**PÉCSI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK**
**DOKTORI ISKOLÁJA**

---

**Gyaraki Réka Eszter**

# A SZÁMÍTÓGÉPES BŰNCSELEKMÉNYEK NYOMOZÁSÁNAK PROBLÉMÁI

**Tézisek**

**Témavezető:**

**Dr. Nagy Zoltán András**

**Habilitált egyetemi docens**

**Tanszékvezető**

**Pécs, 2019**

# TARTALOMJEGYZÉK

**Tartalomjegyzék** ..... **3**

**1 A kitűzött kutatási feladat rövid összefoglalása** ..... **4**

*1.1 A kutatási témaválasztás indoka* ..... *4*

*1.1 A kutatási hipotézisek* ..... *5*

**2 A kutatás során alkalmazott eszközök és kutatási módszerek** ..... **7**

*2.1 A kutatás célja* ..... *9*

**3 A tudományos eredmények összefoglalása, azok hasznosítása, illetve hasznosítási lehetőségei** ..... **11**

**4 Összegzés** ..... **17**

**5 Felhasznált irodalom és a szerző saját publikációi** ..... **19**

# 1 A KITŰZÖTT KUTATÁSI FELADAT RÖVID ÖSSZEFOGLALÁSA

A disszertációban a számítógépes bűncselekményekkel kapcsolatos, jellemzően a nyomozó hatóság által, a büntetőeljárás keretében felmerülő gyakorlati kérdésekkel foglalkoztunk. Az egységes fogalomhasználatnak kérdéséből indultunk ki, vagyis a számítógépes bűncselekmény vagy pedig a kiberbűncselekmény kifejezést lenne-e helyesebb használni. Álláspontunk szerint a két kifejezést egymás szinonimájaként történő használata nem helyes, hiszen mostmár jól elkülöníthető egymástól az off-line módban (azaz internetes hálózat nélkül) elkövetett bűncselekményt az on-line (azaz internetes hálózat felhasználásával) elkövetett bűncselekménytől.

## 1.1 A kutatási témaválasztás indoka

Napjaink számítástechnikai és informatikai fejlődésének, ugrásszerű növekedésének köszönhetően, azok technikai tulajdonságaik révén gyorsabban és kényelmesebben elérhetőek a különböző kereskedelemi szolgáltatások, a pénzügyek intézése, az egymással történő szóbeli vagy írásbeli kommunikáció, az ügyintézések különböző formáihoz, amelynél sokszor a személyes jelenlét sem szükséges.

Az előnyök mellett ugyanakkor megjelentek a számítástechnikai bűncselekmények is, amelyek egyre nagyobb teret hódítanak a világban[1]. Olyan globális problémává vált a számítástechnikai bűnözés, hogy arra már nemcsak az egyes államoknak, de az Európai Unió országainak, a katonai-, gazdasági szövetségeknek is reagálni kell rá nemcsak jogalkotói, hanem jogalkalmazói szinten.

A számítástechnikai bűnözők által okozott károk már a 2016-os IOCTA[2] szerint meghaladják az Európai Unió egyes tagállamaiban a hagyományos bűncselekmények által okozott károkat, a számok mind az elkövetői, mind a sértetti oldalon folyamatosan nőnek, az elkövetési magatartás pedig egyre jobban bővül, így szükséges a még hatékonyabb fellépés a jogalkotók, a nyomozóhatóságok, az ügyészségek és további jogalkalmazók részéről.

[1] Symantec szerint: 2018-ban 978 millió embert érintett 20 országban a számítógépes bűnözés, csak az elmúlt 12 hónapban a fogyasztók 44% -át érintette a számítógépes bűnözés. A számítógépes bűnözés áldozatául esett fogyasztók globálisan 172 milliárd dollárt vesztettek! (forrás: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf, letöltve: 2018. július 31)

[2] Internet Organised Crime Threat Assessment

## 1.1 A kutatási hipotézisek

A kutatás céljához mérten fogalmaztuk meg a hipotéziseket is, amelyből majd a feltevéseink helyessége esetén javaslat megfogalmazása vált célunkká, vagy pedig a külföldi példák alapján egy jobb gyakorlat kialakítása lehetne a követendő minta.

Elsődlegesen a kutatási hipotézisek felállítása esetében célul tűztük ki, hogy a következő kérdésekre megtaláljuk a választ:
Mindenképpen szükséges lenne meghatározni a számítógépes bűncselekmények fogalmát, amely a „Computer Crime" elleni nemzetközi küzdelemhez elengedhetetlen. A fogalom meghatározása hozzájárulna a kriminalisztika, azon belül a kriminál taktikai és kriminálmetodikai módszerek kidolgozásához.

Minden bűncselekmény nyomozása az elkövetés helyének és idejének vizsgálatával kezdődik, amely kriminálmetodikailag az elsődleges feladat[3]. *A számítógépes bűncselekmények elkövetésének térben és időben történő meghatározása, a törvényben használt fogalmak, kifejezések pontosítása a további nyomozási és felderítési eljárás szabályozáshoz hozzájárul.*

Az értekezésben vizsgáltuk az egyes kriminalisztikai eszközöket és a büntetőeljárásjogi szabályozást is, amelyek által számítógépes bűncselekmények esetében az elektronikus adat és rendszerekkel összefüggésben a kényszerintézkedések végrehajtása eltérő-e a - Fenyvesi Csaba által is- „hagyományosnak nevezett"[4] deliktumoktól. Mivel a számítógépes bűncselekmények egy része a kibertérben, azaz a virtuális térben történik, így a tárgyi bizonyítási eszközöket sem lehet a kézzel fogható bizonyítékokkal egy séma alá véve kezelni.

Mivel a számítógépes bűncselekmények nyomozása során központi szerep jut a számítástechnikai eszközökön és rendszerekben tárolt elektronikus adatoknak, bizonyítékoknak így az azokkal kapcsolatos kényszerintézkedések kriminalisztikai és büntetőeljárásjogi szabályait és módszereit helyeztük a vizsgálatunk középpontjába.

[3] Kovács Gyula-Nagy József: Kriminálmetodika elméleti és gyakorlati kérdései (Nemzeti Közszolgálati és Tankönyvkiadó Zrt., Budapest, 2013) 106.
[4] A hagyományos vagy klasszikus bűncselekmények közé tartoznak az élet-és testi épség elleni, a rablás, szexuális támadás stb. deliktumok (Fenyvesi Csaba: A kriminalisztika tendenciái- A Bűnügyi nyomozás múltja, jelene, jövője (Dialóg Campus Szakkönyvek, Dialóg Campus Kiadó, Budapest, 2017) 242.

A leplezett eszközök alkalmazásának lehetőségét a számítógépes bűncselekmények felderítése során szintén érintettük, hiszen az infokommunikációs eszközökön történő kommunikáció és adatok átvitele a bevezetett kényszerintézkedésekkel nem minden esetben valósulhat meg maradéktalanul. A leplezett eszközök és módszerek lehetővé teszik, hogy a számítógépes bűncselekmények jellemzői (gyorsaság, látencia, intellektuális és nemzetközi jelleg) ellenére az elkövető személyét, az elkövetés idejét és az elkövető tartózkodási helyéről a lehető legtöbb információt szerezzenek a nyomozó hatóságok.

Vizsgáltuk továbbá, hogy az igazságügyi szakértőnek milyen szerepe van a számítógépes bűncselekmények nyomozása során. Tudása és különleges szakértelme milyen esetekben jelentkezik és milyen súllyal esik latba a büntetőeljárás során?
A disszertáció középpontjában a számítógépes bűncselekmények és azok nyomozása áll, úgy, hogy megvizsgáljuk a kényszerintézkedésekre vonatkozó büntetőeljárási törvény szabályozását, valamint a kriminalisztikai kihívásokat ennek a modern és dinamikusan fejlődő, változó deliktumnak.

A kutatás középpontjába tehát nemcsak a számítógépes bűncselekmények vizsgálatát helyeztük, hanem a számítógépes bűncselekmények nyomozásának problémáinál a bizonyítékok megszerzésével és értékelésével kapcsolatos kihívásokat és változásokat is vizsgáltuk.

# 2 A KUTATÁS SORÁN ALKALMAZOTT ESZKÖZÖK ÉS KUTATÁSI MÓDSZEREK

A kutatás során az alkalmazott módszerek kiválasztásánál több szempontot is vizsgáltunk. Az adatgyűjtéseket több módszerrel végeztük, egyrészről kvantitatív módszerek közül a kérdőívvel, míg a kvalitatív módszerek közül az interjú készítéssel, illetve akta- és dokumentumkutatással. A módszerek számbavétele során azonban szem előtt tartottuk az általunk választott téma multidiszciplináris jellegét, miszerint a jogtudomány és a kriminalisztika ötvözete, hiszen leginkább a nyomozó hatóság, így a rendőrség és a Nemzeti Adó-és Vámhivatal (NAV) bűnüldözéssel foglalkozó szervei.

A kérdőíves módszer tekintetében mérlegeltük, hogy a hazai szervezetek közül a jogszabályi előírásoknak megfelelően ki és milyen esetekben jogosult a büntetőeljárás lefolytatására és a saját erőforrások tekintetében sikeres lehet-e annak végrehajtása.

A Nemzeti Közszolgálati Egyetemen (továbbiakban: NKE) folyó Közigazgatás-és Közszolgáltatás-Fejlesztési Operatív Program (továbbiakban: KÖFOP) kutatás keretében létrejött Kiemelt Kibervédelmi Kutatóműhelyben végzett tudományos munka keretében az NKE Rendészettudományi Kar hivatásos alap-és mesterképzésben (a levelező munkarendben tanuló hallgatók hivatásos állományúak) résztvevő hallgatók körében a kollégákkal végeztük el a lekérdezést.

A kérdőíves módszer mellett a rendőr kollégák körében azt vizsgáltuk, hogy a szolgálati helyükön ők vagy a közvetlen kollégáik mennyire vannak tisztában a digitális bizonyítékokkal, illetve azzal, hogy milyen teendőik vannak/lehetnek.
A nyomozó hatóságoknál a következő problémákkal találkoztunk a legtöbb esetben:

- munkájuk során nem találkoztak számítógépes bűncselekménnyel;
- amennyiben a nyomozás során informatikai eszközzel vagy elektronikus adattal kapcsolatos kényszerintézkedésre került sor, úgy annak végrehajtásához szakértőt (szaktanácsadót) vettek esetleg igénybe, megkereséssel és segítségkéréssel éltek a Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály, mint szakirányítást ellátó egység felé, illetve a hagyományos bűncselekmények esetén alkalmazandó kriminál taktikai módszert alkalmaztak az ügy nyomozása során;

- a szakmai hiányosságok miatt az ügyészséghez, mint nyomozást felügyelő szervhez fordultak iránymutatásért (nem minden esetben kaptak iránymutatást- jellemzően a nem budapesti ügyészségen);
- a nyomozó hatóság, bár kapott a számítógépes bűncselekmények esetén a hatósági eljárásokkal kapcsolatos oktatást, azonban az nem mindig volt megfelelő mélységű, esetleg téves információkat tartalmazott;
- bár a hatóságok elméletben tudják, hogy mit kell tenni, de nem rendelkeznek megfelelő eszközzel, amivel az adatmentést vagy az informatikai eszköz átvizsgálását el tudnák végezni.

Kutatási szerződést kötöttem a Legfőbb Ügyészséggel, így a Fővárosi Főügyészségen csoportvezető ügyész asszonnyal, dr. Losonczi-Molnár Melindával interjúkészítésre került sor. Az interjú egy része előre meghatározott kérdések alapján zajlott, majd közben nyitottabb, de a tanulmány szempontjából fontos kérdéseket tettem fel egy félig-strukturált interjú keretében. Továbbá a Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály munkatársaival, a Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztályával, valamint a Nemzeti Kibervédelmi Intézet vezetőjével, dr. Bencsik Balázs igazgató úrral is készítettem interjút. Az interjúalanyok kiválasztásának szempontja az volt, hogy olyan személyek legyenek, akik kapcsolatban vannak a büntetőeljárással, a kiberbűncselekményekkel és nem annyira a technikai hiányosságok, mint inkább a jogi szabályozás, illetve a jogszabályok alkalmazásánál látnak problémát.

Egyes részeiben, leginkább a külföldi jogirodalom tekintetében könyvtári és internetes szakirodalomra támaszkodtunk, ami során felhasználtunk a külföldi monográfiákat, tanulmányokat és médiaforrásokat. Mivel összehasonlítás révén kívántuk a magyar és a nemzetközi gyakorlati problémákat szemléltetni, így ezek általában egy fejezeten belül vannak. A szakirodalom kiválasztása során továbbá figyelembe vettük, hogy- bár az 1980-as években is foglalkoztak már többek között Magyarországon is- számítógépes bűncselekményekkel, de az azóta eltelt 25-30 évben nemcsak a számítógépek, mint eszközök fizikai tulajdonságai változtak, hanem azok teljesítménye is hatalmas változáson ment keresztül az egyre szélesebb körben történő felhasználásuk során. Megváltoztak a felhasználói igények velük kapcsolatban, hiszen már a mindennapi használati eszközeink közé tartozik, amelynek fontos szerepe van a magánélettől- a közösségi médiának köszönhetően- kezdve a pénzügyi, - ipari, - közlekedési, -

oktatási szektoron át egészen a kormányok feladatainak és információ éhségének ellátásáig. Az informatikai rendszerekkel szemben támasztott igények teljesítése miatt hatalmas fejlődésnek lehettünk tanúi. Pusztai László egyik, 1989-ben megjelent tanulmányához végzett felmérése szerint 1985-ben Magyarországon, mintegy 36 786 számítógép volt használatban a 4610 gazdálkodó szervezetben, a magánhasználatban pedig körülbelül 53 000 darab, azaz nem sokkal több, mint 90 000 számítógép volt használatban Magyarországon[5]. Ez a szám 2014-ben már a lakosság tekintetében 53,2% (személyi számítógéppel rendelkező lakosság) és 45,4% (laptoppal rendelkezők) a KSH adatai alapján[6].

Egy 2017-ben készült felmérés szerint a minden második személy legalább alapfokú informatikai ismerettel rendelkezik[7]. Mivel jelenleg az ötödik számítógép generációnál tartunk a számítógépek fejlesztése tekintetében, ezért a külföldi és a hazai szakirodalom minden esetben 2000-es években készült szakirodalmat tartjuk fontosnak, az azt megelőzően készült tanulmányokkal pedig csak a szükséges mértékig foglalkoztunk.
Kevés történeti rész kerül bemutatásra, mivel a jelenlegi problémákkal és gyakorlattal foglalkoztunk, ehhez a leíró módszert választottuk.

### 2.1 A kutatás célja

Ray Kurzweil[8] a technológia fejlődésével kapcsolatos véleménye: „Sok tudósra és mérnökre jellemző az, amit én a „tudósok pesszimizmusának” nevezek. Gyakran annyira elmerülnek egy jelenbeli kihívás nehézségeiben és apró részleteiben, hogy nem ismerik fel saját munkájuk és a tágabb értelemben vett tudományterületük hosszú távú hatásait, mint ahogy azokat a sokkal erősebb eszközöket sem veszik számításba, amelyek a technológia minden egyes új nemzedékével hozzáférhetővé válnak.”[9]
Kurzweil fenti megállapítása, amely a Mesterséges Intelligenciával foglalkozó könyvében olvasható, az értekezés írása és a kutatások során sok helyen beigazolódott, annyiban, hogy

[5] Pusztai László: Számítógép és bűnözés In.: Gödöny József (szerk.): Kriminológiai és Kriminalisztikai Tanulmányok 26. (KJK, Budapest, 1989) 85.
[6] KSH adata (forrás: http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_oni006.html, letöltve: 2019. március 22.)
[7] forrás: http://www.parlament.hu/irom41/00208/00208.pdf
[8] Ray Kurzweil a Google fejlesztő igazgatója, futurológus, a technológia jövőben játszott szerepének egyik vizsgálója
[9] Ray Kurzweil: A szingularitás küszöbén- Amikor az emberiség meghaladja a biológiát (Ad Astra 2014, 37.oldal)

nemcsak a kutatásokat, a kutatókat érinti ez a „beszűkülés”, hanem a rendőrséget, azon jogalkotókat is, akik bár érzik a kiberbűnözés jelenlegi negatív hatásait, de sajnos nem kellő időben, vagy nem a hatékony eszközökkel, a jogalkotási rendszer évtizedes sémáját eldobva próbálják meg felvenni a harcot a számítógépes bűnözéssel.

A kutatás során célul tűztem ki, hogy megkeressem azokat a gyenge pontokat a számítógépes bűnözéssel összefüggő jogszabályok területén, amelyek a kiberbűnözés dinamikus fejlődése miatt gondot okozhat a hatóságoknak a nyomozások során. Ezért elsősorban a hazai jogszabályokat tekintettem át, külföldi „jó joggyakorlattal” összevetve.
A nehézségek feltárása és megismerése közelebb vihet ahhoz, hogy a számítógépes bűncselekmények elleni nemzeti és nemzetközi fellépés sikeres legyen.

Mivel egy viszonylag friss és dinamikusan fejlődő bűncselekmény típusokról van szó, így a hipotézisek és tézisek tekintetében szükséges volt, a változékonyságához alkalmazkodó kérdéseket feltenni.

Az értekezés során az alábbi pontokat vizsgáltuk:

1. A számítógépes bűncselekmények esetében az új büntetőeljárásjogi törvényben bevezetett kényszerintézkedések hatékonyságának vizsgálata és javaslatok kidolgozása külföldi példák figyelembevételével.
2. A szakértő kirendelések szükségességének vizsgálata, és a bíróság előtti eljárásban a bizonyítékok összegyűjtése, értékelése. Meddig terjedhet a nyomozóhatóság kompetenciája a számítógépes bűncselekményekben?
3. Az egyes kiberbűncselekmények során más és más sarkalatos problémák merülnek fel, eltérő eljárási cselekmények válnak szükségessé az elkövető kézrekerítése, valamint a bűncselekmény bizonyítása érdekében.
4. A rendőrség kiberbűnözés nyomozásával kapcsolatos oktatásának fontossága, amely első lépése lehet a bűncselekmény eredményes felderítésének.

# 3 A TUDOMÁNYOS EREDMÉNYEK ÖSSZEFOGLALÁSA, AZOK HASZNOSÍTÁSA, ILLETVE HASZNOSÍTÁSI LEHETŐSÉGEI

Első hipotézisünk: *A számítógépes bűncselekmények elkövetésének térben és időben történő meghatározása, a törvényben használt fogalmak, kifejezések pontosítása a további nyomozási és felderítési eljárás szabályozáshoz hozzájárul.*

Ennek a feltételezésnek megfelelően kimondható, hogy a kibertérből származó bűncselekmények üldözése nem lehet hatékony, addig, amíg magát a kiberteret a fizikai térrel azonosítjuk, azaz megpróbálunk határokat szabni és azok között tartva megállapítani a hatóságok illetékességi területét. Ilyenkor fordul elő az, hogy ismeretlen tettes ellen indított nyomozás során a szolgáltató székhelye szerinti hatóság jár el az ügyben, ami nem zárja ki, hogy az elkövető a hatóság illetékességi területén kívül követte el a bűncselekményt.

A következő javaslatot foglmaztuk meg ezzel kapcsolatban:

- az ismeretlen tettes ellen indított nyomozás során annak a hatóságnak kötelessége eljárni, ahol a feljelentést először tették, vagy ahol a bűncselekményt először észlelték.
- az előkészítő eljárás során pedig annak a hatóságnak kell eljárni, amelyik az eljárás során a jogellenes cselekményről először tudomást szerzett.
- amennyiben a cselekmény elkövetése határokon átnyúló bűnözésre mutat, úgy nemzetközi jogsegély, együttműködés keretében van mód az eljárás lefolytatására.

Az idő, mint nyomozást nehezítő tényező, szintén problémát okoz a számítógépes bűncselekmények esetében. Az időnek is jelentősége van, mind az elévülési idő számításakor, mind pedig a felderítés során alkalmazandó cselekmények végrehajtása során. Az sem tisztázott, hogy mikor következik be a jogsértő cselekmény, mi tekinthető kezdő időpontnak?

Az idő jelentőségének egyrészt az elkövetés idejének megállapításakor van jelentősége: a jogellenes cselekmény elkövetésének meghatározásakor érdekes kérdés, hogy mikor tekinthetjük elkövetettnek például az információs rendszer felhasználásával elkövetett csalást abban az esetben, amikor

A számítógépes bűncselekmények elkövetése során az időnek az elévülés és a bizonyítékok beszerzése tekintetében van különleges jelentősége, így a hipotézisünknek ezt a részét bizonyítani nem tudtam.

*Második hipotézisünk: az egyes kriminalisztikai eszközöket és a büntetőeljárásjogi szabályozást is, amelyek által számítógépes bűncselekmények esetében az elektronikus adat és rendszerekkel összefüggésben a kényszerintézkedések végrehajtása eltérő-e a - Fenyvesi Csaba által is- „hagyományosnak nevezett" deliktumoktól. Mivel a számítógépes bűncselekmények egy része a kibertérben, azaz a virtuális térben történik, így a tárgyi bizonyítási eszközöket sem lehet a kézzel fogható bizonyítékokkal egy séma alá véve kezelni.*

A számtógépes bűncselekmény és a számítógépes bűncselekmény között az alábbiak szerint tettünk különbséget:

- Számítógépes bűncselekmény- azaz, ahol magának a számítógépnek, mint elkövetés eszközének jelentősége van, minden olyan bűncselekmény, ami már létezett a számítógép előtt is már ismertek voltak. Ilyenek a sikkasztás, a csalás (Btk. 373.§). Sokkal tágabb kategóriaként értelmeztük, mint a kiberbűncselekményeket, hiszen elkövetésükhöz nem szükséges információs rendszer, hálózat, hanem elegendő maga a számítógép.
- A kiberbűncselekményeknek pedig azok a bűncselekmények tekinthetőek álláspontunk szerint, amelyek már az IT fejlődésével párhuzamosan alakultak ki, és amelyek azok fejlődésével folyamatosan változnak is, ugyanakkor a cselekmény összefügg a kibertérrel, hiszen az elkövetés ott történik. Ilyen bűncselekmények például az információs rendszer vagy adat megsértése (Btk. 423.§), az információs rendszer védelmét biztosító technikai intézkedés kijátszása, amely megvalósulhat akár vírusok, férgek és célzott alapú támadások stb. révén.

Ha a két fogalom között keressük a különbséget, akkor érezhető, hogy a számítógépes bűncselekmények hagyományosabb elkövetést feltételeznek, így a bizonyítékok gyűjtése és értékelése során a „tárgyi" bizonyítási eszköz kifejezés helytálló, hiszen a fizikailag körülhatárolható eszköz, így a számítógép, mint „eszköz" jelenik meg, a valós térben is bekövetkezik a jogellenes cselekmény és ott is érezhető annak hatása.

A számítógépes bűncselekmény esetében az elkövetés a kibertérben történik és az elektronikus információs rendszereket, elektronikus adatokat érinti. Hatása érezhető a valós térben, így a például a 2017-ben bekövetkezett Wannacry zsarolóvírus támadás a kórházak, mint kritikus infrastruktúrák ellen, zavart okozott a betegellátásban.

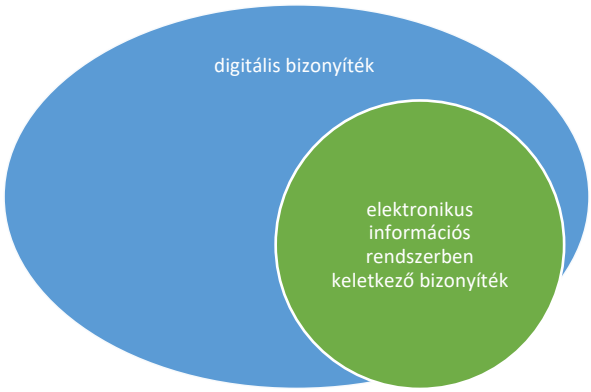
A bizonyítékok értékelése és a büntetőeljárásban nevesített kényszerintézkedések végrehajtása a két „bűncselekmény típus” között eltérő, nem lehet tipikus rendszerbe besorolni, így a fentiek fényében séma szinten említeni a bizonyítás tárgyát sem lehet.

A számítógépes bűncselekmények nyomozásánál és felderítésénél, a bizonyítékok összegyűjtéséhez szükséges a kreatív, nem vonalas, tipikus eljárások bevezetése, kivitelezése. Amennyiben sikerülne különválasztani a kibertérből beszerezhető bizonyítékokat és a bizonyítási eljárásokat a hagyományos bűncselekményektől, úgy lenne értelme a „jó gyakorlat” kialakításának.
Javaslatunk a digitális bizonyítékokkal kapcsolatban, hogy ésszerű lenne az elektronikus információs rendszerben keletkező bizonyítékok fogalmának megalkotása és beemelése a büntetőeljárásról szóló törvénybe. Ezek legáltalánosabb összetevője a következők lehetnek:

- olyan adatok, információk, amelyek a rendszer használata során, a rendszerből vagy arról a számítástechnikai eszközről szerezhető be, amelyen az érintett rendszer fut
- olyan számítógépes programok, amelyek a felhasználók tevékenységét, digitális lábnyomát tartalmazza
- azok az információk, amelyek bár változékonyak és eredetiségük megtartása nehezebben megoldható, mint a tárgyi bizonyítási eszközök esetében
- Az útmutatók készítése - mint ahogyan az ENISA által készített bizonyítással kapcsolatos útmutató ismertetése során is említettem, így a 7.7 alfejezetben ismertetett megoldási javaslatok egy részének bevezetése és tovább gondolása is segíthetné a számítógépes bűnözés elleni küzdelmet.

Digitális bizonyíték: minden elektronikus információs rendszer útján keletkező, a bűncselekmény nyomait tartalmazó bizonyíték, amely lehet bármilyen dokumentumról, tárgyról, eszközről elektronikus úton keletkező és amely az elektronikus információs rendszerben (is) megtalálható, tárolható, onnan előhívható.

Az elektronikus információs rendszerben keletkező bizonyíték fogalma már szűkebb a digitális bizonyíték fogalmánál. A digitális bizonyíték vagy digitális adat és azoknak az elektronikus információs rendszerben, a tárolásukból, módosításukból, törlésükből keletkező bizonyíték.




*1. ábra: Gyaraki Réka. digitális és elektronikus bizonyítékok kapcsolata*

*A számítógépes bűncselekmények nyomozása során központi szerep jut a számítástechnikai eszközökön és rendszerekben tárolt elektronikus adatoknak, bizonyítékoknak így, az azokkal kapcsolatos kényszerintézkedések kriminalisztikai és büntetőeljárásjogi szabályait és módszereit helyeztem a vizsgálatom középpontjába.*

A disszertáció témája szempontjából természetesen a 2012. évi C. törvény, a hazai büntetőtörvénykönyvünk és a 2017. évi XC. törvény, a büntetőeljárásról szóló törvény, valamint azok egyes rendelkezései állnak a vizsgálatom középpontjában.
A feltételezésem alátámasztását szolgálja a külföldi, leginkább Európai Uniós szabályozások és az egyes uniós tagállamok számítógépes bűncselekményekkel foglalkozó szabályozása.

Mivel hazánk is az Európai Unió tagja, így az Unió által hozott irányelvek, rendeletek implementálásával próbál megfelelni a kötelezettségeknek, így jogszabályainkban is sok helyen visszaköszön, ha másképp nem is, a szószerinti angolnyelvű szöveg magyarra történő fordítása által, az uniós szabályok.

A feltételezésünk elsődleges és egyben legfontosabb igazolása a 2014-2019-re vonatkozó Európai Parlament jelentése a számítógépes bűnözés elleni küzdelemről, amelyben felismerik, hogy a merev jogszabályalkotással nem érhető el hathatós eredmény.
Javaslatunk egy olyan keretjogszabály megalkotására lenne szükség, amelyben a változó információs technológiai környezetnek olyan szinten lenne képes eleget tenni, hogy a fejlődő számítógépes bűncselekmények és a kialakuló újabb és újabb elkövetési módszerek ne maradjanak büntetlenül. Mindamellett, hogy nem elég jelenleg, ha ez a változás csak az egyes országokon belül történik meg, hanem szükséges lenne akár Uniós, akár valamennyi ország

tekintetében az azonos deliktumokat közös néven nevezni és egy ténylegesen közös büntetőpolitika kialakítása irányába haladnánk.
Ezen felül megoldást jelenthetne, ha a Számítástechnikai Bűnözésről szóló Egyezmény 2001-ben aláírt szövegét és javaslatait újra gondolnák és konkrétabb célokat és szabályokat alkotnának meg, amely nemcsak a bűncselekmény bekövetkezése esetén szükséges lépéseket fogalmazna meg, hanem a megelőzésre is hangsúlyt fektetne.

*A leplezett eszközök alkalmazásának lehetőségét is vizsgáltam a számítógépes bűncselekményeknél.*
A kiberfelderítés („digitkommandó") előretörése alfejezetben *Fenyvesi Csaba rámutat arra, hogy számtalan akadály nehezíti a digitnyomozást:*

- *az elkövető és a számítógépet használó személye mellett még az elkövetési hely is nehezen azonosítható...*
- *a világ minden pontjáról – ezeket váltogatva is- bűncselekményt lehet elkövetni...*
- *a kibertéri adatok csak virtuálisan léteznek, a szó fizikai értelmében nyomot, anyagmaradványt nem találhat ...az adatok között bányászva*
- *alattomosan rejtve maradhatnak sokáig (vagy örökre) a tettek és következményeik...*[10]*"*

A leplezett eszközök és módszerek ugyanakkor lehetővé teszik, hogy az alábbiak tekintetében, mint:

- az adatok elszórtsága
- az anonimizáló technikák
- a titkosítási technológiák
- amikor egy adott ügyben több állam is érintett
- a személyi jellegű bizonyítékok másodlagossága
- az egyes szolgáltatók megbízhatóságának kérdése

az adott ügyben ne jelentsenek problémát.

Ugyanakkor a kibertérben, mint határoknélküli térben elkövetett deliktumok esetében a hagyományos nyomozások nem minden esetben érnék el a céljukat. Így például a gyermekpornográfia, a fehérgalléros bűncselekmények felderítésében a fedett nyomozó

[10] Fenyvesi Csaba: A kriminalisztika tendenciái (Dialóg Campus Szakkönyvek, Dialóg Campus Kiadó, Budapest, 2017), 218-219

munkája, a környezettanulmány, a lehallgatás, a titkos kutatás, a hely titkos megfigyelése elengedhetetlen, hiszen a sajátos jellemzők miatt a nyílt nyomozásoknál hatékonyabb eredmény érhető el.

*Vizsgáltuk az igazságügyi szakértő szerepét a számítógépes bűncselekmények nyomozása során. Hogyan és meddig végezheti el az informatikai eszközök és adatok vizsgálatát a nyomozó hatóság és mikor szükséges és elengedhetetlen a szakértő vagy szaktanácsadó kirendelése?*
Természetesen a legkézenfekvőbb és pénzkímélő megoldás az lenne, ha a nyomozó hatóságok maguk is rendelkeznének olyan szakértelemmel, amely képessé tenné őket a szakértő helyett eljárva a számítógépes bűncselekmények esetén a vizsgálatok elkészítésére és csak a legvégső esetben lenne szükség szakértőt kirendelni.
Ennek azonban több akadálya is van: egyrészt sérülne a pártatlanság elve, hiszen a bizonyítás annak a feladata is lenne egyúttal, aki a nyomozást vezeti.
Másrészt a hatóság által végzett szakértésnél nagyobb eséllyel fordulna elő a hanyagság, pontatlanság és nem utolsó sorban az elfogultság.
Harmadrészt a szakértők vagy szakértői intézetek rendelkeznek azokkal a technikai eszközökkel, berendezésekkel és nem utolsó sorban tudással, amelyekkel a lefoglalt eszközöket, adatokat át tudják úgy vizsgálni, hogy hiteltérdemlőségükhöz ne férjen kétség.
A további nehézségeket még hosszan lehetne sorolni (így például a pénz és oktatás hiányossága), de addig, amíg a különleges szakértelem nem kerül meghatározásra egyetlen jogszabályban sem, addig a szakértő által nyújtott „pluszt” kell elfogadni.

### 3.1 A disszertáció hasznosítása

A disszertáció során végzett kutatásokat leginkább a gyakorlati tapasztalatokra alapoztuk, ezért elsődleges szempont volt, hogy a számítógépes bűncselekmények nyomozásában részt vevő szerveknél, így a rendőrségen, NAV-nál és az ügyészségen tájékozodjunk a legújabb trendekről és elkövetvési módokról, ezzel is kilépve az íróasztal mögül és a tényleges problémákra rávilágítva az elméletet és a gyakorlatot kívántuk közelíteni.
Elsődlegesen tehát célunk nemcsak a hiányosságok feltárása volt a büntetőeljárásban, hanem javaslatok megfogalmazása révén kiindulási alapot nyújtsunk a számítógépes bűncselekményekkel kapcsolatos változások megindítására.

# 4 ÖSSZEGZÉS

A számítógépes bűncselekmények az egyik legdinamikusabban fejlődő bűnözési típus, amely az informatikai eszközök elterjedésének, elérhetőségének és a folyamatos fejlesztéseknek köszönhetően kihívást jelent az államoknak, a gazdaságnak, a magán-és államiszférának, a társadalomnak, de igazi kihívást jelent a jogalkotóknak és a jogalkalmazóknak.

A XX. század sci-fi és fantasztikus filmjei, regényei, jóslatai a XXI. század technikai fejlődésével kapcsolatban jóval meghaladta az akkor elképzelhető mértéket.

A nyomozó hatóság számára jelenleg igazi kihívást jelent, hogy felvegyék a harcot a számítógépes bűnözőkkel, akik a különböző technikai kihívásokat kihasználva maradnak láthatatlanok és anonimok a kibertérben, miközben a tevékenységük káros hatása érezhető, látható.

A számítógépes bűncselekmények üldözését célul tűzte ki az Európai Unió valamennyi tagállama, amely nemcsak a számítógépes bűncselekmények törvénybe történő nevesítésében, az uniós ajánlásokban, irányelvekben és rendeletek sorozatos megalkotásában, az államok Kiberbiztonsági Stratégiájában nyilvánul meg. A felsőoktatási intézmények keretein belül a szakemberek képzésével, az oktatók folyamatos kutatásával és szakmai fórumok szervezésben észlelhető az a pozitív szemlélet, amely biztosíthatja a hatékony fellépést a számítógépes bűnözőkkel szemben.

Pilisszentkereszt, 2019. április 8.

**SUMMARY**

*„Clearly, we are more and more dependent than ever on Internet-connected computer systems: it is the way we communicate, do our banking, pay our taxes, book our travel, and buy merchandise. We take for granted that these systems will always be there and are set to protect our privacy and are secure. The strength of the Internet and Internet technologies is that we are so connected. However, this strength is also a weakness – these systems are vulnerable to attack from anywhere by anyone, and with little capital investment. The Internet also facilitates maintaining anonymity [...]*[11]

This quote and Mark Russinovich's Zero Day novel perfectly demonstrate the hidden challenges that Internet users meet every day, and with which organizations fighting cyber - crimes have to face on a daily basis.

Cyber-crime is the fastest growing type of crime, and because of the prevalence, accessibility and continuous development of IT devices, they pose a real challenge to the different states, economies, private and government sectors, society, but especially, law makers and law enforcement.

The prediction of the 20th century sci-fi and fantasy movies and novels regarding the 21st century's technical development far exceeded what they thought would be possible then. It is now a real challenge for the investigating authorities to battle cyber criminals who remain invisible and anonymous in cyberspace by utilizing various technical challenges while the detrimental effect of their activity is clearly visible.

All member states of the European Union has set fighting cybercrime as a goal, not only by defining computer crimes in laws, giving EU recommendations and directives, creating a series of regulations, or the states' Cyber Security Strategy. We can now see a positive approach in higher education institutions in training specialists, providing ongoing research opportunities to trainers and organizing professional forums which can all lead to an effective fight against cybercriminal

[11] Russinovich.

# 5 FELHASZNÁLT IRODALOM ÉS A SZERZŐ SAJÁT PUBLIKÁCIÓI


1. 11/2003. (V. 8.) IM-BM-PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról, Pub. L. No. 11/2003. (V. 8.) IM-BM-PM együttes rendelet (é. n.). https://net.jogtar.hu/jogszabaly?docid=a0300011.im
2. 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről, Pub. L. No. 25/2013. (VI. 24.) BM rendelet (é. n.). http://www.police.hu/sites/default/files/25-2013.pdf.
3. 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, Pub. L. No. 60/2013. (IX.30.) HM utasítás (é. n.). https://net.jogtar.hu/jogszabaly?docid=A13U0060.HM&getdoc=1.
4. 295/2010. (XII. 22.) Korm. rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól, Pub. L. No. 295/2010. (XII. 22.) Korm. rendelet (é. n.). https://net.jogtar.hu/jogszabaly?dbnum=1&docid=A1000295.KOR&mahu=1.
5. 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, Pub. L. No. 1139/2013. (III. 21.) Korm. határozat (é. n.). http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845.
6. 1998. évi XIX. törvény a büntetőeljárásról, Pub. L. No. XIX. törvény (é. n.). https://net.jogtar.hu/jogszabaly?docid=99800019.TV&timeshift=fffffff4&txtreferer=00000001.TXT.
7. 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről, Pub. L. No. CVIII. törvény (é. n.). https://net.jogtar.hu/jogszabaly?docid=a0100108.tv#lbj0id3527.
8. 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről, Pub. L. No. LXXIX. törvény. Elérés 2018. május 23. https://net.jogtar.hu/jogszabaly?docid=A0400079.TV&searchUrl=/gyorskereso%3Fpagenum%3D5.
9. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, Pub. L. No. CXII. törvény (é. n.). https://net.jogtar.hu/jogszabaly?docid=A1100112.TV.
10. 2012. évi C. törvény a Büntető Törvénykönyvről, 2012. évi C. Btk. § (é. n.). https://net.jogtar.hu/jogszabaly?docid=A1200100.TV.
11. 2016. évi XXIX. törvény az igazságügyi szakértőkről, Pub. L. No. XXIX. törvény (é. n.). https://net.jogtar.hu/jogszabaly?docid=A1600029.TV&timeshift=fffffff4&txtreferer=00000001.TXT.
12. 2017. évi XC. törvény a büntetőeljárásról, Pub. L. No. XC. törvény (é. n.). https://net.jogtar.hu/jogszabaly?docid=A1700090.TV&timeshift=fffffff4&txtreferer=00000001.TXT.
13. 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről szóló törvény
14. 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló törvény

15. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), Pub. L. No. 2016/679 rendelet (é. n.). https://www.adatvedelmirendelet.hu/wp-content/uploads/2016/07/CELEX3A32016R06793AHU3ATXT.pdf.
16. Az Európai Parlament és a Tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról {SWD(2018) 118 final} - {SWD(2018) 119 final}, Pub. L. No. COM(2018) 225 rendelet. Elérés 2018. augusztus 2. https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0019.02/DOC_1&format=PDF.
17. Európai Bizottság. „A Bizottság közlemenye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának - A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé". Közlemény, 2007.
18. European Commission. „Regulations, Directives and other acts". Elérés 2018. augusztus 6. https://europa.eu/european-union/eu-law/legal-acts_en.
19. „Evaluation report on the seventh round of mutual evaluations »The practical implementation and operation of European policies on prevention and combating cybercrime« - Report on Hungary", é. n. http://data.consilium.europa.eu/doc/document/ST-14583-2016-REV-1-DCL-1/en/pdf.
20. Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, Pub. L. No. JOIN/2013/01 (é. n.). https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001.
21. StPO (Strafprozessordnung) (é. n.). https://dejure.org/gesetze/StPO/100b.html.
22. Számítástechnikai Bűnözésről szóló Egyezmény (é. n.). https://net.jogtar.hu/jogszabaly?docid=A0400079.TV&searchUrl=/gyorskereso%3Fpagenum%3D5.
23. ENSZ. *Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről*, 1994. http://www.uncjin.org.
24. Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) által meghatározott stratégiai célok a kiber-bűnözés ellen harc terén a 2014-2017 közötti időszak tekintetében". http://www.cert-hungary.hu/node/212, 2013. október 25. http://www.cert-hungary.hu/node/212.
25. A számításrechnikai bűnözésről szóló Egyezménynek a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyve (é. n.).
26. Gov. „Kibervédelmi parancsnokságot létesítenek a honvédségen belül". https://hirlevel.egov.hu/2018/03/10/kibervedelmi-parancsnoksagot-letesitenek-a-honvedsegen-belul/, 2018. március 10. https://hirlevel.egov.hu/2018/03/10/kibervedelmi-parancsnoksagot-letesitenek-a-honvedsegen-belul/.

**Felhasznált magyar nyelvű irodalom jegyzéke:**

1. Anti Csaba-Dr. Barta Endre-Dr. Bócz Endre-Dr. Lakatos János-Dr. Romasz Árpád: Kriminältaktika II. (Rejtjel Kiadó 2005,ISBN: 2050000017223
2. Bánáti, János, József Bellegi, Ervin Belovics, Árpád Erdei, Ákos Farkas, és István Kónya. *A büntetőeljárási törvény magyarázata - Az új, 2017. évi büntetőeljárási*

*törvény magyarázata a kodifikációs bizottság korábbi tagjaitól*. Budapest: HVG-ORAC, 2018.
3. Barker, Jonathan. *A terrorizmus*. Budapest: HVG Könyvek, 2003.
4. Bíró Gyula: Kriminalisztika (Kossuth Egyetemi Kiadó, Debrecen, 2004)
5. Blaskó, Béla, Zoltán Hautzinger, Sándor Madai, Anikó Pallagi, Péter Polt, és László Schubauer. *Büntetőjog különös rész II.* Budapest: Rejtjel Kiadó, 2015.
6. Bodó Balázs: A szerzői jog kalózai (Typotex, Budapest, 2011)
7. Bokor József: Informatika jogi szabályozása (Livermore 1. kiadás, 2005)
8. Borbíró Andrea-Gönczöl Katalin-Kerezsi Klára-Lévay Miklós: Kriminológia (Wolters Kluwer, 2017)
9. Budaházi, Árpád, és Zsanett Fantoly. *Büntető eljárásjog I. - Statikus rész*. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, NKE Szolgáltató Kft., 2015.
10. Dr. Balláné Prof. Dr. Fünszter Erzsébet.Dr. Lakatos János: Kriminalsiztika I. (NKE, Budapest 2012)
11. Dr. Csonka Péter: Council of Europe Activities Related to Information Technology Information & Communications Technology Law, Vol.5. No.3, 1996. p(s).
12. Dr. Háger Tamás: A büntetőtörvény időbeli hatályára vonatkozó rendelkezések mint alapvető alkotmányos, garanciális szabályok (https://ujbtk.hu/dr-hager-tamas-a-buntetotorveny-idobeli-hatalyara-vonatkozo-rendelkezesek-mint-alapveto-alkotmanyos-garancialis-szabalyok/)
13. Dr. Idzigné dr. Novák Marianna Csilla: A szakértő státuszváltozása a hazai büntetőeljárásban- különös tekintettel a kizárásra vonatkozó szabályokra (Széchenyi István Egyetem, 2018.)
14. Dr. Kertész Imre - Dr. Pusztai László: A komputerbűnözés és az információs technológiával kapcsolatos egyéb bűnözési fajták. ÜÉ. 29. 1993.4.
15. Dr. Kovács Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai (Doktori Értekezés http://archiv.uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/kovacs_zoltan_2015.pdf
16. Dr. Nagy Zoltán: Konferencia az információtechnikai bűnözésről. MJ. 40. 1993. 2.
17. Dr. Nagy, Zoltán András. *Bűncselekmények számítógépes környezetben*. Budapest: Ad Librum, 2009.
18. Erdei Árpád: Az igazságon alapuló büntető ítélet ideálja és a valóság. Igazság, Ideál és Valóság (Tanulmányok Kardos Sándor 65. születésnapja tiszteletére, Debreceni Egyetem Állam- és Jogtudomány Kar Büntető Eljárásjogi Tanszék, Debrecen 2014)
19. Erdei Árpád: Tanok és tévtanok a büntető eljárásjog tudományában (ELTE Eötvös Kiadó, Budapest 2011)
20. Erdei Árpád: Tény és jog a szakvéleményben (Közgazdasági és Jogi Könyvkiadó, Budapest 1987)
21. Eszteri Dániel: Egy bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések (Infokommunikáció és Jog XIV. évfolyam, 2017.augusztus)
22. Eszteri Dániel:„A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekbe- doktori értekezés PTE ÁJK
23. Eszteri, Dániel. „A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekbe". Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, 2015. http://ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-vedes-ertekezes.pdf.

24. Fantoly, Zsanett, és Anett Erzsébet Gácsi. *Eljárási büntetőjog – Statikus rész*. Szeged: Iurisperitus, 2013.
25. Fenyvesi Csaba: A kriminalisztika tendenciái- A Bűnügyi nyomozás múltja, jelene, jövője (Dialóg Campus Szakkönyvek, Dialóg Campus Kiadó, Budapest, 2017)
26. Finszter Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében. Budapest, 2005-2007. online: users.atw.hu/be/letoltes/Krimjegyzet.doc,
27. Fogarasi Béla: Logika, 4. kiadás, Akadémiai Kiadó, Budapest, 1958., 325. old. (Idézi Gödöny József: Bizonyítás a nyomozásban, Közgazdasági és Jogi Könyvkiadó, Budapest, 1968., 20. old).
28. Gácsi Anett Erzsébet: A Pécsi Ítélőtábla döntése a szakvélemény bizonyítási eszközként történő felhasználásáról, Értékelhető-e okirati bizonyítási eszközként az eljárási szabálysértéssel kirendelt eseti szakértő véleménye a Be. 78. § (4) bekezdése alapján? (Jogesetek Magyarázata 2014/1. szám)
29. Gárdonyi Gergely: Újra a szemle jogi szabályozásáról ( forrás: http://www.bm-tt.hu/rtt/assets/letolt/rt/201801/07_Gardonyi_Gergely_Ujra_a_szemle_jogi_szabalyozasarol.pdf)
30. Gödöny József dr.: Bizonyítás a nyomozásban (Közgazdasági és Jogi Könyvkiadó, Budapest 1968)
31. Gödöny József: Igazságügyi szakértők a nyomozásban (in Kriminalisztikai tanulmányok, Közgazdasági és Jogi Könyvkiadó, Budapest 1964 3. kötet)
32. Gyaraki, Réka, és Béla Simon. „Biztonsági események rendészeti szempontból – A kiberbűncselekmények kezelése". In *Incidensmenedzsment - éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára*, by Csaba Krasznay. Budapest: Dialóg Campus Kiadó, 2017.
33. Gyaraki, Réka. „Számítógépes bűncselekmények és az ellenük való védekezés". In *Információvédelem*, by László Christián, 175–89. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2015.
34. Hautzinger Zoltán: A fegyveres szervek rendeltetésének alaptörvényi szabályozása http://real.mtak.hu/90855/7/67_magyarorszag-uj-alkotmanyossaga-kotet-2011.pdf
35. Hegyaljai Mátyás: A nemzetközi bűnügyi együttműködés (Kül-Világ IX. Évfolyam 2012/4.)
36. Herke Csongor: Büntető eljárásjog (Dialóg Campus Kiadó, Budapest-Pécs, 2010)
37. Horváth, Attila. „Terrorfenyegetettség: célpontok, nagyvárosok közlekedés". *emzetvédelmi Egyetemi Közlemények* 10., sz. 3. (2006): 1–19.
38. Ibolya, Tibor. *A számítástechnikai jellegű bűncselekmények nyomozása*. Budapest: Patrocinium, 2012.
39. Illési Zsolt: Az igazságügyi informatikai szakértés modellezése (forrás: http://robothadviseles.hu/pres/Illesi_Zsolt10.pdf)
40. Jutasi, István. *Az Internet felépítése és működése: Hálózatok, Prtokollok, Biztonság, Netikett*. Szerkesztette Károly Nagy. Budapest: Műszaki Könyvkiadó, 1997.
41. Kármán Gabriella: A kriminalisztikai szakértői bizonyítás (2016)
42. Katona Géza szerk.: Szakértők igénybevétele a nyomozás során (BM Tanulmányi és Kiképzési Csoportfőnökség 1965)
43. Katona Géza: A kriminalisztikai szakértői vélemények értékeléséről (Jogtudományi Közlöny 1963/7. szám)
44. Katona Géza: Bizonyítási eszközök a XVIII-XIX. században (Közgazdasági és Jogi Könyvkiadó, Budapest 1977)
45. Katona Géza: Valós vagy valótlan, Értékelés a büntetőperbeli bizonyításban (Közgazdasági és Jogi Könyvkiadó, Budapest 1990)

46. Kereszty, Béla, Vilmosné Maráz, Ferenc Nagy, és Mihály Vida. *A magyar büntetőjog –Különös része*. Budapest: Korona Kiadó, 2004.
47. Kerezsi Klára-Korinek László-Lévay Miklós-Gönczöl Katalin: Kriminológia, szakkriminológia (Wolters Kluwer, 2012)
48. Kertész Imre: A szakértői bizonyítás (In: Kriminalisztika 1., BM Duna Palota és Kiadó, 2004) 231-232.
49. Király Tibor: A büntetőeljárási jog reformja elé (Magyar Jog 1993/5. szám)
50. Király Tibor: Büntetőítélet a jog határán (Közgazdasági és Jogi Könyvkiadó, Budapest 1972)
51. Komanovics Adrienne: Információszabadság az Európai Unióban, Pécs 2007, doktori értekezés
52. Korinek László: Tendenciák korunk bűnözésében és bűnüldözésében (https://jura.ajk.pte.hu/JURA_2014_1.pdf)
53. Kovács Gábor: az európai Forenzikus Tudományos Térség (eFsa-2020) megalkotásának koncepciója
54. Kovács Gábor: Az Európai Forenzikus Tudományos Térség (EFSA-2020) megalkotásának koncepciója (forrás: https://dfk-online.sze.hu/images/JÁP/2017/1/kovács.pdf,)
55. Kovács László, Illési Zsolt: Cyberhadviselés (Hadtudomány, 2011/1-2)
56. Kovács, László. *A kibertér védelme*. Budapest: Dialóg Campus Kiadó, 2018. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf.
57. Kriminalisztika1-2 (BM Duna Palota és Kiadó, 2004)
58. Kurzweil, Ray. *A szingularitás küszöbén: Amikor az emberiség meghaladja a biológiát*. Ad Astra Kiadó, 2013.
59. Máté, István Zsolt. „Az igazságügyi informatikai szakértő a büntetőeljárásban". Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, 2017. http://pea.lib.pte.hu/handle/pea/16947.
60. Mészáros, Bence. „Mészáros Bence: Fedett nyomozás a bűnüldözésben". Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, 2011. http://ajk.pte.hu/files/file/doktori-iskola/meszaros-bence/meszaros-bence-vedes-ertekezes.pdf.
61. Miskoczy Barna-Szathmáry Zoltán: Büntetőjogi kérdések az információk korában (hvgorac Lap-és Könyvkiadó Kft., Budapest, 2018)
62. Muha, Lajos. „Informatikai biztonsági fogalmak és definíciók". http://lmuha.hu/defins.html. Elérés 2018. március 23. http://lmuha.hu/defins.html.
63. Munk, Sándor: Szemantika az informatikában, Hadmérnök IX., sz. 2. (2014)
64. Munk, Sándor. „Szemantika az informatikában". *Hadmérnök* IX., sz. 2. (2014): 1–21.
65. Nagy Ferenc: A magyar büntetőjog, Általános rész (HVG-Orac, Budapest, 2010)
66. Nogel Mónika: Igazságügyi szakértői vélemény hiteltérdemlősége a büntetőeljárásban- doktori értekezés
67. Nyeste Péter: A leplezett eszközök hatékonysága (Pécsi határőr Tudományos Közlemények XIX. 2017)
68. Parti Katalin: Gyermekpornográfia az interneten (Bíbor Kiadó, Miskolc, 2009)
69. Parti, Katalin, és Tibor Kiss. „III. fejezet, Informatikai bűnözés". In *Kriminológia*, by Andrea Borbíró, Katalin Gönczöl, Klára Kerezsi, és Miklós Lévay, 491–93. Budapest: Wolters Kluwer Kft., 2016.
70. Pusztai László: Számítógép és bűnözés In.: Gödöny József (szerk.): Kriminológiai és Kriminalisztikai Tanulmányok 26. (KJK, Budapest, 1989)
71. Rainer, Lilla. „Az igazságügyi szakértőkkel kapcsolatos szabályozás és feladatok". Elérés 2018. július 13. https://birosag.hu/sites/default/files/allomanyok/Mailath-

palyazat-erdmenyek/MGyTP-BI-1-Rainer_Lilla_Az_igazsagugyi_szakertokkel_kapcsolatos_szabalyozas_es_feladatok.pdf.
72. Ropolyi, László. *Az internet természete*. Budapest: Typotex Kiadó, 2006.
73. Sandra Sarev-Tanel Kerikmae-Kasper Ágnes: Az e-polgárság mint virtuális migráció eszköze Észtországban (Információ és Társadalom, 2016., 2. szám)
74. Simon Béla: Csúcstechnológiai bűnözés és nyomozása ( NKE Rendészettudományi Kar, kiadó 2012)
75. Sorbán Kinga: A digitális bizonyítékok a büntetőeljárásban ( Belügyi Szemle, 2016/11. szám 64. évfolyam)
76. Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés az Amerikai Egyesült Államokban
77. Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban (forrás: https://docplayer.hu/47794558-Az-informatikai-buncselekmenyek-elleni-fellepes-az-egyesult-allamokban.html)
78. Szádeczky Tamás: Szabályozott biztonság. Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2011. Pécs.
79. Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a magyar büntetőeljárásban (Magyar Jog, 2015/11)
80. Szegediné Lengyel Piroska: Számítógépes bűnözés avagy fiatalok a cyber-térben (Hadmérnök, V. évfolyam 2. szám- 2010 június)
81. Székely János: Szakértők az igazságszolgáltatásban (Közgazdasági és Jogi Könyvkiadó, Budapest, 1967) 61-62 o.
82. Szentgáli Gergely: Az Európai Unió kiberbiztonsági törekvései és szervezetei II. (Hadmérnök, VIII. évfolyam 1. szám, 2013. március)
83. Tokaji Géza: A bűncselekménytan alapjai a magyar büntetőjogban (Budapest, KJK, 1984)
84. Tremmel Flórián – Fenyvesi Csaba: Kriminalisztika tankönyv és atlasz. BudapestPécs, 2002. Dialóg Campus.
85. Tremmel Flórián-Fenyvesi Csaba-Herke Csongor: Kriminalisztika (Dialóg Campus Szakkönyvek, Dialóg Campus Kiadó, Budapest-Pécs, 2009)
86. Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus. Budapest,2012
87. Várnay, Ernő, és Mónika Papp. *Az Európai Unió joga*. Budapest: KJK–KERSZÖV Jogi és Üzleti Kiadó Kft, 2002.

**Felhasznált külföldi irodalom:**

1. Elmar Erhardt: Strafrecht für Polizeibeamt (5.Auflage, 2016, W. Kohlhammer gmBH Stuttgart
2. Williams, Janet, szerk. ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence. Metropolitan Police Service, 2012. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
3. Litt, Robert S.: Crime in the computer age: The Law enforcement perspective Akadémiai folyóirat By: Texas Review of Law & Politics. Fall99, Vol. 4 Issue 1,
4. Philip Pfau: Kriminalitat im Rahmen der Informations- und Kommunikationstechnik (Cybercrime) (Grin Verlag, 2018, ISBN:978-3668675667)

5. SOLANO, MILLER SOTO: El crimen on-line. Una mirada a la responsabilidad del proveedor de servicio de Internet. (Spanish) Akadémiai folyóirat, By:. Justicia Juris , ene-jun2012, Vol. 8 Issue 1, Language: Spanish
6. Haley, Kevin. „Norton Cyber Security Insights Report 2017 Global Results". Symantec, 2017. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.
7. Carter, David L.: Computer crime categories. FBI Law Enforcement Bulletin. Jul95, Vol. 64 Issue 7,
8. Herzog, Felix: Straftaten im Internet, Computerkriminalität und die Cybercrime Convention. Criminal Acts on the Internet, Computer Criminality, and the Cybercrime Convention. By: Política Criminal: Revista Electrónica Semestral de Políticas Públicas en Materias Penales. dic2009, Issue 8,
9. ALLEN, JEFFREY; HALLENE, ASHLEY : Digital Evidence, American Journal of Family Law , Spring2018, Vol. 32 Issue 1,
10. Freiling, Felix Glanzmann,Thomas Reiser, Hans P. :Digital evidence- Germany,DFRWS 2017 Europe — Proceedings of the Fourth Annual DFRWS Europe: Characterizing loss of digital evidence due to abstraction layers, In DFRWS 2017 Europe, Digital Investigation March 2017 20 Supplement:S107-S115 Elsevier Ltd, ISSN:1742-2876
11. Marjie T. Britz: Computer Forensics and Cyber Crime: An Introduction, 2013, ISBN: 0132677717
12. Mylonas,Alexios, Meletiadis,Vasilis, Mitrou,Lilian, Gritzalis, Dimitris Digital evidence in germany-smartphone, Smartphone sensor data as digital evidence, In Cybercrime in the Digital Economy, Computers & Security October 2013 38:51-75, Elsevier Ltd, ISSN: 0167-4048, DOI: 10.1016/j.cose.2013.03.007
13. Robinson, Gavin The European Commission's e-Evidence Proposal, European Data Protection Law Review (EDPL) , 2018, Vol. 4 Issue 3, p347-352, 6p; DOI: 10.21552/edpl/2018/3/13,
14. Casey, Eoghan; Barnum, Sean; Griffith, Ryan; Snyder, Jonathan; van Beek, Harm; Nelson, Alex.Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language, In Digital Investigation. September 2017 22:14-45 DOI: 10.1016/j.diin.2017.08.002,
15. Roscini, Marco Digital Evidence as a Means of Proof before the International Court of Justice, Journal of Conflict & Security Law , Winter2016, Vol. 21 Issue 3, p541-554, 14p; DOI: 10.1093/jcsl/krw016,
16. Dr. Catherine D. Marcum: Cyber Crime( 2013, Wolter Kluwer Law§ Business, ISBN: 1454820330)
17. Digital Forensics: Rewiew of Issues in Scientific Validation of Digital Evidence Arshad,Humaira, Jantan,AmanBin, Abiodun, Oludare Isaac, Journal of Information Processing Systems; Apr2018, Vol. 14 Issue 2, p346-376, 31p, ISSN: 1976913X
18. Surveillance as a response to crime in cyberspace, Palfrey, Terry. Information & Communications Technology Law; Abingdon Köt. 9, Kiad. 3, (Oct 2000): 173-193.
19. Pradillo, Juan Carlos Ortiz:Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain, European Journal of Crime, Criminal Law & Criminal Justice , 2011, Vol. 19 Issue 4, p363-395, 33p; DOI: 10.1163/157181711X587800,
20. Robert E. Taylor, Eric J. Fritsch, John Liederbach, Michael R. Saylor, William L. Tafoya: Cyber Crime and Cyber Terrorism (4th Edition) (2018, What's New in Criminal Justice, ISBN:0134846516)
21. Anonymus: Deep Web-Die Dunkle Seite des Internets (2014, Aufbau Digital, ISBN: 3351050100)

22. Mackie, Judith; Taramonli, Chrysanthi; Bird, Robert.Digital Forensics and the GDPR: Examining Corporate Readiness, Konferencia, Proceedings of the European Conference on Cyber Warfare & Security. 2017, p683-691. 9p. 5 Graphs. , International Security & Counter Terrorism Reference Center
23. Palmer, Danny: Hospitals across the UK hit by WannaCrypt ransomware cyberattack, systems knocked offline (2017.) Forrás: https://www.zdnet.com/article/hospitals-across-england-hit-by-cyber-attack-systems-knocked-offline
24. Paul, Ruma: Exclusive: Some Bangladesh Bank officials involved in heist – investigator (2016) Forrás: https://www.reuters.com/article/us-cyber-heist-bangladesh-exclusive/exclusive-some-bangladesh-bank-officials-involved-in-heist-investigator-idUSKBN1411ST?utm_campaign=trueAnthem:+Trending+Content&utm_content=584f82a904d30107e6eeb727&utm_medium=trueAnthem&utm_source=twitter
25. CISAR, P.; CISAR, S. MARAVIC; BOSNJAK, S.:Cybercrime and Digital Forensics-Technologies and Approaches, DAAAM International Scientific Book , 2014, p525-542, 18p. Publisher: DAAAM International.,
26. Janine Kremling, Amanda M. Sharp Parker: Cyber space, Cyber Security, and Cyber Crime (SAGE Publications, 2017, ISBN: 1506347258)
27. Eddy Willems: Cybergefahr : Wie Wir Uns Gegen Cyber-Crime Und Online-Terror Wehren Können 2015, Springer Vieweg, ISBN10 3658047607
28. Andrew Staniforth ,Police National Legal Database , Professor Babak Akhgar , Francesca Bosco: Blackstone's Handbook of Cyber Crime Investigation 26 May 2017
29. Publisher Oxford University Press,
30. Todd G. Shipley, Art Bowker: Investigating Internet Crimes : An Introduction to Solving Crimes in Cyberspace Syngress Media,U.S. 03 Dec 2013, ISBN10 0124078176
31. Dr. Richard H. Ward , Dr. James W. Osterburg: Criminal Investigation : A Method for Reconstructing the Past 29 Apr 2013, Anderson Publishing, Publication City/Country Cincinnati, United State, 7th New edition, ISBN:1455731382,
32. Brett Shavers: Placing the Suspect Behind the Keyboard : Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, 02 Apr. 2013, Syngress Media U.S., ISBN: 1597499854
33. Jason T. Luttgens , Matthew Pepe , Kevin Mandia: Incident Response & Computer Forensics, Third Edition, 01 Sep 2014, MCGRAW-HILL, NY, Professional, ISBN:0071798684,
34. John Sammons: The Basics of Digital Forensics : The Primer for Getting Started in Digital Forensics, 29 Dec 2014 Syngress Media, U.S Rockland MA, 2nd Edition, ISBN: 0128016353,
35. Jason Andress: The Basics of Information Security : Understanding the Fundamentals of InfoSec in Theory and Practice, 2.nd Edition, Syngress Media U.S. ISBN: 01280074443
36. Mark Raskino ,Graham Waller: Digital to the Core : Remastering Leadership for Your Industry, Your Enterprise, and Yourself, 12 Nov 2015 Taylor n Francis Inc., Brookline, ISBN: 1629560731,
37. Matthew Richardson : Cyber Crime : Law and Practice, 28 Mar 2014, Wildy, Simmonds and Hill Publishing, London, UK, ISBN: 0854901361
38. Dr Tim Mishago: Cyber Crime and Regulatory Challenges : What Digital Investors in the Global Market Place Need to Know, 01 Jul 2014, Createspace Independent Publishing Platform, ISBN: 1499230281,

39. M. N. Sirohi: Transformational Dimensions of Cyber Crime, 13 May 2015, Alpha Editions, India ISBN: 8193142233,
40. Marc Goodman: Future Crime: Inside the Digital Underground and the Battle for Our Connected World, 12 Jan 2016, Anchor Books, ISBN: 0804171459
41. Thomas K. Clancy: Cyber Crime and Digital Evidence: Materials and Cases (2011, LexisNexis, ISBN: 978-1422494080)
42. Peter Sommer: Digital Evidence Handbook (2017, VCA, London)
43. Amy Kortuem: Computer Evidence (Crime Solvers)( 2018, Capstone PR, ISBN: 1543529941)
44. Edward J. Appel: Internet Searches for Vetting, Investigations, and Open-Source Intelligence (2017, CRC Press, ISBN: 1138112232)
45. Hinrich de Vries: Einführung in die Kriminalistik für die Strafrechtspraxis (2015, Kohlhammer W., GmbH, ISBN: 3170288105)
46. Buzarovska - Lazetik, Gordana, és Olga Kosevaliska. „Digital Evidence in Criminal Procedures - A comparative approach". Balkan Social Science Review 2, sz. 1 (2013): 66–83.
47. Casey, Eoghan. Digital Evidence and Computer Crime. Burlington: Elsevier, 2004. http://public.eblib.com/choice/publicfullrecord.aspx?p=288741.
48. Barry A.J. Fisher- William J. Tilstone- C. Woytowicz: Introduction to Criminalistics- The Foundation of Forensic Science (Elsevier Academic Press, 2009)
49. Brett Shavers: Cybercrime Investigation Case Studies- An Excerpt from Placing The Suspect Behind the Keyboard (Elsevier, Syngress, USA 2012)
50. Stein Schjolberg: The history of cybercrime 1976-2014, Cybercrime Research Institute GmBH 2014)
51. Susanne Beck, Wolfgang Freter, Bernd-Dieter Meier-Axel Metzger-Carsten Momsen..: Cybercrime und Cyberinvestigations (Nomos, 2015 ISBN: 3848724537)
52. Susan W. BRENNER: Cybercrime: Criminal Threats from Cyberspace (Crime, Media, and Popular Culture) 1st Edition, 2010.
53. Marije T. BRITZ: Computer Forensics and Cyber Crime, Third Edition, Pearson 2013
54. Arkansas Code of 1987, A.C.A §5-27-606 Jurisdiction, Pub. L. No. A.C.A §5-27-606, 1. Elérés 2018. május 10. http://lexisnexis.com/hottopics/arcode/Default.asp,.
55. Barry A.J. Fisher- William J. Tilstone- C. Woytowicz: Introduction to Criminalistics- The Foundation of Forensic Science (Elsevier Academic Press, 2009)
56. Andrea Giménez-Salinas Framis, José Luis González Álvarez: Investigación criminal- Principios, técnicas y aplicaciónes (Madrid, LID Editorial, 2016)
57. Oerlemans, Jan-Jaap Title: Investigating cybercrime (Lay-out: AlphaZet prepress, Waddinxveen Printwerk: Amsterdam University Press, 2017
58. Eneli Laurits: Criminal procedure and digital evidence in Estonia (forrás: journals.sas.ac.uk/deeslr/article/download/2301/2254)
59. Stephen Herzog: Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity (Georgtown Journal Of International Affairs 2017, Volume XVIII)
60. Russinovich, Mark E. Zero day. First edition. New York: Thomas Dunne Books, 2011.
61. Laviero Buono: Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (Ec3) (Sage Journals, 2012
62. Cath Senker: Cybercrime and the Darknet. Arcturus Publishing Ltd. 2017.

63. United Nations Manual on the Prevention and Control of Computer Related Crime. International review of criminal policy. No. 43-44, 1994.
64. Thomas J. Holt, Adam M. Bossler, K. C. Seigfried-Spellar: Cybercrime and Digital Forensic (Routledge, New York 2015)
65. Rebecca Herold: The Privacy Papers- Managing, Technology, Consumer, Employee and Legislative Actions (CRC Company 2002
66. Lu, Yong & Luo, Robert & Polgar, Michael & Cao, Yuanyuan. (Social network analysis of a criminal hacker community. Journal of Computer Information Systems, 2010)
67. Marian Quigley: Encyclopedia of Information Ethics and Security (Information Science Reference, New York, 2008
68. Seymour Bosworth, M.E. Kabay, Eric Whyne: Computer Security Handbook ( 2009, John Wiley n Sons, Inc.)
69. Audrey Guinchard: The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime (Journal of Information Rights, Policy and Practice, 2017)

**Internetes oldalak:**

1. Recommendation X.1205 (04/08), Pub. L. No. X.1205 (é. n.). https://www.itu.int/rec/T-REC-X.1205-200804-I.
2. *How to Make a Paper Bitcoin Wallet*, 208i. sz. https://www.coindesk.com/information/paper-wallet-tutorial/.
3. „A tiltott adatszerzés bűncselekmény - A Kúria is osztja a Legfőbb Ügyészség jogi álláspontját”. http://www.jogiforum.hu/hirek/37906, 2017. július 10. http://www.jogiforum.hu/hirek/37906.
4. „Periféria”. https://pcforum.hu/szotar/perif%C3%A9ria. Elérés 2018. július 30. https://pcforum.hu/szotar/perif%C3%A9ria.
5. OLAF. „Guidelines on Digital Forensic Procedures for OLAF Staff”, 2016. február 15. https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf.
6. How to Make a Paper Bitcoin Wallet, 208i. sz., https://www.coindesk.com/information/paper-wallet-tutorial/.
7. Bányászat - az első lépések”. https://bitcoin.hu/archivum/bevezeto/banyaszat-az-elso-10-lepes/. Elérés 2017. december 5. https://bitcoin.hu/archivum/bevezeto/banyaszat-az-elso-10-lepes/.
8. Bitcoins.hu az első magyar bitcoin portál”. http://bitcoins.hu/. Elérés 2017. december 6. http://bitcoins.hu/.
9. „Tiltott adatszerzés bűncselekmény - A Legfőbb Ügyészség által tett intézkedésekről”. http://www.jogiforum.hu/hirek/37269, 2017. február 17. http://www.jogiforum.hu/hirek/37269.

**A témában írt saját publikációk jegyzéke:**

1. Gyaraki Réka: A nyomozó hatóság és a katasztrófavédelem feladata a kiberbűncselekmények vonatkozásában (SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 15:(4) pp. 113-127.
2. Gyaraki Réka: Jogi szabályozás a nemzeti elektronikus adatvagyon, az azt kezelő információs rendszerek, létfontosságú információs rendszerek és rendszerelemek

biztonságáról (*SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA* 15:(3) pp. 140-154. )

3. Gyaraki Réka: Az ördög pénze? A Bitcoin (DETEKTOR PLUSZ 23: pp. 1-3. )
4. Gyaraki Réka: Money of devil? (In: Radu I Motica, Lucian Bercea, Viorel Pasca (szerk.)
5. Studii și Cercetări Juridice Europene = European Legal Studies and Research: Conferința Internațională a Doctoranzilor în Drept = International Conference of PhD Students in Law. 619 p.
   Konferencia helye, ideje: Bukarest, Románia, 2016.11.25-2016.11.26.
   Temesvár: Universitatea de Vest din Timisoara, Facultatea de Drept, 2016. pp. 173-178.
   (Facultatea de drept Univ. de vest din Timisoara = Faculty of Law West Univ. Timisoara)
6. Gyaraki Réka, Rottler Violetta: Drónok kora- személy-és vagyonbiztonság a XXI. században In: Bányász Péter, Kiss Dávid, Orbók Ákos (szerk.), A tudomány kapujában: Poszter kiadvány. 108 p.
   Konferencia helye, ideje: Budapest, Magyarország, 2015.10.28 Budapest: Magyar Hadtudományi Társaság, 2016. pp. 76-77.
   (ISBN:978-963-12-4965-1)
7. Gyaraki Réka: Az informatikai bűnözés a hazai jogi szabályozás aspektusából (In: Ács Kamilla, Bencze Noémi, Bódog Ferenc, Haffner Tamás, Hegyi Dávid, Horváth Orsolya Melinda, Hüber Gabriella Margit, Kovács Áron, Kis Kelemen Bence, Lajkó Adrienn, Schilli Gabriella Krisztina, Szendi Anna, Szilágyi Tamás Gábor, Varga Zoltán (szerk.), Book of Abstracts = Absztraktkötet: V. Interdiszciplináris Doktorandusz Konferencia. 191p. Konferencia helye, ideje: Pécs, Magyarország, 2016.05.27-2016.05.29. (Pécsi Tudományegyetem Doktorandusz Önkormányzat) Pécs: Pécsi Tudományegyetem Doktorandusz Önkormányzat, 2016. p. 43.
   (ISBN:978-963-429-038-4)
8. dr Gyaraki Réka: The legal regulation of rendering electronic data inaccessible( DE IURISPRUDENTIA ET IURE PUBLICO: JOG- ÉS POLITIKATUDOMÁNYI FOLYÓIRAT 10:(1) Paper 03. 7 p. (2016)
9. Gyaraki Réka: A drónok használatának hazai szabályozása( MAGYAR RENDÉSZET 2016:(1) pp. 43-54. (2016)
10. Gyaraki Réka: Cyber attacks against financial institutions( KRITISCHE ZEITEN: ZEITSCHRIFT FUR HUMANWISSENSCHAFTEN 7:(3-4) pp. 134-140. (2016)
11. Gyaraki Réka: Az elektronikus adat hozzáférhetetlenné tételének jogi szabályozása( TÁRSADALOM ÉS HONVÉDELEM 19:(2) pp. 57-64. (2015)
12. Gyaraki Réka: Számítógépes bűncselekmények és az ellenük való védekezés( In: Christián László (szerk.)Információvédelem. 262 p.
    Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2015. pp. 175-189.
    (ISBN:978-615-5527-24-1)
13. Gyaraki Réka: Számítástechnikai környezetben elkövetett gazdasági bűncselekmények( In: Erik Stenpien, Miskolczi Bodnár Péter (szerk.)X. Jogász Doktoranduszok Országos Szakmai Találkozója. Konferencia helye, ideje: Budapest, Magyarország, 2015.05.16 Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2015. pp. 42-52.(Jog és Állam; 20.)
14. Gyaraki Réka: Az elektronikus adat hozzáférhetetlenné tételének jogi szabályozása( In: Kiss Dávid, Orbók Ákos (szerk.),A haza szolgálatában 2014 konferencia rezümékötet. 170 p. Konferencia helye, ideje: Budapest, Magyarország, 2014.10.31

Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 48-50.
(ISBN:978-615-5491--88-7)

15. Gyaraki Réka: Az informatikai biztonság szükségessége( In: Kiss Dávid, Orbók Ákos (szerk.) A haza szolgálatában 2014 konferencia rezümékötet. 170 p.
Konferencia helye, ideje: Budapest, Magyarország, 2014.10.31 Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 156-158.
(ISBN:978-615-5491--88-7)
16. Gyaraki Réka: Gyermekek biztonsága a kibertérben: Önkormányzati rendészeti kutatás a Nemzeti Közszolgálati Egyetem Rendészetelméleti Kutatóműhely szervezésében, A kiberbiztonság aktuális kérdései, 2014. november 12. 23 p.(2014))
17. Gyaraki Réka: A probléma megoldva?!(TÁRSADALOM ÉS HONVÉDELEM 17:(3-4) pp. 535-543. (2013)
18. Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények( In: Gaál Gyula, Hautzinger Zoltán (szerk.), Tanulmányok "A biztonság rendészettudományi dimenziói - változások és hatások" című tudományos konferenciáról. 524 p.
Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2012. pp. 235-249.(Pécsi Határőr Tudományos Közlemények; 13.)
19. Gyaraki Réka: A számítógépes bűnözés elleni harc az új büntetőtörvénykönyvvel( MAGYAR RENDÉSZET 12:(4) pp. 55-62. (2012))
20. Gyaraki Réka: Internetes csalás vagy SCAM( MAGYAR RENDÉSZET 12:(1) pp. 40-47. (2012))
21. Gyaraki Réka: A tiltott pornográf felvétellel visszaélés bűncselekménye( In: Ádám Antal (szerk.)PhD tanulmányok 11. 671 p.
Pécs: PTE ÁJK Doktori Iskola, 2012. pp. 339-360.)
22. Gyaraki Réka: Az on-line elkövetett szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye (INFOKOMMUNIKÁCIÓ ÉS JOG 6:(41) pp. 215-221. (2010))