fourth and the last types are discussion forums where people discuss topics and share opinions such as Reddit[9]. Although these are not neat distinctions between the usage of these platforms as they are used for multipurpose and may involve all types of activity on one platform, it helps to understand multiple ways in which social media platforms are used.

[3] Miller, et.al (2016) p. 3

[4] Schroeder, Ralph: The Internet in Everyday Life I: Sociability. In: Social Theory after the Internet: Media, Technology, and Globalization. UCL Press, 2018, p. 85. JSTOR, https://doi.org/10.2307/j.ctt20krxdr.7. Accessed 31 May 2022.

[5] Schroeder, (2018) p. 85

[6] Schroeder, (2018) p. 85

[7] Kemp, Simon: "DIGITAL 2022: GLOBAL OVERVIEW REPORT." In: DATAREPORTAL, 26 Jan 2022. https://datareportal.com/reports/digital-2022-global-overview-report. Accessed 30 May 2022.

[8] Kemp, (2020)

[9] Jain, Ankit Kumar, Somya Ranjan Sahoo, and Jyoti Kaubiyal: Online social networks security and privacy: comprehensive review and analysis. In: Complex Intell. Syst, 2021/7. pp. 2158–2159. https://doi.org/10.1007/s40747-021-00409-7.

3. Social Media and Digital Data Privacy:

Social Media applications have access to information about their users about almost everything. Sometimes these tech giants may know us more than our family, friends, and even in some situations, more than ourselves. These applications have data about our screen time, and attention on websites, our clicks, scrolls through our feeds, post likes, shares, comments, and the list goes on[10]. These companies even have access to sensitive information such as our driver's license number, social security number, credit/debit card details, and almost every possible information about us available on networking sites - and even outside it[11]. Hence, these companies have access to almost all our personal and professional life, including our behavioral data[12]. The data is then used for hyper-targeted advertisement campaigns based on our behavioral and engagement data through which these companies earn revenue.

These social media companies have access to information from more than 4.6 billion users. On Facebook alone, seven new profiles are created every second, 350 million pictures and 136,000 photos are uploaded every day, 510,000 comments are posted, and 298,000 statuses are updated daily[13]. Similarly, on Instagram, more than 500 million stories are posted each day, and more than 50 billion photos have been posted so far. The sheer amount of content posted on Facebook and Instagram represents the activity on only these two sites and thereby the user data the social media sites are entrusted with. Hence, with more than 4.6 billion users on social media sites, the amount of data these companies are entrusted with is unimaginable. With vulnerable internet security, one can only think of the havoc created if the data is used for malicious purposes, including surveillance, political manipulation, profiteering by corporations, and blackmailing by cyber security attackers.

4. Government Surveillance, Political Manipulation and Social Media Privacy:

Social Media is increasingly being used by governments and law enforcement agencies globally for surveillance. This undermines the civil rights and civil liberties of individuals who use these platforms for various purposes, including

[10] "Your Social Media Data: What's Collected and How is it Used?" In: juicer, 12 Jan 2021. https://www.juicer.io/blog/your-social-media-data-what-s-collected-and-how-is-it-used. Accessed 30 May 2022.

[11] Cyphers, Bennet: "A Guided Tour of the Data Facebook Uses to Target Ads." In: Electronic Frontier Foundation, 24 Jan 2019. https://www.eff.org/deeplinks/2019/01/guided-tour-data-facebook-uses-target-ads. Accessed 30 May 2022.

[12] "Your Social Media Data: What's Collected and How is it Used?", (2021)

[13] Jain et. al, (2021) p. 2159

criticizing government policies and actions. Surveillance of social media platforms is justified in the name of "enhanced security, limiting disinformation, and ensuring public order", increasingly governments are instituting advanced social media monitoring programs to track users and suppress dissent[14]. According to Freedom House, 89% of internet users, around 3 billion users, were monitored in 2019[15].

China is the leading country that employs the most sophisticated monitoring social media systems in the world, which are aimed at restricting dissent and controlling people's identities. Other countries in Asia, including Vietnam, Pakistan, and Bangladesh, employ sophisticated social media surveillance systems to crackdown on freedom of speech, crack dissent, and even manipulate political outcomes[16]. This monitoring is not limited to authoritarian regimes in the Middle East or Africa but includes liberal democracies such as the United States and the UK. These surveillance programs were used in these countries initially for combating terrorism and serious crimes such as narcotics control and child abuse[17]. However, they are increasingly being used to monitor activists and protestors, screen political views of travelers, and track the students[18]. The increasing surveillance by authoritarian and democratic regimes alike has reprehensible impacts on fundamental freedoms, forcing journalists and activists into self-censorship, while those who continue to express their opinions will face political victimization.

It is not only the governments that are instituting these social media programs to track and suppress dissent, but PR firms associated with politicians are also using social media user data for political purposes. Tech Companies are involved in privacy data breaches by giving user information to these firms. In 2018, Facebook provided access to the personal information of 87 million users to Cambridge Analytica, a data-mining firm associated with Donald Trump's political campaign[19]. This data privacy breach allowed the firm access to information about the American electorate that it used for developing techniques for Trump's Electoral Campaign in 2016[20]. The techniques involved

[14] Shahbaz, Adrian and Allie Funk: "Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance." In: Freedom House. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance. Accessed 31 May 2022.

[15] Shahbaz and Funk

[16] Shahbaz and Funk

[17] Shahbaz and Funk

[18] Shahbaz and Funk

[19] "Social Media Privacy." In: epic. https://epic.org/issues/consumer-privacy/social-media-privacy/. Accessed 30 May 2022.

[20] Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr: "How Trump Consultants Exploited the Facebook Data of Millions." In: The New York Times, 17 Mar

targeted advertising campaigns on Facebook to support Trump, and this was highly effective as Trump's head of digital Media Strategy, Brad Parscale, expressed that these Facebook ads were 100 or 200 times more cost-effective than Hillary Clinton's campaign[21]. The main concern with this data privacy breach is the possibility of distorting democratic discourse through using social media personal data[22].

5. Social Media Data and Advertisement Targeting:

The large swaths of data collected by social media companies are used for micro-targeting users for advertisement campaigns. In the growing world of e-commerce, the behavioral data of users collected through a web of tracking techniques that follow users across the web is becoming increasingly profitable for Social Media Companies such as Meta, the parent company of Facebook, Instagram, and WhatsApp. With companies trying to expand their customer base, these social media firms can earn massive revenues from advertisers willing to pay substantial sums of money for highly selective advertisement campaigns.

Social Media user Data is used by both the social Media Companies themselves and the big data mining companies like Cambridge Analytica. The platforms develop behavioral profiles of their users through algorithmic mining of every single activity. These profiles are then used for targeted advertising campaigns to these users where advertisement companies pay substantial amounts to the Social Media Companies[23]. Similarly, data mining companies access public user data on social media platforms and then analyze the data for developing targeted marketing campaigns and effective marketing strategies[24].

Although the use of user data to entice them into particular consumer patterns is an area of concern but the real worry is when social media companies sell the private data to corporations for profits. A series of internal Facebook emails

---

2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed 31 May 2022.

[21] Ghosh Dipayan and Ben Scott: "Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You." In: TIME, 19 Mar 2018. https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/. Accessed 31 May 2022

[22] Dipayan and Scott, 2018

[23] Leetaru, Kalev: "What Does It Mean For Social Media Platforms To "Sell" Our Data?" In: Forbes, 15 Dec 2018. https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=3891cf002d6c. Accessed 30 May 2022

[24] Neisz, Marley. "The Impact of Data Mining on Data Marketing." In: Corporate Communications Group, 18 Nov 2020. https://ccgcreates.com/the-impact-of-data-mining-on-marketing/. Accessed 31 May 2022.

released by the British Parliament in 2018 highlighted how the company intended to monetize profits by selling user data to app developers, although it did not pursue the idea[25]. The emails also demonstrated how the company dehumanized the platform "users" by treating them as mere data points, in contrast to their public statement where they go to great lengths to show their regard for the "people" using the platforms[26]. An investigation by New York Times in 2018 revealed that Facebook had given access to its users' private data that included private contact details and activities of friends to other tech firms, such as Amazon, Apple, Microsoft, and Netflix[27]. The revelation came in despite Facebook claiming in 2015 that it had stopped third parties from tapping into user data[28]. Therefore, the practices of social media companies are questionable, and it seems that although the use of the web is free, people pay in terms of breach of their privacy.

6. Cyber Security Attacks and Digital Media Privacy Breach:

The data of social media users, even if protected from government surveillance and for minting by social media companies through selling the data, there is still a great susceptibility to privacy breaches through cyber-attacks. The amount of personal data posted by people on these platforms face serious risks from intruders who try to extract information and possibly harm them. There are a series of possible cyber attacks, including traditional and modern attacks. Traditional methods include spam attacks, malware attacks, phishing, and identity attack[29]. The latter two are more dangerous since attackers could impersonate an authentic user and then get access to victim's family and friend list and their confidential information[30]. Cyber security attacks are not limited to traditional methods but evolve with growing technology. This could include hijacking their profiles, using data mining methods on public data available on profiles, and getting access to the location or educational data about the user, which could also put user's physical security in danger[31]. These social platforms are also increasingly becoming sites for cyberbullying and cyberstalking, where attackers harass individuals through intimidating messaging and cyber presence to compel them to perform the tasks[32]. The vulnerability of cyber attacks on social media platforms, particularly on an

[25] Leetaru, (2018)
[26] Leetaru, (2018)
[27] "Facebook's data-sharing deals exposed." In: BBC, 19 Dec 2018. https://www.bbc.com/news/technology-46618582. Accessed 31 May 2022.
[28] "Facebook's data-sharing deals exposed." (2018)
[29] Jain et. al, (2021) p. 2163
[30] Jain et. al, (2021) p. 2162
[31] Jain et. al, (2021) p. 2164
[32] Jain et. al, (2021) p. 2165

individual level, is high because it is extremely difficult for security teams to track the activity of all users, hence increasing the likelihood of targeted attacks on an individual or a group of people that could be in thousands.
In early 2017, a Russian cyber attack targeted 10,000 social media users with a phishing/malware attack that allowed attackers to access and control victims' devices[33]. Social Media websites, even though have stringent cyber security protocols, yet they are still susceptible to hacking, as was the case with LinkedIn 2016, where the credential of 117,000 users was compromised[34]. One of the most rampant cyber security attacks includes financial crimes where attackers target financial institutions through various digital channels, including social media, resulting in the loss of millions of dollars. In 2021, financial institutions were targeted the most among the enterprises that faced cyber attacks through social media. Each social media platform is vulnerable to cyber attacks, but targeting methods on each platform vary, and with billions of users, it becomes extremely challenging to monitor suspicious activities despite all the security protocols.

7. Recommendations: Protecting the Right to Privacy in the Digital Age:

The spurt of digital media has played a significant role in socio-economic progress in the world in the past two decades. It has provided a platform that has empowered billions of people. It contributes to the economic, social, and political empowerment of people. However, it has also enabled an unprecedented state and capitalistic control over the population. The most challenging aspect of digital media is protecting individuals' right to privacy when it is threatened from almost all quarters, including governments and law enforcement agencies, corporations and marketing agencies, and cyber security attackers.
The Right to Privacy is considered an individual human right deserving legal recognition and protection. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) embodies the right to privacy[35]. However, the growth of technology is making it difficult to protect the right to privacy as legislation is developed as a response to new challenges posed to the right to privacy by technological innovation[36]. Hence, legislations are always catching

[33] Wolfe, Spencer: "The Top 10 Worst Social Media Cyber-Attacks." In: Infosecurity Magazine, 20 Oct 2017. https://www.infosecurity-magazine.com/blogs/top-10-worst-social-media-cyber/. Accessed 31 May 2022.
[34] Wolfe, Spencer: "The Top 10 Worst Social Media Cyber-Attacks."
[35] Rengel, Alexandra: Privacy as an International Human Right and the Right to Obscurity in Cyberspace. In Groningen Journal of International Law, 2014/2. pp. 40. https://grojil.files.wordpress.com/2015/04/grojil_volume-2_issue-2.pdf.
[36] Rengel, (2014) p.49

up with technology. Therefore, there are always gaps in protecting the right to privacy. Add to it the fact that all social media platforms get permission from users to get access to the information on their devices, which in legal terms legitimizes the collection of user data even on wider internet and general internet usage.

Therefore, protecting the right to privacy requires an outward forward-looking approach that anticipates the impact of technological innovation on the right to privacy. Therefore, the measures taken to protect digital media privacy should be right-based and user-centered and aim to promote the promise of social media for the empowerment of people while simultaneously protecting their fundamental Right to Privacy. This is critical for the democratic progress of the world. Henceforth, the following recommendations are suggested to protect the individuals from the breach of their private data, with Civil Society having the most critical role to play in the protection of privacy in the digital world:

1. The business of social media companies should be strictly regulated with clearly defined implications, including legal actions, fines, and bans if the abuse of data privacy is established. This also requires government regulatory authorities to be more efficient and effective, keeping a stringent check on the social media companies.
2. Civil Society and digital rights activists must raise awareness among people about the information collected by social media companies to enable people to develop a more cautious approach when posting sensitive information on the internet.
3. Regulations should be made where these platforms are required to explicitly and boldly inform the users they will be collecting when the user signs up for using the platform. These companies should not force users to accept its privacy conditions or else not be able to use the service. This is illegitimate and legal actions should be taken against the companies.
4. Regulations should also be made for data collection by data mining companies of public data on profiles, ensuring no user data is collected without explicit approval.
5. The most challenging aspect is preventing and restricting government and law enforcement agencies from surveilling people on social media and using it to suppress dissent. Civil Society along with rights advocacy groups, should raise awareness among the people about how they are being monitored.

8. Conclusion

The great promise of empowering people through social media comes along with the perils of civil rights and liberties, particularly the right to privacy and

freedom of speech. The breach of the right to privacy is practiced by almost all actors, including state and private actors, for monitoring people, advertisement targeting, and cybercrimes. The protection of rights requires traditional approaches, such as improving legislation and effective regulation of the internet through improving cyber security, and non-traditional approaches, including raising awareness among people about their right to privacy on digital platforms and requiring social media companies to explicitly require permission for collection of data, albeit only for using restricted purposes. The ultimate objective is ensuring that digital media continues to be empowering for people, while their fundamental rights including right to privacy is protected.

Bibliography

- Cyphers, Bennet: “A Guided Tour of the Data Facebook Uses to Target Ads.” In: Electronic Frontier Foundation, 24 Jan 2019. https://www.eff.org/deeplinks/2019/01/guided-tour-data-facebook-uses-target-ads. Accessed 30 May 2022.
- Ghosh Dipayan - Ben Scott: “Facebook’s New Controversy Shows How Easily Online Political Ads Can Manipulate You.” In: TIME, 19 Mar 2018. https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/. Accessed 31 May 2022.
- Jain, Ankit Kumar - Somya Ranjan Sahoo, - Jyoti Kaubiyal: Online social networks security and privacy: comprehensive review and analysis. In: Complex Intell. Syst, 2021/7. pp. 2157–2177. https://doi.org/10.1007/s40747-021-00409-7.
- Kemp, Simon: “DIGITAL 2022: GLOBAL OVERVIEW REPORT.” In: DATAREPORTAL, 26 Jan 2022. https://datareportal.com/reports/digital-2022-global-overview-report. Accessed 30 May 2022.
- Leetaru, Kalev: “What Does It Mean For Social Media Platforms To "Sell" Our Data?” In: Forbes, 15 Dec 2018. https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=3891cf002d6c. Accessed 30 May 2022.
- Miller, Daniel, et al: What Is Social Media? In: How the World Changed Social Media: 1st ed., vol. 1, UCL Press, 2016, pp. 1–8. JSTOR, https://doi.org/10.2307/j.ctt1g69z35.8. Accessed 31 May 2022.
- Neisz, Marley. “The Impact of Data Mining on Data Marketing.” In: Corporate Communications Group, 18 Nov 2020. https://ccgcreates.com/the-impact-of-data-mining-on-marketing/. Accessed 31 May 2022.
- Rengel, Alexandra: Privacy as an International Human Right and the Right to Obscurity in Cyberspace. In Groningen Journal of International Law, 2014/2. pp. 33-54. https://grojil.files.wordpress.com/2015/04/grojil_volume-2_issue-2.pdf.
- Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr: “How Trump Consultants Exploited the Facebook Data of Millions.” In: The New York Times, 17 Mar 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed 31 May 2022.

- Schroeder, Ralph: The Internet in Everyday Life I: Sociability. In: Social Theory after the Internet: Media, Technology, and Globalization. UCL Press, 2018, pp. 82–100. JSTOR, https://doi.org/10.2307/j.ctt20krxdr.7. Accessed 31 May 2022.
- Shahbaz, Adrian - Allie Funk: "Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance." In: Freedom House. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance. Accessed 31 May 2022.
- Wolfe, Spencer: "The Top 10 Worst Social Media Cyber-Attacks." In: Infosecurity Magazine, 20 Oct 2017. https://www.infosecurity-magazine.com/blogs/top-10-worst-social-media-cyber/. Accessed 31 May 2022.

Thai Van Ha
PhD Student (University of Pécs, Faculty of Law)

The Fight Against Money Laundering and Terrorist Financing in the Digital Age

Abstract

While advancements in technology such as the internet and social media have brought about enormous positive changes in our lives, they have also facilitated the growth of an environment that is more receptive to illegal behaviour. The use of the internet not only makes it possible for criminals to commit cybercrimes like financial fraud, but it also makes it possible for them to launder the money they get from their illegal activities, which enables them to keep going and even expand their businesses. Cybercriminals are able to target victims all over the world thanks to the anonymity, speed, and ease offered by the internet and other information and communication technologies. This makes investigations more difficult and generates cross-jurisdictional concerns.
This study aims to explore the nature of the problem, as well as emerging challenges, and contextual issues connected to the use of information and communication technologies to facilitate money laundering and the financing of terrorism.

Keywords: Money laundering, terrorist financing, cybercrime, anti-money laundering, FATF

1. Introduction

One of the most significant shifts in the structure of the international monetary system over the past decade has been the introduction of new technology, products, and services related to this sector. Although these new technologies, products, and related services have the potential to stimulate financial innovation and efficiency, as well as increase financial inclusion, they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illegal activities.
Despite its characteristics have remained unchanged, the phenomenon of money laundering has evolved over time with the development of technology. Using digital technology to conceal and transfer money while employing ever more sophisticated and convoluted methods has transformed the illegal activity of money laundering into a global problem. In general, there are three stages

involved in the process of money laundering; but it is still impossible to monitor all money transfers, discover the identities of the true holders of each transaction, and figure out what their true objectives and purposes are.

2. Money laundering and terrorist financing concepts

Money laundering is one of the economic crimes. The United States of America officially acknowledged it as a separate criminal violation for the first time in the early 1980s, in conjunction with the expansion of illegal drug trafficking and the earnings from it. Over time, modifications have been made to anti-money laundering laws as a direct result of changes in the socioeconomic and political context. These modifications were made in an effort to provide a more appropriate response to emerging problems. Due to the linked nature of money laundering and financing of terrorism, both of these types of criminal activity were brought under the scope of anti-money laundering laws after the 9/11 attacks in the United States.

In general, money laundering is the process by which the proceeds of crime are made to look legitimate. The primary objective of money laundering is to facilitate the transfer of funds, the remittance of money, the concealment of the money's illicit origin, and its reintroduction into the legal economic system so that the money launderer can enjoy the benefits without fear of being prosecuted. In other words, money laundering simply refers to concealing the source of money due to its criminal origins.

One of the most difficult tasks of analysis is the calculation of the money laundering value. Although it is claimed to be the third biggest industry in the world, estimating the extent of the issue has proven extremely complicated and produced controversial results. For instance, according to the estimates provided by the International Monetary Fund (IMF), the market for money laundering accounts for between 2 and 5 percent of the world's Gross Domestic Product (GDP). This results in an estimate that falls somewhere in the range of $600 billion and $1.5 trillion.[1] This estimate coincides with the findings presented in the report compiled by Price.[2] In 2009, the United Nations Office on Drugs and Crime (UNODC) estimated that money laundering accounted for 2.7 percent of worldwide GDP, which is equivalent to US$1.6 trillion. This figure is supported by The Financial Action Task Force

[1] Lilley, Peter: Dirty dealing: the untold truth about global money laundering, international crime and terrorism. Kogan Page Publishers, 2003.

[2] Price, A: Anti-money laundering: Reconsidering the risks. Ernst& Young, 2002.

(FATF).[3] But less than one percent of the world's illegal financial flows are being seized, frozen, or otherwise confiscated.[4]

Generally speaking, there are three stages involved in the process of laundering money: placement, layering, and integration. The first step, which is known as placement, refers to the point at which the currency is introduced into the retail market or the financial system. The goals of the launderer are to first remove the cash from the place where it was originally stashed in order to escape detection by the authorities, and then to later convert the cash into other forms of assets. The next stage, namely layering, is where the origin of the actual ownership of the funds is concealed or otherwise disguised. In order to accomplish this, criminals create complicated and complex layers of financial transactions. They do that in order to separate the illegal cash from the activity that originally generated it. The final process is the integration, where the money is integrated into the legitimate economic and financial system. At this stage, money appears to have been legally earned. At this stage, it is extremely difficult to distinguish between legal and illegal assets.[5]

Money laundering can have negative effects on both the economy and society.[6] Due to the impossibility of accurately estimating the scope of money laundering, it is also impossible to determine its effects. Money laundering poses a potential risk to the proper functioning of market processes and can undermine the competitive environment among legitimate businesses. It is possible that the prevalence of money laundering will lead to an increase in the incidence of other forms of criminal activity. Money laundering provides fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal activities.

The funding of terrorist activity by terrorist finance. It may entail funds from legal sources, such as personal donations and revenues from businesses and charitable organisations, as well as illegal sources, such as drug trafficking, fraud, smuggling of guns and other products, kidnapping, and extortion. Terrorists employ procedures similar to those of money launderers in order to elude authorities and conceal the identities of their sponsors and the final recipients of the funds. If criminal gains are used to fund terrorist activities, there is a direct link between terrorist funding and money laundering.

---

[3] United Nations Office on Drugs and Crime: Illicit money: how much is out there. 2011. Available: https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html

[4] United Nations Office on Drugs and Crime, 2011.

[5] Buchanan, Bonnie: Money laundering - a global obstacle. In: Research in International Business and Finance, 2004/1. pp.115-127.

[6] McDowell, John, and Gary Novis: The consequences of money laundering and financial crime. In: Economic Perspectives, 2001/2. pp.6-10.

3. Money laundering and terrorist financing in the digital age.

Technological advancements and the introduction of virtual money have posed a new challenge to anti-money laundering (AML) and counter-terrorist financing (CFT) regulation. With the technological evolution of the payment system, particularly the global banking and financial system, there have been various cycles of evolution, such as the transition from cash to the use of prepaid cards or the introduction of electronic payments. The ability of criminal organizations to exploit legislative and operational flaws to acquire illicit economic benefits has likewise evolved through time.

The presence of cyber technologies that contribute to money laundering at all three stages and provides a new perspective. In the placement stage, one of the most essential roles played is that of electronic money, which is the primary form of cash used in the online environment in order to carry out transactions. Cyber-launderers can use electronic money to conduct transactions on the Internet in order to purchase foreign currency or valuable assets, which they can then resell for a profit. When conducting transactions, the use of electronic money eliminates the requirement for the people involved to be physically present. This also eliminates the risk of someone snatching cash. After this step, the layering process begins, in which the cyber-launderers spend the money that was deposited through a series of transactions in an attempt to remove the funds from the source of the illegal activity.

The process of layering might involve activities such as transferring money from one offshore account to another and purchasing things with the intention of later reselling them. Utilizing the Internet at this point in the process is by far the most practical approach to making the laundering process easier. Because the movement of funds takes place in virtual space in a fraction of a second, cyber-launderers are able to establish an extensive chain of operations in a short period of time. Additionally, the transactions can be carried out through a multi-jurisdictional financial system, which makes it difficult for regulators in one country to identify the relationship between transactions that took place in other jurisdictions.[7]

At the final stage of integration, cyber-launderers perform the final processes that allow them to fully legalise cash. At this step, the commonly accepted laundering mechanism is the use of invalid invoices for various items or services offered. It is apparent that the possibility of illegally exploiting these new opportunities has grown significantly.[8]

---

[7] Philippsohn, Steven: Trends in cybercrime - An overview of current financial crimes in the Internet. In: Computers & Security, 2001/1, pp. 53-53.

[8] Hugel, Paul, and Joseph Kelly: Internet gambling, credit cards and money laundering. In: Journal of Money Laundering Control, 2002, pp. 57-65

In today's data-driven financial ecosystem, cyber crime has emerged as a major issue for authorities, with criminals using computer systems and online financial services to commit money laundering, fraud, and other crimes. While cyber crime cost the global economy roughly $3 trillion in 2015, that figure was expected to climb to $6 trillion by 2021. Over the next five years, the cost of cyber laundering is predicted to rise by almost 15% every year, reaching over $10.5 trillion in 2025.[9] According to a 2017 survey, the Asia Pacific region is increasingly being targeted by fraud, with a 35% increase in cybercrime per year, with a concentration on account takeovers and payment fraud. Mobile devices account for one-third of all transactions.[10]
On the other hand, terrorism has also gone through significant changes over the years, notably with regard to the issues of propaganda aimed at personal recruitment and terrorist finance, both of which are of greater concern to the international community as a whole. Cyberterrorism activities that are used as tools include things like spreading terrorist propaganda to recruit new members. Social media, private or encrypted messaging channels are also used to organise criminal and terrorist actions. Another type of cyberterrorism activity is the financing of terrorism, such as when illegal money is collected online to buy money, weapons, drugs, and supplies for a terrorist action.

4. The challenges posed by cyber laundering and cyber financing terrorism.

It is widespread practice to engage in the activity of cyber-laundering over the Internet. This involves utilizing particular pieces of hardware and software in order to establish connections in anonymity and non-traceability of one's location. This is done in order to deceive law enforcement officials. The term "cyber laundering" refers to the practice of moving illegal financial transactions into the online realm using various forms of information technology and the Internet. In addition, the constant development of computer systems brings forth new security concerns, which may make it easier for money launderers to take advantage of these systems.[11] Because of its speed, ease of access, anonymity, and lack of geographical boundaries, the Internet is frequently exploited for the purposes of money laundering and financing terrorist organisations. Because of these traits, thieves are able to conduct any

[9] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
[10] https://www.newsmaker.com.au/news/268855/asia-pacific-cyberattacks-up-35-year-on-year-as-global-organized-fraud-rings-turn-their-attention-to-emerging-financial-services#.Ypxr8CtBzIU
[11] Granville, Johanna: Dot. con: the dangers of cyber crime and a call for proactive solutions. In Australian Journal of Politics & History, 2003/1, pp.102-109.

transaction without being able to identify the person or parties that are participating in the transaction.

4.1. The ease and speed of transaction

Virtual environments and digital currencies have become a challenge for governments (such as counter-terrorism agencies) and security experts because of the ease with which money launderers and terrorists can use them in the absence of traditional financing sources. Many legal experts believe that the country's rapidly expanding economy could provide a haven for money launderers, fraudsters, and terrorists to hide and move money around without being observed in the real world. Some argue that money laundering in the virtual environment is a real threat that demands regulation similar to that in the real world.[12]

The ease with which massively multiplayer online games can be utilized for economic crimes such as money laundering, fraud, and terrorism financing is also an increasing concern.[13] Many believe that there is a possibility and opportunity to permit the movement of significant sums of money across international borders without restrictions and with minimal danger of detection. There is a clear consensus of opinion that virtual environments are a possible target for cybercriminals, money launderers, and terrorist financiers.

4.2. The transnational nature of cybercrimes

An individual in one country may commit a crime by using an online platform hosted in another jurisdiction to conduct an offence in a third jurisdiction. Investigating cybercrime, money laundering, and terrorist financing necessitates significant international collaboration among jurisdictions linked by geography and information systems. Because jurisdictional borders are permeable while dealing in cyberspace, international coordination and cooperation are critical in combating cybercrime. Investigations into cybercrime, internet-facilitated money laundering, and terrorist financing necessitate close collaboration with the commercial sector. The private sector's online infrastructure is not generally built with security and collaboration with law enforcement authorities as top priorities. Instead, cooperative approaches to gaining mutual assistance from among partners helps to deal with the cybercrimes.

---

[12] Jones, Clare: Can You Ever Regulate the Virtual World Against Virtual Economic Crime?. In Journal of International Commercial Law and Technology, 2012/4, pp.339-349.

[13] Sullivan, Kevin: Virtual Money Laundering and Fraud - Second Life and Other Online Sites Targeted by Criminals, 2008. Available at: https://www.bankinfosecurity.com/virtual-money-laundering-fraud-a-809

Furthermore, an increasing number of money laundering cases involve persons and legal entities from several nations, as well as methods and instruments applicable to a number of governments and self-governing territories. Transnational criminal organisations take advantage of differences in national laws to launder money as quickly and easily as possible. They also use new technology and ways to communicate in a big way.

4.3. Anonymity

The absence of physicality in Internet-based activities represents a new approach to daily routines and presents an opportunity for new money laundering techniques. Using the Internet does not require the user's true identification. Consequently, a great degree of anonymity is achievable. Studies have shown that the anonymity afforded by virtual surroundings is another factor that contributes to the attraction of these settings for engaging in illegal activity. With the emergence and growth of online commercial and financial services, criminals have had greater opportunities to derive profits from online fraud, so there is a greater need to conceal the source of their illegal funds. Computers and computer systems offer money launderers a degree of anonymity and the opportunity to move illegal funds quickly between accounts while avoiding the customer due diligence and transaction monitoring checks that conventional AML/CFT systems would normally impose. Cybercrime differs from traditional crimes in many different ways, including its universality and complexities, in particular, its anonymity, concealment, and invisibilities. The anonymity of cyberspace makes identity tracing a noteworthy predicament, which poses obstacles to detection and investigations.[14]

4.4. The lack of sufficient legislation

There may not be enough regulation or aspects of associated technological advancements to tackle cybercrime. The nature of the cyber threat is continuously shifting in response to advances in technology, and cybercriminals are also continually adapting their methods. 15 Another weakness of the legislation is that there are no "red flag" indicators included. These are indicators that might potentially alert service providers, investigators, and law enforcement agencies to the presence of behaviour that constitutes cyber laundering or financing of terrorism. Indicators that raise a red flag are an important tool that can assist service providers, investigators, or

[14] Yar, Majid, - Kevin F: Steinmetz. Cybercrime and society. Sage, 2019.
[15] Emerson, R. Guy: Limits to a cyber-threat. In: Contemporary Politics, 2016/2, pp.178-196..

law enforcement agencies in determining whether a particular activity or the financial transactions carried out by an account holder or entity are normal or vary from normal activity and require further investigation. Investigations into classic forms of money laundering and the financing of terrorism typically involve the identification of a number of warning signs and indicators. This will also be the case for online money laundering or the financing of terrorist activities. It's also possible that law enforcement authorities don't have enough experience to properly investigate online crimes. A lack of coordination on the domestic level between the law enforcement authorities that are responsible for investigating cybercrime and money laundering might make this situation even more problematic.

5. FATF and anti-money laundering

The first international regulations on money laundering can be found in the United Nations (UN) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (or Vienna Convention in 1988), and the UN Convention against Transnational Organised Crime (or Palermo Convention in 2000). The Vienna Convention of 1988 is still only applicable to the laundering of drug manufacturing and sales revenue.[16] The Palermo Convention of 2000, which expanded the definition of money laundering offences to include the proceeds of severe crimes, marked a significant shift in the UN strategy. By creating a foundation for more effective coordinated national laws against money laundering, this Convention increases the government's ability to combat severe crimes. In addition, the UN Convention on Corruption was established in 2003. A step forward in the UN's fight against money laundering is the adoption of an all crimes approach to money laundering offences.
The Financial Action Task Force (FATF) is an independent inter-governmental body that was created in 1989 in Paris. The FATF is recognised as an inter-governmental body, which is to set international standards and promote effective implementation of legal, regulatory, and operational measures specifically towards money laundering and terrorist financing. One year after its establishment, the FATF issues 40 recommendations which are recognised as the global AML/CFT standards. The Recommendations have been amended several times, but most notably in 1996, 2001, 2003, and 2012. The biggest change to the recommendations came in 2001, when eight special recommendations were introduced to combat terrorist financing following the terrorist attacks in September 2001. A ninth special recommendation was

[16] Ryder, Nicholas:Money Laundering-an Endless Cycle? A Comparative Analysis of the Anti-money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada. Routledge, 2012.

introduced in 2004, and all nine have subsequently been incorporated into the most recent set of 40 recommendations.[17]

The FATF Recommendations are a dynamic instrument that adapts in response to shifting global threats, vulnerabilities, and dangers related to money laundering and terrorist financing, as well as to difficulties encountered during implementation. Customer due diligence (CDD) and related processes have significantly improved transaction transparency and made it more difficult for criminals and terrorist funders to abuse the financial system. However, while being a crucial component of the AML/CFT system, CDD still faces implementation and effectiveness issues.[18]

The FATF promotes a "risk-based approach" to prevent and detect money laundering. A risk-based approach means "enhanced CDD measures have to be taken" in higher risk circumstances.[19] The FATF provides guidance for determining such circumstances; customer risk factors include whether the business relationship is conducted in unusual circumstances, whether the customers are from foreign jurisdictions, or whether the businesses are excessively complex given the nature of the company's business. The risk-based approach is fundamental to the effective execution of the amended FATF Standards on Combating Money Laundering, the Financing of Terrorism, and Proliferation, which FATF members adopted in 2012. Thus, the FATF actively monitors the risks associated with new technologies. The FATF takes into account country or geographic risk factors, such as nations designated as lacking effective AML procedures, countries subject to sanctions, and countries identified as having high levels of corruption or other criminal activity.

Recommendation 1 of the 40 recommendations states that members are required to perform regular risk assessments, because money launderers will utilise whatever methods they can, and will naturally target weaknesses. The risk-based approach recognizes that it is impossible to pursue money laundering without focusing on the circumstances in which it is most likely to occur.

[17] Financial Action Task Force: What do we do. Available at: https://www.fatf-gafi.org/about/whatwedo/

[18] Financial Action Task Force : Opportunities and Challenges of New Technologies for AML/CFT. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf

[19] Demetis, Dionysios S: Technology and anti-money laundering: A systems theory and risk-based approach. Edward Elgar Publishing, 2010.

6. Suggestions to combat money laundering and terrorist financing in the digital age

Internet banking, mobile payment systems, and other forms of digitalization are becoming increasingly popular. High rates of technological advancement and the introduction of new technologies in all spheres of human activity, including the activities of financial agencies, provide criminal organisations, groups, and individuals with the opportunity to circumvent the conventional money laundering schemes that are already being monitored by national and international control bodies. The fight against money laundering and terrorist financing in the digital age need to take into account the following issues:

6.1. Improving the legal norms in combating money laundering and terrorist financing

There is an obvious need to develop international legal standards applicable not only on a national or regional scale, but also to the entire world community. Given the fact that the global community is now unable to effectively combat Internet-based money laundering and terrorist funding, it is imperative that a regulatory framework be developed to tackle this crime. The scale of the threat is very great, and therefore action is required to develop legal measures that could eliminate both existing and possible danger. Cooperation between governments, and international and regional organisations is therefore essential.

Research has shown that efficient legal systems and sound banking systems are important for curbing money laundering activities. The FATF Standards contain requirements such as: The criminalization of money laundering and the funding of terrorism; Freezing and confiscation of the proceeds of crime; Know your customer (KYC) regulations and procedures to prevent criminals or terrorists from becoming customers of or conducting business with private sector and regulated enterprises such as banks and investment firms; Monitoring procedures designed to detect suspicious transactions based on KYC data; Reporting by the private sector of questionable transactions and other financial information, such as significant cash deposits and foreign wire transfers; and The analysis of reports filed by regulated entities, and the dissemination of the analysed data to local and international law enforcement and regulatory agencies.[20] All of these steps may aid the investigation and prosecution of money laundering and terrorist financing, as well as the freezing, confiscation, and repatriation of criminal proceeds. AML requires the collection and analysis of vast quantities of financial data and results in a significant improvement in financial transparency. Thus, increasing the

[20] Alexander, Kern: The international anti-money-laundering regime: the role of the financial action task force. In: Journal of Money Laundering Control, 2001/3, pp.231-248.

effectiveness of national and international AML systems helps to enhance the likelihood of detecting instances of money laundering. This approach is also true for the cyber laundering and cyber financing of terrorism.

6.2. Enhancing the customer due diligence process

Banks, financial institutions, and other financial service providers must verify the identities of their customers and the nature of their business through the CDD process in order to comprehend the money laundering threats that financial systems confront. CDD refers to the act of gathering identifying information in order to authenticate a customer's identification and estimate their level of criminal risk more precisely. On a fundamental level, CDD requires businesses to gather a customer's name and address, as well as information about their business and account usage. Companies should next verify this information using official documents such as driver's licenses, passports, bills, and incorporation paperwork to guarantee that clients are being truthful. CDD is the core of the KYC process, which requires businesses to have a deeper understanding of their customers, their financial activity, and the danger of money laundering or terrorism financing that they may pose. In accordance with Recommendation 10 of the FATF's 40 recommendations, all FATF member states must include CDD regulations into their domestic AML/CFT law.

In addition, to assist commercial websites and internet payment service providers in mitigating the danger of criminal behaviour, there is also a need for online identity verification solutions, such as the electronic identity cards used in certain jurisdictions. If internet payment service providers adequately monitor their clients' financial transactions, the lack of face-to-face contact at the beginning of the online payment service provider may be eliminated.

6.3. Complementing virtual currencies and asset regulation

The Convention on Cybercrime in 2001, also known as the Budapest Convention on Cybercrime or simply the Budapest Convention, is the first international treaty intended to combat cybercrime by harmonising national laws, enhancing investigative techniques, and fostering greater international cooperation. In addition to the Budapest Convention, which seeks to establish consistent legal frameworks and investigative powers among its signatories, jurisdictions have also sought to address one of the most pressing concerns regarding crypto currencies by subjecting this sector to AML/CFT regulation and supervision. By classifying these firms as "reporting institutions" under the AML rules, such as has enforced AML/CFT requirements on digital currency exchanges. This necessitates that exchangers of digital currencies implement adequate countermeasures against money laundering and terrorist financing threats related to cryptocurrencies and increase the transparency of digital currency activities. In addition, these digital currency exchangers must

also provide further information on their business profile and activities, as well as submit regular reports on digital currency transactions.

6.4. International cooperation and personal training

On the one hand, the problem of money laundering through the Internet is transnational, and it is impossible to combat this type of crime without the collaboration of nations, international organisations, and the development of international legal rules. The establishment of a network for the exchange of information, control, and combined action, as well as the creation of new concepts that foresee potential criminal attempts to exploit technology for money laundering, will be made feasible through close cooperation and mutual consultations. In addition, this connection will enable legislators and law enforcement organisations to swiftly respond to new difficulties and eliminate potential dangers in a timely manner.

On the other hand, many law enforcement organisations, detectives, and related individuals are unprepared to deal with the new realities of cybercrime and the sophisticated money-laundering techniques used by organised crime groups. Due to inadequate investment in education and research, developing nations frequently have a shortage of knowledge workers. Inadequate employment prospects for these knowledge workers is also one of the reasons why workers look elsewhere for better opportunities. Financial support should be offered to the training sector in order to enhance the number of trained workers available. All participants in the program should receive specialized training to ensure that they fully understand their jobs and have the skills necessary to carry out their responsibilities.

7. Conclusion

Technology is changing quickly these days, and people can reach almost any opportunity through the Internet. Without a doubt, the financial sector is one of the areas that is changing because of technology. At the same time, as the financial sector has grown, it has brought with it new money laundering and terrorist financing threats. This is a sign of a new age of financial crime, which is characterised by complex connections and undefined geographic areas.

The paper identifies the risks that are posed by the development, adoption, and application of technology. New technologies could make AML/CFT faster, cheaper, and more effective, but they also make it harder to figure out what's going on. The FATF Standards are a flexible tool that changes in response to new money laundering and terrorist financing threats, vulnerabilities, and risks, as well as to problems that come up when they are put into place. New technologies need to be used in a responsible way to combat money laundering and terrorist financing. To keep up with how quickly technology changes, financial institutions must adapt their risk-based approach to take into account

how new technologies might affect money laundering and terrorist financing. It is also very important that states develop the capabilities to collect, use, and share electronic evidence of cyber-laundering and terrorist activity both online and offline, as well as allocate sufficiently resources to training for related entities.

Bibliography

- Alexander, Kern: The international anti-money-laundering regime: the role of the financial action task force. In: Journal of Money Laundering Control, 2001/3, pp.231-248.
- Buchanan, Bonnie: Money laundering - a global obstacle. In: Research in International Business and Finance, 2004/1. pp.115-127.
- Demetis, Dionysios S: Technology and anti-money laundering: A systems theory and risk-based approach. Edward Elgar Publishing, 2010.
- Emerson, R. Guy: Limits to a cyber-threat. In: Contemporary Politics, 2016/2, pp.178-196..
- Granville, Johanna: Dot. con: the dangers of cyber crime and a call for proactive solutions. In Australian Journal of Politics & History, 2003/1, pp.102-109.
- Hugel, Paul, and Joseph Kelly: Internet gambling, credit cards and money laundering. In: Journal of Money Laundering Control, 2002, pp.57-65
- Jones, Clare: Can You Ever Regulate the Virtual World Against Virtual Economic Crime?. In Journal of International Commercial Law and Technology, 2012/4, pp.339-349.
- Lilley, Peter: Dirty dealing: the untold truth about global money laundering, international crime and terrorism. Kogan Page Publishers, 2003.
- McDowell, John, - Gary Novis: The consequences of money laundering and financial crime. In: Economic Perspectives, 2001/2. pp.6-10.
- Philippsohn, Steven: Trends in cybercrime - An overview of current financial crimes in the Internet. In: Computers & Security, 2001/1, pp.53-53.
- Price, A: Anti-money laundering: Reconsidering the risks. Ernst& Young, 2002
- Ryder, Nicholas: Money Laundering-an Endless Cycle? A Comparative Analysis of the Anti-money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada. Routledge, 2012.
- Sullivan, Kevin: Virtual Money Laundering and Fraud - Second Life and Other Online Sites Targeted by Criminals, 2008. Available at: https://www.bankinfosecurity.com/virtual-money-laundering-fraud-a-809

- Yar, Majid, and Kevin F: Steinmetz. Cybercrime and society. Sage, 2019.

Melléklet – A konferencia programja

„Az internet és a közösségi media jogi kihívásai”

című nemzetközi online videokonferencia

2022. 04. 27. 9 óra

Magyar nyelvű szekció

Szekcióvezető: Balázs Gáti

9:00 – 9:05	**A konferencia megnyitója**
9:05 – 9:20	**Prof. Dr. Kőhalmi László** (tanszékvezető egyetemi tanár – PTE-ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék) *A közösségi média szerepe a gyermekkereskedelemben*
9:20 – 9:35	**Ripszám Dóra** (PhD-hallgató Pécsi Tudományegyetem) *A közösségi média szerepe a gyermekkereskedelemben*
9:35 – 9:50	**Mitrovics Zoltán**(PhD-hallgató Pécsi Tudományegyetem) *Skype-alapú kapcsolattartás a hazai börtönökben*
9:50 – 10:05	**Nárcisz Projics** (PhD-hallgató Pécsi Tudományegyetem) *Valótlan médiatartalommal kapcsolatos különleges személyiségvédelmi eszköz*

10:05-10:20	**D. Horváth Vanessza** (PhD-hallgató Pécsi Tudományegyetem) *Az online gyermekpornográfia elleni küzdelem jogi kihívásai*
10:20-10:35	**Gáti Balázs** (PhD-hallgató Pécsi Tudományegyetem) *A „Schrems II.” ítélet lehetséges hatásai a nemzetközi jogalkotásra*

Angol és német nyelvű szekció

Szekcióvezető: Tóth Dávid

9:00 – 9:05	**A konferencia megnyitója**
9:05 – 9:20	**Aleksander Wróbel** (Jan Dlugosz University in Czestochowa, adjunktus) *Selected Aspects of Criminal Law Protection of End-users of Cryptocurrencies in Polish Law*
9:20 – 9:35	**Prof. Boguslaw Przywora** (Jan Dlugosz University in Czestochowa, egyetemi tanár) *Access to information in the Constitution of the Republic of Poland*
9:35 – 9:50	**Szabó Barbara** (PhD-hallgató Pécsi Tudományegyetem) *Crimes committed on online surfaces*
9:50 – 10:05	**Németh Henrietta** (PhD-hallgató Pécsi Tudományegyetem) *Verbreitung von Drogen im Darknet*
10:05 – 10:20	**Novák Pál** (PhD-hallgató Pécsi Tudományegyetem, tanársegéd PTE-ETK) *Could blockchain really decentralize the internet?*

10:20 – 10:35	**Jahan Bushrat** (PhD-hallgató Pécsi Tudományegyetem) *Legal Challenges of E-Contracts Conducting Online Businesses: A Comparative Study*
10:35-10:50	**Namsrai Battulga** (PhD-hallgató Pécsi Tudományegyetem) *Legal and ethical issues of big data algorithm-based decisions, and AI*
10:50 – 11:05	**Rohail Kasi** (PhD-hallgató Pécsi Tudományegyetem) *Right of Privacy Invasion by Social Media Applications*
11:05 – 11:20	**Thai Ha Van** (PhD-hallgató Pécsi Tudományegyetem) *The fight against money laundering and terrorist financing in the digital age*
11:20 – 11:35	**Agnieszka Franczak** (Cracow University of Economics, Institute of Law, egyetemi docens) *Protection of taxpayers' personal data on the internet. Some remarks on the judgment of the European Court of Human Rights of 12 January 2021, LB v Hungary - Application No. 36345/16*
11:35 – 11:50	**Tóth Dávid** (PTE-ÁJK, adjunktus) *Theories on the connection between social media and crime*