Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

Mezei Kitti

Büntetőjogi válaszok az informatikai kihívásokra

Doktori (PhD) értekezés tézisei

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

Pécs, 2019

1. A témaválasztás indokolása, aktualitása[1]

Nem túlzás azt állítani, hogy az informatika és a technológiai fejlődés mindenkinek az életét érinti, és arra hatást gyakorol. Ez a dinamikus fejlődés a jogrendszert is folyamatos kihívások elé állítja. Éppen ezért az új technikai újítások esetén szükségessé válik, hogy az ezekkel kapcsolatban felmerülő jogi kérdésekre, problémákra reagálni tudjon. Ez különösen fontossá vált azért, mert az egyes társadalmi és gazdasági folyamatok is egyre inkább függnek az információs rendszerektől. Az információs társadalom egyik jellemzőjévé vált az infokommunikációs eszközök számának, sokféleségének és komplexitásának a növekedése. Az innováció egyre inkább az egyes gazdasági ágazatok működését, illetve a gazdasági szereplők versenyképességét határozza meg.

Azonban a gyors ütemű informatikai fejlődésnek az előnyei mellett megvannak a veszélyei is, hiszen a modern technológiák adta lehetőségeket a bűnelkövetők is kihasználják. Ennek köszönhetően jelentek meg nagy számban az informatikával összefüggő bűncselekmények, amelyek körét ma már rendkívül nehéz behatárolni, köszönhetően az új technológiák megjelenésének (pl. Internet of Things[2], mobilinformatikai eszközök), a megvalósítható funkciók bővülésének, illetve a hálózatok használatának az elterjedésének, amelyek magukkal hozzák az újabb elkövetési módokat, illetve büntetendő cselekmények körét (pl. „hacking", számítógépes vírusok, adatlopások).[3] Ma már szinte bármelyik hagyományos bűncselekmény elkövethető az új eszközök segítségével. Mindez a jogalkotást és a jogalkalmazást is kihívások elé állítja különösen a büntetőjogi szabályozásra tekintettel, illetve a minősítés kérdéseiben. A büntető igazságszolgáltatás hatékonyságának növelése napjainkban sürgetően veti fel e téma kutatásának az igényét. Ennek ellenére a hazai szakirodalom keveset foglalkozik a büntetőjog és az informatika összefüggéseivel, ezért a témát érintő tudományos kutatások hiánypótlónak tekinthetők.

Az internetnek számos előnye van, amelyek egyben a használatával összefüggő visszaélések térnyerését, illetve a hatékonyabb bűnelkövetést is lehetővé teszik. Az internetre csatlakozott eszközök és felhasználók száma évről évre növekvő tendenciát mutat, így a kiterjedt online

[1] A doktori értekezés az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV és ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának támogatásával 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 bekapcsolható legyen a rendszerbe.

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

jelenlét az elkövetők számára még inkább lehetővé teszi a tömeges informatikai támadások kivitelezését. Az internet esetén egy egész világra kiterjedő hálózatról van szó, amely azonnali és valós idejű kapcsolatteremtésre ad lehetőséget, és a lényegét az elektronikus formában megjelenő adat, információ adja („Big Data" jelenség)[4]. Az internet speciális, de egymással összefüggő tulajdonságokkal rendelkezik, amelyek megkönnyíthetik az elkövetést azonban már egy új színtéren:

Az internet globális jellege egy határon átívelő bűnözést tesz lehetővé. Az elkövetők a világ bármely pontján kereshetnek célpontokat, illetve sebezhetőségeket, és ehhez még arra sincs szükségük, hogy akár ugyanabban az országban tartózkodjanak a kiválasztott sértettel az elkövetéskor. Ennek köszönhetően a büntető eljárásjogban is összetett joghatósági és illetékességi kérdések megválaszolásra várnak a mai napig.

Az internet a „hálózatok hálózataként" egyben decentralizált és rugalmas hálózatok létrehozására nyújt lehetőséget, amelyek az elkövetők laza szerveződését segítik elő például az elkövetők számára egymás között a feladatoknak, a szakmai tudásuknak, jártasságuknak és a kifejlesztett technikai eszközeiknek a megosztását teszik lehetővé. Az internet egyben egy kommunikációs csatornaként is szolgál, amely a különböző bűncselekmények elkövetésében is fontos szerepet tölthet be.

Ennek köszönhetően napjainkra az informatikai bűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé nőtte ki magát, amelynek motorját az online feketegazdaság adja (pl. Darknet fórumok), ahol a különböző támadásokat elősegítő eszközök és egyéb illegális szolgáltatások is elérhetőek.

Az internet anonimitást biztosít, amelyet az elkövetők fokozhatnak a különböző titkosítást és magasabb fokú anonimitást biztosító eszközök bűnelkövetési célú felhasználásával (pl. TOR hálózat és a kriptovaluták használata). Azonban azok számára is relatív névtelenséget kínál, akik kevésbé jártasak az informatika világában, mert egy IP cím, e-mail cím, vagy ál-Facebook profil mögé rejtőznek és ezekben az esetekben is még nehéz lehet a konkrét személyek lenyomozása és azonosítása.

Mindemellett a sértettekkel egy távoli kapcsolatfelvételt garantál, ezáltal megszünteti azokat a szociális akadályokat, amelyekkel az elkövetőknek a valóságban, akár egy személyes találkozáskor kellene szembe nézniük, ezáltal ez is megkönnyíti számukra az elkövetést**.** Az ilyen típusú bűnözésre magas fokú látencia jellemző, mert a gyanútlan felhasználók sokszor

[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.

nem is észlelik, hogy bűncselekmény sértettjévé váltak vagy egyszerűen a hatóságok felé nem jelentik (pl. bankkártya-visszaélések, pénzintézetek ellen intézett támadások) amely tovább nehezíti a felderítést.

További előnye az internetnek, hogy a segítségével könnyedén lehet végrehajtani adat vagy program manipulációt minimális költség mellett, mert az információk elektronikus megjelenítésnek köszönhetően lehetőség van az adatok másolására minőségi veszteség nélkül, valamint módosítására anélkül, hogy annak sokszor 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 az interneten keresztül és akár több millió rendszert megfertőzni egyidejűleg, vagy például egy botnet hálózat segítségével az elkövetők nagyszabású támadásokat tudnak végrehajtani, amely teljes rendszer leálláshoz vezethet.[5]

2017-ben az informatikai bűnözés által okozott kár 600 milliárd dollár értékben realizálódott a különböző sértetti körnél (pl. vállalatok, pénzintézetek, kormányzati szervek stb.) és a szakértők szerint ez 2021-re meg fog duplázódni, ami úgy gondolom, hogy rávilágít arra, hogy mekkora potenciált rejt magában a technológiák bűnelkövetési célú felhasználása az elkövetői oldalról, míg egyben mekkora kockázatot és veszélyt a sértetti oldalról.[6]

2. Az értekezés tárgya és szerkezete

A büntetőjog és az informatika összefüggéseinek vizsgálata a legtágabb értelemben olyan hatalmas területet ölelne fel, amely túlterjeszkedne egy doktori értekezés keretein, ezért a kutatás tárgykörének meghatározása során fontosnak tartottam, hogy ezt korlátok közé szorítsam. Egyrészt elsősorban a büntető anyagi jogi kérdésekkel foglalkozom, és csak érintőlegesen büntető eljárásjogi kérdésekkel. Másrészt az értekezés kizárólag az informatikai, valamint az információs rendszerek felhasználásával elkövetett gazdasági, anyagi haszonszerzésre irányuló bűncselekményekkel kapcsolatos szabályozási kérdésekre fókuszál. Az értekezés célja a szabályozással kapcsolatos hiányosságokat feltárása és az erre vonatkozó javaslatok kidolgozása.

Az értekezés három nagy szerkezeti részre tagolódik. A bevezetést követő első nagy rész a történeti és fogalmi alapvetés, amely az informatikai bűnözés elleni fellépés nemzetközi

[5] KOOPS, Bert-Jaap: The Internet and its Opportunities for Cybercrime. Tilburg School Legal Studies Paper Series No. 09/2011. 740-741. o.
[6] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf [2018.05.23.]

dimenzióját vizsgálja, így különös tekintettel az Európai Unió és az Egyesült Államok szabályozási történetére. Emellett a fogalmi kérdések tisztására kerül sor, kiemelten az informatikai bűnözés meghatározására fókuszálva.

Ezt követően az egyes informatikai támadásokkal kapcsolatos büntetőjogi kihívásokat vizsgálom a tekintetben, hogy az Európai Unió, illetve a hazai és az Egyesült Államok szabályozása mennyiben tud ezekre reagálni, így a vonatkozó rendelkezések részletes elemzésére került sor. Ebben a fejezetben a büntető anyagi jogi szabályozás mellett a hazai új büntetőeljárásról szóló törvény elektronikus bizonyítékokkal összefüggő rendelkezéseire és az ezzel kapcsolatos uniós jogalkotási törekvések bemutatása is megvalósult.

Ezután az utolsó rész következik, amelyben az informatika és internet segítségével elkövetett „hagyományos" gazdasági bűncselekmények szabályozási kihívásainak elemzésére kerül sor, így a bankkártyákkal kapcsolatos visszaélésekre, a szervezett bűnözés megjelenésére az interneten és az ezzel összefüggő bűncselekményekre, így külön figyelmet fordítva a pénzmosásra a virtuális térben, valamint a kriptovaluták büntető anyagi és eljárásjogi kihívásaira.

3. A szakirodalom és az alkalmazott módszertan áttekintése

Az alkalmazott kutatási módszerek bemutatása mellet fontos, hogy sor kerüljön a felhasznált szakirodalmi források rövid bemutatására. Az értekezés elkészítése során a témakör szempontjából releváns uniós, hazai és amerikai jogforrások kerültek felhasználására. A joganyag elemzése mellett az egyes részeknél hangsúlyt fektettem a vonatkozó joggyakorlat bemutatására, valamint az adott kérdésköröket tárgyaló, releváns magyar és nemzetközi jogirodalmat dolgoztam fel.

A téma sajátos jellegéből adódóan egy interdiszciplináris módszer alkalmazása vált szükségessé. A kutatás során még a normatív és dogmatikai módszer alkalmazására került sor, valamint a vizsgálat során az egyes részeknél a logikai és kritikai elemzésé is. Emellett hangsúlyt fektettem a komparatív módszerre különösen az uniós, hazai és amerikai szabályozás vonatkozásában, amely során érintettem az anyagi büntetőjogi rendelkezések hasonlóságait és különbözőségeit.

4. Összefoglalás

Összeségében elmondható, hogy mind az Európai Unióban és mind az Egyesült Államokban a kezdeti törekvések az informatika bűnözéssel kapcsolatban egészen az 1970-es évekig nyúlnak vissza. További közös vonásként említhető, hogy a meglévő, hagyományos bűncselekményekre vonatkozó szabályozás helyett megkezdődött a speciális és önálló anyagi büntetőjogi rendelkezések megalkotása ezen új típusú bűncselekményekre vonatkozóan. Az Európa Tanács több évtizedes munkájának eredményére 2001-ig kellett várni, amikor is elfogadásra került az első kötelező erejű, multilateriális jogi dokumentum, a Budapesti Egyezmény. Az egyezmény célja a számítástechnikai bűnözés elleni küzdelem alapjainak a megteremtése. Az egyezmény az aláíró felek számára keretet biztosít a nemzetközi együttműködéshez és olyan államok számára is nyitott a ratifikációja, amelyek nem tagjai az Európa Tanácsnak, így többek között az Egyesült Államok is ratifikálta. Valamennyi, az informatikai bűnözést szabályozni célzó új, nemzetközi dokumentumnak, kezdeményezésnek az alapjait a Budapesti Egyezmény adja és a mai napig a legjelentősebb egyezménynek számít ezen a területen, azonban vannak szabályozási hiányosságai, mert a technológiai fejlődés már meghaladta. Ezért a másik nagy előrelépést uniós szinten a 2013-as új irányelv jelentette, amely az információs rendszerek elleni támadásokkal szemben lép fel a minimumszabályok megalkotásával és az eddig hiányos szabályozást az új típusú támadásokra vonatkozóan részben orvosolta (pl. botnetek, kritikus infrastruktúrák elleni támadások, személyazonosság-lopás), és ezeket a tagállamoknak kötelezően át kellett ültetniük a saját jogrendszerükbe, és a tagállamok közötti bűnügyi együttműködés erősítése révén.

Az Egyesült Államok szövetségi szinten, először 1984-ben, az uniós törekvésekhez képest előbb szabályozta már a számítógépes bűncselekményeket a CFAA-ban. Ahhoz, hogy a törvény lépést tudjon tartani a technológiai fejlődéssel már nyolcszor módosították 1986-tól 2008-ig. A módosítások elsődleges célja az volt, hogy a törvény hatályát minél szélesebb körben kiterjesszék, például a szövetségi érdekű számítógép szűk fogalmától egészen eljutottak egy sokkal tágabb értelemben vett számítógép meghatározáshoz, amely alá vonható lényegében majdnem valamennyi háztartási eszköz, amelyet a világ bármely részén használnak. A CFAA hatályos szabályozása hét bűncselekményt tartalmaz, azonban egy kiforrót esetjog még hiányzik e területen.

Fontos belátni, hogy az informatikai bűnözés egy komplex problémakört foglal magában, mellyel szemben többlépcsős stratégiának az alkalmazása válik indokolttá. Ebben kiemelt jelentősége van elsődlegesen a prevenciónak, különösen a felhasználókhoz igazított oktatásnak,

ismeretterjesztésnek, mert sokszor ezek a bűncselekmények elkerülhetők lennének, ha körültekintőbben járnának el és ezáltal kiküszöbölhető lenne a sértetti közrehatás, amely jelentősen megkönnyíti az elkövetők számára az elkövetést. Elsődlegesen nem a felelősség keresése cél, hanem a károk, negatív következményeknek a lehetőség szerinti elkerülése vagy legalább azok mérséklése. Ez pedig általában nem a büntetőjog feladata.[7]

Emellett fontos, hogy a jogalkalmazók (pl. bíróság, ügyészség, rendvédelmi szervek) számára is biztosítva legyen a modern technológiákkal összefüggő jogi kihívásokat érintő, speciális oktatás. Örvendetes, hogy erre vonatkozóan már megfigyelhetők európai és hazai törekvések is.[8]

A fokozott együttműködés elősegítése is lényeges elem a magánszektor és a bűnüldöző hatóságok, illetve az egyes bűnüldöző hatóságok között, mert az eddigi tapasztalat is azt mutatja, hogy a sikeres felderítésekhez, a hatékony nyomozás lefolytatásához mindez nélkülözhetetlen.

Fontos a harmonizált, egységes nemzetközi szabályozás megteremtése mind anyagi, mind eljárásjogi tekintetben nemzetközi szinten, ami azért is kihangsúlyozandó, mert egy határokon átívelő bűnözésről van szó és az elkövetők kihasználhatják a különböző országok jogrendszerének a szabályozási hiányosságait, azok differenciáltságát. Például az Európai Unióban a szabályozást sikerült egységesíteni az új irányelv révén.

Az országok általában különböző megoldást alkalmaznak a kiberbűncselekményekre vonatkozóan vagy egy külön törvényben történő szabályozást választanak, vagy a többségük a nemzeti büntető törvénykönyvébe iktatott rendelkezéseket alkalmaz egy önálló fejezetben vagy a különös részben szétszórtan elhelyezett tényállásokkal megvalósítva.

Magyarországon az új. Btk.-ban az informatikai bűncselekmények önálló fejezetbe lettek illesztve, ami mindenképpen egy jó megoldásnak és haladásnak tekinthető az új védett jogi tárgyakra tekintettel. A hazai szabályozás mind a Budapesti Egyezmény és a 2013-as irányelv rendelkezéseivel is összhangban áll, és az informatikai támadásokat széleskörűen szabályozza. Azonban kritikai megjegyzéseim és javaslataim a következők:

---

[7] KORINEK (2010): i.m. 51. o.

[8] Például az Európai Jogi Akadémia (Academy of European Law) rendszeresen szervez képzéseket, szemináriumokat az technológiákkal összefüggésben. 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.; Magyarországon az Országos Bírósági Hivatal a kiberbűnözéssel kapcsolatos bírósági hálózat felállításáról döntött. Mind a bíróság és mind az ügyészség rendszerén belül erre vonatkozó képzések jelentek már meg. https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja

- Az információs rendszerben végzett művelettel jogtalan haszonszerzés nélkül is kárt tudnak okozni, ezért indokolt lenne ennek egy külön fordulatba történő szabályozása az információs rendszer vagy adat elleni bűncselekménynél.
- Ezzel szoros összefüggésben véleményem szerint szükség van a kár büntetőjogi fogalmának a kiterjesztése egy értelmező rendelkezéssel.
- A közérdekű üzem és az uniós 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 fogalmak közelítése indokolt.
- Megfontolandó az is, hogy amennyiben az adott bűncselekmény elkövetésekor az információs rendszer mint elkövetési eszköz kerül alkalmazásra, akkor ez jelentős mértékben növeli az ilyen jellegű cselekmények társadalomra veszélyességét, ezért a jogalkotó ezt az egyes bűncselekményeknél (pl. csalás, zsarolás) minősített eseteként szabályozza.

Az új büntetőeljárásról szóló törvényünk is már a kor kívánalmainak megfelelő rendelkezéseket tartalmaz, így már külön nevesíti a bizonyítási eszközök között az elektronikus adatot, valamint részletesen szabályozza a rá épülő kényszerintézkedéseket. A Be. azonban a lefoglalás módszertani kérdéseivel nem foglalkozik, annak ellenére, hogy ennek komoly jelentősége van, ezért a lefoglalás menetére vonatkozóan hiányzik még egy világos útmutatás, ami az ezzel kapcsolatos kérdéseket orvosolná. A szabályozás előremutató, mert már olyan kérdésekkel is foglalkozik mint a virtuális vagyontárgyak lefoglalása (pl. a fizetésre használt kriptovaluták). Azonban ez még nem nyújt megoldást a teljes problémára, mert a hatóságokat több tényező is hátráltathatja a nyomozás során például a titkosított (pl. jelszóval vagy biometrikus azonosítóval védett) informatikai eszközök, a privát kulcs ismeretének a hiánya, valamint az a tény, hogy a jogosult soha nincs fizikai birtokában a kriptovalutáknak, ezért önmagában a lefoglalás nem elégséges, hanem ezeket kikényszerített tranzakcióval lehetne kizárólag biztosítani.

Az Európai Unión belül egy régóta fennálló problémát kívánnak orvosolni az új elektronikus adatok határon átnyúló megszerzésére vonatkozó rendelettel, amely megteremtené annak a lehetőségét, hogy a hatóságok közvetlenül az internetszolgáltatókat keressék meg az elektronikus bizonyítékokkal kapcsolatban. Ez nagy előre lépést jelent a hatékonyabb és gyorsabb büntetőeljárások lefolytatása érdekében.

A kiberbűncselekményekkel kapcsolatban a másik jelentős eljárásjogi problémaként a joghatóság kérdése emelhető ki, ami a kiberbűnözés sajátosságában keresendő, hogy

transznacionális jellegű. Emellett az elkövetők számára rendelkezésre állnak különböző módszerek és programok, hogy elrejtsék helyzetüket és személyazonosságukat, így földrajzilag azonosíthatatlannak mutatkozhatnak. A legnagyobb problémát az anonimitás jelenti, amelyet számos program használata nyújthat számukra. Amennyiben a joghatóság megállapítása és az eljárás lefolytatása megtörténik, akkor pedig sokszor a kiadatás jelent további problémát.

A bankkártyákkal és különböző átutalásokkal kapcsolatos visszaélések az informatikai bűnözés egyik kiemelt területeként kezelhető. Az elkövetők az ún. skimming technikákat alkalmazzák a card-present csalás terén, hogy a fizikailag hozzáférhető bankkártya adatokat megszerezzék, míg ennél nagyobb számban vannak jelen az interneten megvalósuló card-not-present csalások, amelyek során különböző adathalász technikák alkalmazásával szerzik meg a gyanútlan sértettek adatait, amelyek továbbra is rendkívül nagy kihívást jelentenek különösen a pénzintézetek körében. Az elkövetők gyakran értékesítik a megszerzett adatokat a Darknet fórumokon keresztül.

A bűnelkövetők gyorsan átveszik és integrálják az új technológiákat a különböző bűncselekmények elkövetésekor és olyan üzleti modellt alkalmaznak, amelyeknek az alapját egyre inkább az internet használata jelenti. A hagyományos szervezett bűnözői csoportok esetében is megfigyelhető az informatikai újítások kihasználása, amely magában foglalja az interneten történő terjeszkedést mint például az illegális online kereskedelmet és a széles körben hozzáférhető, titkosított kommunikációs csatornák használatát és egyéb informatikai újításokat. Megállapítható, hogy az új technológiai vívmányok lényeges és maradandó hatással vannak a bűnözés természetére. Az is kétségtelen tény, hogy az informatikai bűnözés egy hatalmas profit-orientált és szolgáltatás-alapú üzletté nőtte ki magát, azonban az még mindig nem világos, hogy ez a piac milyen mértékben van az egyes tradicionális szervezett bűnözői csoportok kezében, illetve mennyiben tekinthető az új típusú kiberbűnözöi csoportok tevékenysége szervezett bűnözésnek egyáltalán. Ugyanis a szervezett bűnözés és az informatikai bűnözés kapcsolatára vonatkozóan még mindig nincs egy világos koncepció, különösen azért, mert nehéz a szervezett bűnözés hierarchikus, homogén struktúrájába az informatikai bűnözést beilleszteni. A „kiberbűnözői ipar" rendkívül erőssé és fejletté vált, azonban még mindig a fejlődésének korai szakaszában van, éppen ezért kevés a rendelkezésre álló adat, különösképpen a szervezettségi szintjére vonatkozóan. Összeségében elmondható, hogy az internet mint egy új színtérként szolgál mind a régi és mind az új típusú „szervezett" bűnözésnek, illetve mindkettő egymás mellett tud működni anélkül, hogy egymást kizárnák és ez köszönhető az online tér speciális jellegének.

A pénzmosással összefüggésben megállapításra került, hogy az online banki műveletek felvethetik ugyan a pénzmosás gyanúját, azonban a saját pénzmosás deliktumának megállapításához szükséges eredetleplezési célzatot nem lehet kiterjesztően értelmezni. Ennek következtében kiemelten fontos az utócselekmények célzatának a körültekintő vizsgálata, vagyis az, hogy az elkövető által kifejtett leplezési cselekményeknek mi a céljuk. Azok az alapbűncselekményből származó haszon realizálását szolgálják-e, vagy magát az alapbűncselekmény leplezését, annak érdekében, hogy az illető a büntetőjogi felelősségre vonást elkerülje, vagy valóban a pénz bűnös eredetét és annak további útját kívánják leplezni továbbá, hogy ezek a műveletek mennyiben alkalmasak a leplezési cél eléréséhez. A friss kúriai döntés felhívta a figyelmet arra is, hogy fokozottan vizsgálni kell, hogy az adott cselekmény az alapbűncselekmény tényállási elemének részeként vagy önállóan, – pénzmosásként – értékelendő, elkerülve ezáltal a kétszeres értékelést. A pénzmosás gondatlan alakzata esetében - így a pénzfutárok alkalmazásakor - pedig fokozottan kell vizsgálni az elkövető tudattartalmát.

Fontos, hogy az új technológiai kihívásokra a jogalkotás adekvát módon és gyorsan tudjon reagálni. A kriptovaluták jó például szolgálhatnak erre, mert a mai napig egy szürke zónát képeznek és jogi státuszuk bizonytalan. Azonban az kétségtelen, hogy a decentralizált rendszernek és a pszeudoanonim tranzakcióknak köszönhetően a bűnelkövetési célú felhasználásuk egyre inkább jelen van. A kriptovalutákkal kapcsolatban felmerülő visszaélések tekintetében általában 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 értékelhetjük. Örvendetes lenne ezért egy konkrét virtuális vagyontárgyakkal kapcsolatos szabályozás kialakítása a jövőben, amire a kriptovaluták jelensége jó indokot ad erre. A jövőben továbbra is a legnagyobb kihívást a titkosítást és anonimitást biztosító eszközök bűnelkövetési célú felhasználása fogja jelenteni, amely további szabályozási kérdéseket fog felvetni.

5. A szerző publikációs jegyzéke

1. **Cyberterrorism and the terrorist use of the Internet.** Annals of the Timisoara West University Series 2018/2. pp. 21-34.
2. **A Kúria harmadfokú végzése a jogtalan elsajátításról és a pénzmosásról.** Jogesetek Magyarázata 2018/3-4. pp. 21-28.
3. **A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In:** In: Sárközy Tamás (szerk.) Magyar Jogászegyleti Értekezések. Magyar Jogász Egylet (2018) pp. 157-173.
4. **Az Európai Unió Bűnügyi Adatvédelmi Irányelvéről** (társszerző: dr. Nagy Zoltán András) In: Gaál Gyula - Hautzinger Zoltán - A XXI. század biztonsági kihívásai (2018) pp. 229-234.
5. **Cyberterrorism - How real is the threat?** (közlésre elfogadott, megjelenés alatt) Studia Iuridica Yearbook of 2017. PTE ÁJK, 2018.
6. **Az informatikai bűnözés elleni nemzetközi fellépés - különös tekintettel az Európai Unió és az Egyesült Államok szabályozására.** JURA 2018 24:(1) pp. 349-360. (2018)
7. **A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon.** Pro Futuro 2018/1. pp. 66-83. (2018)
8. **Pénzmosás a kibertérben.** (társszerző: dr. Nagy Zoltán András) Infokommunikáció és Jog 15:(70) pp. 26-31. (2018)
9. **A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa**. (társszerző: dr. Nagy Zoltán András) 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., 6 p.
10. **The regulation of crimes against information systems in Hungary.** Journal of Eastern- European Criminal Law 2: pp. 203-216. (2017)
11. **Az informatikai bűncselekmények.** egyetemi jegyzet (társszerző: dr. Nagy Zoltán András) Pécs: PTE Állam- és Jogtudományi Kar, 2017. 90 p.
12. **Organised cybercrime groups and their illicit online activities.** Studia Iuridica Yearbook of 2016. PTE ÁJK, 2017. pp. 143-160. (társszerző: dr. Nagy Zoltán András)
13. **Az online gyermekpornográfia elleni küzdelem aktuális kérdései.** Infokommunikáció és Jog 14:(68) pp. 32-37. (2017) (társszerző: dr. Dornfeld László)
14. **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. (társszerző: dr. Tóth Dávid)
15. **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) (társszerző: dr. Nagy Zoltán András)

16. **The organised criminal phenomenon on the Internet.** Journal of Eastern-European Criminal Law (2) pp. 137 -149. (2016) (társszerző: dr. Nagy Zoltán András)
17. **Információs bűncselekmények.** Büntetőjogi Szemle 1-2: pp. 81-86. (2015) (társszerző: dr. Tóth Dávid)
18. **Information related crimes in Hungary.** In: Ігор Пасічник (szerk.) МАТЕРІАЛИ IV Міжнародної науково-практичної конференції МАЛИНОВСЬКІ ЧИТАННЯ. Ostroh: pp. 111-117. (társszerző: dr. Tóth Dávid)
19. **The forever changed economic crime.** NATSIONAL'NYI UNIVERSYTET "OSTROZ'KA AKADEMIYA". NAUKOVI ZAPYSKY. SERIYA PRAVO 12: (2) p. on-line. 16 p. (2015) (társszerző: dr. Kőhalmi László)
20. **The concept and typical forms of economic crime.** Journal of Eastern-European Criminal Law 4:(2) pp. 33-42. (2015) (társszerző: dr. Kőhalmi László)