Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

Mezei Kitti

A kiberbűnözés egyes büntetőjogi szabályozási kérdései

Doktori értekezés tézisei

Témavezetők:
Prof. Dr. Tóth Mihály DSc. professor emeritus
Dr. Nagy Zoltán András habil. egyetemi docens

Pécs, 2019

TARTALOMJEGYZÉK

I. A kitűzött kutatási feladat rövid összefoglalása

1.1. A témaválasztás indokolása, aktualitása[1]

Nem túlzás azt állítani, hogy a technológiai innováció mindannyiunk életét érinti. Ez a dinamikus fejlődés a jogrendszert is folyamatos kihívások elé állítja, ezért szükséges, hogy az új technikai újításokkal kapcsolatban felmerülő jogi kérdésekre, problémákra reflektálni tudjunk. Mindez azért is különösen fontos, mert az egyes társadalmi és gazdasági folyamatok egyre inkább függenek az információs rendszerektől, valamint meghatározhatják a gazdasági szereplők versenyképességét. Az információs társadalom egyik jellemzőjévé vált az infokommunikációs eszközök számának, sokféleségének a növekedése és használatuk széleskörű elterjedése.

A gyors ütemű informatikai fejlődésnek a nyilvánvaló előnyei mellett megvannak a maga veszélyei is, hiszen lehetőséget teremt a bűnözés eddig ismeretlen formái számára. Éppen ezért a kiberbűnözés jelenti napjaink egyik legnagyobb kihívását. Az új technológiák megjelenése (pl. mobilinformatikai és okoseszközök, Internet of Things[2]), a megvalósítható funkciók bővülése, illetve az információs hálózatok használatának az elterjedése magukkal hozzák az újabb elkövetési módokat, illetve büntetendő cselekmények körét.[3] A tisztán informatikai bűncselekményeken kívül (pl. hacking, adatmanipuláció, számítógépes vírusok) ma már szinte bármelyik hagyományos bűncselekmény (pl. csalás, zsarolás, pénzmosás) is elkövethető az információs rendszerek használatával, az interneten keresztül. Mindez kihívások elő állítja mind a jogalkotást a büntetőjogi szabályozásra tekintettel, mind a jogalkalmazást a büntetendő magatartások minősítéseinek kérdéseiben.

A büntető igazságszolgáltatás hatékonyságának növelése egyre sürgetőbben veti fel e téma kutatásának az igényét. Ennek ellenére a hazai szakirodalom keveset foglalkozik az informatikai bűnözés aktuális szabályozási kihívásaival a büntetőjogban, ezért a témát érintő tudományos kutatás hiánypótlónak tekinthető.

---

[1] A doktori értekezés az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV és ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának keretében készült.

[2] Az „Internet of Things”, vagy rövidítve „IoT”, mellyel a mindennapjainkban használt - gyakran „okos” elnevezésű - eszközök az interneten keresztül is elérhetőek, és képesek egymással akár önállóan is kommunikálni. Ennek a kommunikációnak a motorja az ún. M2M (machine-to-machine) technológia, ami olyan adatáramlást jelent, mely emberi közreműködés nélkül, gépek között zajlik. A kommunikáció minden olyan gép között létrejöhet, amely a megfelelő technológiával (érzékelőkkel, chipekkel) van ellátva ahhoz, hogy csatlakozzon a rendszerhez.

[3] NAGY Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum Kft. Budapest, 2009. 23-24. o.

Az internetnek számos olyan jellemzője van, amelyek egyben a használatával összefüggő visszaélések térnyerésére, illetve a bűncselekmények hatékonyabb elkövetésére is lehetőséget teremtenek. Az internetre csatlakozott eszközök és felhasználók száma évről évre növekvő tendenciát mutat. Mivel egy egész világra kiterjedő hálózatról van szó, amely azonnali és valós idejű kapcsolatteremtésre nyújt lehetőséget, a kiterjedt online jelenlét lehetővé teszi a tömeges informatikai támadások végrehajtását. A lényegét az elektronikus formában megjelenő nagy mennyiségű adat, információ jelenti („Big Data" jelenség)[4]. Az internet ennélfogva speciális, de egymással összefüggő tulajdonságokkal rendelkezik, amelyek egyúttal megkönnyíthetik a különféle bűncselekmények elkövetését, azonban már egy új színtéren.

Az internet globális jellege lehetőséget nyújt a határon átívelő bűnözés számára. Az elkövetők a világ bármely pontján kereshetnek célpontokat, illetve sebezhetőségeket, és ehhez még arra sincs szükségük, hogy az elkövetéskor fizikailag akár egy országon belül tartózkodjanak, a bűnözői infrastruktúrájukat is különböző államokból irányíthatják. Ez pedig olyan összetett joghatósági és illetékességi kérdéseket vet fel a büntető eljárásjogban, amelyek a mai napig megválaszolásra várnak.

Az internet egyben decentralizált és rugalmas hálózatok létrehozására ad lehetőséget, amelyek az elkövetők laza szerveződését segítik elő például, hogy egymás között megoszthatják a szakmai tudásukat és jártasságukat, valamint az általuk kifejlesztett technikai eszközöket. Az internet egyben egy kommunikációs csatornaként is szolgál, amely a különböző bűncselekmények elkövetésében is fontos szerepet tölthet be. Ennek következtében napjainkra a kiberbűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé nőtte ki magát, amelynek motorját az online feketegazdaság adja (pl. Darknet fórumok), ahol a különböző kibertámadásokat elősegítő eszközök és egyéb illegális szolgáltatások is elérhetőek. Emellett az internet relatív névtelenséget biztosít, és ezt a bűnelkövetők fokozhatják a különböző titkosítást és anonimitást biztosító technológiák használatával, amelyek alkalmasak a személyazonosság elrejtésére. Ezért a szervezett bűnözés, de a terrorizmus képviselői is előszeretettel használják az internetet, legyen szó illegális online kereskedelemről vagy propagandaterjesztésről.

Azzal, hogy a sértettekkel egy távoli kapcsolatfelvételt garantál, az internet megszünteti azokat a szociális akadályokat is, amelyekkel az elkövetőknek a valóságban, akár egy személyes találkozáskor kellene szembenézniük. Az ilyen típusú bűnözésre magas látencia

[4] A „Big Data" kifejezés az interneten megjelenő hatalmas mennyiségű adatmennyiségre utal, amely új társadalmi jelenségként a jogalkotást és a jogalkalmazást is kihívások elé állítja. Lásd ZŐDI Zsolt: Jog és jogtudomány a Big Data korában. Állam- és Jogtudomány 2017/1. 95. o.

jellemző, mert a gyanútlan felhasználók sokszor nem is észlelik, hogy bűncselekmény áldozatává váltak és a hatóságok felé nem jelentik az esetet (pl. bankkártya visszaélések, pénzintézetek ellen intézett támadások), amely tovább nehezíti a felderítést.

Az információs rendszerek segítségével és az internet közbeiktatásával könnyedén lehet végrehajtani adat- vagy program manipulációt minimális költségek mellett, mert az információk elektronikus megjelenítésének köszönhetően lehetőség van az adatok másolására minőségi veszteség nélkül, valamint módosítására anélkül, hogy annak látható nyoma lenne.

Az online környezet lehetővé teszi az automatizált műveleteket, amelyek rendkívül gyorsan, jelentős kárt tudnak okozni, mivel egy rosszindulatú program képes sokszorosítani önmagát és akár több millió rendszert megfertőzni egyidejűleg (pl. a WannaCry zsarolóvírus), vagy egy botnet-hálózat segítségével az elkövetők nagyszabású támadásokat tudnak végrehajtani, amely akár az adott rendszer teljes leállásához is vezethet.[5]

2017-ben a kiberbűnözés által okozott kár 600 milliárd dollár értékben realizálódott a különböző sértetti köröknél (pl. vállalatok, pénzintézetek, kormányzati szervek stb.) és a szakértők szerint ez 2021-re meg fog duplázódni. Mindez úgy gondolom, rávilágít arra, hogy mekkora lehetőség rejlik az új technológiák által nyújtott előnyök bűnelkövetési célú felhasználásában, ugyanakkor mekkora veszélyt és kockázatot hordoz a felhasználókra nézve.[6]

Az utóbbi években Magyarországon is jelentős emelkedés tapasztalható az informatikai bűncselekmények számában. Míg öt évvel ezelőtt csak 250 csalást követtek el információs rendszer felhasználásával, addig 2017-ben ez megközelítette a 4 és fél ezret. Ez idő alatt az információs rendszer vagy adat megsértésével kapcsolatos regisztrált bűncselekmények száma megtízszereződött, 52-ről 580-ra nőtt.[7]

1.2. Az értekezés tárgya és szerkezete

A disszertációmban elsősorban büntető anyagi jogi, és csak érintőlegesen büntető eljárásjogi kérdésekkel foglalkozom. Továbbá kizárólag az ún. tisztán informatikai bűncselekményekre, valamint a technológiai fejlődésnek az egyes – tágabb értelemben vett – gazdasági bűncselekményekre gyakorolt hatására fókuszálok.

---

[5] KOOPS, Bert-Jaap: The Internet and its Opportunities for Cybercrime. Tilburg School Legal Studies Paper Series No. 2011/9. 740-741. o.
[6] MCAFEE: Economics Impact of Cybercrime – No Slowing Down Report February 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf [2018.05.23.]
[7] LAJTÁR István: A kiberbűnözésről. Ügyészek Lapja 2019/1. 49. o.

Az értekezés négy nagy szerkezeti részre tagolódik. A bevezetést követő II. fejezetben a kiberbűnözés fogalmának a tisztázásával foglalkozom, ami azért is különösen fontos, mert máig nincs egy általánosan elfogadott jogi definíciója. Törekedtem mind a nemzetközi, mind a hazai szakirodalmi álláspontok széleskörű bemutatására, amelyek összevetése alapján meghatározható az informatikai bűnözés tágabb és szűkebb értelemben vett fogalmába tartozó bűncselekményi kör.

Ezt követően a kiberbűnözés elleni fellépés nemzetközi és uniós vonatkozásaival foglalkozom. Továbbá kiemelten vizsgálom az Egyesült Államok szabályozás történetét, amely elsőként szankcionálta és határozta meg az informatikai bűncselekmények széleskörét, ezért a kutatási téma szempontjából megkerülhetetlen.

A történeti részt követően az egyes kiberbűncselekményeket részletesen elemzem. Összehasonlítom a nemzetközi és uniós rendelkezéseket, valamint a hatályos hazai és amerikai szabályozás szerinti tényállásokat. Az alábbi három fő kibertámadás büntetőjogi minősítésével kezdem: a jogosulatlan belépéssel, illetve a DDoS-támadásokkal és a rosszindulatú programokkal. Ezután, az informatikai környezetben elkövetett csalással és zsarolással, valamint az egyéb informatikai visszaélésekkel kapcsolatos kérdésekkel (pl. személyes adatokkal és jelszavakkal való visszaélés) folytatom.

A III. fejezetben a modernizációnak a gazdasági bűncselekményekre gyakorolt hatásával kapcsolatos problémakört vizsgálom. Kiemelten érintem a bankkártyákkal összefüggő deliktumokat, ezen kívül a szervezett bűnözés megjelenését az interneten és a pénzmosás aktuális kérdéseit. A témakört a kriptovaluták büntető anyagi és eljárásjogi kihívásainak bemutatásával zárom.

A IV. fejezetben kiemelt szerepet kap az elektronikus bizonyítékokkal összefüggő szabályozási újdonságok bemutatása, így a hazai büntetőeljárásról szóló törvény[8] (a továbbiakban: Be.) hatályos rendelkezései és az erre vonatkozó uniós jogalkotási törekvések, Kiemelten foglalkozom továbbá a titkosítást és az anonimitást biztosító technológiák nyomozásra gyakorolt hatásával, valamint a joghatósági kérdésekkel a kiberbűncselekmények elkövetése esetén.

[8] 2017. évi XC. törvény a büntetőeljárásról

II. A kutatás módszerei és célja

2.1. A kutatás módszerei

Az értekezés elkészítése során a témakör szempontjából lényeges nemzetközi, uniós, magyar és angolszász jogforrások kerültek felhasználásra. A joganyagok elemzése mellett az egyes részeknél hangsúlyt fektettem a vonatkozó joggyakorlatok bemutatására, valamint az adott kérdésköröket tárgyaló, releváns nemzetközi, hazai jogirodalmat és kutatási eredményeket dolgoztam fel.

A téma sajátos jellegéből adódóan interdiszciplináris keretek között tekintem át a technológiai fejlődés következtében megjelenő új kihívásokat és az ezekre adható válaszokat a büntetőjogban. A jogösszehasonlító módszertan szintén jelen van az értekezésben. Összevetem a különböző szabályozási szinteket és azok rendelkezéseit, illetve a vonatkozó joggyakorlatot, különös figyelemmel azok hasonlóságaira és különbözőségeire.

A kutatás során alkalmazom még továbbá a normatív és a dogmatikai módszert, valamint az egyes részeknél a logikai és kritikai elemzés is szerepet kap is.

2.2. A kutatás célja, problémafelvetés

Az értekezésemben a következő kutatási kérdésekre keresem a választ:

1. Alkalmas-e a jelenlegi szabályozási környezet nemzetközi, uniós és hazai szinten, valamint az Egyesült Államokban a kiberbűnözés elleni fellépésre?
2. Képes-e a hazai büntetőjogi szabályozás és jogalkalmazás reagálni, alkalmazkodni a technológiai fejlődés következtében bekövetkezett változásokra az egyes gazdasági bűncselekmények esetén?
3. Alkalmasak-e az uniós és a hazai törekvések a büntetőeljárás során felmerülő technológiai kihívásokkal kapcsolatos aktuális szabályozási kérdések megoldására, különös tekintettel az elektronikus bizonyítékokra?

III. A kutatási eredmények bemutatása és összefoglalása

Összeségében elmondható, hogy mind a nemzetközi színtéren, mind az Egyesült Államokban egészen az 1970-es évekig nyúlnak vissza a kiberbűnözéssel kapcsolatos kezdeti törekvések. Közös vonásuk, hogy a meglévő, hagyományos bűncselekményekre vonatkozó szabályozás helyett, elkezdték a speciális és önálló anyagi büntetőjogi rendelkezések megalkotását az új típusú informatikai bűncselekmények vonatkozásában. Az Európa Tanács több évtizedes munkájának eredményére 2001-ig, a Budapesti Egyezmény[9] elfogadásáig kellett várni. Ez az első olyan kötelező erejű, multilateriális és a mai napig legjelentősebb jogi dokumentum, amely a kiberbűnözés elleni küzdelem alapjait teremtette meg. Az aláírásához csatlakozó országok számára keretet biztosít a nemzetközi együttműködéshez, továbbá olyan államok előtt is nyitva áll, amelyek nem tagjai az Európa Tanácsnak, így többek között az Egyesült Államok is ratifikálta. A Budapesti Egyezmény elősegíti az informatikai bűnözés elleni küzdelmet nemzetközi, uniós és az egyes országok regionális szintjén, különösen a közös büntető anyagi és eljárásjogi szabályokkal, valamint a technikai jellegű fogalmak világos meghatározásával.

A másik nagy előrelépést uniós szinten a 2013-as irányelv[10] jelentette, amely az információs rendszerek elleni támadásokkal szemben lép fel a szükséges minimumszabályok megalkotásával. Felismerték, hogy rendkívül fontos a harmonizált és egységes szabályozás megteremtése mind büntető anyagi, mind eljárásjogi tekintetben, ami azért is kihangsúlyozandó, mert egy határokon átívelő bűnözésről van szó, és az elkövetők kihasználhatják a különböző országok jogrendszerének a szabályozási hiányosságait, differenciáltságát.

Az egyes országok általában különböző szabályozási megoldást választanak a kiberbűncselekmények körében. Jellemző, hogy vagy egy külön törvényben szabályozzák ezen deliktumokat, vagy a nemzeti büntető törvénykönyvükbe önálló fejezetbe iktatják a vonatkozó rendelkezéseket, vagy a különös részben helyezik el szétszórtan a tényállásokat.

Az Egyesült Államok az előbbi megoldást alkalmazva, szövetségi szinten, először 1984-ben, az uniós törekvéseket megelőzve szabályozta az informatikai bűncselekményeket, méghozzá egy külön törvénykönyvben. Ahhoz, hogy a Computer Fraud and Abuse Act (CFAA) lépést tudjon tartani a technológiai innovációval már nyolc alkalommal módosították 1986 és 2008

[9] Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye, amelyet a 2004. évi LXXIX. törvénnyel hirdettek Magyarországon

[10] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. HL L 218/8. 2013.8.14.

között. A változtatások közös céljaként felismerhető, hogy a törvény hatályát minél szélesebb körben igyekeztek kiterjeszteni. Például a szövetségi érdekű számítógép szűk fogalmától eljutottak a tágabb értelemben vett számítógép meghatározáshoz, amelynek hatálya alá tartozik lényegében majdnem valamennyi, a világ bármely részén használt, akár egy háztartási eszközként funkcionáló számítógép is. Továbbá a büntetendő cselekmények körét is fokozatosan bővítették, így jutottak el a hatályos szabályozás szerinti hét informatikai bűncselekményhez.

3.1. Az informatikai bűncselekmények

Az első kutatási kérdésemmel kapcsolatban azt vizsgáltam, hogy a jelenlegi szabályozási környezet nemzetközi, uniós és hazai szinten, valamint az Egyesült Államokban mennyiben alkalmas a kiberbűnözés elleni fellépésre. Ezzel összefüggésben a következőkre jutottam:

A Budapesti Egyezmény elfogadása óta eltelt időben a technológiai fejlődés a megállapodás egyes rendelkezéseit már meghaladta, ezért szükségessé vált, hogy további jegyzőkönyvvel egészítsék ki, amely orvosolná ezeket a szabályozási hiányosságokat.

A 2013-as irányelv már az új kihívásokra részben reagált azzal, hogy az információs rendszerek elleni támadásokkal kapcsolatos büntetőjogi szabályait az újabb veszélyforrások figyelembevételével határozta meg (pl. büntetendő és szigorúbb büntetés alkalmazását teszi lehetővé a botnetekkel végrehajtott vagy a kritikus infrastruktúrák ellen irányuló kibertámadások esetén, valamint a személyazonosság-lopást is említi).

Magyarországon az elmúlt években az informatikai bűncselekmények szabályozása a nemzetközi és uniós elvárásoknak megfelelően alakult. A Btk. hatályba lépésével már annak önálló fejezetébe lettek illesztve, ami mindenképpen egy üdvözítő megoldás és haladás az új védendő társadalmi értékek elismerése felé. Nóvumként jelent meg az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) tényállása, amely a vagyon elleni bűncselekmények között kapott helyet, amelyet a jogalkotó az eltérő jogtárgy védelemmel indokolt.

Az értekezésemben vizsgáltam a leggyakrabban előforduló informatikai támadásokat, így kiemelten a jogosulatlan belépést, DDoS-támadásokat és a rosszindulatú programokkal kapcsolatos büntetőjogi szabályozási és minősítési kérdéseket. Mindezek alapján úgy gondolom, hogy a magyar szabályozás jelenleg alkalmas arra, hogy az informatikai környezetben elkövetett büntetendő magatartások széleskörét lefedje az információs rendszer elleni bűncselekmények körében, így az információs rendszer vagy adat megsértése (Btk. 423.

§) és ezen rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424. §) tényállásaiban.

A jogalkotó azonban egyes kérdésekben adós maradt, például nem határozza meg pontosan az előbbi bűncselekmény minősített eseténél [Btk. 423. § (3) bekezdés], hogy mi tekinthető jelentős számú információs rendszernek, tehát a jogalkalmazókra hárul ez a feladat, hogy egy erre vonatkozó gyakorlatot dolgozzanak ki. A joggyakorlat részben egyes kérdéseket megválaszolt, ugyanis a hacking rendelkezés második fordulatánál [Btk. 323. § (1) bekezdés] a Kúria elvi éllel mondta ki, hogy a jogosultság keretein való túllépés is akkor minősül bűncselekménynek – az első fordulat szerinti jogosulatlan belépéshez hasonlóan –, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik.[11]

A másik felmerült problémakör az etikus hackinghez kapcsolódik, amely sokszor éles vita tárgyát képezi, és visszavezethető arra, hogy hiányzik a megfelelő szabályozása és gyakorlata. A szakirodalmi álláspont szerint az információs rendszer tulajdonosa vagy egyéb jogosultja által más számára engedélyezett biztonsági tesztelés, illetve támadás tartozik ebbe a tevékenységi körbe. Erre utal rendelkezéseiben a Budapesti Egyezmény és a 2013-as irányelv is, amelyek szerint a büntetendő cselekményt jogosulatlanul kell elkövetni, ami azt jelenti, hogy ez a rendszer jogosultjának az engedélye nélkül történik. Ez különösen akkor vitatott, ha a hacker valamilyen sebezhetőségre hívja fel a figyelmet, különösen, ha a nagy nyilvánosság felé is közvetíti. A konkrét ügy során ezért a bíróságnak vizsgálnia kell az eset összes körülményére tekintettel a következőket: a hacker cselekménye mennyiben veszélyes a társadalomra, milyen szándék húzódott e magatartása mögött, valamint közérdekű bejelentésnek tekinthető-e az eljárása a megtámadott fél felé.

A hazai és amerikai szabályozást összevetve megállapítható, hogy utóbbi részletesebben szabályozza az egyes informatikai bűncselekményeket. Példaként említhető, hogy a jogosulatlan hozzáféréssel kapcsolatban több tényállást alkottak, valamint a DDoS-támadásra és a számítógépes vírusokra vonatkozó rendelkezéseknek hat minősített esete van, sőt külön számítógépes csalás és zsarolás deliktuma is rendelkezésre áll. Esetenként a kiszabható büntetések is sokkal szigorúbbak, ha például az elkövetőt korábban elítélték már informatikai bűncselekmény elkövetéséért, akkor akár tíz vagy húsz évig terjedő szabadságvesztést is megállapíthat a bíróság, továbbá az esetjoga is sokkal gazdagabb. A különbségek is tetten érhetők, azonban ez részben betudható annak, hogy a CFAA alapját az angolszász jogrendszer

[11] BH 2017.12.392.

képezi. Az amerikai szabályozás egyes tényállásoknál a felelősség alapján differenciál, amely érintheti az elkövetési magatartáshoz (tudatos vagy szándékos elkövetés) vagy az eredményhez kapcsolódó felelősséget (szándékosan vagy gondatlanságból vagy hanyagságból történő károkozás), míg a Btk. kizárólag a szándékos elkövetést rendeli büntetni. További különbség, hogy az amerikai jog a védett számítógéphez való hozzáférés korlátozásának két típusát határozza meg: a technikai védelem (code-based) és a szerződés (contract-based) alapján. A magyar szabályozás azonban megköveteli a technikai intézkedés megsértését vagy kijátszását a tényállásszerűséghez, valamint a 2013-as irányelv is rögzíti, hogy például felhasználói szabályzat vagy szolgáltatási feltételek révén korlátozó szerződéses kötelezettségek vagy megállapodások nem vonhatnak maguk után büntetőjogi felelősséget. Hasonló elkövetői kör büntethető mindkét törvény alkalmazásában, így aki a hozzáférési jogosultsággal nem rendelkező („kívülálló") személy vagy jogosultsággal rendelkező, de ennek kereteit túllépő („bennfentes") személy.

A CFAA legnagyobb hiányossága abban ragadható meg, hogy az egyes alapvető fogalmakat nem tisztázza, így többek között „a jogosulatlan hozzáférést" (unauthorized access), valamint a számítógépes adatot, avagy a CFAA-ban használt elnevezés alapján „az információt" (information) és a hozzáférést biztosító jelszavat, valamint a programokat sem. Következésképp, ezeknek az értelmezése a jogalkalmazókra hárul, különösen a precedensek megteremtésével. Ezzel szemben a hazai szabályozás e tekintetben jobban alkalmazható, mert ezen fogalommeghatározások elérhetők a Btk. rendelkezései között. A CFAA esetében látszik, hogy védendő jogi tárgyként elsősorban a védett számítógép áll a középpontban, amelyet alátámaszt az is, hogy a fogalmának tisztázása több évtizedes folyamat eredménye. Ezzel szemben a magyar tényállások fordulatai az információs rendszert, valamint a számítógépes adatot egyaránt védik. Mindkét szabályozás reagál arra, hogy a támadások indítására szolgáló eszközöket, programokat már akár szolgáltatásként is igénybe lehet venni vagy akár megvásárolni az interneten keresztül. Ez a kibertámadások végrehajtását rendkívül megkönnyíti, hiszen könnyen hozzá lehet jutni a bűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár a már kész botnet infrastruktúrához, és ezért is fontos, hogy már az előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra.[12]

[12] Lásd Btk. 424. § információs védelmét biztosító intézkedés kijátszása, valamint CFAA 1030. § (a)(6) hozzáférést biztosító jelszavakkal vagy egyéb információkkal való visszaélés.

3.2. A technológiai fejlődés hatása a gazdasági bűncselekményekre

A második kutatási kérdésemben arra kerestem a választ, hogy képes-e hazai büntetőjogi szabályozás és jogalkalmazás reagálni, alkalmazkodni a technológiai fejlődés következtében bekövetkezett változásokra az egyes gazdasági bűncselekmények esetén. Ezzel kapcsolatban az alábbi következtetésekre jutatottam:

Az új fizetési eszközök használatának elterjedésével egyidejűleg megjelennek azok a bűnelkövetők, akik vissza kívánnak élni velük, ezzel párhuzamosan pedig új elkövetési módok megjelenésével is számolni kell. Éppen ezért fogadták el a 2019-es irányelvet[13], amelynek célja a minimumszabályok meghatározása volt az immateriális és materiális, speciális védelemmel ellátott készpénz-helyettesítő eszközök védelme érdekében. A szabályozás újdonsága abban ragadható meg, hogy már a hatálya alá tartoznak a fizetésre használt virtuális fizetőeszközök, vagyis a kriptovaluták, valamint a mobilalkalmazások a hozzátartozó jelszóval együttesen, amennyiben alkalmasak fizetési utalások lebonyolítására. A Btk. hatályba lépése óta megfelel az irányelvben rögzített bűncselekmények tényállási elemeivel szemben támasztott követelményeknek, ezért ezek módosítására nincs szükség. Mindezek alapján a hazai szabályozási környezet megfelelő, és úgy vélem, hogy elsősorban a jogalkalmazók számára jelent kihívást az új elkövetési módoknak a nyomon követése, továbbá az egyes elkövetési magatartások minősítése okozhat problémát a gyakorlatban. Ezért is törekedtem arra, hogy részletesen ismertessem a bankkártyákkal és különböző banki átutalásokkal kapcsolatos visszaéléseket, amelyek a kiberbűnözés egyik kiemelt részterületeként értékelhetők. A card-present csalás terén az elkövetők az ún. skimminget és újabb technikákat alkalmaznak annak érdekében, hogy a fizikailag hozzáférhető bankkártya adatokat minél könnyebben megszerezzék. Ennél azonban nagyobb számban vannak jelen az internet használatához köthető card-not-present csalások, amelyek során az adathalászok egyre kifinomultabb technikák alkalmazásával szerzik meg a gyanútlan felhasználók adatait. Ezek egyaránt különösen nagy kihívást jelentenek nem csak a nyomozó hatóságok, hanem a pénzintézetek számára is.

A bűnelkövetők gyorsan átveszik és integrálják az új technológiákat a különböző bűncselekmények elkövetésekor és olyan üzleti modelleket alkalmaznak, amelyeknek az alapját egyre inkább az internet használata jelenti. A hagyományos szervezett bűnözői csoportok is felismerték az internet használatában rejlő lehetőségeket. Megfigyelhető az

[13] Az Európai Parlament és a Tanács (EU) 2019/713 irányelve (2019. április 17.) a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról. HL L123/18, 2019.5.10.

informatikai újítások kihasználása, amely magában foglalja például az illegális online kereskedelmet és a titkosított kommunikációs csatornák használatát.

Megállapítható, hogy az új technológiai vívmányok lényeges és maradandó hatással vannak a bűnözés természetére. Már a hagyományos szervezett bűnözés is kihasználja az internet nyújtotta előnyöket, például az illegális kereskedelmi tevékenységüket a magas fokú anonimitást biztosító Darknet piactereken és fórumokon folytatják (pl. kábítószer-kereskedelem, gyermekpornográfia). Mellettük megjelentek olyan kiberbűnözői csoportok is, amelyek sajátos üzleti modellt alkalmaznak (Criminal-to-Criminal), amelynek keretében az informatikai bűncselekmények elkövetéséhez szükséges eszközöket és szolgáltatásokat nyújtanak. Ezen kívül akár szaktudásukkal segíthetik a bűnszervezeteket egyes súlyos bűncselekmények elkövetésében, valamint az informatikai infrastruktúrájuk fenntartásában. Előbbi esetben éppen ezért, akár a hazai szabályozás szerinti bűnszervezetben elkövetett bűncselekmény jogkövetkezményei miatt is felelősségre lehet vonni az illetőt, míg utóbbi esetben a bűnszervezetben részvétel miatt. 2019-ben a bűnszervezet büntetőjogi fogalma szűkült, mert már további többletkövetelménnyé vált annak bizonyítása is, hogy a csoport hierarchikusan szervezett és konspiratívan működik. A kiberbűnözői csoportok azonban természetüknél fogva nehezen illeszthetők be a szervezett bűnözés hierarchikus, homogén struktúrájába. Összeségében elmondható, hogy az internet új színtérként szolgál mind a régi szervezett, és mind az új típusú bűnözésnek, illetve mindkettő egymás mellett tud működni anélkül, hogy egymást kizárnák, amely az online tér speciális jellegének köszönhető.

Manapság a pénzmosás különböző – akár már online – pénzügyi műveletek láncolatát foglalja magában, célja a pénz bűnös eredetének elrejtése és tisztára mosása a pénzintézetek hálózatában. A gyakorlatban a saját pénzmosással kapcsolatban, különösen az eredetleplezési célzatra tekintettel merülnek fel kérdések. Az egyes tranzakciók ugyan felvethetik a pénzmosás gyanúját, de a saját pénzmosás deliktumának megállapításához szükséges eredetleplezési célzatot nem lehet kiterjesztően értelmezni. Ennek következtében kiemelten fontos az utócselekmények célzatának a körültekintő vizsgálata, például egy adott pénzösszeg banki továbbutalása az alapbűncselekményből származó haszon realizálását szolgálja-e, vagy magát az alapbűncselekmény leplezését. Az elkövetőnek ez esetben mi a magatartásával célja, hogy a büntetőjogi felelősségre vonást elkerülje, vagy valóban a pénz bűnös eredetét és annak további útját kívánja leplezni. Továbbá vizsgálandó, hogy ezek a műveletek mennyiben alkalmasak a leplezési cél eléréséhez, ugyanis, ha ezek tételesen nyomon követhetőek, illetve átláthatók, akkor alkalmatlanok a jogtárgysértésre, ezért nem jön létre bűncselekmény. A Kúria döntésében elvi éllel mondta ki, hogy egy adott elkövetési magatartás (vagy magatartássorozat) egyidejűleg

az alapbűncselekmény és a pénzmosás tényállását nem merítheti ki.[14] Ez azért is kizárt, mert a kétszeres értékelés tilalmába ütközne, ennek ellenére az ügyészségnél megfigyelhető egy a halmazatot bővítő gyakorlat. Ezen kívül a legnagyobb kihívást a pénzmosás terén a pénzfutárok (money mule) alkalmazása jelenti. Egyre gyakrabban az interneten keresztül jogszerű tevékenység látszatát keltve toboroznak, szerveznek be embereket, hogy a bűncselekményekből származó pénzek továbbutalását vagy felvételét végezzék. A különböző bankszámlákra felaprózott kisebb pénzösszegek nem feltűnők, így a pénzmosás ellenőrzéseken sem akadnak fent, ezért igencsak nehéz a felderítésük. A pénzfutárok tudattartamának a vizsgálata kiemelten fontos, mert ez lesz az elkövetési magatartásuk minősítésének az alapja.

Napjainkban már a kriptovalutákkal összefüggésben elkövetett bűncselekmények is egyre nagyobb számban fordulnak elő (pl. csalás, informatikai bűncselekmények, zsarolás, illegális ügyletek során fizetőeszközként jelenik meg), amelyek esetében nem is a bűncselekmény helyes minősítése okozhat problémát a gyakorlatban, hanem az, hogy az elkövetés tárgyát hogyan sorolhatjuk be jogi szempontból, és annak értékét hogyan határozzuk meg. A felderítésük nehézsége pedig a technológiai korlátokból adódik, abból, hogy decentralizált rendszerrel rendelkeznek. Az Unióban felismerték, hogy a kriptovaluták használata és a különböző átváltó, valamint pénztárcaszolgáltatók szolgáltatásainak az igénybevétele pénzmosási és terrorizmus finanszírozási kockázatot hordoz magában. Ezért az ötödik pénzmosás elleni irányelvnek[15] a hatályát már e szolgáltatókra is kiterjesztették, és nekik is meg kell felelni a szigorúbb pénzmosás elleni, avagy „ismerd meg az ügyfeled” szabályoknak. Azonban a kriptovaluták egymás közötti átváltását biztosító szolgáltatókra, valamint a kriptotőzsdékre és a kereskedési platformokra nem alkalmazható az új szabályozás. Továbbá az ilyen szolgáltatások igénybevétele nélkül is van lehetőség a kriptovalutákkal kapcsolatos műveletek végzésére. Újdonságként említhető, hogy az irányelv először határozta meg a virtuális fizetőeszközök fogalmát. A hazai szabályozás vizsgálata során megállapítható, hogy különösen a pénzmosás hazai tényállása világít rá arra, hogy jelenleg e deliktum elkövetési tárgyának, a bűncselekményből származó „dolognak” a fogalmát ki kellene terjeszteni a kriptovalutákra is egy értelmező rendelkezés keretében. Továbbá a jognak nem csak a kriptovalutát, hanem a vele kapcsolatba hozható tevékenységi kört is szabályoznia kell, például az átváltó-, befektetési és pénztárcaszolgáltatókét a pénzügyi vagy kiegészítő pénzügyi

[14] Bfv.I.830/2017/16.

[15] Az Európai Parlament és a Tanács (EU) 2018/843 irányelve (2018. május 30.) a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról. HL L 156/43. 2018.6.19.

szolgáltatások keretében, amelyhez a háttérjogszabály módosítása szükséges, tehát ez elsődlegesen nem a büntetőjog feladata.

3.3. A technológiai kihívások a büntetőeljárás során

A harmadik kérdésem arra vonatkozott, hogy alkalmasak-e az uniós és a hazai törekvések a büntetőeljárás során felmerülő technológiai kihívásokkal kapcsolatos aktuális szabályozási kérdések megoldására, különös tekintettel az elektronikus bizonyítékokra. Ezzel kapcsolatban az alábbi megállapításokat tettem:

Az elektronikus bizonyítékok szerepe egyre inkább felértékelődött a büntetőeljárásban. Ennek megfelelően a Be. is már a kor kívánalmainak megfelelő rendelkezéseket tartalmaz, így a korábbi szabályozáshoz képest előre lépés, hogy külön nevesíti a bizonyítási eszközök között az elektronikus adatot, valamint részletesen szabályozza a rá épülő kényszerintézkedéseket. Azonban a lefoglalás módszertani kérdéseivel nem foglalkozik, annak ellenére, hogy komoly jelentősége van, ezért ennek menetére vonatkozóan hiányzik még egy világos, a gyakorlatban alkalmazható útmutatás. Az új szabályozás előremutató, mert már olyan kérdésekkel is foglalkozik, mint a virtuális vagyontárgyak lefoglalása (pl. a fizetésre használt kriptovaluták). Ugyanakkor ezek még nem nyújtanak megoldást a felmerülő problémákra, mert a hatóságokat több tényező is hátráltathatja a nyomozás során, például az az informatikai eszközöknél használt titkosítást biztosító technológiai védelem (pl. privát kulcs ismeretének hiánya, jelszóval vagy biometrikus azonosítóval védett eszközök és az önvádra kötelezés tilalmának az esete). Emellett amiatt, hogy a jogosult soha nincs fizikai birtokában a kriptovalutáknak, még ha a lefoglalás önmagában sikeres is, akkor sem feltétlenül elégséges, mert rövid időn belül ezek továbbutalhatóak, amennyiben a terhelt rendelkezik a pénztárca fájlról biztonsági másolattal. Éppen ezért ennek biztosítására kikényszerített tranzakció alkalmazására lenne szükség.

A bűnügyi nyomozások során további nehézséget okoz, hogy az elektronikus bizonyítékok gyakran más országokban találhatók, ezért ezek beszerzéséhez igazságügyi együttműködésre és kölcsönös jogsegélyre van szükség. Ezen eljárások azonban rendkívül lassúak, éppen ezért ezt a régóta fennálló problémát egy új rendelet elfogadásával kívánnák orvosolni uniós szinten, amely az elektronikus bizonyítékok határon átnyúló megszerzésének gyorsítását és hatékonyabbá tételét szolgálná. Ehhez két új eszközt szeretnének bevezetni: a közlésre kötelező és a megőrzésre kötelező európai határozatot, amelyek segítségével a hatóságok közvetlenül a szolgáltatókat tudják megkeresni és kötelezni az elektronikus bizonyítékok átadására vagy

megőrzésére. A rendelet részben a Budapesti Egyezmény által is meghatározott adatkategóriákat szabályozza (előfizetői, hozzáférési, tranzakciós és tartalmi), amelyek eltérő szenzitivitásúak, ezért az egyes adattípusoknál az igazságügyi hatóságoknak a beavatkozási lehetősége is differenciáltan jelenik meg. Továbbá a jelenlegi szabályozási környezet nem tud mit kezdeni a felhőszolgáltatókkal, ugyanis sok esetben nem tudják megállapítani, hogy a szolgáltató által tárolt adat egyáltalán hol található az adott pillanatban, így azt sem, hogy melyik állam jogosult eljárni. Azonban az új rendelet részben ezt a kérdéskört is orvosolná azzal, hogy közvetlenül meg lehet a szolgáltatókat keresni, egy másik állam közreműködése nélkül.

Mindezzel szoros összefüggésben jelentős eljárásjogi problémaként merül fel a joghatóság kérdése, amely a kiberbűnözés sajátosságában, a határon átnyúló vagy transznacionális jellegében keresendő. Ez azt jelenti, hogy gyakran az elkövető és a sértett különböző országokban tartózkodik, valamint harmadik országban található információs rendszer közbeiktatásával követik el a bűncselekményt. A bűnelkövetők által használt anonimitást biztosító technológiák a helyzetet bonyolítják, mert könnyedén eltudják rejteni és személyazonosságukat, így földrajzilag azonosíthatatlannak mutatkozhatnak. Az államok a joghatóságuk meghatározásakor elsősorban a hagyományos területi elvet követik, azonban a felvázolt esetek is rávilágítanak arra, hogy ez nem alkalmazható kielégítően a kiberbűncselekmények esetében, ezért e téren mindenképpen paradigmaváltásra van szükség. Amennyiben a joghatóság megállapítása megtörténik, és az eljárás sikeresen zárul, akkor a kiadatás még mindig további problémát jelenthet.

Vitathatatlan tény, hogy a kiberbűnözés negatív hatást gyakorol a társadalomra. Fontos belátni, hogy ez egy olyan komplex problémakör, amellyel szemben egy többlépcsős stratégiának az alkalmazása indokolt. A büntetőjog csak ultima ratio megoldás lehet, a hatékony fellépéshez ezen kívüli eszközökre is szükség van. Például uniós szinten két fontos jogi eszköz áll még rendelkezésre: a GDPR[16] az adatvédelmi incidensek haladéktalan jelentésére kötelezi a vállalkozásokat az egész EU területén, amennyiben ezt elmulasztják, akkor súlyos bírságokkal sújthatják őket. A NIS irányelv[17] pedig az alapvető szolgáltatásokat nyújtó szereplőknek állapít meg kötelezettségeket az információ- és hálózatbiztonság fenntartása érdekében, valamint e szolgáltatóknak a kiberbiztonsági eseményekről a nemzeti hatóságokat is értesíteniük kell.

[16] Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete 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) HL L 119/1. 2016.5.4.

[17] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. HL L 194/1. 2016.8.19.

A fokozott nemzetközi együttműködés és kapcsolattartás elősegítése is lényeges elem, különösen a magánszektor és a bűnüldöző hatóságok, illetve az egyes nyomozó hatóságok között, mivel az eddigi tapasztalat is azt mutatja, hogy a sikeres felderítéshez és a hatékony nyomozás lefolytatásához mindez nélkülözhetetlen.

Továbbá kiemelt jelentősége van a prevenciónak, különösen a felhasználókhoz igazított oktatásnak, ismeretterjesztésnek, mert sokszor az informatikai bűncselekmények elkerülhetők lennének, ha körültekintőbben járnának el, és ezáltal kiküszöbölhető lenne a sértetti közrehatás, amely jelentősen megkönnyíti az elkövetők helyzetét. Elsődlegesen nem a felelősség keresése a cél, hanem a károk, negatív következmények lehetőség szerinti elkerülése vagy legalább azok mérséklése. Ez pedig nem a büntetőjog feladata.[18]

3.4. De lege ferenda javaslatok

Az információs rendszerben végzett műveletekkel jelentős kárt tudnak okozni, ezért indokoltnak tartom az információs rendszer vagy adatmegsértés tényállásának egy külön fordulatban történő szabályozását. A károkozást a jogalkotó az információs rendszer felhasználásával elkövetett csalásnál értékeli csak, azonban e bűncselekménynél a jogtalan haszonszerzés célzat megléte is szükséges a tényállásszerűséghez. Ezzel szoros összefüggésben véleményem szerint a jelenlegi szabályozási rendszerben a büntetőjog kár fogalma helyett a vagyoni hátrány alkalmazása megfelelőbb lenne mindkét bűncselekmény esetén, mivel utóbbi a vagyonban bekövetkezett értékcsökkenésen kívül magában foglalja az elmaradt vagyoni előnyt is. Azonban ez sem jelent teljes megoldást, mivel az elkövetési magatartással összefüggésben a kár sokszor ténylegesen nem következik be, de felmerülhetnek az információs rendszert ért támadást követően a helyreállítással kapcsolatos kiadások, költségek. Javaslom ezért a kár vagy vagyoni hátrány büntetőjogi fogalmának a kiterjesztését egy értelmező rendelkezéssel, amely magában foglalná a vagyoni hátrányok kiküszöböléséhez szükséges költségeket is.

A Btk. közérdekű üzem és a 2013-as irányelv szerint alkalmazott kritikus infrastruktúra fogalma nem fedi egymást, így a cselekmény minősítése vitatott lehet, különösen a szociális jólét, a közegészség intézményei ellen intézett támadások esetében, ezért a meghatározások közelítését javaslom.

Amennyiben az adott bűncselekmény elkövetésekor az információs rendszer mint elkövetési eszköz kerül alkalmazásra, akkor ez jelentős mértékben növeli az ilyen jellegű cselekmények

[18] KORINEK László: Tendenciák korunk bűnözésében, bűnüldözésében. MTA székfoglaló előadás, 2013. 51. o.

veszélyességét a társadalomra nézve. Ezért javaslom, hogy a jogalkotó ezt az egyes bűncselekmények tényállásában minősített esetként szabályozza, például az általam vizsgált csalás és zsarolás tényállásainál.

3.5. Javaslatok a jogalkalmazó számára

Fontos, hogy a jogalkalmazók (bíróság, ügyészség, nyomozó hatóság) számára is biztosítva legyen a modern technológiákkal összefüggő jogi kihívásokat érintő, speciális oktatás, amely során megismerik a legújabb informatikai trendeket, elkövetési módokat és naprakész tudásra, ismeretekre tehetnek szert. Örvendetes, hogy erre vonatkozóan már megfigyelhetők európai és hazai törekvések is, például az Európai Jogi Akadémia (Academy of European Law) rendszeresen szervez képzéseket, szemináriumokat kifejezetten az igazságügyi szervek dolgozóinak. Magyarországon az Országos Bírósági Hivatal a kiberbűnözéssel kapcsolatos bírósági hálózat felállításáról döntött, valamint az ügyészség is létrehozta a Számítógépes Bűnözéssel Foglalkozó Országos Ügyészségi Hálózatot. Erre vonatkozó képzések jelentek már meg mind a bíróság, mind az ügyészség rendszerén belül.[19] Továbbá javaslom, hogy a jövő jogalkalmazói, a joghallgatók is már megismerjék és foglalkozzanak az új technológiák jogi vetületeivel az egyetemi oktatás keretében. Éppen ezért fontosnak tartom, hogy az e témakörbe tartozó kutatási eredmények szervesen beépüljenek az oktatásba is.

[19] Lásd BUONO, Laviero: Updating and diversifying the training offer for EU legal practitioners to meet the challenges posed by the new technologies. ERA Forum 2017. 1-6. o.; LAJTÁR: i.m. 51. o. https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja

IV. Summary

The growing adoption of the Internet provides increasing opportunities to commit crime. In general cybercrime is increasing in scale and impact. Combating cybercrime requires a different approach from that which has been traditionally taken in respect of most crimes. In contrast to the offline world where criminals normally need to be physically present at the crime scene, on the internet criminals do not need to be even close to the crime scene. They can attack a large number of victims globally with minimum effort and risk by hiding their identity.

In my thesis, I examined mainly the substantive criminal law regulations in regard with cybercrime at international and EU level, in Hungary and the United States. The Convention on Cybercrime is the first international treaty on cybercrime and its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The 2013/40/EU Directive's objectives are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities. The Hungarian Criminal Code's relevant provisions meet the requirements of the international, EU law and include the following cybercrimes: breach of information system and data, compromising or defrauding the integrity of the computer protection system or device and information system fraud. While the current version of the Computer Fraud and Abuse Act in the United States includes seven types of criminal activity from unauthorized computer access to computer extortion.

The dissertation deals with the most prevalent and dangerous types of cybercrime schemes such as hacking, DDoS attacks and malware. All of these schemes rely on the malicious, unauthorized use of computerts to penetrate into another person's computer or network. Trends suggest considerable increases in the scope, sophistication, number and types of attacks, number of victims and economic damage. The cyber-attacks often target critical infrastructures. Along with technical attacks, social engineering techniques have become an essential tactic for the commission of many, often complex cyber-attacks or other cyber-facilitated crimes suchs as payment fraud. Payment card transactions are the most widespread noncash payment method used and criminals abuse of their use by card-present and card-not-present methods. Money mules provide a key service in the laundering of criminal proceeds from cybercrimes.

There are two more important factors worth highlighting: Crime-as-a-Service and anonymisation. The Crime-as-a-Service business model drives the digital underground

economy by providing a wide range of commercial services that facilitate almost any type of cybercrime. Criminals are freely able to procure such services, such as the rental of botnets, DDoS attacks, data theft, to commit crimes themselves. This has facilitated a move by traditional organised crime groups into cybercrime areas. The anonymisation techniques used in parts of the Internet, known as Darknets, allow users to communicate freely without the risk of being traced.

Cryptocurrencies have the potential to become an ideal instrument for money laundering, since the decentralized system of virtual currencies allows their potential misuse for criminal purposes. Entry to and exit from the system is typically via an exchanger. Exchange services are offered in the digital underground economy. However, legitimate exchangers are also exploited, particularly those which carry out little Know Your Customer (KYC) processes. Due to the fifth anti-money laundering directive member states in the EU must ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered. In a trend mirroring attacks on banks and their customers, cryptocurrency users and exchangers have become victims of cybercrimes themselves. Conventional crimes may be committed via cryptocurrencies such as fraud and extortion. They are less treacable and their decentralised system challenges the legislators of substantive criminal law, procedure (e.g. seizure related questions) and law enforcement as well as.

Judicial cooperation is essential to tackle cybercrime. Although the whole concept of a territorially based investigative approach conflicts with the borderless nature of cybercrime and it also challenges for law enforcement to secure and collect electronic evidence from abroad. The new e-evidence regulation could solve partially the problem, since the law enforcement authorities in any EU Member States would be allowed to force providers like Facebook or Google to hand over personal data from users, even if the provider is located in a different country. Furthermore, it is forward-looking that the new Hungarian Criminal Procedure Law introduced coercive measures based on electronic data. Although encyprtion, anonymisation and jurisdiction issues pose great challenge during the criminal procedure.

Besides criminal law's provisions, the NIS directive has a strong and positive impact on the cybersecurity of critical infrastructures, while the GDPR protects personal data in the EU.

The most effective defence against cybercrime is the education of potential victims. Law enforcement should therefore continue to support prevention and awareness campaigns aimed at raising awareness in relation to these threats.

V. A szerző publikációs jegyzéke

1. MEZEI Kitti (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK-MTA TK JTI. Budapest-Pécs, 2019. p. 204.
2. MEZEI Kitti: A szervezett bűnözés az interneten. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK-MTA TK JTI. Budapest-Pécs, 2019. pp. 125-147.
3. MEZEI Kitti: A pénzintézetek ellen intézett kibertámadások büntetőjogi vonatkozásai. Infokommunikáció és jog 2019/1. pp. 14-20.
4. MEZEI Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jog 2019/5. pp. 305-314.
5. MEZEI Kitti: A pénzmosás a gyakorlatban, különös tekintettel a saját pénzmosásra és az ún. „money mule" jelenségre. Kriminológiai Közlemények 79. pp. 161-168.
6. MEZEI Kitti: Cyberterrorism and the terrorist use of the Internet. Annals of the Timisoara West University Series 2018/2. pp. 21-34.
7. MEZEI Kitti: A Kúria harmadfokú végzése a jogtalan elsajátításról és a pénzmosásról. Jogesetek Magyarázata 2018/3-4. pp. 21-28.
8. MEZEI Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In: Sárközy Tamás (szerk.) Magyar Jogászegyleti Értekezések. Magyar Jogász Egylet (2018) pp. 157-173.
9. MEZEI Kitti - NAGY Zoltán András: Az Európai Unió Bűnügyi Adatvédelmi Irányelvéről. In: Gaál Gyula - Hautzinger Zoltán (szerk.): A XXI. század biztonsági kihívásai (2018) pp. 229-234.
10. MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés - különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018 24:(1) pp. 349-360. (2018)
11. MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. pp. 66-83. (2018)
12. MEZEI Kitti – NAGY Zoltán András: Pénzmosás a kibertérben. Infokommunikáció és Jog 15:(70) pp. 26-31. (2018)
13. MEZEI Kitti – NAGY Zoltán András: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Szent Lászlótól a modernkori magyar rendészettudományig. Pécs, Magyarország: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, (2017) pp. 163-168.
14. MEZEI Kitti: The regulation of crimes against information systems in Hungary. Journal of Eastern- European Criminal Law 2: pp. 203-216. (2017)
15. MEZEI Kitti – NAGY Zoltán András: Az informatikai bűncselekmények. egyetemi jegyzet. Pécs: PTE Állam- és Jogtudományi Kar, 2017. p. 90
16. MEZEI Kitti – NAGY Zoltán András: Organised cybercrime groups and their illicit online activities. Studia Iuridica Yearbook of 2016. PTE ÁJK, 2017. pp. 143-160.
17. MEZEI Kitti – DORNFELD László: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és Jog 14:(68) pp. 32-37. (2017)

18. MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós, Barabás A. Tünde (szerk.) A negyedik magyar büntetőkódex: régi és újabb vitakérdések. 384 p. Budapest: MTA Társadalomtudományi Kutatóközpont, 2017. pp. 297-308.
19. MEZEI Kitti – NAGY Zoltán András: A véleménynyilvánítás szabadsága az interneten, avagy a szolgáltatók felelőssége. Demokrácia, jogállam, közigazgatás: Ünnepi tanulmányok Csefkó Ferenc c. egyetemi docens 70. születésnapjára. pp. 17-27. (2017)
20. MEZEI Kitti – NAGY Zoltán András: The organised criminal phenomenon on the Internet. Journal of Eastern- European Criminal Law (2) pp. 137 -149. (2016) (társszerző: Nagy Zoltán András)
21. MEZEI Kitti – TÓTH Dávid: Információs bűncselekmények. Büntetőjogi Szemle 1-2: pp. 81-86. (2015)
22. MEZEI Kitti – TÓTH Dávid: Information related crimes in Hungary. In: Ігор Пасічник (szerk.) МАТЕРІАЛИ IV Міжнародної науково-практичної конференції МАЛИНОВСЬКІ ЧИТАННЯ. Ostroh: pp. 111-117.