Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése

Dr. Krasznay Csaba
https://doi.org/10.47707/Kulugyi_Szemle.2021.2.09

Összefoglalás: *Egy kiberbiztonsággal foglalkozó szakembernek Magyarországgal kapcsolatban egészen biztosan a kiberbűnözés visszaszorítását célzó Budapesti Egyezmény jut először az eszébe. Az Európa Tanács 2001-ben elfogadott Számítástechnikai Bűnözésről Szóló Egyezménye világszerte olyan referenciaként szolgál, mely a kibertér számos szabályozási hiányossága mellett szinte egyetlenként világos feladatrendszert szab a csatlakozó államok számára azzal kapcsolatban, hogy nemzeti jogukban hogyan kezeljék az egyre jobban elharapódzó kiberbűncselekményeket. Meg kell tehát becsülni ezt a megállapodást, mely felett azonban egyes vélemények szerint eljárt az idő, és ezért egyes keleti nagyhatalmak jelentős erőfeszítéseket tesznek egy új megállapodás elérése érdekében. Jelen tanulmány célja összefoglalni az egyezmény húszéves tapasztalatait és bemutatni annak jövőképét.*[1]

Kulcsszavak: *kiberbűnözés, kiberbiztonság, Budapesti Egyezmény, Európa Tanács*

Abstract: *A cyber security expert will surely think of the Budapest Convention on Cybercrime in relation to Hungary. The Convention on Cybercrime of the Council of Europe, adopted in 2001, serves as a reference worldwide that, besides the many regulatory gaps in cyberspace, almost unambiguously sets out a clear set of responsibilities for acceding states on how to deal with the growing number of cybercrimes in their national law. It is necessary to appreciate this agreement however, it is considered by some to be outdated and therefore some of the great powers*

1 a szerző a Nemzeti Közszolgálati Egyetem EJK Kiberbiztonsági Kutatóintézetének intézetvezetője

of the East are making significant efforts to reach a new agreement. The goal of this paper is to summarize the 20 years of experience of the Convention and to present its vision.

Keywords: *cybercrime, cybersecurity, Budapest Convention on Cybercrime, Council of Europe*

Az ET szerepe a kiberbiztonság európai politikáinak alakításában és a kiberbűnözés elleni küzdelemben

A kiberbűnözés nagyságrendje kétségkívül folyamatosan növekszik. Egyre több klasszikus bűncselekmény elkövetése során használnak fel információs rendszereket vagy hajtják végre azokat a kibertérben. Mindezt oly módon, hogy az elkövetők és az áldozatok térben távol, sokszor különböző kontinensen vannak. Elkerülhetetlen tehát, hogy a kiberbűnözés elleni küzdelem is új dimenziókat kapjon, és leküzdje azt a hiányosságot, amit egy rendészeti szakember a következőképpen fogalmazott meg: „a kiberbűnözés elleni képesség északról délre, a hajlandóság pedig nyugatról keletre jelentősen csökken". Ennek érdekében jelentős nemzetközi erőfeszítésekre van szükség, melyben az Európa Tanácsnak (ET) fontos szerep jut.

Noha az Európa Tanács kiberbiztonsággal kapcsolatos hozzájárulásai között kiemelkedő szerepet játszik a Budapesti Egyezmény néven is ismert Számítástechnikai Bűnözésről Szóló Egyezménye (Budapest Convention on Cybercrime), amelyről a későbbiekben részletesen fogunk szólni, érdemes megemlíteni, hogy ezen túlmenően az ET intézmények, programok és más szakmai tevékenységek egész sorával járul hozzá a kiberbűnözés elleni védelemmel, általános kiberbiztonsággal kapcsolatos európai politikák alakításához.

Az egyezmény, amely a számítógépes rendszerekkel és hálózatokon elkövetett bűncselekmények különböző kategóriáit lefedő első, nemzetközi hatókörű és kötelező jogérvényű szabályozásnak tekinthető, több éves előkészítő munka után kerülhetett a dokumentumot

kézjegyükkel ellátó politikusok elé. Az előzmények 1997-ig nyúlnak vissza, és abban a felismerésben gyökereznek, hogy a kibertérben kibontakozó bűncselekményeknek – tekintettel azok határokon átnyúló jellegére – csakis globális összefogással lehet gátat vetni. Az ET elkötelezettsége a kiberbiztonság európai, sőt globális előmozdítása mellett nem csupán az egyezmény megkötése előtti években öltött egyre erőteljesebben testet. A kibertér problémái, fenyegetettségei és azok hatékony kezelése a híres konvenció aláírását követő időszakban is meghatározó helyet foglalnak el az Európa Tanács munkájában.

A Budapesti Egyezmény rendelkezései alapján a közös európai politikák előmozdítására, a kiberbiztonsággal kapcsolatos kapacitások fejlesztésére, a kooperációt európai szinten segítő kapcsolatponti hálózat (az ún. 24/7 Network) kiépítésére és segítésére állandó intézmények épültek, illetve hosszú távú célzott projektek indultak az Európa Tanács égisze alatt. Érdemes felfigyelni arra is, hogy miközben az Európai Unió formálisan nem részese a Budapesti Egyezmény aláíróinak, az ET kapcsolódó kiberbiztonság-elősegítő intézményrendszerében és projektjeiben, elsősorban az ún. T-CY Bizottság munkájában, valamint a legfontosabb regionális projektekben és akciókban nagyon is aktív szerepet vállal. Az ET kiberbűnözés elleni, illetve általában a kiberbiztonságot erősíteni hivatott tevékenységének jelentőségét mutatja egyebek mellett az is, hogy (az aláírók között tehát nem szereplő) EU kibervédelmi koncepcióinak, stratégiai dokumentumainak kialakításakor lényegében valamennyi kulcskategória megformálása és szövegezése közvetlenül támaszkodik az ET Budapesti Egyezményében lefektetett fogalmi rendszerre (Council of Europe, 2020a).

Hasonlóan nagy jelentőségű (az ET kiberbiztonsági erőfeszítései hatókörének tekintetében) továbbá az a tény is, hogy az egyezmény aláírói között az Európa Tanács tagországain kívül több más olyan állami szereplő (az USA, Kanada, Japán és Dél-Afrika) is megtalálható, amely aktívan részt vett a megállapodás elveinek kialakításában. Ez a széleskörű részvétel ugyanis az egyik legfontosabb biztosítéka az egyezményben foglalt jogelvek globális szintű érvényesülésének (Council of Europe, 2009).

Az Európa Tanács kiberbiztonsággal kapcsolatos folyamatos szerepvállalására az alábbi – folytonosságot biztosító – kezdeményezések születtek meg az egyezmény aláírását követő időkben:

a.) intézmények

Cybercrime Convention Committee (T-CY)

A legfontosabb, folyamatosan működő konzultatív szervezet az ún. T-CY Bizottság, vagy más néven Budapesti Egyezmény Bizottság (angolul Cybercrime Convention Committee), amely a megállapodást aláíró államok képviselőit tömöríti. Tevékenységének átfogó célja az egyezmény rendelkezései megvalósításának az elősegítése. Fontos feladata a témához kapcsolódó információáramoltatás az aláíró államok között, valamint az esetlegesen szükségessé váló kiegészítések és módosítások megvitatása.

Cybercrime Programme Office (C-PROC)

Az ET Bukarestben székelő Kiberbűnözés-elleni Program Irodája (angolul Cybercrime Programme Office) célja, hogy – a Budapesti Egyezmény normarendszere alapján – támogassa a nemzetközi közösség tagjainak jogszolgáltatási kapacitásépítését annak érdekében, hogy azok naprakészen legyenek képesek szembeszállni a kiberbűnözés jelentette kihívásokkal (Council of Europe, 2020b).

Octopus Konferenciák

Az ET által évente-másfél évente megrendezett ún. Octopus Konferenciák jelentik a legfontosabb (és egyben legszélesebb) nemzetközi fórumot, amelyen mintegy 80 nemzet hivatalos képviselői vitathatják meg a kibertér aktuális biztonsági kérdéseit. A fórum egyben a nemzetközi szervezetek, a tudományos élet és a vállalati szektor szereplőivel folytatott eszmecseréknek is platformot biztosít.

b.) kapacitásépítő projektek

GLACY+

Az ET kiberbiztonsági szerepvállalásához egész sor kapacitásépítő kezdeményezés, projekt tartozik. A GLACY+ az ET és az EU közös vállalkozása, amelynek célja, hogy az afrikai, ázsiai-óceániai és latin-amerikai térségek országaiban segítse a kiberbiztonság erősítésével kapcsolatos tapasztalatok terjesztését. Három prioritási területe: a kiberbűnözés elleni törvények és szakpolitikák kialakítása; a rendőri szervezetek kapacitásainak erősítése a kiberbűncselekmények felderítéséhez és a büntetőjogi hatóságok felkészítése a kiberbűncselekményekkel összefüggő ügyek tárgyalására.

CyberSouth

A CyberSouth hasonlóan közös projekt, amelyben az ET és az EU közösen igyekszik erősíteni az EU Déli Partnerségéhez tartozó államok (Algéria, Jordánia, Libanon, Marokkó és Tunézia) kiberbűnözés elleni jogi kapacitásait és intézményrendszerét. Fókuszában állnak az eljárásjogi reformfolyamatok is, az igazgatási szereplők közötti együttműködések, valamint a köz- és magánszféra együttműködéseinek a kialakítása. A projekt prioritásai közé tartozik továbbá a nemzetközi együttműködések elősegítése is a kiberbűnözés elleni területeken.

EndOCSEA@Europe

Az EndOCSEA@Europe program (az ET Gyerekjogi Részlege és a bukaresti C-PROC közös kezdeményezése) nemzeteken átívelő, interdiszciplináris együttműködések révén mozdítja elő a gyermekek ICT-eszközökön keresztül történő kizsákmányolása elleni küzdelmet. A projekt három egymást kölcsönösen erősítő komponensből

áll, fókuszában (egyebek mellett) a témához kapcsolódó eljárásjogi reformfolyamatok támogatásával, igazságszolgáltatási szakemberek továbbképzésével, illetve figyelemfelkeltő akciókkal.

iPROCEEDS-2

Az iPROCEEDDS-2 több, már említett kezdeményezéshez hasonlóan az ET és az EU közös projektje. Célterülete a Nyugat-Balkán hat állama (Bosznia-Hercegovina, Szerbia, Montenegró, Koszovó, Albánia és Észak-Macedónia), valamint Törökország. Egyes kiberbűnözési formákkal (elsősorban az internetes pénzmosással) kapcsolatos jogi eljárási lépések támogatása, az elektronikus bűnjelek és bizonyítékok megszerzését és tárolását szolgáló jogi kapacitások erősítése, segítése a feladata.

CyberEast

A CyberEast projekt lényegében a korábban említett CyberSouth projekt „tükörképe": szintén az ET és az EU közös vállalkozása. Célja az EU Keleti Partnerségéhez tartozó államok (Örményország, Azerbajdzsán, Belarusz, Georgia, Moldova és Ukrajna) igazságszolgáltatási és rendvédelmi szerveinek támogatása a kiberbűnözés elleni küzdelemben a kapacitások növelése, illetve a hatóságok közötti együttműködések erősítése révén. Alapvető célkitűzése a Budapesti Egyezmény normarendszerének alapján álló törvénykezési és szakpolitika-alkotási folyamatok elősegítése. Célja ugyanakkor ezeknek az országoknak a jogi-rendvédelmi szervezeteinek aktív bekapcsolása nemzetközi együttműködésekbe a kiberbűnözés elleni fellépés során. (Council of Europe, 2019)

Octopus Project

Az Octopus Project az ET legújabb, 2021 januárjában indult projektje: az egyezményt aláíró országok, illetve a megfigyelői státuszú államok, valamint más közszféra- és magán szervezetek önkéntes

együttműködése a Budapesti Egyezmény megvalósulását támogató különféle lépésekre és intézkedésekre. Ezek között szerepel az Idegengyűlölet és Rasszizmus elleni Első Kiegészítő Jegyzőkönyv megvalósításának támogatása, a kiberbűnözéssel szembeni nemzetközi együttműködéseket támogató Második Kiegészítő Jegyzőkönyv rendelkezéseinek előmozdítása, a T-CY Bizottság munkájának segítése, valamint természetesen a témához kapcsolódó Octopus Konferenciák szervezése is.

A Budapesti Egyezmény bemutatása

Az Európa Tanács legismertebb kiberbiztonsági projektje azonban kétségkívül a Budapesti Egyezmény. Az ehhez vezető első fontos nemzetközi jogi dokumentum a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) által kibocsátott 1986-os jelentés volt a kiberbűnözés területén. Ezzel iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez, valamint a kodifikáció elősegítéséhez. Az Európa Tanács a 1980-as évek második felében állított fel egy szakértői bizottságot a számítógépes bűncselekményekkel kapcsolatos ismeretek összegyűjtésére és a veszélyek felmérésére. A bizottság kiemelt célja volt, hogy a kriminalizálandó magatartásokat magában foglaló ajánlást dolgozzanak ki a tagállamok számára. Az első uniós dokumentum így az ET 9. (89.) számú ajánlása (Computer-Related Crime) lett, amely tartalmaz egy minimumlistát. A kezdeti büntető eljárásjogi aggodalmakra válaszul megszületett az ET 95. (13.) számú ajánlása, amely kifejezetten az információs technológiákkal kapcsolatos eljárási problémákra törekedett megoldást nyújtani (Gyaraki, 2012, 237–239. o., valamint Mezei, 2018a, 349–350. o.).

2001 novemberében Budapesten írták alá az Európa Tanács által előkészített Számítástechnikai Bűnözésről Szóló Egyezményt azaz a Budapesti Egyezményt, amelyet az ET tagjain kívüli országok is

aláírhatnak és ratifikálhatnak. A Budapesti Egyezmény a korábbi ajánlásokhoz képest továbblépést jelent, és újabb jogi normákat fogalmaz meg. Egységes értelmezést nyújtva definiálja a számítógépes technikai fogalmakat: számítástechnikai rendszer (computer system), számítástechnikai adat (computer data), szolgáltató (service provider), illetve átmenő adat (traffic data). Mind az anyagi, mind az eljárásjogi szabályozást tartalmazza. Az anyagi jogban a tényállások köre bővült, újabb jogsértéseket szabályoz (például eszközökkel való visszaélés, a gyermekpornográfiával kapcsolatos bűncselekmények). Az egyes bűncselekménytípusokat logikusan csoportokba rendezi.

A Budapesti Egyezmény négy részre osztható: a 2–13. cikk a büntető anyagi jogi részt tartalmazza, a 14–22. cikk a büntetőeljárási jogi résszel foglalkozik, magában foglalva az eljárásjogi rendelkezések alkalmazási körét, a forgalmi adatok valós idejű összegyűjtését az internetes szolgáltatók részéről, és a joghatósági kérdésekkel zárul. A 23–35. cikk pedig a nemzetközi együttműködésre vonatkozó irányelveket fogalmaz meg. Valamennyi aláíró felet kötelezi a kölcsönös jogsegélynyújtásra, illetve együttműködésre a nyomozások és eljárások során, különösen az elektronikus bizonyítékok összegyűjtése érdekében. Végül a 36–48. cikk a záró rendelkezésekben az egyezmény hatályára, a fenntartásokra, a módosításokra, a viták rendezésére és az egyezmény felmondására vonatkozó részekre tér ki.

Az anyagi jogi szabályozás terén kimondja, hogy minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, amelyek ahhoz szükségesek, hogy a belső jogával összhangban bűncselekménynek minősüljön az alábbi cselekmények jogosulatlan és szándékos elkövetése: a számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények (I. cím) körében a jogosulatlan belépés (2. cikk), a jogosulatlan kifürkészés (3. cikk), a számítástechnikai adat megsértése (4. cikk), valamint a számítástechnikai rendszer megsértése (5. cikk), végül az eszközökkel való visszaélés (6. cikk).

A második bűncselekménycsoportot a számítógéppel kapcsolatos bűncselekményekként határozza meg (II. cím), amelyek körében a számítógéppel kapcsolatos hamisítást (7. cikk) és a számítógéppel kapcsolatos csalást (8. cikk) különbözteti meg.

Végül a harmadik csoportot a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények (III. cím) képezik: a gyermekpornográfiával kapcsolatos bűncselekmények (9. cikk) és a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények (10. cikk).

E részben a tisztán informatikai bűncselekmények, avagy kiberbűncselekmények bemutatására törekszünk (lásd a kiberbűnözés fogalmáról bővebben Mezei, 2019a, 21–22. o.). A Budapesti Egyezmény értelmében a jogosulatlan belépés (2. cikk) bűncselekményét követi el, aki a számítástechnikai rendszerbe vagy annak bármely részébe (legyen az tárolt vagy forgalmi adat, mappák, egyéb komponensek, adathordozók stb.) jogosulatlanul és szándékosan belép. A szerződő felek kiköthetik, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy számítástechnikai adatok megszerzésére irányuló, illetve más tisztességtelen céllal kövessék el (Council of Europe, 2001, 9–10 o.). A büntetendő cselekményt jogosulatlanul kell elkövetni, ami azt jelenti, hogy ez a rendszer vagy a rendszer egy része jogosultjának vagy egyéb jogosultjának az engedélye nélkül történik (például a rendszer tulajdonosa által engedélyezett tesztelés nem minősül ennek). (Az etikus hacking kapcsán lásd Mezei, 2019a, 25–26. o., Papp, 2002, 41–54. o., Szathmáry, 2020, 330–346. o.) Nem büntetendő azonban, ha a számítástechnikai rendszerhez ingyenes és nyilvános hozzáférés áll rendelkezésre.

A jogosulatlan kifürkészés (3. cikk) esetén büntetendő a számítástechnikai rendszeren belüli, az abból származó, illetőleg a rendszerbe irányuló számítástechnikai adatok nem nyilvános továbbítása során technikai eszközök felhasználásával történő jogosulatlan és szándékos kifürkészése, ideértve az ilyen számítástechnikai adatokat továbbító, a számítástechnikai rendszerből származó elektromágneses sugárzást. Azonban a szerződő felek kiköthetik, hogy

a bűncselekményt tisztességtelen céllal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el. A kifürkészés technikai eszköz alkalmazásával megvalósulhat például a felhasználói fiókok feltörésével vagy az ún. távoli asztal hozzáférést biztosító program használatával, melyek segítségével jogosulatlanul férhetnek hozzá az adatokhoz.

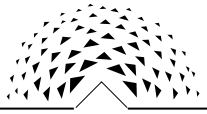
Az elosztott túlterheléses, ún. DDoS-támadásokat és a rosszindulatú programok segítségével végrehajtott támadásokat (lásd bővebben Mezei, 2018b, 66–83. o., Sorbán, 2018, 369–386. o.) is kriminalizálja a Budapesti Egyezmény, a számítástechnikai adat (4. cikk), valamint a rendszer megsértése (5. cikk) keretében. Előbbi szerint bűncselekménynek minősül a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése. A szerződő felek azonban fenntarthatják annak kikötését, hogy ennek eredményeként jelentős kár következzen be. A rendelkezés célja, hogy megfelelő védelmet biztosítson a számítástechnikai adatoknak és programoknak a károkozó magatartások esetén. Utóbbi miatt büntetendő, aki a számítástechnikai rendszer működését a számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével jogosulatlanul és szándékosan, jelentős mértékűen akadályozza. Az akadályozásnak jelentős mértékűnek kell lennie, azonban, hogy mi minősül ennek, azt a szerződő felek szabadon határozhatják meg. Például jelentősnek tekinthető az olyan mértékű, formájú és gyakoriságú adatküldés egy meghatározott rendszerre, ami jelentős hátrányt okoz a rendszer használatában, vagy a más rendszerekkel folytatott kommunikációra való alkalmasságát illetően (például ilyenek a DDoS-támadások, kártékony kódok, amelyek lényegesen lassíthatják a rendszer működését, vagy programok, amelyek spam formájában tömeges kéretlen e-mailt küldenek a címzettnek, hogy akadályozzák a kommunikációt) (Council of Europe, 2001, 12. o.).

A Budapesti Egyezmény szabályozza az eszközökkel való visszaélést (6. cikk), amelynek értelmében bűncselekménynek minősülnek a következő jogosulatlan és szándékos magatartások: a 2–5. cikkben foglalt valamely bűncselekmény elkövetése érdekében létrehozott vagy átalakított számítógépes program, vagy egy számítógépes jelszó, illetve hasonló, a számítástechnikai rendszerbe vagy annak bármely részébe való belépést lehetővé tevő számítástechnikai adat előállítása, értékesítése, a felhasználás céljából való megszerzése, az ország területére való behozatala, a forgalomba hozatala vagy a más módon történő hozzáférhetővé tétele. Továbbá az előbb említett eszközöknek a birtoklása valamely kiberbűncselekmény elkövetésére való felhasználás érdekében. A szerződő felek azonban a belső jogukban kiköthetik, hogy a büntetőjogi felelősséget meghatározott számú dolog birtoklása alapozza csak meg. Fontos, hogy csak a meghatározott célzat fennállása esetén büntetendők a felsorolt magatartások, valamint a szerződő felek kötelesek legalább a számítógépes jelszavak vagy belépési adatok értékesítését, a forgalomba hozatalát vagy a más módon történő hozzáférhetővé tételét büntetendővé tenni (Council of Europe, 2001, 13. o.).

E téren a büntetőjogi szabályozása különösen indokolt, mert napjainkra a hozzá nem értő felhasználók is akár könnyen hozzá tudnak jutni a kiberbűncselekmények elkövetéséhez szükséges ismeretekhez és programokhoz (Mezei, 2019b, 142. o.).

A Budapesti Egyezmény a gyakorlatban, rendőrségi szemszögből

Az tagadhatatlan, hogy már az egyezmény aláírása és a magyar jogrendszerbe történő beemelése előtt is – ez több lépcsőben történt a büntető anyagi és eljárásjogi törvényekbe – Magyarországon jelen volt a kiberbűnözés. A nyomozóhatóság már 2001 előtt, pontosabban a hatályba lépés 2004. július 1-i dátumát megelőzően is nyomozott



számítógépes bűncselekményekkel összefüggésben. A számítógépes bűncselekmények száma azóta egyre nő, és az elkövetés egyre kifinomultabbá válik, amelyben szerepet játszik az online tér népszerűsége, az IT-eszközök számának növekedése és nem utolsósorban a szervezett bűnözés fizikai térből a kibertérbe történő áthelyeződése is.

A nyomozóhatóság számára a kiberbűncselekmények jellemzői közül is a legnagyobb kihívást a büntetőeljárás során a nemzetközi jelleg jelenti, amely során a hatóság együttműködése, a joghatóság eldöntése, az ügyek áttétele, az elkövetők cselekményének büntetőjogi megítélése és a felelősségre vonásának megállapítása az elsődleges feladat. A rendőrségre vonatkozó, a kiberbűnözés nyomozásának módját kijelölő büntetőeljárásjogi és büntető anyagi jogi keretet többek között az egyezmény adja meg. Emellett további uniós rendeletek, ajánlások, irányelvek, így például az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv, előírásainak megfelelően járnak el a nyomozások közben.

Ahogy azt korábban láthattuk, az egyezmény négy részre osztható fel. Ezek gyakorlati implementálása a magyar joganyagba és a rendőrségi gyakorlatba az évek során folyamatosan történt meg. Az első részben foglaltakat a büntető anyagi szabályozás változásai következtében a számítástechnikai rendszer és adatok elleni bűncselekmények Büntető Törvénykönyvbe történő beemelésének szabályozásával kezdték meg, mely a ma már hatálytalan 1978. évi IV. törvény 300/C.§-ában került kodifikálásra. A régi Btk-t módosító 1994. évi IX. törvénnyel megjelent a magyar büntetőjogi rendelkezések között a számítástechnikai bűncselekmény önálló tényállása is. Ennek a tényállásnak a hatálya alá tartozott szinte valamennyi számítógépes környezetben elkövetett bűncselekmény, amelynek szabályozása az új Büntető Törvénykönyvben jelentősen változott, hiszen több új törvényi tényállás került a helyére.

Az egyezményben meghatározott, gyermekek ellen elkövetett szexuális abúzus, bántalmazás is rövid idő alatt bekerült a ma már hatálytalan Büntető Törvénykönyvbe, a „Tiltott pornográf felvétellel

visszaélés" cím alatt. Ez az új Btk-ban, a gyermekpornográfia tényállásában, az elkövetési magatartás tekintetében egyértelműen a kibertérben történő elkövetést emeli ki, többek között említve a terjesztést, tartást, hozzáférhetővé tételt, megszerzést és „egy számítástechnikai rendszerben vagy egy számítástechnikai adattároló-egységen való birtoklása" által történő elkövetést. Életkori határként a 18. életévüket be nem töltött személyeket mint sértetteket jelöli meg. Ugyanakkor, ahogy a Genval 7. körös jelentéséből kitűnik, a cselekménybe bele kell érteni a gyermekek szexuális kizsákmányolásával kapcsolatos jogi szabályozással összefüggésben a „grooming" jelenségét is, amelynek jelentése: becserkészés. Ez a magyar büntetőjogban egy előkészületi cselekményt jelent, ezért ez leginkább a „törekszik rábírni" fordulattal került be a tényállásokba.

Egyértelmű változást a 2012. évi C. törvény életbelépése jelentett a jogalkalmazó szerveknél, amikor bekerült a törvénykönyvbe az információs rendszer felhasználásával elkövetett csalás (Btk. 375.§), valamint a XLIII. fejezet, melynek címe a *Tiltott adatszerzés és az információs rendszer felhasználásával elkövetett bűncselekmények*. Így külön nevesítésre kerültek az információs rendszer vagy adat megsértése (Btk. 423.§), az Információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424.§) törvényi tényállások, mindazok mellett, hogy a szerzői vagy szerzői joghoz kapcsolódó jogok megsértése bűncselekményének elkövetési magatartása is a technológiai változásokhoz igazodva módosult.

Az egyezmény második szakasza változásokat hozott a büntetőeljárási jogba. A büntetőeljárásról szóló 2017. évi XC. törvényben a tárgyi bizonyítási eszközök közé bekerült az elektronikus adat, amelynek fogalma az egyezmény szövegében megadott számítástechnikai adat fogalmával megegyező: *elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.*

A kényszerintézkedések közül az elektronikus adat lefoglalása és megőrzésre kötelezésének bevezetése jelenti a kiberbűncselekmények nyomozása során az informatikai eszközön vagy rendszerben tárolt adatoknak a büntetőeljárás során bizonyítékként történő felhasználását, átvizsgálását és az eljárásban annak változatlanságának megőrzését, ami korábban problémát jelentett, hiszen erre vonatkozó szabályozás nem létezett. Mivel az elektronikus bizonyítékok egyik legnagyobb problémája, hogy azok kevésbé statikusak, bizonyítékként való felhasználásuk komoly akadályokba ütközött. Ugyanakkor egy 2016-os jelentésben, amelyben megvizsgálták valamennyi európai uniós tagállamban a számítástechnikai bűnözés megelőzésének és az ellene folytatott küzdelemnek a hatékonyságát (Genval jelentés), megállapításra került, hogy a jelentés elkészítésében közreműködő nyomozóhatóságok tagjai, beleértve az Ügyészséget is, az elektronikus bizonyítékokkal – elektronikus adatokat értve alatta – kapcsolatban, azok bizonyítékként történő felhasználása, lefoglalása és átvizsgálása esetén jellemzően a hagyományos nyomokra, bizonyítékokra vonatkozó eljárási rend szerint jártak el.

A kibertérben elkövetett bűncselekmények nyomozását segítik azok a nyomozási technikák és intézkedések, melyeket a Budapesti Egyezmény nemzeti jogba emelése előtt is alkalmaztak az egyes országok. Így elsősorban azok az együttműködések nagyon hatékonyak, amelyek az elektronikus adatok beszerzését, vizsgálatát hivatottak segíteni. Az egyes büntetőeljárásokban az adatkérések (megkeresések), az IP-címek egyszerű megállapításai mindennaposság váltak, ezek gyakran segítik a nyomozások sikerességét, melyhez az egyezmény széles körű alkalmazása igen jelentősen hozzá tudott járulni.

Az egyezmény harmadik része a nemzetközi együttműködések terén használt szabályozásokat, a joghatóságot rendezi. A magyar nyomozóhatóságok más, külföldi, illetve nemzetközi hatóságokkal a kiberbűncselekmények felderítése és nyomozása terén rutinszerűen működnek együtt, rendszeresen küldenek a nemzetközi szerződéseknek megfelelő megkereséseket, adatkéréseket, ezek mellett

pedig az esetleg nem hazánkban indult, de magyar állampolgárt is érintő nyomozásokban, kényszerintézkedésekben (kutatás, lefoglalás, őrizetbevétel) is kiveszik a részüket.

A Számítógépes Bűnözésről szóló Egyezmény 2001-es aláírása óta viszont a technológia olyan mértékben változott, hogy az abban meghatározott alapvető büntető anyagi, eljárásjogi részek már elavultak. A legtöbb esetben azonban az egyezmény alapkoncepciója a hazai és nemzetközi gyakorlatban megtartásra került. A technológia rohamos fejlődése ellenére is észrevehető ugyanakkor, hogy a kiberbűncselekmények nyomozásában a speciálisan képzett szakemberek a jogszabályi környezetet továbbra is megtartva képesek az újabb és újabb kibertérben elkövetett bűncselekmények nyomozásában, az elektronikus bizonyítékok beszerzésében, vizsgálatában és kiértékelésében magas szintű szakmai munkát végezni. Ezek alapján elmondható, hogy az egyezmény által meghatározott keretek továbbra is alkalmasak a kiberbűnözéssel kapcsolatos nyomozások végrehajtására, a szakemberek pedig ennek mentén támogatni tudják az általános bűnügyi feladatokat ellátó nyomozók és a Nemzeti Adó- és Vámhivatal nyomozóinak munkáját, valamint a szakkérdések megválaszolásában is segítséget tudnak nyújtani.

A hazai nyomozó szervek az egyezmény követelményeinek hatására, valamint a kiberbűncselekmények számának folyamatos és erőteljes emelkedésére választ adva jelentős szervezeti átalakuláson mentek keresztül az elmúlt 20 évben. Jelenlegi csúcsszervként a Készenléti Rendőrség Nemzeti Nyomozó Irodán belül a Korrupció és Gazdasági Bűnözés Elleni Főosztály Csúcstechnológiai Bűnözés Elleni Osztálya 2017-es átalakulásával jött létre a KR NNI Kiberbűnözés Elleni Főosztálya. Ez utóbbin belül már négy osztály veszi fel a harcot a kibertérből érkező jogellenes cselekményekkel: a Nyomozó Osztály, amelyen belül van a Gyermekvédelmi Alosztály és a Nyomozó Alosztály, a Felderítő Osztály, a Kiberes Csalások Alosztályával és a Kiemelt Ügyek Alosztályával, a Forenzikus Osztály és az Elemző-értékelő Osztály.

A Budapesti Egyezmény napjainkban

Noha elfogadásakor a Budapesti Egyezmény igazi mérföldkőnek számított a kiberbűnözésre adott egységes európai szabályozás alapjaként, napjainkban egyre inkább erősödnek azok a kritikus hangok, amelyek az egyezmény felülvizsgálatát sürgetik. Érdemes tehát áttekinteni, hogy miként állja meg a helyét a Budapesti Egyezmény a 21. században, részletesen ismertetve azokat a szabályozási dilemmákat, amelyek kihívások elé állítják a részes országokat!

Az egyezmény napjaink egyik legjelentősebb nemzetközi jogi instrumentuma, amelyet 65 ország ratifikált, a részesek között pedig nemcsak európai országok találhatóak, hanem tengerentúliak is, köztük az Amerikai Egyesült Államok és Japán. Az egyezmény részesein túl az Európa Tanács több mint 20 olyan országot tart számon, ahol a számítógépes bűncselekményekkel kapcsolatos jogszabályok az egyezménnyel összhangban vannak, és több mint 50 országról, amelyek az egyezmény szabályaira épültek. Érdekesség, hogy Svédország 2021 közepén tervezi ratifikálni az egyezményt, 20 évvel azután, hogy azt aláírta. Az egyezmény értékelésénél fontos figyelembe venni azt, hogy az nem egy önmagában létező jogi instrumentum, a nemzetközi térben számos szerződés, az Európai Unióban pedig uniós jogi aktus egészíti ki annak szabályait, így teremtve meg a kiberbűncselekmények elleni fellépés komplex rendszerét. Mindenképpen említést érdemel, hogy a Budapesti Egyezmény úgynevezett minimum harmonizációt valósít meg, vagyis azt vázolja fel, hogy melyek azok az alapvető szabályok, amelyeket a részes államok jogának tartalmaznia kell, ezen túl azonban nagy szabadságot biztosít a részeseknek, akik az egyezmény szabályainál szigorúbb követelményeket bármikor, enyhébb követelményeket pedig abban az esetben fogalmazhatnak, meg, amelyekben ezt az egyezmény kifejezetten lehetővé teszi. A gyermekek szexuális kizsákmányolásával kapcsolatos rendelkezések tekintetében a Budapesti Egyezményt számos ponton megismétli, illetve kiegészíti a Lanzarote Egyezmény, azaz az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és

szexuális zaklatás elleni védelméről szóló egyezménye. A nők elleni erőszak online formái (pl. az interneten megvalósuló pszichológiai erőszak, fenyegető zaklatás) esetében pedig az Isztambuli Egyezmény, azaz az Európa Tanács Egyezménye a nők elleni és a családon belüli erőszak megelőzéséről és felszámolásáról nyújt kiegészítő védelmet.

Az Európai Unió tagállamaiban a Budapesti Egyezmény elfogadását követően számos olyan dokumentum született, amely a számítógépes bűncselekmények elleni fellépést mozdítja elő, ezek:

- az Európai Parlament és a Tanács 2011/92/EU irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról;
- Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról; valamint
- Az Európai Parlament és a Tanács 2019/713/EU irányelve a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról.

A felsorolt normákon felül folyamatban van a büntetőügybeli elektronikus bizonyítékokra vonatkozó közös európai szabályok kidolgozása is, amelyek várhatóan rendeleti formát fognak ölteni.

Az egyezmény a kiegészítő védelmet biztosító nemzetközi szerződések ellenére is több ponton elavultnak számít. Az informatika területén azonban nem számít kirívónak a technológiák gyors avulása, amely annak ellenére is hatással van az egyezményre, hogy azt a megalkotói törekedtek a technológiasemlegesség nevében megfogalmazni. Az információtechnológia fejlődésének irányát és tempóját vélhetően az egyezmény szövegezői el sem tudták képzelni. Néhány évvel azután, hogy az egyezményt elfogadták, a web2.0 berobbant a köztudatba, az internetalapú szolgáltatások korábban elképzelhetetlen

sokaságát kínálva. Míg 2000-ben pusztán 361 millió internet felhasználó volt, ma már 4,66 milliárd ember használja a világhálót. A kétezres években kezdtük el tömegesen használni a kamerával is felszerelt okostelefonokat, a legnépszerűbb közösségi oldalakat szintén az évezred első felében hozták létre (a Facebookot 2004-ben, a YouTube-ot 2005-ben, a Twittert 2006-ban). A felhasználók és szolgáltatások számának bővülésével természetszerűleg együtt járt, hogy olyan jogsértések is megjelentek az online környezetben, amelyek korábban csak a fizikai térben valósulhattak meg.

Noha vitathatatlan az egyezmény jelentősége a kiberbűncselekmények nemzetközi harmonizációjának előmozdításában, számos kritika megfogalmazható az egyes rendelkezések kapcsán. Jelen rész egyfelől a terminológiai következetlenségekre helyezi a hangsúlyt, az egyes terminusokon keresztül bemutatva a problémás területeket, másfelől felhívja a figyelmet az egyezmény szerkezetével kapcsolatos következetlenségekre, valamint utal azokra a büntetőjog határán elhelyezkedő ártalmas magatartásokra, amelyeket a dokumentum jelenleg nem kezel.

Kiberbűncselekmény fogalma

Annak ellenére, hogy az egyezmény eredeti, angol nyelvű címében megjelenik a kiberbűncselekmény kifejezés, a normaszöveg nem definiálja és nem is használja magát a fogalmat. A címadás dacára tehát a kiberbűncselekmény nem számít jogi fogalomnak, helyette az egyezmény a számítógépes rendszer és adatok elleni bűncselekmény, a számítógéppel kapcsolatos bűncselekmény, valamint a tartalommal kapcsolatos bűncselekmény fogalmakat nevesíti. Bár ez pusztán dogmatikai kérdésnek tűnhet, az egyes fogalmak pontos tisztázása nagyon fontos lenne a nemzeti szabályok közelítése érdekében. Egyes álláspontok szerint a kiberbűncselekmény fogalom kizárólag azokat a deliktumokat foglalja magában, amelyek esetében az elkövetés számítógépes hálózaton valósul meg (Commission of the European Communities, 2007), más szerzők szerint azonban minden olyan cselekmény kiberbűncselekmény, amelynek számítógépes vonzata van (Gercke, 2012).

A gyermekpornográfia fogalma

Nagyon sok más nemzetközi jogi instrumentumhoz hasonlóan a gyermekek szexuális kizsákmányolását bemutató tartalmakhoz kapcsolódó bűncselekményeket a Budapesti Egyezmény is a gyermekpornográfia kifejezéssel illeti. Ez a meghatározás azonban sokak szerint elbagatellizál egy komoly bűncselekményt (Gillespie, 2018), mivel ahogyan az EPCAT luxemburgi terminológiai iránymutatása írja, a pornográfia szót az olyan kereskedelmi céllal gyártott felvételekre használjuk, amelyekben felnőttek közös beleegyezés alapján végeznek szexuális cselekményeket (Greijer és Doek, 2016). A gyakorlatban szélesebb körben elterjedt a gyermekek szexuális bántalmazását ábrázoló tartalom (angolul: child sexual abuse material), valamint a gyermekek szexuális kizsákmányolását ábrázoló tartalom (angolul: child sexual exploitation material) kifejezések használata, amely jobban kifejezi azt, hogy itt valójában nem közös beleegyezéssel készül, aktust ábrázoló felvételekről, hanem szexuális erőszakról és bántalmazásról van szó.[2]

Az anyagi büntetőjogi rész struktúrája

Az egyezmény kriminalizálandó cselekményeket felsoroló 1. része összesen négy csoportba sorolja a részes államok által büntetendővé nyilvánítandó cselekményeket. A négy csoport a következő:

- a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények;
- számítógéppel kapcsolatos bűncselekmények;
- tartalom-bűncselekmények;
- szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.

2 Előbbi kifejezést az nemzetközi szervezetek, civil szervezetek pl. az INHOPE használják (https://www.inhope.org/EN), utóbbit pedig az Europol használja szakmai dokumentumokban (https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation).

Az egyezmény által meghatározott kategóriák között jelentős átfedések vannak, hiszen ahogy az ITU által kibocsátott jelentés is kiemeli, három kategória a védelem tárgya alapján csoportosít (számítástechnikai rendszer és adat elleni bűncselekmények, tartalom-bűncselekmények, szerzői vagy szomszédos jogok megsértésével kapcsolatos cselekmények), egy pedig az elkövetés módjára (számítógéppel kapcsolatos bűncselekmények) helyezi a fókuszt (Gercke, 2012).

A büntetőjog határterületei és a Budapesti Egyezmény

Az egyezmény jelenleg a tartalommal kapcsolatos bűncselekmények között egyedül a gyermekpornográfiát szabályozza. Az egyezményhez 2006-ban kiegészítő jegyzőkönyvet fűztek, amely a rasszizmussal és az idegengyűlölettel kapcsolatos deliktumokat hivatott szabályozni. Napjainkban azonban számos olyan tartalommal kapcsolatos bűncselekmény van, amelyeket mind nemzetközi, mind nemzeti szinten elkezdtek szabályozni a jogalkotók. Ilyen cselekmény a hozzájárulás nélkül hozzáférhetővé tett szexuális felvételek (köznyelvi nevén a bosszúpornó) közzététele (Sorbán, 2020), a kibertérben elkövetett zaklatás (cyberharassment), illetve a cyberbullying (Monori, 2016).

Adatvédelmi aggályok az eljárásjogi rendelkezésekkel összefüggésben

Az adatvédelem (*privacy*) már az egyezmény megszövegezésekor is olyan alapvető jognak számított, amelyre jelentős figyelem fordult a korszerű számítógépes technológiák által lehetővé tett nagymértékű adatfeldolgozással összefüggésben. A Budapesti Egyezmény számos olyan eljárásjogi rendelkezést tartalmaz, amelyek biztosítják a nyomozó hatóságok számára, hogy adatmegőrzésre, adatok szolgáltatására, illetve együttműködésre kötelezzenek magánszemélyeket, illetve piaci szereplőket (pl. internetszolgáltatókat) is (Sorbán, 2019). Az egyezmény 16. 17. és 18. cikkei szólnak az adatmegőrzésről,

míg a 19–20. cikkek az adatok lefoglalásáról, a házkutatásról, illetve a lehallgatásról. Az egyezmény ezen rendelkezései Magyarországon már a régi Be.-ben is helyet kaptak (Sorbán, 2016) és (Máté, 2014), annak ellenére, hogy kritikus hangok világszerte arra figyelmeztettek, hogy veszélyeket rejthet magában, ha a nyomozó hatóságoknak tág körben van lehetőségük a magánszféra megsértésére a büntetőeljárás keretei között, anélkül, hogy pontos iránymutatások állnának rendelkezésre arról, hogy meddig terjedhet a nemzeti hatóságok jogköre (Baron, 2002).

A Budapesti Egyezmény jövője

Mivel az egyezmény a mai napig a számítógépes bűncselekményekkel kapcsolatos nemzetközi szabályozás egyik kiindulópontja, folyamatos fejlesztés alatt áll. Az évek során az Európa Tanács számos útmutatót adott ki az egyes szakaszok értelmezésével kapcsolatban, ezeken felül pedig egy jelentősebb módosítás is folyamatban van. 2017-ben született döntés arról, hogy az egyezményhez egy második kiegészítő jegyzőkönyvet fűznek, amely a bizonyítékok határokon átívelő összegyűjtésének, az egyes internetes közvetítő szolgáltatók szerepének, a jogsegélynek, valamint az adatvédelemnek a kérdéseit fogja rendezni a 21. századi elvárásoknak megfelelően. A 2. kiegészítő jegyzőkönyv tervezett szövegét várhatóan a 2021. év folyamán hozzák nyilvánosságra.

Minden kritikája ellenére tehát a Budapesti Egyezmény egy élő, folyamatosan fejlődő jogi aktus, melyet világszerte széles körben elfogadnak. Éppen ezért teremthet nehéz helyzetet a kiberbűnözés elleni harcban egy olyan kezdeményezés, melyet Oroszország indítványozására egyre több ENSZ-tagállam támogat, és melynek célja a jelenlegi globális megközelítés helyett egy, a nemzeti szuverenitást jobban kiemelő egyezmény megalkotása. Az internet nem ismer határokat, így nehezen elképzelhető, hogy egy, az egyezményhez hasonló, határokon átnyúló megegyezés nélkül érdemben üldözhetők

lesznek például az internethasználók milliárdjait érintő internetes csalások vagy a gyermekeket érintő szexuális visszaéléseket megjelenítő internetes tartalmak.

Köszönetnyilvánítás

A tanulmány megírásában jelentős segítséget nyújtottak, és ezért köszönet illeti a Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézetének kutatóit, dr. Gyaraki Rékát, dr. Mezei Kittit, dr. Nyáry Gábort és dr. Sorbán Kingát.

Irodalom

Baron, Ryan MF. (2002). A critique of the international cybercrime treaty, *IO CommLaw Conspectus* 263 (2002), 277. o.

Commission of the European Communities (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime COM (2007) 267 final A letöltés ideje: 2021. március 8. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

Council of Europe (2001). Explanatory Report to the Convention on Cybercrime. European Treaty Series – No. 185. A letöltés ideje: 2021. március 5. https://rm.coe.int/16800cce5b

Council of Europe (2009). Project on Cybercrime. Final Report (September 2006 - February 2009). A letöltés ideje: 2021. március 4. https://rm.coe.int/16802fa0b7

Council of Europe (2019). Cybercrime and Cybersecurity Strategies in the Eastern Partnership region. A letöltés ideje: 2021. március 4. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

Council of Europe (2020a). 2020 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime. A letöltés ideje: 2021. március 4. https://rm.coe.int/24-7-november-2020-meeting-report/1680a1271d

Council of Europe (2020b). C-PROC Activity Report for the Period of October 2019 – September 2020. A letöltés ideje: 2021. március 4. https://rm.coe.int/sginf-2020-32-c-proc-activity-report-oct-2019-sept-2020/1680a05aea

Gercke, Marco (2012). Understanding cybercrime: phenomena, challenges and legal response. A letöltés ideje: 2021. március 8. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=AroundWeb

Gillespie, Alisdair A. (2018). Child pornography. *Information & Communications Technology Law*, 27 (2018), 1., 30–54. 31. o.

Greijer, Susanna, Doek, Jaap (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. A letöltés ideje: 2021. március 8. https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf

Gyaraki Réka (2012). A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN-kód megadása sikeres vagy biztonságos az internet?! *Pécsi Határőr Tudományos Közlemények*, XIII. 237–238.

Máté István Zsolt (2014). A digitális bizonyíték. In: Törő Csaba – Cservák Csaba – Rixer Ádám – Fábián Ferenc – Miskolczi Bodnár Péter – Deres Petronella – Trencsényiné Domokos Andrea (szerk.): *IX. Jogász Doktoranduszok Országos Szakmai Találkozója 2013*, Budapest, Károli Gáspár Református Egyetem, pp. 86–94.

Mezei Kitti (2018a). Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. *JURA 24*, 1 pp. 349–360.

Mezei Kitti (2018b). A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro*, 2018/1.

Mezei Kitti (2019a). A kiberbűnözés szabályozási kihívásai a büntetőjogban. *Ügyészek Lapja*, 4–5.

Mezei Kitti (2019b). A szervezett bűnözés az interneten. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. MTA Társadalomtudományi Kutatóközpont–PTE ÁJK, Budapest–Pécs, 2019.

Monori Zsuzsanna (2016). Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. *In Medias Res*, V. (2016) 2., 246–261.

Papp Péter (2002). Etikus hacking. *Belügyi Szemle*, 2002/11–12.

Sorbán Kinga (2016). A digitális bizonyíték a büntetőeljárásban. *Belügyi Szemle* 64 (2016) 11., 81–96.

Sorbán Kinga (2018). Vírusok és zombik a büntetőjogban – Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res*, 2018/2.

Sorbán Kinga (2019). Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában: Felelősség és kötelezettségek. *In Medias Res*, VIII (2019), 1 pp. 84–101.

Sorbán Kinga (2020). A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle* 68 (2020) 10. 81–104.

Szathmáry Zoltán (2020). Etikus és nem etikus hacking – a kéretlen sérülékenységvizsgálat büntetőjogi kérdései. *Magyar Jog*, 2020/6.