PÉCSI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK
DOKTORI ISKOLÁJA

Gyaraki Réka Eszter

A SZÁMÍTÓGÉPES BŰNÖZÉS NYOMOZÁSÁNAK PROBLÉMÁI

PhD értekezés

Témavezető:

Dr. Nagy Zoltán András

Habilitált egyetemi docens

Tanszékvezető

Pécs, 2019

Tartalomjegyzék

1 BEVEZETÉS

1.1 A kutatási témaválasztás indoka

A témaválasztásomat elsősorban a gyakorlati életben, a Budapesti Rendőr-főkapitányságon eltöltött, aktív rendőri (vizsgálói és nyomozói) munka során szerzett gyakorlati tapasztalat befolyásolta. Ezen időszakban a bűnügyi területen tapasztalható szokások és rutinszerűen elvégzett eljárási cselekményeknél sokszor fájóan begyakorolt munkavégzést tapasztaltam. A számítógépes (vagy számítógépes környezetben elkövetett) bűncselekmények esetében érezhetővé vált, hogy az addigi rutint már az informatika világában elkövetett deliktumok bizonyításához szükséges bizonyítékok megszerzése és az eredetének hitelt érdemlő bemutatása, felhasználása már sokkal nagyobb kihívást jelent számunkra, ami a változékony és befolyásolható környezetnek (is) köszönhető.

Természetesen - hacsak kezdetleges eszközökkel és módszerekkel is- de a nyomozó hatóságok igyekeztek mindent megtenni annak érdekében, hogy legalább kapitányságonként 1-2 ember tudását gyarapítsák a különböző továbbképzéseken.

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, informatikai jellegű 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 –, mind jogalkotói, és mind jogalkalmazói szinten is.

[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: Kevin Haley, „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.

A kiberbűnözők által okozott károk már a 2016-ban megjelent Internet Organised Crime Threat Assessment (továbbiakban: IOCTA) szerint is 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 nyomozó hatóságok, az ügyészségek és további jogalkalmazók részéről.

Végső soron a témaválasztás esetében nyugodt szívvel lehetett a kutatást elkezdeni, hiszen az adott téma már rendelkezik elméleti háttérrel, kutatható és minden kétségét kizáróan aktuális és ebből következően lehetséges lett olyan új eredmények produkálása, amely a mindennapi gyakorlathoz képes új eredményeket szolgáltatni.

1.2 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 krimináltaktikai 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, hogy a Fővárosi Főügyészségen csoportvezető ügyész asszonnyal, dr. Losonczi-Molnár Melindával interjút készítsek, amelynek 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[2]. Ez a szám 2014-ben már a lakosság tekintetében 53,2% (személyi számítógéppel rendelkező lakosság) és 45,4% (laptoppal rendelkezők) a KSH adatai alapján[3].

Egy 2017-ben készült felmérés szerint a minden második személy legalább alapfokú informatikai ismerettel rendelkezik[4]. 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.

[2] Pusztai László: Számítógép és bűnözés In.: Gödöny József (szerk.): Kriminológiai és Kriminalisztikai Tanulmányok 26. (KJK, Budapest, 1989) 85.
[3] KSH adata (forrás: http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_oni006.html, letöltve: 2019. március 22.)
[4] forrás: http://www.parlament.hu/irom41/00208/00208.pdf

Kevés történeti rész kerül bemutatásra, mivel a jelenlegi problémákkal és gyakorlattal foglalkoztunk, ehhez a leíró módszert választottuk.

1.3 A kutatás célja

Ray Kurzweil 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."*[5]

Kurzweil fenti megállapítása, amely a mesterséges intelligenciával foglalkozó könyvében olvasható, az értekezés írása és a kutatások során sok helyen beigazolódott, annyiban, hogy nemcsak a kutatásokat, a kutatókat érinti ez a „beszűkülés", hanem a rendőrséget, azon jogalkotókat is, akik bár érzik a számítógépes bűnözés 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 tűztük ki, hogy megkeressük azokat a gyenge pontokat a számítógépes bűnözéssel összefüggő jogszabályok területén, amelyek a számítógépes bűnözés dinamikus fejlődése miatt gondot okozhat a hatóságoknak a nyomozások során. Ezért elsősorban a hazai jogszabályokat tekintettük 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 viszonylag friss és dinamikusan fejlődő bűncselekmény típusokról van szó, így a hipotézisek és tézisek tekintetében szükséges volt, ehhez a változékonyságához alkalmazkodó kérdéseket feltenni.

[5] Ray Kurzweil, *A szingularitás küszöbén: Amikor az emberiség meghaladja a biológiát* (Ad Astra Kiadó, 2013), 37.

Az értekezés során az alábbi pontok vizsgálatára került sor:

1. A számítógépes bűncselekmények esetében az új büntetőeljárásjogi törvényben bevezetett kényszerintézkedések hatékonyságának vizsgálata és javaslatok kidolgozása külföldi példák figyelembevételével.

2. A szakértő szerepének és a kirendelés szükségességének vizsgálata, a bizonyítékok összegyűjtése, illetve értékelése. Meddig terjedhet a nyomozó hatóság kompetenciája a számítógépes bűncselekmények nyomozása során a digitális bizonyítékok esetében?

3. Az egyes számítógépes bűncselekmények során más és más sarkalatos problémák merülnek fel, eltérő eljárási cselekmények válnak szükségessé az elkövető kézre kerítése, valamint a bűncselekmény bizonyítása érdekében.

4. A rendőrség számítógépes bűnözés nyomozásával kapcsolatos oktatásának, képzésének fontossága, amely első lépése lehet a bűncselekmény eredményes felderítésének.

A fent említett négy vizsgálati ponttal összefüggésben a következő kérdések megválaszolását tartottuk fontosnak:

- A számítógépes bűncselekmények esetében hogyan lehet biztosítani a kényszerintézkedések végrehajtása során az elektronikus bizonyítékok hitelességét?
- Mi történik azokkal az adatokkal, elektronikus információs rendszerben tárolt bizonyítékokkal, amelyek lefoglalásra kerülnek, de nem a bűncselekmény elkövetésének tárgya, milyen eljárási cselekményt lenne szükséges olyan esetben foganatosítani és mi a jelenlegi gyakorlat?
- Az új, 2018. július 1-jén hatályba lépő büntetőeljárásról szóló törvény rendelkezik arról, hogy mi a teendő az elektronikus adatok lefoglalásakor, ugyanakkor be kell látni, hogy a jogszabályok merevsége miatt esetlegesen akár bizonyítékként felhasználható adatok semmisülhetnek meg vagy a kényszerintézkedésre vonatkozó szabályok szó szerinti betartása miatt sérülnek az azt elszenvedő jogai. Az elektronikus bizonyítékokkal kapcsolatos nemzetközi (európai uniós tagállamok és az Egyesült Államok egyes országaiban, valamint a főbb bűnüldöző szervek szabályozási hátterével összefüggő) szabályozásának vizsgálata és a hazai megvalósulásának összevetése által lehet-e egy következtetést levonni azzal

kapcsolatban, hogy lehetséges egy sémát, egy módszertant megalkotni, vagy bűncselekmény típusonként több szabályozást kell felállítani?

Az elektronikus bizonyítékok rendszerével összefüggésben kitérünk a digitális kutatásra, mint a bizonyítékok összegyűjtésének lehetőségére, annak alkotmányossági és büntetőeljárásjogi szempontból aggályos pontjaira és a fentebb írt kérdések miatt az egyes bűncselekményeket is vizsgáljuk nyomozási szempontból.

A kutatás során fontosnak tartottuk, hogy tisztában legyünk azzal, hogy az elektronikus bizonyítékok lefoglalásának tekintetében szükséges-e az bizonyítékokat tartalmazó eszköz lefoglalása és annak a helyszínről történő elszállítása. Elegendő lehet-e a helyszínen történő mentés és dokumentálás, illetve a hatóság jelenleg mi alapján dönt, hogy az egyes bűncselekmények esetén a lefoglalást csak az adattal szemben hajtják végre vagy az azt tartalmazó eszközt, rendszert is lefoglalják? A (ház)kutatás során az informatikai eszközök megtalálása és átvizsgálása tekintetében a nyomozó hatóság részéről szükséges átvizsgálása, a rendszerhez történő hozzáféréshez szükséges jelszavak megismerése, amennyiben az nem áll rendelkezésükre, illetve a (ház)kutatást elszenvedő fél nem tudja, vagy nem akarja azt a rendelkezésre bocsájtani, milyen lehetőségek vannak a hatóság kezében?

A kényszerintézkedések további vizsgálata során foglalkoztunk az adatok megőrzésre kötelezéssel, valamint az adatok hozzáférhetetlenné tételével -ideiglenes és végleges- továbbá az adatok gyors megőrzésre kötelezés jogszabályi hátterének és gyakorlati megvalósulásának értelmezésével és problémáival.

A nyomozás során igénybe vehető eszközök és módszerek tekintetében – mivel határon átnyúló bűnözésről és határok nélküli kibertérről beszélünk, - a nyomozások végrehajtása a nemzetközi együttműködés nélkül sokszor lehetetlen, ugyanakkor az országok különböző jogrendszere és eljárási cselekményei miatt nehézségekbe ütközik.

A bizonyítékok megszerzése tekintetében ugyanakkor nemcsak a kényszerintézkedések állnak a hatóság rendelkezésére, hanem más hatóságtól történő adatkérés, valamint a nyílt forrásból származó információgyűjtés (Open Source Intelligence- OSINT), amely sokszor tévesen van azonosítva a közösségi médiákon vagy közösségi oldalakon (Social Media) található önkéntesen megadott információk megismerésével és felhasználásával.

Szintén fontosnak tartottuk annak vizsgálatát, hogy a hatóság milyen esetekben, és a nyomozási eljárás melyik szakaszában vesz igénybe szakértőt, illetve szaktanácsadót. Ezért az utolsó fejezetben a szakértő igénybevételének lehetőségeit és szükségességét vizsgáljuk. A nyomozó hatóság tagjaival történő interjúkészítés során több esetben is arra hivatkoztak a szakértő igénybevételének szükségessége kérdésénél, hogy az állománynál hiányzik a szakértelem, esetleg nem is mernek adatot lementeni, vagy nem is tudják, hogy hogyan kell, illetve a nyomozást felügyelő ügyészség mindenképpen elvárja tőlük a szakértő kirendelését.

Vizsgáltuk azt, hogy nehezíti vagy megkönnyíti az eljárást, illetve az eljárás mely szakaszában lehet szükséges a szakértő kirendelése és az egyes bűncselekmények esetében mely kérdéseknél indokolt a bizonyításhoz a szakértő vagy szaktanácsadó igénybevétele.

A 2012. évi C. törvény a Büntető Törvénykönyvről (továbbiakban: Btk.) a (számítógépes)bűncselekmények elkövetési magatartásai, a bűncselekmény alanya, az elkövetés tárgya-, eszköze indokolttá teszi, hogy a büntetőeljárásban és a nyomozás és előkészítő eljárás részletes szabályairól szóló Kormányrendeletben általánosan meghatározott kényszerintézkedések és egyéb eljárási szabályok helyett konkrétabban fogalmazzon a jogalkotó.

1.4 Akció és reakció[6]

Ahhoz, hogy elfogadjuk azt az egyik gyakran hangoztatott megállapítást, hogy a XXI. század egyik legnagyobb kihívása közé tartozik a számítógépes bűnözés, meg kellett, hogy vizsgáljuk annak történetét, nemcsak a statisztikák fényében, az okozott károk és a sértettek számának növekedését vizsgáltuk, hanem a számítógépes bűncselekmények fejlődését is kiindulva a külföldi, jellemzően amerikai példákból.

A számítógépes bűnözés nem kontrollált bűncselekmény, minden nap és mindenhol megtörténik. Attól függően, hogy a világ melyik területét nézzük, csak becslések vannak azzal kapcsolatban, hogy ténylegesen mennyi számítógépes bűncselekmény is történik (látencia). Ez a szám 2017-ben csaknem 450 milliárd dollár körül volt, amelyek tényleg csak becslések, hiszen annak pontos kárértékét meghatározni azt gondoljuk lehetetlen. A hagyományos egyedül

[6] Az alfejezet Dr. Kiss Tibor PhD javaslata alapján került be a disszertációba.

a tavalyi évben, és ez csak várható. Ahhoz, hogy további nézőpontot kapjunk, az elmúlt évben ellopott rekordok száma is meglehetősen magas, több mint 2 milliárd, beleértve legalább 100 millió egészségbiztosítási állományt, többnyire USA-t. A legnagyobb probléma nem annyira az, hogy annyi bűncselekmény van az interneten, hogy a vállalatok sokáig rájönnek, hogy felfedjék, hogy megsértették őket, és kevéssé segítenek megakadályozni a terjedést. Amikor a hírek megsértéséről hall, hogy általában a hónap után van, túl késő ahhoz, hogy bármit is tegyen. Az alsó sor, a számítógépes bűnözés itt marad, és az egyetlen dolog, amit tehetünk, készüljön.

Az első, már számítógépes bűncselekménynek nevezhető jogellenes cselekmény az 1960-as éveket megelőzően történt, amikor még az akkori használatban lévő számítógépek tudása és mérete messze nem hasonlított a ma használatban lévő számítógépektől. Hamis lyukkártyával az Amerikai Egyesült Államokban sikkasztást követtek el egy bankban[7]. A következő, ismertebb bűncselekmény volt az 1971 -ben John Draper által elkövetett úgynevezett „telefonos csalás". Ő volt az első úgynevezett phone phreaker, aki már a bűncselekményét az akkori kor technikai fejlődésével követte el, hiszen rájött arra, hogy egy Cap'n Crunch reggeli müzli dobozaiban található, ajándék, egy síp ugyanazt a hangot adja ki, mint az akkori telefonkapcsolós számítógépek. Egy „kék dobozt" épített a sípra, amely lehetővé tette számára, hogy ingyenes hosszú távú telefonhívásokat kezdeményezzen, majd kiadta a használati utasítást. A telefonvonalas csalások esetei az 1970-es években jelentősen emelkedtek az Egyesült Államokban[8].

Még mindig az USA-ban történt számítógépes bűncselekménynek nevezhető esetben, egy elkövető az egyik new york-i bankban egy számológép segítségével, amelyet számítógépként használt, több mint 2 millió dollárt sikerült „ellopni" (1973-ban történt az eset).

A következő eset 1978 -ban történt, amikor is megjelentek az első online elektronikus hirdetőtábla-rendszerek, ami előnyben részesített kommunikációs módszer lett a számítógépes világ számára. Ez lehetővé tette a gyors, ingyenes információcserét, beleértve a számítógépes hálózatokba való hekkelésre vonatkozó tippeket és trükköket.[9]

[7] Dr. Pergel Józsefné: A számítógépes csalás és egyéb számítógépes bűncselekmények (Statisztikai Szemle, 79. évfolyam, 2001, 9. szám) 763.
[8] Karl de Leeuw, Jan Bergstra: The history of Information Security- A Comprehensive Handbook (Elsevier, 2007)
[9] forrás: Pandasecurity.com

Mivel eljutottunk a hekkeléshez, így Kevin D. Mitnick könyveiben is megjelent Ian Murphy, aki Zap kapitánynak is neveztek 198-ben az első személy volt, akit számítógépes bűnözés miatt elítéltek az USA-ban. Behatolt egy AT&T hálózatba, és megváltoztatta a belső órát, így más tarifával jutott az órákon kívüli díjak feltöltéséhez csúcsidőben.

Nem kellett már túl sokat várni arra, hogy megszülessen 1982-ben az Elk Cloner, ami egy vírus. Ez az egyik első olyan ismert vírus, amely elhagyta az eredeti operációs rendszert, és elterjedt a „világhálón", megtámadta az Apple II operációs rendszereket és floppy lemezen terjedt el.

A fentiek hatásásra 1986 -ban az Egyesült Államok kongresszusa elfogadta a *Computer Fraud and Abuse Act*-et, vagyis a számítógépes csalás és visszaélések törvényét, így a hekkelés és a lopás jogellenessé, büntetendővé válik.

A törvény elfogadása ellenére 1988-ban Robert T. Morris jr., A Cornell-i végzős hallgató önálló replikáló férget bocsátott ki a Védelmi Minisztérium APRANET-jére, ám a féreg kicsúszott az irányításából és, több mint 600 000 hálózatba kapcsolt számítógépet fertőzött meg. Morris egy 10 000 dolláros büntetést kapott és 3 éves próbaidőre bocsátották

1989–ben az első nagyszabású ransomware esettanulmányról számoltak be. A vírus az AIDS-vírus kvízjévé vált, és letöltés után 500 dollárnyi számítógépes adatot tárolt. Ugyanakkor az USA-ban egy másik csoportot is letartóztattak, amely ellopta az amerikai kormányzati és a magánszektor adatait, és eladta azt az orosz KGB-nek.

Említést érdemel még az 1990 -es a „Doom légió" és a „Megtévesztés Mesterei", akik két cyber alapú banda volt és online háborút folytattak. Aktívan blokkolták egymás kapcsolatait, hatoltak be a számítógépekbe és lopták az adatokat. Ez a két csoport nagyszámú telefonbeszélgetés volt, amely számos telefonról híres volt a nagyszámítógépes infrastruktúrában.

1993-ben történt Kevin Poulson elfogása és elítélése a telefonrendszerekbe való behatolása miatt. Az LA rádióállomásra érkező összes telefonvonal fölötti ellenőrzést átvette azért, hogy garantálja a telefonos verseny nyerését. Öt évre ítélték el a szövetségi büntetés-végrehajtási intézetben, és az első, aki az internethasználat tilalmát tartalmazza a büntetésében[10].

1995-től már makro-vírusok jelentek meg. A makróvírusok az alkalmazásokba ágyazott számítógépes nyelveken írt vírusok. Ezek a makrók futnak az alkalmazás megnyitásakor, mint

[10] Seymour Bosworth, M.E. Kabay, Eric Whyne: Computer Security Handbook (2009, John Wiley n Sons, Inc.)

például szövegszerkesztő vagy táblázatkezelő dokumentumok, és a hekkerek számára ez egyszerű módja a rosszindulatú programok „szállítására”.

Az, hogy a XX. században történt számítógépes- pontosabban, online elkövetett számítógépes bűncselekmény egyre súlyosbodó helyzeteket teremt, egyik jól dokumentált esete, amikor 1996 -ban a CIA akkori igazgatója, John Deutsch arról tanúskodik a kongresszusnak, hogy a külföldi szervezett bűnözési csoportok aktívan próbálják megragadni az amerikai kormányzati és vállalati hálózatok feletti hatalmat. Az US GAO (US Government Accountability Office) bejelentette, hogy a fájljaikat a hackerek legalább 650 000-szer támadták meg, és legalább 60% -uk sikeres volt.

1997 - Az FBI arról számol be, hogy az amerikai vállalatok több mint 85% -át hekkelték, és a legtöbb nem is tudja. A Chaos Computer Club meghekkelte a Quicken szoftvert, és pénzátutalásokat hajtott végre anélkül, hogy a bank vagy a számlatulajdonos tudott volna róla[11].

Megjelent a Melissa vírus 1999-ben. Ez a mai napig a legvirulensebb számítógépes fertőzés, és a kártékony programokat író személyek első bűncselekménye. A Melissa vírus is makro-vírus volt, azzal a szándékkal, hogy átvegye az e-mail fiókok feletti felügyeletet és tömeges e-maileket küldjön a felhasználóknak. A vírusírót a feltételezések szerint, több mint 80 millió dolláros kárt okozott a számítógépes hálózatoknak.

Tovább kutatva a számítógépes bűnözés fejlődését, megállapíthattuk, hogy a XXI. századra az online támadások száma és típusai exponenciálisan nőnek. Az internet terjedése, felhasználása és népszerűsége újabb és újabb azzal összefüggő bűncselekményeket hozott magával. A szerzői művek interneten keresztül történő hozzáférése többek között olyan számítógépes bűncselekmények elkövetését indukálta, mint az ügyfelek hitelkártya-információinak online közzétételét, aminek hatására több millió dolláros károk keletkeznek.

A Denial of Service (DDoS) támadások számos alkalommal indultak például az AOL, Yahoo! Ebay ellen[12]. A hamis hírek az Emulex részvényeinek közel 50% -os összeomlását okozzák. Az I Love You vírus terjed az interneten. Clinton elnök azt mondta, hogy nem használja az e-mailt a lányával való beszélgetéshez, mert a technológia nem biztonságos.

[11] Thomas J. Holt, Adam M. Bossler, K. C. Seigfried-Spellar: Cybercrime and Digital Forensic (Routledge, New York 2015)
[12] Rebecca Herold: The Privacy Papers- Managing, Technology, Consumer, Employee and Legislative Actions (CRC Company 2002)

2002 -ben a Shadow Crew honlapja elindult. A honlap üzenőfal és fórum volt a fekete kalapos hekkerek számára. A tagok közzéteszhették, megoszthatták és megtanulhatták, hogyan kövessenek el számtalan számítógépes bűncselekményt, és elkerüljék azoknak a rögzítést. Az oldal 2 évig tartott, mielőtt a titkosszolgálat leállította volna. 28 embert letartóztattak az Egyesült Államokban és 6 másik országban[13].

Az „SQL Slammer" a történelem leggyorsabban terjedő féregévé válik 2003 januárban. Megfertőzte az SQL-kiszolgálókat, és olyan szolgáltatási támadást hozott létre, amely már régóta befolyásolta a sebességet az interneten. A fertőzési sebesség tekintetében a szinte 75 000 gépen 10 perc alatt terjedt el[14].

2007 – re a hekkelés, az adatok lopása és a rosszindulatú programok fertőzéseinek száma egyre csak nőtt. Az ellopott rekordok száma, a vírussal megfertőzött gépek száma világszinten milliókra emelkedett és dollárban számítva milliárdokra az okozott károk összege. Abban az évben történt az első kiberháborúként emlegetett orosz-észt kiberháború, amikor is Észtországot kibertámadás ért 2007. április 27-én.Ez egy olyan túlterheléses támadás volt, amelynek indítéka politikai jellegű volt és amely rámutatott a kibertámadások egy másfajta veszélyére[15]. Innentől kezdve talán a világ egyre többször felfigyelt a komolyabb és súlyosabb támadásokra, így a 2010-ben a Stuxnet vírusra, amely az iráni atomdúsító ellen történt, vagy a 2017-es vírustámadások, amelyek földrajzi elhelyezkedésre tekintet nélkül több kritikus infrastruktúra informatikai rendszereit, államok kormányait és magánhasználatban lévő informatikai eszközeit és - rendszereit is érintette.

A kibertámadások száma pedig azóta is rohamosan nő. A támadással érintett területek- mind földrajzi mind gazdasági téren változó.

[13] Lu, Yong & Luo, Robert & Polgar, Michael & Cao, Yuanyuan. (Social network analysis of a criminal hacker community. Journal of Computer Information Systems, 2010) 51. 31-41
[14] Marian Quigley: Encyclopedia of Information Ethics and Security (Information Science Reference, New York, 2008
[15] Orbók Ákos: A kibertér, mint hadszíntér (forrás: http://biztonsagpolitika.hu/publikaciok-2013/orbok-akos-a-kiberter-mint-hadszinter-2013-julius-19, letöltve: 2019. április 01.)

Amennyiben újra és újra végignézzük a fent felsorolt eseteket, megállapíthatjuk, hogy a számítógépes bűncselekmények több fejlődési szakaszon mentek keresztül, amelynek során nemcsak az elkövetők motivációja, hanem az elkövetők száma, az elkövetés módszere és az elkövetők célpontja is megváltozott:

I. Kezdetben az elkövető haszonszerzésre törekedett. Kihasználva az akkori kor friss találmányát, a számítógépet és a saját leleményességüket, kreativitásukat, amivel már kisebb-nagyobb összeghez tudtak jutni. Feltételezhetőleg a bűncselekményének elkövetési célpontja nem eshetőleges volt, hanem célzottan, meghatározott pénzintézet ellen követték el a deliktumot. Az 1960-70-es években álláspontunk szerint inkább kezdetleges szakasza volt ez a számítógépes bűncselekmények szempontjából.Érdekesség, hogy Svédországban 1973. április 2.-án elfogadták a Data Protection Act-et, amely a számítógépes bűncselekmények elleni fellépés egyik állomása volt[16].

II. Az 1980-as években az okozott károk mértéke nőtt, a bűncselekmény módszere finomult. Az elkövetők már jártasabbak voltak az informatika világában, akár tanulmányaik, akár önképzésük révén. Még mindig az anyagi haszonszerzés volt a fő cél. Az adatok megszerzése leginkább a pénzügyi visszaélések miatt történt. Ebben a korszakban mind az Egyesült Államok, mind pedig az OECD már jogi dokumentumban reagált az új típusú bűncselekményre. A második szakaszban többek között Németországban, Kanadában, Ausztriában, Japánban, Görögországban megalkották a számítógépes bűncselekményekkel, a számítógépes kémkedéssel kapcsolatos törvényeiket[17].

III. Az 1990-es években már megjelentek a kiemelt létesítmények, rendszerek ellen elkövetett támadások, de még a politikai célzat nem jelent meg annyira markánsan. Az ismertebb támadások inkább az USA-ban történtek. Már kifejezetten számítógépes bűncselekmények elleni fellépéssel összefüggő törvények születtek például az Egyesült Királyságban[18].

[16] Stein Schjolber: The History of Cybercrime 1976-2014 (Cybercrime Research Institute, 2014) 24.
[17] U.az.25-32.
[18] 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)

IV. 2000-ben a számítógépes bűncselekményeknél ténylegesen megfigyelhető, hogy az anyagi haszonszerzés mellett megjelentek a politikai indíttatású támadások. Újabb és újabb bűncselekmények jelentek meg, valamint a korábban már deliktumnak minősülő cselekményeket számítógép vagy információs rendszer felhasználásával követték el. Az informatikai környezet miatt a bűncselekmények sokkal jobban rejtve maradtak. Az elkövetett deliktumok száma folyamatosan nő egyenes arányban a kárértékkel. A haszonszerzés mellett sokkal inkább a felhasználók adatainak (amelynek feketepiaci értéke nagyobb, mint az aranynak) megszerzése a cél. Megjelentek többek között a kriptovaluták, a titkosított hálózatok.

Megjelent a kibertámadás, mint fogalom és ezzel párhuzamosan a kiberterrorizmus is, amely egyes vélemények szerint a 2001. szeptember 11.-ei terrortámadással vette kezdetét. Ebben a korszakban fogadták el és írták alá a Számítástechnikai Bűnözésről szóló Egyezményt és hazánkban is megszületett a Btk.-ban az első számítógépes bűncselekménnyel kapcsolatos tényállás, a 300/C.§ a számítástechnikai rendszer és adatok elleni bűncselekmény[19]. Megjelentek az államok kiberbiztonsági stratégiái, valamint a NATO 5. cikke, amely kimondja, hogy a kibertámadás fegyveres támadásnak minősül.

V. Jelenleg is tartó időszak, amikor már az információs rendszerbe történő behatolás mellett, az afölötti rendelkezés és befolyásolás jelenik meg.

A számítógépes bűncselekmény társadalomra veszélyességének bizonyosságát annak fejlődési szakaszai is jól mutatják. A kezdetleges ad hoc jellegű elkövetéseket felváltotta a sokkal tudatosabb elkövetés, amikor már nagyobb és nagyobb elkövetési érték a cél. Az elmúlt közel két évtizedben már nemcsak a pénz jelent meg, hanem az adatok megszerzése, az információs rendszerek, eszközök befolyásolása.

[19] A Büntető Törvénykönyvről szóló 1978. évi IV. törvény (hatálytalan)

1.5 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.

1. Minden bűncselekmény nyomozása az elkövetés helyének és idejének vizsgálatával kezdődik, amely kriminálmetodikailag az elsődleges feladat[20]. *A számítógépes bűncselekmények elkövetésének térben és időben történő meghatározása, a törvényben használt fogalmak, kifejezések pontosítása a további nyomozási és felderítési eljárás szabályozáshoz hozzájárul.*

2. 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"[21] 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.

3. 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.

[20] Kovács Gyula-Nagy József: Kriminálmetodika elméleti és gyakorlati kérdései (Nemzeti Közszolgálati és Tankönyvkiadó Zrt.,Budapest, 2013) 106.
[21] 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.

4. 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.

5. 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.

1.6 A tudományos célok

A disszertáció tudományos célja nemcsak az, hogy átfogó képet lehessen kapni a számítógépes bűncselekmények nyomozásának kriminalisztikai vetületéről, megoldásairól, hanem azokat a nehézségeket és büntetőeljárási hibákat és problémákat is a vizsgáljuk, amelyek álláspontunk szerint tovább gondolást, vagy a technika fejlődése miatt egy rugalmas jogszabályi keretet igényelne. Így mintegy objektív és használható képet lehet kapni a jó- és rossz gyakorlatról, és sikerülhet egy általánosan elfogadható szabályt alkotni az elektronikus bizonyítékok, mint tárgyi bizonyítási eszközökről és a megszerzésükkel kapcsolatos eljárásról.

1.7 Számítógépes bűncselekmények vagy kiberbűncselekmények?

A számítógépes bűncselekmények története[22] az 1950-es évekre nyúlik vissza, amikor is a számítógépet „bemutatták" a globális társadalomnak, de ekkor még használatuk csak szűkebb körben volt jellemző.

A számítógépek fejlődése, használatára való áttérés lett az indikátora annak, a „hagyományos" bűncselekmények újfajta elkövetési módszere, illetve újabb bűncselekménytípusok jelenjenek meg, ezáltal kiváltva sokszor az ember-ember közötti közvetlen kapcsolatot.

Tekintsük történetiségében a bűncselekmények tudományos elemzését. Az 1980-as években a szerzők nem egy egységes fogalom megalkotására helyezték a hangsúlyt, hanem a cselekményfajták felől közelítettek.

A német *Manfred Möhrenschlager*, az akkor elfogadott bűncselekmények mellé, tehát az adat vagy program manipuláció, a szabotázs és adatváltoztatás, a gépidő - lopás mellett megjelent a személyes adatokat veszélyeztető támadás is.[23]

A belga *Jean Spreutels* a számítógépes szabotázs, az adat vagy program kifürkészése, az adat és/vagy program manipuláció, a komputer jogosulatlan használata mellett a számítógépes hamisítás és a rendszerbe történő jogosulatlan behatolással bővíti az általa alkotott listát.[24]

A nemzetközi jogi dokumentumok is csupán a cselekménytípusok felsorolását tartalmazták, a fogalom meghatározás mellőzésével.

Az elsőként az *12 (81) sz. Európa Tanács Ajánlás a Gazdasági bűncselekményekről*, mint computer crime elnevezéssel foglaltak össze néhány bűncselekményt, igaz csupán példálódzva.

Az *OECD* 1983-85 között készült jelentés négy jogsértő cselekményt nevezett meg:

- számítógépes csalás,

- számítógépes hamisítás,

[22] Stein Schjolberg: The History of Cybercrime 1976-2014 (Cybercrime Research Institute GmBH 2014, ISBN: 9783734732942) 16.oldal
[23] vö. Revue ..... p. 321.
[24] vö. Revue ..... p(s). 164-172

- számítógépes szabotázs,

- szerzői jogi jogsértések.[25]

E körben fontos nemzetközi dokumentum a *9 (89) sz. Európa Tanács Ajánlása a „Számítógépes-környezetben elkövetett bűncselekményekről”*, amely címében átfogó elnevezést használ, tartalmi meghatározás nélük. Ez a dokumentum, nemcsak, hogy leír egy minimális és egy fakultatív listát, hanem a szankcionálni javasolt bűncselekményeket definiálja.

I. Az ET. minimális listája:

a. A számítógépes csalás.

b. A számítógépes hamisítás.

c. A számítógépes adatokban és programokban történő károkozás.

d. A számítógépes szabotázs.

e. A jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén.

f. A jogellenes titokszerzés.

g. Védett számítógépes programok jogellenes másolása.

h. A félvezető topográfiák jogellenes másolása.

II**.** Az ET. fakultatív listája:

a. A számítógépes adatok és/vagy programok megváltoztatása.

b. A számítógépes kémkedés.

c. A számítógép jogellenes használata.

[25] OECD Computer - Related Criminality: Analysis of Legal Police. Paris, 1986. (továbbiakban: OECD - Analysis) p. 28.

d. Védett programok jogellenes használata.[26]

Mind a mai napig a legátfogóbb nemzetközi jogi dokumentum a 2001. november 23-án, *Budapesten* aláírt, a *Számítástechnikai Bűnözésről szóló Európa Tanácsi Egyezmény*. Ismét az egyezmény címe utal a használni kívánt összefoglaló elnevezésre.

Az egyezmény az 1989-es ET Ajánlás óta eltelt egy évtizednyi technikai fejlődésre és az ezzel együtt megjelenő visszaélésekre utalva az alábbi bűncselekményeket sorolja.

I. Cím: A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények

2. cikk: A jogtalan belépés

3. cikk: A jogtalan kifürkészés

4. cikk: Az adatok sértetlensége elleni cselekmény

5. cikk: A rendszer sértetlensége elleni cselekmény

6. cikk: Visszaélés eszközökkel

II. Cím: A számítástechnikai bűncselekmények

7. cikk: A számítástechnikai hamisítás

8. cikk: A számítástechnikai csalás

III. Cím: A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények

9. cikk: A gyermekpornográfia.

[26] Council of Europe Legal Affairs: Computer - Related Crime. Recommendation No.R. (89) 9. Strasbourg, 1990. ISBN 92-871-1792-6
(továbbiakban: CE Recommendation (89) 9. p(s). 36-69..Revue Revue Internationale de Droit Penal 1993/1-2 p(s). 673-680. (francia nyelven) és p(s). 681-690. (angol nyelven), [továbbiakban: Revue..]
Dr. Nagy Zoltán: Konferencia az információtechnikai bűnözésről. MJ. 40. 1993. 2. 102-104.l.
Dr. Kertész Imre - Dr. Pusztai László: A komputerbűnözés és az információs technológiával kapcsolatos egyéb bűnözési fajták. ÜÉ. 29. 1993.4. 17-18.l.
Dr. Csonka Péter: Council of Europe Activities Related to Information Technology Information & Communications Technology Law, Vol.5. No.3, 1996. p(s).180-186.82.

10. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények. [27]

A fentiekből látható az akkor még jellemzően offline bűncselekmények sokrétűsége miatt az egységes fogalomalkotás bizonytalansága az 1980-as és 1990-es években.

Az angolszász irodalomból kiemeljük Cath Senker meghatározását, amely általánosnak nevezhető. A szerző számítógépes bűncselekménynek tart minden olyan cselekményt, amelyhez a számítógépet jogellenes céllal használtak. ideértve a csalást, személyazonosság-lopását, a szerzői jogsértéseket, gyermek pornográf képek terjesztését.[28]

1994-ben került kiadásra Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről[29] A ENSZ 8. kongresszusát követően, a Szervezet Közgyűlése elfogadta a 45/121. számú határozatát a számítógépes bűncselekményekkel kapcsolatos regulációról. A határozat szerint az ENSZ 1994-ben egy Kézikönyvet adott ki a számítógépes deliktumok (computer crime) megelőzéséről és azok kezeléséről, de nem adja meg pontosan a computer crime fogalmát, azonban meghatározza azokat a tulajdonságokat, melyekkel ezek a deliktumok rendelkeznek.

A Kézikönyv által meghatározott leggyakoribb típusú bűncselekmények:

- A számítógép manipulációjával elkövetett csalás (Compter Fraud or Computer Manipulation).

- A számítógépes hamisítás (Computer Forgery).

- Károkozás számítógépes adatokban vagy programokban, illetve a számítógépes adatok vagy programok megváltoztatása (Damage to or modifications of Computer Data or Programs).

- Jogosulatlan hozzáférés számítógépes rendszerekhez és szolgáltatásokhoz (Unauthorized Access to Computer Systems and Service).

- Jogi védelem alá eső számítógépes programok jogosulatlan reprodukálása (Unauthorized Reproductin of Legally Protected Computer Programs)

[27] European Treaty Series No. 185. Serie des européens no. 185 Kiadja az ET Információs és Dok. Központja. Budapest. 2001. Fordította: Dr. Villányi József (továbbiakban: 2001. Kiber-crime)
[28] Cath Senker: Cybercrime and the Darknet. Arcturus Publishing Ltd. 2017. p. 101.
[29] United Nations Manual on the Prevention and Control of Computer Related Crime. International review of criminal policy. No. 43-44, 1994. pp. 5-46.

A bűncselekmények összefoglaló elnevezésének bizonytalanságát az Európa Tanács 2004-es Jelentése (Octopus Programme) úgy próbálja feloldani, hogy kétféle cselekménytípust határoz meg, egyfelől a számítógépes bűncselekményt (computer crime, szinonimként a computer-related crime) azonosítja számítógépben tárolt (kezelt) adatok, ideértve programok elleni bűncselekményekkel, míg másfelől a kiberbűncselekményeknek a számítógépes hálózatokhoz kötött bűncselekményeket tekinti.[30]

Az Európai Parlament, a Tanács és a Régiók Bizottság Közleménye[31] – „A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé (COM (2007) 267" rámutatott arra, hogy nincs pontos meghatározása a „számítógépes bűnözésnek", a „számítástechnikai bűnözés" vagy „számítógéppel kapcsolatos bűnözés" fogalmaknak. A Közlemény immár nemcsak egy-egy bűncselekményt, hanem bűncselekménycsoportokat határoz meg:

1. Az elektronikus hálózatok felhasználásával, valamint az azokkal kapcsolatos bűnözés terjedésével összefüggésben egyre jobban terjed a csalás, az identitás-lopás, az adathalászat, a kéretlen levelek, a rosszindulatú kódok felhasználásával elkövetett csalás, amely a hagyományos bűncselekmények közül az illegális nemzetközi kereskedelem, kábítószer kereskedelem, fegyverkereskedelem, veszélyeztett fajok kereskedelmével van összefüggésben.

2. Az illegális tartalmú (pl.: a gyermekek szexuális kizsákmányolásával, terrorcselekményekkel, rasszizmussal és gyűlöletbeszéddel) kapcsolatos weboldalak az Unión belüli vagy az azon kívül eső államokba történő mozgatását, amely cselekmény jogellenességének megállapítása nélkül a nyomozó hatóságok felderítését a bűncselekmények vonatkozásában megnehezíti.

3. Az elektronikus hálózatokkal kapcsolatos bűncselekmények a botnet hálózatokon keresztüli kritikus infrastruktúrát veszélyeztető támadások egyik lehetősége. A Bizottság már 2007-ben utalt a zsarolóvírusokkal kapcsolatos veszélyekre, amelyek az elektronikus információ rendszerek nem megfelelő védelmének a révén valósulnak meg.

Az Európai Bizottság Közleménye gyakorlati tapasztalatokra alapozva a bűncselekmények három kategóriáját határozza meg:

[30] Organised Crime in Europe: the threat of cybercrime (Octopus Programme). COE Publishing, Strasbourg, 2005. p. 86.
[31] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:HTML

„*Az első kategóriába a bűncselekmények hagyományos formái tartoznak, úgymint csalás vagy hamisítás, a számítógépes bűnözéssel összefüggésben azonban mindenekelőtt az elektronikus kommunikációs hálózatokon és információs rendszereken (továbbiakban: elektronikus hálózatok) keresztül elkövetett bűncselekmények sorolandók ide.*

A második kategória az illegális tartalom elektronikus médián keresztüli közzétételére vonatkozik (többek között a gyermekek szexuális kizsákmányolásával kapcsolatos anyagok vagy faji gyűlölet keltése).

A harmadik kategóriába az elektronikus hálózatokkal kapcsolatos bűncselekmények tartoznak, úgymint az információs rendszerekkel szembeni támadások, a hozzáférés megtagadása és a hackertevékenység. Az ilyen típusú támadások a döntő jelentőségű európai létfontosságú infrastruktúrák ellen is irányulhatnak, és számos területen kihathatnak a fennálló sürgősségi riasztórendszerekre, ami az egész társadalomra nézve végzetes következményekkel járhat.

Mindhárom bűncselekmény-kategória közös jellemzője, hogy az elkövetés terjedelme, valamint az adott bűncselekmény és hatásai közötti földrajzi távolság igen jelentős lehet. Következésképpen az alkalmazott nyomozási módszerek technikai szempontjai gyakran ugyanazok."[32]

Ugyanakkor egy az Európai Parlamentnek, Tanácsnak, a Régiók Bizottságának dokumentuma, „*A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé meghatározása* (*Towards a general policy ont he fight against cyber crime*)" szintén három jellemzőjét vonja[33]:

- Olyan hagyományos bűncselekmények, amelyek elkövetése során azonban az internetet használják (például csalás vagy hamisítás). Ezek közé tartozik például a személyiséglopás vagy az ehhez is köthető adathalászat (amelynek során az internetes bűnözők hamis banki honlapot hoznak létre, hogy az ügyfeleket becsapva rávegyék őket jelszavuk vagy adataik megadására és ezáltal ellopják a pénzüket). Az internet a kábítószerek, fegyverek és a veszélyeztetett fajok nemzetközi kereskedelmét is átalakította.

[32] Európai Bizottság.:„A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának - A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé", Közlemény, 2007. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52007DC0267 . Letöltve.2018. október 20.
[33] Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52007DC0267&from=EN, letöltve: 2019.február 15.

- Illegális tartalmak közzététele, például terrorizmusra, erőszakra, rasszizmusra, idegengyűlöletre vagy gyermekek szexuális zaklatására ösztönző anyagoké.

- Az elektronikus hálózatokra korlátozódó bűncselekmények, újszerű, gyakran kiterjedt és nagyszabású bűncselekmények, amelyek az internet előtti időszakban nem voltak ismertek. Az ilyen típusú bűncselekmények informatikai rendszerek elleni támadásokat, esetenként az állam kritikus fontosságú informatikai infrastruktúrái, és így közvetlenül az állampolgárok elleni fenyegetéseket jelentenek. Ezek a támadások történhetnek „botneteken" (az angol „robot networks", azaz robothálózatok szó rövidítése) keresztül, ahol a bűnözők „malware"-t, (rosszindulatú számítógépes programokat) terjesztenek, amelyek a letöltést követően a felhasználó számítógépét is „zombigéppé" változtatják). Az így megfertőzött számítógépekből álló hálózatot használják aztán bűncselekmények elkövetésére a felhasználók tudta nélkül.

A nemzetközi jogirodalomban és a nemzetközi dokumentumokban olvasható meghatározások után tekintsük át a hazai próbálkozásokat. Döntően az angolszász computer crime kifejezés terjedt el, ahogy a német nyelvterületen is a Computer Kriminalitat terminológiát alkalmazták, ehhez igazodtak a hazai szerzők is a sokszor a tanulmányukban is. Hazánkban *Polt Péter* „úttörőként" írt először a számítógépes bűncselekményekről, és abban foglalt állást, hogy a számítógép egyszerre lehet a bűncselekmény tárgya és eszköze.[34]

Ahogy *Pusztai László,*[35] úgy *Nagy Zoltán*[36] is a számítógépes bűncselekmények négy fő alaptípusa között tett – korábban - különbséget: a számítógépes visszaélést, az adatkikémlelést, a szabotázst és a gépidőlopást. Tegyük hozzá, hogy e tanulmányok sem határoztak meg összefoglaló definíciót e tárgykörben.

Az 1990-es évektől az internet használatának megjelenésétől, majd folyamatos elterjedésével a bűncselekmények és a nem kriminalizált visszaélések köre mind mennyiségében, mind minőségében bővült. Aztán egy évtized múlva a bűncselekmények köre tovább bővült, mivel a technológia lehetővé tette és teszi ma is, hogy a felhasználók ne csak fogyasztói legyenek az Interneten közölt tartalmaknak, hanem azok előállítására is képesek lettek. Ugyanebben az időben a torrent-technológia megjelenésével a szerzői jogsértések drámaian növekedtek.

[34] Dr. Polt Péter: A számítógépes bűnözés. BSZ. XXI. 1983. 6. 60-64.l.
[35] Dr. Pusztai László: Számítógép és bűnözés. KKT. XXVI. kötet. Budapest, 1989. 106-107.l.
[36] Dr. Nagy Zoltán: Az informatika és a büntetőjog. MJ. 38. 1991. 1. 21-23.l.

A 2000-es évektől az „informatikai” előtag használatával osztályozták az informatikai bűnözést (IT crime, information technology crime), ami a fogalomalkotók szerint magában foglalja a számítástechnikai bűnözést (computer crime), és a számítógépes hálózatokon megjelenő bűnözést (internet crime, cyberspace crime). E meghatározást hazai adaptációját olvashatjuk legújabban[37].

Le kell szögeznünk, hogy egyfelől a hálózatokon elkövetett bűncselekményekhez is számítástechnikai eszközöket használnak, továbbá nehezen válik ketté a virtuális térbeli és a számítógépes bűnözés. Ha a „producta scelerist” számítógépen tárolják, akkor az számítástechnikai bűnözés, ám ha ezt interneten továbbítják egy másik felhasználónak, akkor az internetes bűnözés. Ugyanígy a számítógépes bűncselekmények körébe vonható a 2001-es Budapesti Egyezményben idesorolt számítógépes csalást és számítógépes hamisítást hálózaton felhőszolgáltatón keresztül követnek el, az már az internetes bűnözés körébe sorolható.

A fogalomalkotási kísérleteket tovább bonyolítja az, hogy a valós térbeli bűncselekmények elkövetéséhez is egyre gyakrabban használnak számítógépeket, számítástechnikai eszközöket, azok kommunikációs lehetőségeit. Így nemcsak okirathamisítások, hanem akár ölési cselekmények is elkövethetők ezen eszközök alkalmazásával, mobileszközökön kommunikálnak, vagy ma már akár fegyvert is „nyomtathatnak” 3D nyomtatók alkalmazásával.

Az interneten a tartalom bűncselekmények zöme már ismert, szabályozott és verbális közléssel elkövethető bűncselekmény vagy szabálysértés.

Ugyanakkor észlelhető a számítógépes bűncselekmények megjelenésével kapcsolatban egy újfajta megközelítése a bűncselekmények osztályozásának. Ennek illusztrálására az alábbi dokumentumokat hívjuk fel.

A Budapesti Egyezmény 2002-ben született és 2006. március 1-től hatályos jegyzőkönyvvel egészült ki, amely az informatikai környezetben elkövethető rasszista és idegengyűlölő cselekmények elleni fellépést sürgette a tagállamoktól, amelyet további kiegészítő jegyzőkönyvek is követtek.

[37] Parti Katalin – Kiss Tibor: Informatikai bűnözés (In *Kriminológia*, by Andrea Borbíró, Katalin Gönczöl, Klára Kerezsi, és Miklós Lévay, Budapest: Wolters Kluwer Kft., 2016.) 491–493.

Továbbá itt említjük a 2013/42 EU direktíváját, amely a kritikus infrastruktúrák veszélyeztetettségére hívta fel a figyelmet.

Azaz a cselekmények fogalom meghatározás helyett inkább a motívumokra (pl. személyiséget, közösséget sértő cselekmények) és a bűncselekmények elkövetésének a céljaira (pl. haszonszerző, titoksértő stb.) helyezzük a hangsúlyt.

A bűncselekmények körének folyamatos bővülése megnehezíti a fogalomalkotást, holott tudományos elemzést, kutatást, akkor lehet hitelesen végezni, ha annak tárgyát meghatározzuk.

A számítógépes bűncselekmények egységes fogalom meghatározása hozzásegítené mind az Európai Unió, mind pedig a nyomozó hatóságok sikeres harcát a bűnözőkkel szemben.

Ugyanakkor, egyes vélemények szerint nem lehet közös elnevezés alá vonni a cselekményeket azok heterogenitása miatt.

Az, hogy foglalkoztatja a jogalkotókat a számítógépes bűncselekmények meghatározása kétségtelen, hiszen az Európai Bizottság 2007-es Közleményében[38] hangot adott annak, hogy az idáig nem került meghatározásra a számítógépes bűnözés (cyber crime), általuk is számítógépes bűnözésnek nevezett fogalma „*A társadalmunkban egyre nagyobb jelentőséggel bíró információs rendszerek biztonságának számos vonatkozása van, amelyek közül az egyik legfontosabb a számítógépes bűnözés elleni küzdelem. A számítógépes bűnözés közösen elfogadott fogalommeghatározása hiányában a »számítógépes bűnözés«, »számítástechnikai bűnözés«, »számítógéppel kapcsolatos bűnözés« vagy »csúcstechnológiás bűnözés« kifejezéseket gyakran használják szinonimaként. E közlemény alkalmazásában »számítógépes bűnözés« alatt „olyan bűncselekmények értendők, amelyeket elektronikus kommunikációs hálózatok és információs rendszerek felhasználásával vagy ilyen hálózatokkal és rendszerekkel szemben követnek el”.*

Magunk részéről a vita lezárásaként az alábbi megjegyzést tesszük, bármennyire is elterjedőben van – különösen az angolszász országokban - a kiberbűncselekmény elnevezés, magunk ezt a definíciót szűkebbnek tartjuk a számítógéphez kötött bűncselekmények körének meghatározásához, lévén, hogy csak hálózaton elkövetett bűncselekmények köre vonható ide.

[38] Európai Bizottság.:„A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának - A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé”, Közlemény, 2007. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52007DC0267,

Éppen ezért a számítógépes bűncselekmény elnevezést használjuk a későbbiekben, azzal, hogy a számítógépes bűnözés nemcsak az újtípusú bűncselekményeket ölelik fel, hanem minden olyan bűncselekményt, amelyhez a számítógépet eszközként vagy célként használnak, és a bűncselekmény elkövetése offline vagy on-line módban történik.

1.8 A számítógépes bűncselekmények elleni küzdelem jogi és technikai vetületei

Az lehetséges-e, hogy az elmúlt évtizedekben a számítógépes bűncselekmények társadalomra és gazdaságra gyakorolt hatására „egy prakticista elvetéssel el lehetett hárítani a számítógépes kapcsolatos bűnözés jogi szabályozásának kérdését?" fogalmazta meg Pusztai, amikor az 1980-as években egy felmérést végzett el a Magyarországon használtban lévő számítógépek számával összefüggésben.

Első lépésben szükségét érezzük annak, hogy tisztázzuk, milyen speciális ismérvei vannak tehát ennek a deliktumnak:

Informatikai eszközök és/ vagy rendszerek segítségével, vagy informatikai eszközök és hálózatok ellen elkövetett bűncselekmények, amelyek céljai lehetnek a rendszerben tárolt adatok megszerzése, a jogosultak számára hozzáférhetetlenné tétele, továbbá az elektronikus rendszerbe vetett bizalommal visszaélés. A számítógépes bűncselekmények célja lehet anyagi haszonszerzés vagy az informatikai rendszerbe vetett bizalom megszerzése, vagy a tárolt elektronikus adatok illetéktelen felhasználása, az azzal történő visszaélés illetve tartalommal kapcsolatos vagy az elleni jogellenes cselekmény.

A (kiber)tér, vagyis a helyszín tekintetében[39]- kétféle elkövetést lehet megkülönböztetni:

- Az egyik elkövetés az internetes térben, azaz kibertérben elkövetett bűncselekmény típusaihoz tartozik, amikor sem a cselekmény, sem az elkövető nem lép ki a fizikai térbe, azaz a virtuális világban marad. Ilyen bűncselekmény a jellemzően jelszó feltöréssel

[39] A magyar jogrendszer és tudomány merevnek minősül abból a szempontból, hogy az elkövetés helye, az elkövetés eszköze vagy akár a sértett meghatározása szempontjából csak a kézzel fogható, vagy behatárolható helyet, dolgot nevesít, míg ezek körébe sem a virtuális tér, sem az elektronikus adat nem tartozik (a szerz.).

vagy az információs rendszer befolyásolásával megvalósuló cselekmények, amelynek elkövetéséhez ténylegesen csak az internet, illetve a világháló szükséges.

- A másik eset a számítástechnikai eszközök felhasználásával (számítógép, laptop, telefon stb.) az internetes hálózaton keresztül, de a valós, fizikai térben végrehajtott deliktumokat követően valósítható meg, mint pl. egy fényképezőgéppel, videófelvevővel készített gyermekpornográf felvétel feltöltése, vagy a hamis, meghamisított készpénz-helyettesítő fizetési eszköz illetőleg a hamis, a meghamisított, erőszakkal, fenyegetéssel vagy más módon történt valódi készpénz-helyettesítő fizetési eszköz megszerzését követően, annak felhasználásával elkövetett card-present vagy card-not-present csalások.

A számítógépes bűncselekmények elleni küzdelem jogi dilemmája az, hogy e bűncselekmények megelőzése és felderítése kétféle úton történhet meg: jogszabályi és technikai megoldásokkal. Ez a két út sokszor nem választható el, hiszen a jogszabályok megalkotásának menete sokkal lassabb, mint a technika fejlődése. Ugyanakkor a technika fejlődésének maradéktalan felhasználása a számítógépes bűnözők ellen sem képzelhető el a hatályos jogszabályok ismerete nélkül.

Szomorúan konstatálhatjuk, hogy a tág értelemben vett büntetőjogi szabályozás folyamatos késésben van.

Az elmúlt évtizedekben számos nemzetközi dokumentum született, amely e területtel foglalkozik. Ehelyütt csak a legfontosabbnak tartott jogi dokumentumokat idézzük ide.

Rögtön szemünkbe ötlik, hogy a számítástechnika és hálózati technika fejlődésével a bűncselekmények köre bővült és ez a folyamat napjainkban is tart és a jövőben is ez várható.

Magyarországon a 2004. LXXIX. törvénnyel kerültek átültetésre a Budapesti Egyezmény szabályai, aminek az egyik legnagyobb hibája, hogy az angolról magyarra történő fordítása szó szerinti lett, így kezdetben (sajnos talán még most is) a jogalkalmazók sokszor saját szájízük szerint értelmezik azt.

Szükségesnek érezzük említést tenni azokról a technikai, technológiai megoldásokról, amelyek segítik a jogalkotók és nyomozó hatóságok, ügyészségek munkáját a számítógépes bűncselekmények elleni küzdelemben.

Bűnügyi szempontból a folyamatosan fejlődő hardverek és szoftverek veszélye az újabb és újabb visszaélésekre nyújthatnak lehetőséget.

Az internet nemzetközi jellege önmagában már komoly problémát vet fel, hiszen a más országok szerverein tárolt tartalmak, adatok elérése jogi és technikai nehézségeket vethetnek fel.

Külön probléma a felhő-szolgáltatás. A felhőszolgáltatás (cloud computing) napjaink olyan új technikai megoldása, amely tehermentesítik a felhasználót attól, hogy nagytömegű adatot tároljanak, illetve különböző programokat telepítsenek számítógépére.

A felhőszolgáltatások típusai Máté István Zsolt[40] és Kovács Zoltán[41] tanulmányai ismeretében:

- szoftver-szolgáltatás: a web-böngészőn keresztül érhetők el különböző szoftverek,

- platform-szolgáltatás: alkalmazás üzemeltetéséhez szükséges környezetet biztosítja, terheléselosztással, frissítéssel,

- infrastruktúra-szolgáltatás: virtuális hardver szolgáltatása, tárhely, számítási stb. kapacitás szolgáltatása.

A technikai részleteknél talán érdekesebbnek tűnhet a hozzáférés lehetőségei szerinti csoportosítás:

- privát felhő: csak a dedikált felhasználó veheti igénye, akár egy felhasználó is létrehozhatja saját magának,

- publikus felhő: mások számára is nyitva áll a szolgáltatások igénybevétele,

- hibrid felhő: az előzőek kombinációja.

A bűnügyi jogsegély nehézsége felhőszolgáltatás esetében:

- általában a kettős inkrimináció, mint feltétel (tartalomközlés esetében ez kétséges),

[40] Máté István Zsolt: Felhőszolgáltatás- A kiberbiztonságtól a szakértői bizonyításig (Rendészetelmélet, forrás: http://www.rendeszetelmelet.hu/Graphics/pdf/Mate_Istvan_Zsolt_Felhoszolgaltatasok.pdf, letöltve: 2019. április 02.)

[41] Kovács Zoltán Felhőalapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél (Hadmérnök, 2011. december, VI. évfolyam) 176-188.

- nem lokalizálható, hogy mely országban vannak a szerverek,

- a felhő-szolgáltató együttműködési hajlandósága.

Az informatikai tudás ma már készségszinten hozzátartozik a mindennapjainkhoz. A jogszabályok betartása a büntetőeljárás különböző cselekményeinek elvégzése közben kivitelezhetetlen azon tudás nélkül, amely megkönnyíti vagy néhány esetben felesleges kiadások nélküli eredményt hoz.

Bármely deliktum nyomozása, felderítése során szükséges lehet az elkövetőnél vagy a bűncselekmény helyszínén található informatikai eszközök gyors vizsgálata. Ilyen esetben nemcsak azzal kell tisztába lenni, hogy egy mobiltelefon milyen operációs rendszert használ, vagy ahhoz az adott mobileszköz tartalmához hogyan lehet hozzáférni, hanem azt is, hogyan találjuk meg a szükséges információkat úgy, hogy a későbbiekben is hozzáférhetőek maradjanak, továbbá alkalmasak legyenek minden kétséget kizáróan a bizonyításra.

1.9 A jogalkotással szemben támasztott követelmények a nemzetközi dokumentumokban

Látható, hogy a számítógépes bűncselekmények (számítógépes környezetben elkövetett, avagy kiberbűncselekmények) kriminalizálása az ezredfordulón elkerülhetetlen feladatot rótt a jogalkotókra.

E tárgykörre vonatkozó jogszabályok által figyelembe veendő – általános – követelményekre hívja fel a figyelmet az ENSZ Közgyűlése 2000-ben a Közgyűlés által elfogadott 55/63 számú határozata[42] az információs technológiák bűncselekményekhez való felhasználása elleni harcról a jogalkotást illető részéből az alábbiakt emeljük ki:

1. Az államoknak biztosítaniuk kell, hogy a jogszabályaik és joggyakorlatuk felszámolja a védett zónákat az információs technológiákkal való visszaélések esetében.

2. Az információs technológiákkal való nemzetközi jellegű visszaélések esetében koordinálni kell a nyomozó hatóságok együttműködését a nyomozásban és a vádemelésben az érintett államok között.

[42] ENSZ Kézikönyve, A Website of a UNODC (forrás: http://www.uncjin.org/Documents/EighthCongress.html)

3. Az államoknak meg kell osztaniuk egymással az információkat azokról a problémákról, amelyekkel az információs technológiák bűncselekményekhez való felhasználása elleni harc során találkoznak.

5 Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

4. A nyomozó hatóságok személyzetét ki kell képezni és felszereléssel kell ellátni az információs technológiákkal való visszaélések elleni fellépés érdekében.

5. A jogrendszereknek védeniük kell az adatok számítógépes bizalmasságát, integritását és elérhetőségét a jogosulatlan megkárosítástól, és biztosítaniuk kell, hogy a visszaéléseket büntetni rendelik.

6. A jogrendszereknek lehetővé kell tenniük a bűnügyi nyomozásokkal kapcsolatos elektronikus adatok megőrzését, és az ezekhez való gyors hozzáférést.[43]

Majd röviddel ezután az ENSZ Közgyűlése 56/121 szám alatt ismét egy határozatot fogadott el az információs technológiával kapcsolatos visszaélések elleni küzdelemről, amelyben sürgeti a tagállamok közötti együttműködést. Felhívja a tagállamokat arra, hogy az információs technológiákkal a visszaélésekkel kapcsolatos nemzeti jogszabályok, politikák és gyakorlat kialakításakor figyelembe vegyék a nemzetközi és regionális szervezetek munkáját és azok eredményeit.

Konkrét bűncselekmények de lege ferenda javaslatot tartalmaz az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról, amely 2005/222/IB tanácsi kerethatározatot váltotta fel.

Az Európai Unió által kibocsátott irányelv, - amelynek tartalmát a tagállamoknak magukévá kell tenni, bár a belső jogforrási szintet önállóan határozhatják meg – célkitűzése az, hogy közelítse az Európai Unió tagállamainak büntetőjogát az információs rendszerek elleni támadások terén. A dokumentum minimumszabályokat állapít meg az információs rendszer elleni támadásokkal kapcsolatos büntetőpolitika kialakításához, továbbá meghatározza azokat a deliktumokat, amelyek az információs rendszerek elleni támadásnak minősülnek.

[43] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/63 350

A nemzetállami büntetőjogok közelítéséhez mindössze négy deliktumok kötelező beemelését írta elő:

- Információs rendszerekhez való jogellenes hozzáférés (3. cikk),

- Rendszert érintő jogellenes beavatkozás (4. cikk)

- Adatot érintő jogellenes beavatkozás (5. cikk)

- Jogellenes adatszerzés (6. cikk).

Továbbiakban bűnrészesi alakzatokra, joghatósági kérdésekre és más fontos körülmények kriminalizálására hívta fel a tagállamok figyelmét.

A számítógépes bűncselekményt, nem tipizáltan, egy rendszerbe veszi a jogalkotó, hanem kibertérben vagy információs rendszer felhasználásával, vagy az ellen elkövetett elkövetési magatartásokat vagy elkövetés tárgyát, megemlíti, továbbá a korábbi és a hatályos büntetőeljárási törvényeink is tartalmazza, ezzel is eleget tesz a 2001-ben elfogadott Számítógépes Bűnözésről szóló Egyezményben foglaltaknak.

Ugyanakkor visszautalunk arra, hogy a számítógépes bűncselekmények fogalma nem került ez idáig meghatározásra, addig a kiberháború fogalma már meghatározásra került a jogalkotók által: a 60/2013. (IX. 30.) HM utasításban foglalkoznak az információs fenyegetésekkel (így utal a bekövetkezett a 2007-es Észtországot érő orosz kibertámadásra), amelyet követően a világ gondolkodása a háborús konfliktusok helyszínéről megváltozott. Az utasítás már nyíltan kimondja, hogy az iráni urándúsítót ért vírustámadás kiberháborúként értelmezhető.

A fent említett HM utasítás kimondja[44]: „*A fenyegetett célok változnak, egyre szélesebb körű szolgáltatások veszélyeztethetők. A támadó célja infokommunikációs eszközök alkalmazásával a vezetési és irányítási rendszerek feletti irányítás megszerzése, a támadott fél erőinek lekötése, reagáló képességének felmérése, a nemzeti kritikus infrastruktúrák, a nemzeti adatvagyon veszélyeztetése vagy a katonai műveletek, katonai erő hatékony alkalmazásának blokkolása, befolyásolása. ..... A támadás forrása lehet hacker tevékenység, szervezett bűnözés, ideológiai vagy politikai szélsőség, kormányzati támogatással rendelkező agresszió*. ”

[44] 60/2013. (IX.30) HM utasítás

Sem a Büntető Törvénykönyv (2012. évi C. törvény), sem a Büntető Eljárásról szóló 2017. évi XC. törvény (továbbiakban: Be.) nem tartalmazza a számítógépes bűnözés (computer crime) fogalmát. Még az 1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiája sem nevezi meg, hogy mit is értünk számítógépes bűnözés alatt.

2 A SZÁMÍTÓGÉPES BŰNCSELEKMÉNYEK

2.1 A számítógépes bűncselekmények kriminalisztikai szempontból

A számítógépes bűnözést kriminalisztika felől közelítve történő három területet különíthetünk el A. Sussmann szerint[45]:

1. A számítógép központú bűnözés (Computer Centred Crime): A típus jellemzője, hogy a bűncselekmény célpontja az informatikai rendszer, a hálózat, az adattároló, vagy más eszköz jelenik meg (pl. kereskedelmi weboldal tartalmának módosítása). Ez tekinthető egy új bűncselekmény típusnak is, mely új eszköz- rendszert használ (ti. a számítógépet).

2. Számítógéppel segített bűnözés (Computer Assisted Crime): Amikor a számítógépet, mint eszközt használja az elkövető a cselekmény elkövetése során, ami a tevékenységének megvalósítását könnyíti, de nem feltétlenül szükséges hozzá (pl. gyermekpornográfia). Itt hagyományos bűncselekményekről beszélhetünk, új módszerek alkalmazása mellett.

3. Járulékos számítógépes bűnözés (Incidental Computer Crime): Itt a számítógépes rendszer a bűncselekmény szempontjából mellékes a bűncselekmény szempontjából, lényegében egy hagyományos eszköz kiváltását jelenti (pl. könyvelés számítógéppel, papír alapú dokumentáció helyett).

Más szempontból, akár a valós térben, akár a virtuális térben elkövetett bűncselekmények nyomozása során tisztázandó a bűncselekmény motívuma, célzata.

A számítógépes bűncselekmények ismerévei tehát:

- Az anyagi haszonszerzés, mint jellemző motívum: A számítástechnikai bűncselekmények elkövetése jellemzően anyagi, gazdasági és pénzügyi haszonszerzési célzattal történik.

- Az információbiztonságot sértő cselekmények, adatok megszerzése céljából: Az informatikai rendszerekben adatok formájában tárolt információk védelmet igényelnek, melyre az információvédelem vonatkozik. Ez utóbbi fogalom olyan

[45] Michael A. Sussmann: The critical challenges from international high-tech and computer- related crime at the millenium (Duke J. Comp. N Int'I L 450, 1997)

eljárások és intézkedések összességét jelenti, amely lehetővé teszi az azonosítási és hitelesítési eljárások kialakítását, a hozzáférési rendszer létrehozását (jogosultságok kiosztását, a jogosultságok ellenőrzését), az adatok és a programok sérthetetlenségének biztosítását, az adatok bizalmasságának (titkosság: az információkhoz vagy adatokhoz csak az arra jogosultak és csak az előírt módon férhetnek hozzá) garantálását, a naplózási rendszer megvalósítását a szervezeten belül. A különböző védett, bizalmas adatok sértetlenségéhez fűződő érdek kiemelten fontos, és aminek illetéktelen személyek vagy csoportok általi megszerzése nemcsak komoly károkat okoz, hanem az elkövetőknek akár elképzelhetetlen bevételi forrás is. Ez utóbbi például a rendvédelem, közigazgatás, igazságügy vagy nemzetbiztonság területein, a politikai pártoknál kezelt a személyes, illetve minősített adatok illetéktelen megszerzése.

Mivel a számítógépes bűncselekmények magyarországi nyomozásában a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnüzés Elleni Főosztálya kiemelt szerv, így az általuk kialakult típusok mindenképpen figyelmet érdemel:

- Klasszikus cybercrime: adathalászat, más szerverek ellen irányuló, azok működésében kárt okozó kibertámadások, internetes csalások, on-line banking csalások.

- Gyermekek online szexuális kizsákmányolása: gyermekpornográfia, egyéb (szexuális zsarolás, beszervezés stb.) nemi élet szabadsága és nemi erkölcs elleni bűncselekmények.

- Készpénz-helyettesítő fizetési eszközök (ahogy az oktatási anyagban szerepelt: bankkártyával kapcsolatos bűnözés, mint például a card-present és a card- non present típusú elkövetés) használatával elkövetett deliktumok.

A számítógépes bűncselekmények fogalmának elemeit a fentiek szerint a nyomozás szempontjából releváns körülmények alapján összegezhetjük:

- informatikai eszközök és/vagy rendszerek segítségével, vagy

- informatikai eszközök és hálózatok ellen elkövetett bűncselekmények,

- amelyek célja a rendszerben tárolt adatok megszerzése, hozzáférhetővé tétele, vagy

- a jogosultak számára hozzáférhetetlenné tétele, melynek célja lehet anyagi haszonszerzés vagy
- az informatikai rendszerbe vetett bizalom megszerzése.

Külön kategóriát képeznek azok a számítógéphez kapcsolódó bűncselekmények, amelyeket a törvény más tényállás alapján büntet (például pedofília), de ebben a részben azzal külön nem kívánunk foglalkozni.

2.2 A számítógépes bűncselekmények körében felmerülő fogalmak

A számítógép

A számítógépet, mint eszközt, anélkül is ismerjük, hogy annak pontos fogalmát tudnánk. Mivel az értekezésben több helyen is használjuk e kifejezést, így illendőnek tartjuk, ha meghatározásra kerül. A Cambridge enciklopédia[46] meghatározása szerint a számítógép (computer) olyan elektronikus gép, amely szavak, számok és képek tárolására, szervezésére és keresésére, számítások elvégzésére és más gépek vezérlésére szolgál.

A számítógép olyan berendezés, amely képes bemenő (input) adatok fogadására, amelyeken különböző előre beprogramozott műveletek végrehajtására és az eredményül kapott adatok kijelzésére (output)[47].

Az internet

Az internet (Internetworking System – rövidítése) más nevén világháló (world wide web, röviden: www), amely egyrészt számítógép-hálózati technológiát, másrészt a számítógép hálózatok világméretben együttműködő hálózatát, azaz egy világmozgalmat is jelent[48].

Az internet a számítógép-hálózatok hálózata, amelyben a számítógép-hálózat olyan LAN (Local Area computer Network), amelynek számítógépeit egy, vagy több közös hozzáférésű fizikai közeg kapcsolja össze[49].

---

[46] forrás: https://dictionary.cambridge.org/dictionary/english/computer, letöltve: 2019. március 20.
[47] Fekete Gábor: A számítógép hardverelemeinek fejlődése (Debrecen, 2009, Debreceni Egyetem Informatikai Kar) 5.
[48] Jutasi István:, *Az Internet felépítése és működése: Hálózatok, Protokollok, Biztonság, Netikett*, szerk. Nagy Károly (Budapest: Műszaki Könyvkiadó, 1997), 5.o.
[49] Vö. Jutasi István: A Internet felépítése… 10.o.

Az internet decentralizált, azaz nem hierarchikus rendben vannak a központok, hanem a hálózat egyenrangú csomópontokból, úgynevezett node-ból áll, amelyek felhőkben (cloud) találhatóak. Az internetről vagy világhálóról bővebben a 3.3. pontban, Az Internet tulajdonságai között fogunk még szólni.

Az informatika

„Az informatika az adatok dinamikus beszerzésének, indexelésének, terjesztésének, tárolásának, keresésének, visszahívásának, megjelenítésének, integrálásának, elemzésének, szintézisének, megosztásának (magába foglalva az együttműködés elektronikus eszközeit) és publikálásának technológiai, társadalmi és szervezeti eszközeit és vonatkoztatásait kutatja, fejleszti és használja úgy, hogy az információk a társadalom minden rétegéből származó használók javára váljanak."[50]

Cyberspace vagy kibertér

Muha Lajos megfogalmazásában a kibertér: „Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszerek és beágyazott processzorokat és vezérlőket."[51]

A kibertér fogalmát sokan helytelenül használják. Az, hogy a kifejezést megértsük nagy segítség Kovács László Kibertér védelme című monográfiája, amelyben többek között rámutat arra, hogy a kiberteret sokan tévesen azonosítják az internetes térrel, holott ez jóval több. „*A kibertér: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva*"[52].

Az internet jellemzői, amelyek a nyomozati munka specialitását jelzi Ropolyi László tanulmánya Internet tulajdonságot és Internetes tevékenységformát nevezünk meg:[53]

[50] President's Commitee of Advisors on Science and Technology, 2000
[51] Muha Lajos: „Informatikai biztonsági fogalmak és definíciók", http://lmuha.hu/defins.html, elérés 2018. március 23., http://lmuha.hu/defins.html. Letöltve: 2018. július 07.
[52] Kovács László: *A kibertér védelme* (Budapest: Dialóg Campus Kiadó, 2018), 17, https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf. Letöltve: 2018. október 01.
[53] Ropolyi László: *Az internet természete* (Budapest: Typotex Kiadó, 2006), 31.

- számítógépek, illetve hálóhelyek közötti biztonságos adatforgalom révén fájlok le- és feltöltése (ftp-zés), valamint mindenféle adminisztratív, üzleti, banki, tőzsdei, termelési, fogyasztási és kulturális célú fájltranszferek

- elektronikus levelezés és egyéb (korábban postainak nevezett) hasonló szolgáltatások

- automatikus adat-és információkezelő rendszerek által támogatott önszerveződő tevékenységek és közösségek (hírcsoportok, diszkussziós listák, fórumok, csevejcsatornák, szerepjátékok) fenntartása és kiszolgálása

- intézményi és személyes honlapok, naplók (blogok), rádióműsorok (podcast-ok) szerkesztése, az ezek között való böngészés, illetve szörfölés

- hálózatba kapcsolt számítógépek összehangolt működtetése révén virtuális és megaszámítógépek, a „világméretű számítógép" kialakítása és hasznosítása.

2.3 A számítógépes bűncselekmények kriminológiai jellemzői

A számítógépes bűncselekmények jellemzőinek felsorolása során megfigyelhetőek azok a tényezők, amelyekkel a kibertérben történő deliktumok nyomozásánál a hatóságok szembesülnek[54]:

A gyorsaság, amely nem feltétlenül magának a cselekmény előkészületének, vagy a tett végrehajtásának a „sebességére" vonatkozik, hanem sokkal inkább azt, hogy a deliktum végeredménye gyorsan bekövetkezik. A kibertámadásokhoz készített, megírt vírusok, programok készítése, annak tervezett, vagy véletlenszerű elküldése cégeknek, állami szervezeteknek vagy magánszemélyeknek az internetsebességétől is függ.

Ugyanez vonatkozik a készpénz-helyettesítő fizetési eszköz hamisítás vagy adatszerzés esetére is, amikor a készpénz-helyettesítő fizetési eszköz másolásra alkalmas eszközt (Skimming- a készpénz-helyettesítő fizetési eszköz alkalmas berendezés) megvásárolják, és azt kihelyezik az ATM-re vagy az elkövető, mint pincér vagy eladó a kezében tartva, lemásolja a mágnescsíkot,

[54] Gyaraki Réka „Számítógépes bűncselekmények és az ellenük való védekezés", in Információvédelem, (szerk: László Christián) Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2015, 182.o.

vagy a klasszikus adathalász módszerrel telefonon vagy más, infokommunikációs eszközön keresztül megszerzi a felhasználók adatait és azokat felhasználják, vagy eladják.

A gyorsaság viszont attól a pillanattól kezdődik, amikor a sértett rákattint a vírust tartalmazó e-mailre vagy linkre, amikor a készpénz-helyettesítő fizetési eszköz behelyezi az ATM leolvasó nyílásába, vagy terminálba. Onnan kezdve a technikai eszköz segítségével pillanatok alatt települ a program és vagy akár azonnal vagy meghatározott időpontban vagy billentyűzetkombináció leütése után szerzik meg az adatokat vagy a hatalmat a számítógép vagy információs rendszer felett. Többek között ennek a tulajdonságnak is köszönhetően könnyű a bűnelkövetők és nehéz a nyomozó hatóságok helyzete. A gyorsaság nemcsak az adatok, információk sebességét jelenti, hanem a technika fejlődését is, mellyel lépést kell tartani. A gyorsaság miatt a sértettek vagy potenciális sértettek is veszélyben vannak, hiszen előfordulhat, hogy nem észlelik időben a sérelmükre elkövetett bűncselekményt, vagy annyi idő telt már el az elkövetés óta, ami a nyomozást megnehezíti. Ugyanakkor a gyorsasággal kapcsolatban fontos kiemelni, hogy a cselekmény előkészítése, maga az elkövetés nem biztos, hogy gyorsan történik, hiszen a különböző programok elkészítése hosszú időt vesz igénybe. A gyorsaság függ még a kor technikai újításaitól és az elkövetők szakmai fejlettségétől, tudásától a sértettek biztonság tudatosságától, az informatikai eszközök védelmi rendszerétől.

A magas fokú látencia, amelynek az egyik oka, hogy a számítógépes bűncselekmények áldozatai egyáltalán nem vagy nem időben észlelik, hogy bűncselekmény áldozatai lettek. A sértettek, mivel a jogsértés a virtuális térben megy végbe, így vagy később, vagy egyáltalán nem veszik észre, hogy ellenük bűncselekményt követtel el, az informatikai rendszerben tárolt adataikkal visszaélés történt. Parti Katalin megállapítása szerint „az online világban az azonosíthatatlanság olykor egyébként jogkövető embereket is bűncselekmények elkövetésére indít. A felderítési arány csekély, a látencia óriási.[55]” Ugyanakkor sok esetben előfordul az is – főleg bankok vagy nagyobb cégek esetében – hogy az ellenük elkövetett bűncselekményeket eltitkolják és/vagy az esetek többségét nem jelentik a hatóságok felé[56]. Sok esetben azért, mert attól félnek, hogy az ügyfelek bizalma irányukban meginog. A cégek, pénzintézetek esetében az Európai Unió 2018. május 25-től életbelépett általános adatvédelmi rendeletének (GDPR)[57]

[55] Parti Katalin: A számítógépes bűnözés és az internet (Kriminológiai Tanulmányok 40., 2003) 196.
[56] A pénzintézetek, hitelintézetek nem jelentik, hogy akár ők maguk, vagy az ügyfeleik támadás áldozatai lettek, ami az ügyfelek elvesztésétől, az üzletfelek rossz megítélésétől, partnerek elvesztésétől való félelem miatt történhet
[57] „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

köszönhetően az incidens bekövetkezése utáni 72 órán belül be kell jelenteni azt. Magyarországon incidenskezeléssel foglalkozó szervezet a Nemzeti Kibervédelmi Intézet, ahol bár eddig is foglalkoztak incidenskezeléssel és azok nyilvánosságra hozatalával, az új rendelet óta a bejelentéseket a Nemzeti Adatvédelmi és Információszabadság Hatósága, a NAIH felé kell bejelenteni.

Másik oka a magas fokú látenciának, hogy az elkövetőknek nem szükséges az elkövetés helyszínén tartózkodni. A különböző kommunikációs eszközök segítik, hogy a cselekményüket távolról irányíthassák, így a tettenérés szinte kizárt, a nyomozó hatóság részéről a felderítés a hagyományos eszközökkel lehetetlen. Ahogyan a gyorsaság jellemzőjénél is említettük, a bűnözők nemcsak, hogy távolról irányítják az eszközöket, hanem előfordulhat az is, hogy egy előre meghatározott időpontra aktivizálják az adott programot, ami idő bekövetkeztekor hajtja végre a módosításokat, így szerezvén meg az adatokat az áldozatok eszközeiről, amelyek észlelése csak nagy körültekintés mellett lehetséges vagy még úgy sem.

A nemzetközi jelleg, mint jellemző. A hagyományos bűncselekmények esetében- így például a szervezett bűncselekményeknél, kábítószer-és fegyverkereskedelem esetében – a határokon átnyúló bűncselekmények egyébként is nehezítik azok felderíthetőségét és az elkövetők kézre kerítését. A kibertér nem egy körülhatárolt, fizikai határokkal rendelkező terület, hanem egy olyan virtuális hely, ami jellegénél fogva biztosítja az információk és kommunikációk áramlását anélkül, hogy az akadályokba ütközne. Hiába eltérő a jogi szabályozása országonként, épp a nemzetközi jellemző miatt nehezedhet, illetve megtagadható akár a gyanúsított felelősségre vonása vagy a kényszerintézkedések végrehajtása[58]. Korinek László hangsúlyozza, hogy *a nemzetközi kriminalitásra nemzetközi bűnüldözéssel kell válaszolni*[59]. Ám ezt ő maga sem gondolja ennyire egyszerűnek, amikor azzal folytatja, hogy az *egyes államok egymástól meglehetősen eltérő jogrendszereihez igazodó büntető igazságszolgáltatás nem globalizálható*[60]. A kibertérben elkövetett bűncselekmények esetén nem szükséges, hogy az elkövető és az áldozat egy helyen vagy ugyanazon a földrészen tartózkodjon, a támadások

(é. n.), https://www.adatvedelmirendelet.hu/wp-content/uploads/2016/07/CELEX3A32016R06793AHU3ATXT.pdf.

[58] Emlékezetes a kuruc.info ügye, amelyben a mai napig nem sikerült a holokauszt tagadással kapcsolatos interneten megjelent cikke miatt (is)az aloldal blokkolását végrehajtani. Az adat végleges hozzáférhetetlenné tételéhez szükséges IP cím megadása szükséges lenne, amely, ha olyan országban van, ahol az adott cselekmény nem bűncselekmény, akkor a végrehajtást az arra jogosult szervezet meg fogja tagadni.

[59] Korinek László: Tendenciák korunk bűnözésében és bűnüldözésében (forrás: https://jura.ajk.pte.hu/JURA_2014_1.pdf, letöltve: 2019. február 02.) 120.

[60] u.az

és a jogellenes cselekmények elkövethetők, a megszerzett adatok, információk továbbíthatók, módosíthatók.

A számítástechnikai környezetben elkövetett bűncselekmények technikai, technológiai jellege abban nyilvánul meg egyrészt, hogy a különböző számítástechnikai eszközök fejlesztése, azok fejlődése és minél szélesebb körben történő terjedése és használata fokozza a számítógépes bűnözés népszerűségét és korábban az informatikai eszközök nélkül végrehajtott deliktumok helyett a bűnözők az anonimitásuk és a nagyobb pénzszerzés és áldozatuk számának növelése érdekében szívesebben kezdték el a számítástechnikai eszközöket és információs rendszereket használni. Minden újabb és újabb számítástechnikai vívmányt a számítástechnikai bűnözők felhasználják bűncselekmények elkövetése során. A legnagyobb problémát az jelenti, hogy sem a hatóságok, sem a társadalom nincsenek felkészülve e bűnözés elleni védekezésre, sokszor eszközök, felkészítés és tudás tekintetében le vannak maradva, az önképzésük vagy a szervezet általi képzésük hiányos, illetve lokális, azaz a szervezeti hierarchia magasabb szintjén található egységek esetén megoldott, míg a kerületi, helyi szinten sem a technikai eszközök, berendezések, sem a szakember nem áll rendelkezésre. Ezt a jellemzőt támasztja többek között alá a később ismertetett Evasys kérdőív eredménye.

Az anonimitás vagy névtelenség, amit a világháló, a virtuális tér biztosít, és ami összefüggésbe hozható a technológiával és annak fejlődésével. Az anonimitás, azaz a személyazonosság rejtve maradása mindig is kihívást jelentett a hatóság részére- gondoljunk csak anno népszerű névtelen levelekre vagy a névtelen telefonhívásokra, de a személyiség fel nem fedésének lehetőségét az internet a technológiával képes biztosítani. Jelenleg nincsen olyan hazai és/vagy nemzetközi jogszabály, amely büntetné azokat, akik egyáltalán nem adják meg nevüket, adataikat, vagy fiktív névvel regisztrálnak egy közösségi oldalon vagy hamis adatokkal hoznak létre e-mail fiókot. A névtelenséget persze nemcsak az internet „sötét bugyrának” titulált dark net használja ki és él a felhasználóik megóvása miatt vele, hanem a hagyományos és mindenki számára könnyen elérhető keresőmotorok segítségével elérhető oldalak esetében sem tiltott vagy nem megfelelően szankcionált az anonimitás.

A fizikai világban történő elkövetés esetében a hatóságok sokszor eredményesebben tudnak fellépni, mivel minden embernek van egy egyedi, azonosítható nyoma (név, lakcím, DNS stb.) addig a virtuális térben a technológiával a digitális lábnyomok elrejthetők, megsemmisíthetők, de akár többszörözhetők.

Az anonimitás biztosítása ráadásul úgy tűnik, mintha érdekében állna az országoknak és az internet szolgáltatóknak, hiszen a már említett Európai Unió Adatvédelmi Rendelete az IP címet személyes adatnak minősítette és ezáltal a nyomozó hatóságok egyik kedvelt nyílt forrásból származó információgyűjtési lehetősége a www.centralops.net, amelyen keresztül egy adott e-mail cím, vagy weboldal hosting szolgáltatójára vonatkozó adat, IP címe, vagy esetleg a regisztráló neve megismerhető volt. Ez a lehetőség 2018. május 25.-e után, amíg a rendeletnek nem tudnak (vagy akarnak) megfelelni, nem marad legális forrás. Ez az a jellegzetesség, ami miatt a számítógépen elkövetett bűncselekmények száma felfelé ível.

A nehéz felderíthetőség, mint egyik legfontosabb jellemző azt jelenti, hogy a számítógépes bűncselekmények elkövetését nehezen, vagy csak későn lehet észlelni. Sokszor a nyomozó hatóságok járatlansága, képzetlensége is nehezíti a nyomozást. De ugyanúgy nehézséget jelent a különböző nyomozó szervek rosszabb technikai felszereltsége és felkészültsége. Elkövetői oldalról nézve, a felhasználók névtelensége vagy álnevek használata miatt nehéz a személyazonosság meghatározása. Megnehezíti a felderítést az elkövetők által megszerzett adatok titkosítása és/vagy megsemmisítése. A számítástechnikai eszközök, berendezések helyrehozhatatlan megrongálása is megnehezíti a nyomozó hatóság munkáját. Tekintettel arra, hogy a kibertérben nincsenek országhatárok, az elkövetés helyét is nehéz meghatározni.

A nyomozás során - az eredményes befejezés érdekében - szükséges az elkövető és a sértett személyének megállapítása, az elkövetett cselekmény felderítése, a tárgyi bizonyítékok beszerzése, esetleg a további bűncselekmény megakadályozása, a sértettek kártalanítása, valamint a végcélként a retorzió alkalmazása, amelyet szintén a jellemzők között felsorolt anonimitás és látencia nehezíti.

3 A SZÁMÍTÓGÉPES BŰNCSELEKMÉNYEK NYOMOZÁSÁVAL KAPCSOLATOS HAZAI ÉS NEMZETKÖZI SZERVEZETEK

Az informatikához kapcsolódó bűncselekmények kezelésével kapcsolatba hozható nyomozást végző szervezetek tagozódása tekintetében a centralizáltság jellemző. A 25/2013 (VI.24.) BM rendelet felsorolja a nyomozó hatóság „speciális" szerveit, amelyek közül két szervezet nevében található meg, hogy kifejezetten a számítógépes bűncselekmények nyomozásával foglalkoznak, míg a többi, 19 megyei szervezet esetében nincs kifejezetten az ilyen típusú bűncselekmények nyomozásában eljáró egység jelenleg. Jellemzően a gazdaságvédelmi vagy a bűnüldözési osztályok emberei végzik a számítógépes bűncselekmények nyomozását.

A számítógépes bűncselekményekkel együtt szükséges megemlíteni a kibervédelemmel - azaz a kibertérből érkező támadásokkal - foglalkozó nemzetbiztonsági szervezeteket is. Akár a kritikus infrastruktúrák elleni (kiber)támadások megelőzése és elhárítása érdekében nemcsak a rendőrségnek és a Terrorelhárítási Központnak van kiemelt feladata, hanem a BM Országos Katasztrófavédelmi Főfelügyelőségnek és az 1995. évi CXXV. törvény (Nbtv.) hatálya alá tartozó szervezeteknek - így az Alkotmányvédelmi Hivatal, a Katonai Nemzetbiztonsági Szervezet, a Nemzetbiztonsági Szakszolgálat (ezen belül a Nemzeti Kibervédelmi Intézet), az Információs Hivatalnak is, továbbá a Magyar Honvédségnek is kiemelt feladata van, hiszen 2026-ig a jelenlegi tervek szerint egy kibervédelmi parancsnokságot kívánnak létrehozni az országot érő kibertámadások elhárítása és az ellene történő védekezés érdekében[61].

A rendőrség feladatait az Alaptörvény a nemzetbiztonsági szervezetek feladataival együtt említi. *A különös feladat- és hatáskörű rendőrségként foghatók fel a nemzetbiztonsági szolgálatok, amelyeknek, illetőleg tagjaiknak, Magyarországon nincs nyomozati hatáskörük, de rendőri intézkedések és kényszerítő eszközök alkalmazásának joga megilleti őket, beleértve a fegyverhasználat lehetőségét is*[62] - húzott párhuzamot Korinek a két szerv között.

[61] eGov, „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/. Letöltve: 2018. október 01.

[62] Korinek László: A rendőrség szerepe, funkciói és típusai (forrás: http://rendeszet.hu/hatarrendeszetitagozat/Sodorvonalon.pdf, letöltve: 2019. március 2.) 145.

Hautzinger a rendőrség és a nemzetbiztonsági szervezetek között az alábbiak szerint tesz különbséget: *a rendőrség alapvető feladata a bűncselekmények megakadályozása, felderítése, a közbiztonság, a közrend és az államhatár rendjének védelme, míg a nemzetbiztonsági szolgálatok rendeltetése hazánk függetlenségének és törvényes rendjének védelme, nemzetbiztonsági érdekeinek érvényesítése*[63].

A számítógépes bűncselekmények nyomozásával kapcsolatos teendőket a rendőrségről szóló törvény hatálya alá tartozó szervezetek végzik a bűncselekmény jellegétől, a hatáskör és illetékességtől függően.

3.1 Rendőrség

Magyarország közbiztonságáért, a rendvédelmi, bűnüldözési és bűnmegelőzési feladatok ellátásáért a Belügyminisztériumhoz tartozó rendőrség felelős. A rendőrség feladatait elsősorban az 1994. évi XXXIV. törvény a rendőrségről szabályozza, de munkájuk során tekintettel kell lenniük az 2017. évi XC. törvényre, a 2012. évi C. törvény, büntetőtörvénykönyvre, illetve a 25/2013 (VI.24) BM rendelet a rendőrség hatásköréről és illetékességéről szóló rendeletre, amely a rendőrség szervezeti tagolódását szabályozza. Ezen jogszabályokon kívül a nyomozó hatóság a 100/2018. (VI.8) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól szóló rendelet és további belső utasítások alapján látja el feladatait.

A rendőrség meghatározott jogok és kötelezettségek szem előtt tartása és amellett végzi, mindeközben védik az állampolgárok biztonságát és a gondoskodnak a törvények betartásáról és betartatásáról. Ugyanakkor a rendőrség feladata talán az egyik legösszetettebb, hiszen a közrendvédelmi, bűnügyi és szabálysértési terület mellett ellát egyéb feladatokat is. A rendészeti tevékenység alapvető irányultsága a rend, a biztonság fenntartása, megőrzése emeli ki Madai[64].

[63] Hautzinger Zoltán: A fegyveres szervek rendeltetésének alaptörvényi szabályozása (forrás: http://real.mtak.hu/90855/7/67_magyarorszag-uj-alkotmanyossaga-kotet-2011.pdf, letöltve: 2019. március 10.) 74.
[64] Madai Sándor: Integrációs változatok a rendészetben, In Horváth M. Tamás- Bartha Ildikó: Közszolgáltatások megszervezése és politikái (Dialóg Campus, Budapest-Pécs 2016) 265.

A rendőrség bűnügyi feladatai ellátása során – ahogy már fentebb is említettük- az Alaptörvényen, azonkívül a büntetőeljárásról szóló törvény, a Büntető Törvénykönyvről szóló 2012. évi C. törvény, a rendőrségről szóló 1994. évi XXXIV. törvény és a rendőrség hatásköréről és illetékességéről szóló 25/2013 (IV.24) BM rendelet és további, az ügyek szempontjából szükséges jogszabályok szem előtt tartásával végzi. Minden büntetőeljárás megindításánál az első lépés a hatáskör és illetékesség vizsgálata, amely alapján az elkövetés helye, jellege, az elkövetett kár mértéke alapján folytatja le az arra jogosult szerv a vizsgálatot. Továbbá az Európai Unió tagállamai között folytatott bűnügyi jogsegély- bűntetőügyekben folytatott együttműködés, valamint európai elfogatóparancs alapján folytatott átadási eljárás[65], illetve nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény alapján segítik a határon átnyúló bűncselekményekkel kapcsolatos kényszerintézkedések végrehajtását, az elkövetők elfogását és azok kiadatását, átadását. Többek között ez utóbbi két jogszabály valamint nemzetközi szerződések (két vagy több fél által megkötött multilaterális szerződések) is segítik a számítógépes bűncselekmények nemzetközi jellegével összefüggő nehézségek leküzdését a nyomozó hatóságok között.

Mivel a nyomozással kapcsolatos problémák elsődlegesen a rendőrség feladatainak végrehajtása során fordul elő, így összességében azzal kívánunk foglalkozni, míg a fejezetben az Alaptörvényhez igazodva, a rendőrség mellett a nemzetbiztonsági szervezetek számítógépes bűnözés mellett jelentkező kibervédelmi és kiberbiztonsági kihívásait is tárgyaljuk.

3.2 Terrorelhárítási Központ

Az Rtv. hatálya alá tartozó szervezet továbbá a Terrorelhárítási Központ, amely nem a számítógépes bűncselekményekkel, sokkal inkább a kibervédelemmel kapcsolatos feladataik ellátása miatt szükséges egy röviden foglalkozni a terrorcselekmények elhárításával, megakadályozásával és megelőzésével kapcsolatos szervezettel.

A Terrorelhárítási Központ feladatát egyrészt az 1994.évi XXXIV. törvény határozza meg, valamint a 295/2010. (XII.22.) Korm. rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól. A rendőrségről szóló törvény és az említett kormányrendelet alapján a TEK nyomozati jogkört nem gyakorol - ugyanakkor a 2012. évi C.

[65] 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről

törvényben, a Büntető Törvénykönyv 314-316.§-ban taglalt terrorcselekménnyel összefüggésben az internet felhasználásával történő szerveződést, terrorsejtek szerveződését, az ezekkel összefüggésben történő szerveződéseket, csoportokat, személyeket felderít és megfigyelhet, valamint a kritikus infrastruktúrák vagy az azokon kívüli kiemelt létesítmények – akár azok informatikai rendszereinek - védelme, az ellenük történő támadás megakadályozása, felderítése és *azok védelmére vonatkozó nemzeti program kidolgozásában, a veszélyeztetettség értékelésében és biztonsági intézkedési tervek kidolgozásában*.[66]

Ahogy említettük nem rendelkezik a klasszikus értelemben vett nyomozati jogkörrel, így a törvényben előírt tevékenysége során az Rtv. 7/E.§-a alapján együttműködik a rendőrséggel, valamint a magyar nemzetbiztonsági szolgálatokkal és külföldi titkosszolgálati szervezetekkel is.

3.3 Nemzeti Adó- és Vámhivatal (NAV)

A Nemzeti Adó-és Vámhivatal feladatai a klasszikus adó és illetékkiszabások mellett a büntetőeljárások lefolytatása. A NAV Bűnügyi Főigazgatóság Központi Nyomozó Főosztály Információtechnológiai Osztály feladata a különböző informatikai eszköz felhasználásával elkövetett jogellenes cselekmény nyomozása. A Főigazgatóság hatáskörébe tartozik az egy milliárd forintot meghaladó értékre üzletszerűen, vagy bűnszövetségben elkövetett bűncselekmények, a bűnszervezetben elkövetett bűncselekmények, valamint az olyan bűncselekmények nyomozása, amelyeket az elkövető személye, vagy az elkövetés körülményei, illetve a bűncselekmény társadalomra való veszélyességének kiemelkedő foka miatt a Bűnügyi Főigazgatóság hatáskörbe vont, illetve utalt bűncselekmények nyomozása.

- az interneten elkövetett bűncselekmények felderítés és nyomozása
- az internetes keresés, monitorozás, nyomrögzítés és az online szemlék
- helyszíni adatmentések (live forensic)

[66] „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.), 20, https://net.jogtar.hu/jogszabaly?dbnum=1&docid=A1000295.KOR&mahu=1 3.§ (1) bekezdés c.] pontja. Letöltve: 2018. szeptember 21.

- együttműködés a magyarországi jogvédő szervezetekkel (Pro Art, Artisjus), a Készenléti Rendőrség Nemzeti Nyomozó Irodával és a Nemzeti Kibervédelmi Intézettel

- nemzetközi együttműködés, bűnügyi jogsegélyek teljesítése (pl.: Europol Copy, IOS akciók)

- konferenciák és képzések tartása.

A szerzői vagy szerzői joghoz kapcsolódó jogok bűncselekménye során az IT osztály feladata internetes monitorozás, azon során a jogsértések feltárása a jogsértés módjának meghatározása, továbbá az okozott vagyoni hátrány meghatározása, a jogsértő azonosítása, a Btk.77.§-a alapján a jogsértő adat eltávolítására tett indítvány és annak ellenőrzése.

3.4 A magyarországi kibervédelemmel és kiberbiztonsággal foglalkozó szervezetek

A számítógépes bűncselekmények mellett több szakirodalom is említi a kibervédelmet is és kiberbiztonságot. Amennyiben az elmúlt években bekövetkezett globális kibertámadásokra gondolunk, amelyek veszélyeztették az államok biztonságát, a társadalmat és a gazdaságot, érzékeny adatokat és információkat szereztek meg vagy tettek hozzáférhetetlenné, ezen esetekben kiemelt feladata volt nemcsak a számítógépes bűncselekményekkel foglalkozó szervezeteknek, hanem a kibervédelemmel és kiberbiztonsággal összefüggő állami- és a magánszférához tartozó szerveknek is. A feltűnt zsaroló- és trójai vírusok, a malware-ekkel elkövetett támadásokra, azok veszélyére és a kötelező, illetve ajánlott cselekvésekre adnak választ az országok kibervédelmi stratégiái, valamint az azok végrehajtására felhatalmazott szervezetek.

3.4.1 Nemzeti Kibervédelmi Intézet

A Nemzetbiztonsági Szolgálat Nemzeti Kibervédelmi Intézet (röviden: NBSZ NKI) rövid ismertetése szintén megkerülhetetlen. Habár közvetlenül nem is tartozik a számítógépes bűncselekmények nyomozását végző szervezetek közé, ennek ellenére feladatuk szorosan összefügg a számítógépes, pontosabban a kibertérben elkövetett jogellenes cselekményekkel,

amikor is riasztást, jelzést és értesítést tesznek közé a hivatalos honlapjukon és közösségi médián keresztül a rosszindulatú kibertámadásokkal, interneten vagy más kommunikációs eszközön keresztül érkező adathalász levelekkel, infokommunikációs eszközöket és rendszereket érő sebezhetőségekkel kapcsolatban, továbbá a többi kibervédelemmel foglalkozó szervezeteknek (CERT-eknek) és együttműködnek a nyomozást folytató hatóságokkal is.

Az Ibtv. 2015. évi módosításának eredményeként 2015. október 1-jén megalakult a Nemzeti Kibervédelmi Intézet- a Nemzetbiztonsági Szakszolgálat keretei között-, amelyen belül három szakmai szervezeti terület került elkülönítésre a tevékenységüknek megfelelően:

- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterület (a Kormányzati Eseménykezelő Központ, azaz a GovCERT);

- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);

- a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási-, és sérülékenység vizsgálati (GovCERT) szakterület.[67]

A három terület mellett az NKI feladata még többek között a honvédelmi és a kritikus információs infrastruktúrák védelme, de a kibertámadásokkal kapcsolatos feladatok elvégzése is.

A GovCERT alapvető feladata az állami és önkormányzati szervek informatikai biztonsági támogatása, amely egyrészt preventív jellegű, (értve ezalatt a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követését és a sérülékenység menedzsmentet), másrészt pedig reaktív jellegű, a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően - a kezelésük koordinációjára irányul.

A sérülékenység menedzsment során GovCERT információkat gyűjt a szoftver-sérülékenységekről és káros szoftverekről, megvizsgálják azok relevanciáját az állami IT rendszerek tekintetében és általános körben vagy célzottan tájékoztatják a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében ezen rendszereket üzemeltetőket. Az

[67] forrás: NKI

incidenskezelési tevékenység során a GovCERT 24 órás ügyeletet működtet, ahol folyamatosan fogadja az IT rendszereket érő incidensek bejelentéseit, és megteszi az alapvető intézkedéseket (incidens nyilvántartásba vétele, bejelentő visszatájékoztatása, alapvető információk azonosítása, stb.). A bejelentett incidens felszámolása során a következő lépés a jogosultsággal és/vagy képességgel rendelkező szerv/személy tájékoztatása a teendőkről, szükség esetén kapcsolattartás a bejelentővel, valamint az érintett incidens felszámolásának nyomon követése (incidens-koordináció). Amennyiben szükséges, az incidensre utaló jelek alapján a GovCERT összegyűjti az incidens felderítéséhez szükséges információkat (pl. naplóadatok) és ezek elemzésével megkísérlik rekonstruálni az incidens kiváltó okait, egyúttal javaslatot tesznek a hasonló incidensek megelőzését vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekre.

A Nemzeti Kibervédelmi Intézet mellett a kibertérrel összefüggő veszélyekkel és támadásokkal kapcsolatban egyéb- a disszertációhoz nem kapcsolható- feladatai vannak a Katonai Nemzetbiztonsági Szolgálatnak, a Magyar Honvédségnek, de ezeket most nem szerettük volna részletezni.

3.5 Az Európai Unió számítógépes bűnözés elleni fellépésének szervezetei

A számítógépes bűncselekmények számának évről évre történő növekedése és az elkövetők által okozott gazdasági, erkölcsi károk, és nem utolsó sorban az államok és állampolgárok biztonságának veszélye miatt az Európai Unió folyamatos lépéseket tesz annak érdekében, hogy megfelelően fel tudja venni a harcot ennek a folyamatosan fejlődő bűncselekménynek a megakadályozása és megelőzése érdekében.

Az Európai Unió 1993-ban a maastrichti szerződéssel hozta létre a II. pillérként a közös kül- és biztonságpolitika dimenzióját az Unió közös értékének, alapvető érdekeinek, függetlenségének megőrzése miatt az ENSZ Alapokmányával, a Helsinki Záróokmány alapelveivel és a Párizsi Charta céljaival összhangban.[68]

[68] Várnay Ernő-Papp Mónika: Az Európai Unió joga (KJK Kerszöv. 2005) 845.

Ugyanakkor mégsem a II. pillérben- hiszen abban a kiberbiztonsággal kapcsolatos szabályozás foglalt helyet, hanem az Unió III. pilléréhez, az igazságügyi együttműködéshez tartozott a számítógépes bűncselekmények.

Az Unió lisszaboni szerződés értelmében- amely megszüntette a hárompilléres szerkezetet[69]- *„az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében elfogadott irányelvekben szabályozási minimumokat állapíthat meg a bűncselekményi tényállások és a büntetési tételek meghatározására vonatkozóan az olyan különösen súlyos bűncselekmények esetében, amelyek jellegüknél vagy hatásuknál fogva a több államra kiterjedő vonatkozásúak, illetve amelyek esetében különösen szükséges, hogy az ellenük folytatott küzdelem közös alapokon nyugodjék.*

Ezek a bűncselekményi területek a következők: terrorizmus, emberkereskedelem és a nők és gyermekek szexuális kizsákmányolása, tiltott kábítószer-kereskedelem, tiltott fegyverkereskedelem, pénzmosás, korrupció, pénz és egyéb fizetőeszközök hamisítása, számítógépes bűnözés és szervezett bűnözés."[70]

A fentiek fényében az Európai Unió nemcsak irányelveket, ajánlásokat fogalmazott meg a számítógépes bűncselekmények aktuális kihívásaira, hanem a nyomozással és az igazságszolgáltatással kapcsolatos szerveket is létrehozott.

3.5.1 Európa Tanács (ET)

Az ET 2001. november 23-án Budapesten fogadta el a Számítástechnikai bűnözésről szóló egyezményt (Convention of Cybercrime). Az Egyezmény 2004. július 1-jén lépett életbe. Az Európa Tanács 5 tagállama – így Magyarország[71] is – ratifikálta a konvenciót. 2011. október 1-ig az Európa Tanács 31 tagja, valamint az Egyesült Államok részéről is az egyezmény elfogadásra és törvénybe iktatása megtörtént. A számítástechnikai bűnözésről szóló

[69] Urszán József: A súlyos és szervezett bűnözés elleni fellépés feladatai az Európai Unióban (forrás: www.nemzetesbiztonsag.hu/letoltes.php?letolt=406, letöltve: 2019. március 12.)
[70] Lisszaboni szerződés 69/b cikke
[71] „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. letöltve: 2018. szeptember 20.

egyezményt a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv[72] követte.

A Számítástechnikai Bűnözésről szóló Egyezmény védeni kívánja a számítástechnikai rendszerek, a hálózatok, az adatok hozzáférhetőségének sérthetetlenségét, az ilyen rendszerek titkosságát. Biztosítani kívánja a rendszerek, a hálózatok, az adatok visszaélésszerű használatának megelőzését és bűncselekménnyé nyilvánítását is. Továbbá meghatározza a számítógépes bűnözés elleni hatékony fellépést lehetővé tévő felderítést, a nyomozást és bűnüldözést a nemzeti és nemzetközi szinten. Az értelmező rendelkezések körében az egyezmény több alapfogalmat definiál, mint számítástechnikai rendszer (computer system), számítástechnikai adat (computer data), szolgáltató (service provider), illetve forgalmi adat (traffic data), viszont a számítástechnikai bűncselekmény (cybercrime) fogalmának meghatározásával adós marad. Az egyezmény a büntető anyagi jogi szabályok körében négy csoportra osztja a bűncselekményeket. Az első csoportot a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények, a második csoportot a számítógéppel kapcsolatos bűncselekmények, a harmadik csoportot a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények, a negyedik csoportot pedig a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények jelentik.

3.5.2 Az Európai Unió Tanácsa

Az Európai Tanács megbízásából készült 1994-ben az Információs társadalommal[73] szemben tanúsított alábbi elvárásokat (célkitűzéseket) fogalmazta meg:

- az informatikai eszközöket szabványosítani kell;
- ha nem szabványosak az eszközök, elveszik a lényeg, az információáramlás;
- azért kell szabványosítani, mert az üzleti élet, a versenyszféra ellenérdekelt;
- a monopolhelyzetek megszüntetése, különös tekintettel a telekommunikációra;

[72] „A Számítástechnikai Bűnözésről szóló Egyezménynek a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyve” (é. n.).
[73] Komanovics Adrienne: Információszabadság az Európai Unióban, Pécs 2007, doktori értekezés

- a jog hosszú ideig elfogadta a monopolhelyzetet, mert a beruházás e területeken nagyon sokba kerül, de most már nem fogadják el ezt az érvelést;

- a szellemi alkotások megfelelő szintű védelme;

- a szerzői jogban ez teljesen új terület, a zene-, kép-, film-letöltések, amire még (akkor sem volt és ma sincs) nincs megfelelő szabályozás, védelem;

- a magánszféra védelme, mivel ez van kitéve a legnagyobb veszélynek. Felismerték, hogy a mai világban a magánszférát egyetlen eszközzel lehet védeni, és ez a jog. A magánszemélyt technikai eszközzel már nem lehet az állammal szemben megvédeni;

- az adatbiztonság szabályainak kidolgozása (A vírusok elleni védelemmel összefüggésben az Európai Tanács megállapította, hogy olyan rendszert nem lehet építeni, amibe nem lehet belenyúlni, de olyat igen, hogy ez ne maradjon észrevétlen);

- a Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról.

Az Európai Unió Tanácsa 2005 februárjában elfogadta az információs rendszerek elleni támadásról szóló kerethatározatot[74], amelyben a korábban használatos számítógépes rendszer fogalom helyett már az információs rendszer (information system) fogalom jelenik meg. Az egyes fogalmak összevetésekor megfigyelhető, hogy annak ellenére, hogy a megjelölés különbözik (információs rendszer – számítógépes rendszer) a fogalmak tartalma gyakorlatilag megegyezik.

A kerethatározat az üldözendő magatartásokat a következőkben csoportosítja:

1. Információs rendszerekhez való jogsértő hozzáférés

2. Rendszerbe való jogsértő beavatkozás

3. Adatokba való jogsértő beavatkozás

[74] A Tanács 2005/222 IB Kerethatározata az információs rendszer elleni támadásokról (forrás: https://publications.europa.eu/hu/publication-detail/-/publication/708d86d8-ab9a-4e18-9bda-ac37405a3185, letöltve: 2019. március 20.)

A kerethatározatot 2013-ban felváltotta az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv[75]. Az új irányelv különös figyelmet fordít az úgynevezett botnetekre és a személyazonossághoz kapcsolódó bűncselekményekre, valamint súlyosabb szankciókat helyez kilátásba abban az esetben, ha az informatikai bűncselekményt bűnszervezetben követik el. Ezen felül előírja, hogy a büntetőeljárás során figyelembe kell venni azt a körülményt, ha a bűncselekményt az elkövető alkalmazotti minőségben követi el.

3.5.3 Európai Unió Belső Biztonsági Állandó Bizottsága (COSI)

Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) meghatározta a stratégiai célokat a számítógépes bűnözés területén. Az Állandó Biztonság célja a belső biztonság területén, hogy megkönnyítse a tagállamok közötti operatív tevékenységek koordinálását. A belső biztonsággal kapcsolatban ez, az operatív együttműködéssel kapcsolatos rendőrségi és vámügyi együttműködést, a külső határok védelmét és a büntetőügyekben folytatott igazságügyi együttműködést érinti. A COSI operatív szerepére tekintettel Magyarországot a Belügyminisztérium képviseli.

A 2014-2017 közötti időszakban a COSI elsősorban

- a nagy károkozással járó, online és bankkártyás fizetéssel összefüggő, továbbá
- az áldozatok részére komoly hátránnyal járó – például a gyerekek sérelmére elkövetett – számítógépes bűncselekmények, valamint
- a kritikus infrastruktúrát és számítógépes rendszereket érintő informatikai bűncselekmények tekintetében kíván hatékony lépéseket tenni a kialakítandó védekezés érdekében[76].

A stratégia kitér a lehetséges informatikai rendszer-sebezhetőségek beazonosításának problematikájára is. Az informatikai támadásokat okozó bűnözést illetően is definiálásra kerültek a problémák, így például:

[75] Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltozásáról (forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32013L0040, letöltve: 2019. március 21.)
[76] Europol jelentése (forrás: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017, letöltve: 2019. március 23.)

- kevés információ a bűnözői hálózatokról;
- a kockázatokhoz kapcsolódó tudatosság hiánya;
- jogi akadályok fennállta az információcserében;
- az elégtelen bűnfelderítői együttműködés;
- az állam jogalkalmazó és igazságszolgáltató szerveinek elégtelen felkészültsége;
- az incidensek azonosításának és besorolásának országonként eltérő formája;
- a civilszféra alacsony szintű bevonása;
- az Európai Unión kívüli cselekmények jelentős hatása;
- az alacsony mértékű felderítés;
- a kis szám a bűnelkövetői elfogások terén[77].

A COSI a 2018-2021-es időszakra vonatkozóan továbbra is prioritásként kezeli a szervezett bűnözés és a kiberbűnözés kérdését, amikor is kiemeli, hogy a kibertámadások 400 milliárd euró kárt okoznak évente és három további területre kíván a jelzett időszakban összpontosítani[78]:

- fellépés az informatikai rendszerek elleni támadásokkal szemben
- a készpénz-helyettesítő fizetési eszközökkel való visszaélések felszámolása
- a gyermekek online biztonságának fokozása, többek között a gyermekbántalmazást ábrázoló tartalmak előállítása és terjesztése elleni küzdelem révén.

[77] „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. Letöltve: 2017. október 30.

[78] Európai Tanács, Az Európai Unió Tanácsa: A szervezett bűnözés elleni küzdelem az Unióban (forrás: https://www.consilium.europa.eu/hu/policies/eu-fight-against-organised-crime-2018-2021/, letöltve: 2019. március 22.)

3.5.4 Az Európai Rendőrségi Hivatal (Europol)

Az Európai Unió bűnüldöző hatósága, amelynek fő feladata, hogy tevékenységével segítse az Unió biztonságosabbá tételét. Az Európai Unió kormányközi, koordinációs és jogi végrehajtó szervezete. Feladatai közé tartozik az EU tagállamok hatóságainak támogatása, a kölcsönös információ-megosztás a nemzeti rendőrségekkel és a különböző bűnügyi adatok szakszerű elemzése. Hatáskörébe tartozik többek között a terrorizmus, a kábítószer-kereskedelem, a nemzetközi szervezett bűnözés, az ipari jog megsértése és termékhamisítás, az illegális bevándorlás, továbbá a lopott autók csempészése, a pénzmosás és az euró hamisítása elleni fellépés és megelőzés[79].

Hivatalos ügynökséggé 2010-ben vált, ezáltal egy sokkal integráltabb együttműködés kialakítása, kidolgozása lett a fő feladata. Az Europol célja, hogy javítsa az európai bűnüldöző hatóságok eredményességét és együttműködését a nemzetközi bűnözés súlyos formái, a szervezett bűnözés és a terrorizmus megelőzésében és leküzdésében. Az Europol szorosan együttműködve végzi a tevékenységét az Európai Unió 27 tagállamának bűnügyi hatóságaival, csakúgy, mint az USA, Kanada, Ausztrália és Norvégia bűnüldöző szerveivel. Ennek eredményeképp az Europol évi 13.500 határokon átnyúló nyomozáshoz nyújt hathatós segítséget elsősorban az adatbegyűjtés, - elemzés, és -megosztás, valamint a koordináció eszközeivel. Az Europol eseti alapon részt vesz még a tagállamok területén tevékenykedő, ún. Közös Nyomozó Csoportok munkájában, ahol speciális eszközökkel és információkkal segíti a bűntények felderítését. Az Europol munkáját ezen felül segíti még a tagállamok és partnerországok által delegált, mintegy 145 összekötő tiszt is, akik az Europol székházában, Hágában tartanak fenn irodát, és a minél gyorsabb és hatékonyabb együttműködést, a személyes kapcsolatokat és a kölcsönös bizalom kiépítését segítik elő.

Az Europol 1999. július 1-jén kezdte meg teljes körű működését, azt követően, hogy a tagállamok ratifikálták az Europol-egyezményt. 2010. január 1-jén az ezen egyezmény helyébe lépő, az Európai Rendőrségi Hivatal (Europol) létrehozásáról szóló 2009. április 6.-i, 2009/371/IB számú tanácsi határozat (tanácsi határozat) elfogadása után, az Europol új jogi kerettel és kiterjesztett feladatkörrel rendelkező, teljes jogú uniós ügynökséggé vált.

[79] Tóth Tamás: Az Europol tevékenysége (Nemzet és Biztonság 2012/5-6. szám) 72-73.

Az Europol segíti az EU tagállamait a bűnüldözési tevékenységek során, például az alábbi területeken[80]:

- tiltott kábítószer-kereskedelem
- terrorizmus
- embercsempészet, emberkereskedelem és gyermekek szexuális kizsákmányolása
- iparjogvédelmi jog megsértése és termékhamisítás
- pénzmosás
- pénz- vagy egyéb fizetőeszköz hamisítása – az Europol az euró hamisítás elleni küzdelem legfőbb európai felelőse.

Az Europol tagállamoknak nyújtott támogatása a következőket foglalja magába:

- az információcsere és a bűnügyi hírszerzés megkönnyítése az európai bűnüldöző hatóságok között az Europol információs és elemző rendszerei, valamint a biztonságos információcsere-hálózati alkalmazás (SIENA) segítségével
- a tagállamok műveleteihez műveleti elemzés készítése, illetve támogatás nyújtása
- a tagállamoktól vagy egyéb forrásból, illetve az Europoltól származó információk és adatok alapján stratégiai jelentések (pl. veszélyértékelések) és bűnügyi elemzések készítése[81]
- szakértelem és technikai támogatás biztosítása az EU-n belüli nyomozásokhoz és műveletekhez, az érintett tagállamok felügyelete és jogi felelőssége mellett.

Az Europol a fentieken kívül a bűnügyi elemzések elősegítésével, a nyomozási technikák harmonizálásával és a tagállamokban adott képzésekkel is foglalkozik.

Ezen feladatai ellátásában segíti az Europol Információs Rendszer (továbbiakban: EIS), amely lényegét tekintve az Europol bűnügyi adatbázisa, elsődleges ellenőrző rendszere. A rendszer

[80] Európai Unió- Europol (forrás: https://europa.eu/european-union/about-eu/agencies/europol_hu, letöltve: 2019. március 12.)
[81] Europol Work Programmes

működtetésének célja, hogy az Europol mandátumába tartozó, súlyos megítélésű (a Btk. szerint legalább 5 év szabadságvesztéssel fenyegetett), és legalább két tagországot érintő bűncselekmények esetén a tagállamokban folyamatban levő nyomozásokat összekapcsolja, ezáltal orientálva és támogatva a nemzeti bűnüldöző hatóságok operatív, műveleti tevékenységét[82].

Az EIS gyakorlati haszna abban áll, hogy segítségével megállapítható, hogy az Europol mandátumába tartozó ügyek esetében egy másik Europol tagország rendelkezik-e a hazai nyomozáshoz kapcsolható információval. „Találat" esetén a tagállamok adatszolgáltató nyomozó szervei a nemzeti egységek közvetítésével kapcsolatba léphetnek egymással, és megállapodhatnak az információk felhasználhatóságát illetően. Magyarországon az Europol nemzeti egység az Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központjában (ORFK NEBEK Iroda[83]) található.

Az EUROPOL felállított egy Csúcstechnológiai Bűnözés Elleni Központot, amely 3 területen tevékenykedik munkacsoportokban:

- a gyermekek szexuális kizsákmányolása
- készpénz-helyettesítő fizetési eszköz - csalások
- és a 3. munkacsoport, amelyből 2013 januárjában megalakult az EC3.

3.5.5 Europol-Számítástechnikai Bűnözés Elleni Központ (European Cybercrime Centre, EC3)

Az Európai Bizottság 2012. március 28-án nyújtotta be a javaslatát a számítástechnikai bűnözés elleni küzdelem európai központjának létrehozására, amely a Stockholmi Program egyik fontos eleme, amelynek célja a polgárok védelme, valamint a szervezett bűnözés és a terrorizmus elleni küzdelem javítása[84].

[82] Hugo Brady: Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime (A Journal of Policy and Practice, Volume 2, Issue 1, 2008) 103–109
[83] Hegyaljai Mátyás: A nemzetközi bűnügyi együttműködés (Kül-Világ IX. évfolyam 2012/4.) 3-4.
[84] Az Európai Tanács tájékoztatása. A Stockholmi Program (forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034, letöltve: 2019. március 16.)

A központot Hágában az Európai Rendőrségi Hivatalon belül hozták létre és működését 2013. január 11-én kezdte meg. A központ célja, hogy:

- európai kapcsolattartó pontként működjön a számítástechnikai bűnözés elleni küzdelemben,
- részt vegyen unión belüli rendészeti koordinációban,
- operatív támogatással segítse a tagállami rendészeti szerveket a konkrét nyomozások során.

A Központ feladata elsősorban a számítógépes bűnözés elleni harc koordinálása, különös hangsúlyt fektetve a nagy nyereséggel járó bűnözés elleni tevékenységre. A további feladatok között megtaláljuk még a személyazonosság-lopás elleni küzdelmet, az elektronikus bankszolgáltatásokat érintő bűncselekmények elleni harcot, a gyermekek szexuális kizsákmányolása elleni harcot, illetve az Európai Unió kritikus infrastruktúráinak és informatikai rendszereinek korlátozott védelmét[85].

Az EC3 45 főből áll, többek között elsőrendű kibernetikai szakértőkkel kezdte meg tevékenységét, nincs önálló nyomozati jogköre.

A célok tükrében az EC3-nak 5 feladatköre van tehát:

- Az adatgyűjtés a számítógépes bűnözésről. Ezen adatok feldolgozása, egy számítógépes bűnözési helpdesk üzemeltetése a tagállami nyomozó hatóságok részére
- A számítógépes bűnözés elleni nyomozás támogatása a tagállamok számára, azzal, hogy támogatja a közös nyomozócsoportok létrehozását egy vagy több tagállam együttműködésével, valamint megteremti és koordinálja a tagállamok közötti együttműködést a számítógépes bűncselekmények nyomozásában. Továbbá szoros együttműködést teremt az EUROJUST-tal és az INTERPOL-lal.
- Értékeli és elemzi a kibertérből érkező fenyegetéseket, módszereket és ezekből előrejelzi a számítógépes bűnözés alakulását.

[85] Szentgáli Gergely: Az Európai Unió kiberbiztonsági törekvései és szervezetei II. (Hadmérnök, VIII. évfolyam 1. szám, 2013. március) 299-300.

- A magánszférával történő szoros együttműködés, valamint a CERT-ekkel történő kapcsolattartás annak érdekében, hogy felkészültek legyenek a kibertámadásokkal kapcsolatban és fel tudjanak lépni ellene.

- K+F és a képzés során szorosan együttműködik a CEPOL-lal, a tagállamok nyomozó hatóságaival és igazságügyi szervezeteivel, akiknek a folyamatos képzését, forenzikus eszközeik fejlesztését támogatja.

Az EC3 hatáskörébe tartozó fókuszpontok a számítógépek és a hálózati infrastruktúrák ellen végrehajtott bűncselekmény kivizsgálása, valamint a különböző internetes bűncselekmények (FP Cyborg), a gyermekek szexuális kizsákmányolása (FP Twins) mellett a bankkártyákkal történő csalások és a személyes adatokkal történő visszaélések is (FP Terminal).

A Központ kiemelt feladata, hogy figyelmeztesse a tagállamokat az esetleges fenyegetettségekre. Szintén lényeges lépés az online szervezett bűnözői csoportok felkutatásának és azonosításának támogatása, ezt erősítve a Központ tagállami szinten is képes segítséget nyújtani konkrét nyomozásokhoz.

3.5.6 Európai Kiberbűnözés Elleni Akciócsoport (European Cyber Crime Task Force)

Az akciócsoportot 2010-ben alakították. A szakértői csoport az Europol, az Eurojust és az Európai Bizottság képviselőiből, valamint a tagállami számítógépes bűnözéssel foglalkozó egységek vezetőiből áll. A csoport hozzájárul az informatikai bűncselekmények elleni küzdelem harmonizált európai megközelítésének fejlesztéséhez és támogatásához, valamint célba veszi azokat a problémákat, amelyeket az információs technológia bűncselekményekhez való felhasználása okoz[86].

[86] Europol (forrás: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, letöltve: 2019. március 20)

3.5.7 The European Union's Judicial Cooperation Unit (Eurojust)

A szervezetet a Tanács 2002/187/IB határozata hozta létre, amelyet a Tanács 2008. december 16-i 2009/426/IB határozata módosított (Eurojust Határozat)[87]. Az Eurojust feladata a nemzeti nyomozó hatóságok és ügyészségek hatékonyságának növelése a határokon átívelő, súlyos és szervezett bűncselekmények ügyeiben, és végső soron annak előmozdítása, hogy a bűncselekményt elkövetők felelősségre vonása gyorsan és eredményesen megtörténjék. Az Eurojust 2002-ben jött létre. A 28 tagállam mindegyike magas beosztású nemzeti képviselőt delegál a Hága székhelyű Eurojusthoz, akik tapasztalt ügyészek, bírák, vagy velük azonos hatáskörű rendőrtisztek. Ők végzik az Eurojust feladatait a nemzeti hatóságok nyomozásainak és ügyészi eljárásainak koordinálásában. Ugyanakkor a tagállamok jogrendszereinek különbözőségéből adódó nehézségeket és gyakorlati problémákat is megoldanak. A nemzeti tagokat helyetteseik, asszisztenseik és kiküldött nemzeti szakértők segítik. Azoknak a harmadik államoknak, amelyekkel az Eurojust együttműködési megállapodást kötött, összekötő ügyésze vagy bírója lehet az Eurojustnál. Ilyennel jelenleg Norvégia és az Egyesült Államok rendelkezik. Az EU jog lehetővé teszi, hogy az Eurojust összekötő ügyészt vagy bírót küldjön harmadik államokba. Az Eurojust ad otthont az Európai Igazságügyi Hálózat, a népirtás, emberiség és háborús bűncselekmények elleni kontaktpontok hálózata, továbbá a közös nyomozócsoportok szakértői hálózata titkárságának is.

Az Eurojust mintegy 260 fős EU személyzettel rendelkezik, amely segíti a nemzeti hatóságok és az EU szervek kéréseire való gyors reagálást is. Partnerei mind a nemzeti hatóságok, mind az olyan EU formációk, mint pl. az Európai Igazságügyi Hálózat, az Europol, az OLAF (amennyiben az Európai Unió pénzügyi érdekeit érintő bűncselekményről van szó), a Frontex, a Sitcen, a Cepol, az Európai Igazságügyi Képzési Hálózat, továbbá minden más, a szerződések keretein belül elfogadott rendelkezések alapján kompetens szerv[88].

Az Eurojust 2017-es éves jelentése alapján 70 számítógépes bűncselekményekkel összefüggő ügyekben és többek között aktívan részt vett a 2017-ben világszerte több kritikus infrastruktúrát is érő No Petya-zsarolóvírus támadással kapcsolatos nyomozásokban[89].

[87] Eurosjust Hivatalos Honlapja (forrás: http://www.eurojust.europa.eu/Pages/languages/hu.aspx, letöltve: 2019. március 20.)
[88] 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)
[89] Eurojust: Éves jelentés 2017

3.6 A kibervédelem és kiberbiztonság európai szereplői

Ahogy a magyarországi szervezetek között is fontosnak tartottuk, hogy a kibervédelemmel és a kiberbiztonsággal foglalkozó szervezeteket is megemlítsük, így az Európai Unió ezen szereplőit is megemlítjük, mint a számítógépes bűncselekményekkel is kapcsolatos szereplőket.

3.6.1 ENISA (European Network and Information Security Agency)

Az Európai Unió Hálózat- és Információbiztonsági Ügynökség (ENISA) szakértői központként működik Európában. Az Ügynökség székhelye Görögországban, Kréta szigetén, Heraklionban található, az operatív irodai Athénban van. ENISA aktívan hozzájárulj a magas szintű hálózat- és információbiztonság fenntartásához (NIS) az Unión belül.

Az Ügynökség szorosan együttműködik a tagállamokkal és a magánszektorral, azért, hogy tanácsot és megoldásokat találjon a kiberbiztonság megteremtéséhez. Ez magában foglalja nemcsak a páneurópai kiberbiztonsági gyakorlatok szervezését, a fejlesztését a National Cyber Security stratégiákat, a CSIRT együttműködést és kapacitásbővítést, hanem tanulmányok elkészítését a biztonságos „cloud" rendszerek elfogadására, az adatvédelmi kérdésekről, az adatvédelmet erősítő technológiákról és a magánélethez kapcsolódó új technológiákról (eIDs= e-személyigazolvány), és meghatározza a számítógépes fenyegetések és mások aktuális trendjeit. Az ENISA is támogatja, kidolgozza és végrehajtja az Európai Unió kiberbiztonsági politikájával és azokat érintő jogokkal kapcsolatos ügyeket[90].

ENISA tevékenységének három területe:

- Ajánlások
- Tevékenységek, amelyek a politikai döntéshozatal és végrehajtás
- „Hands On" munka (amikor az ENISA együttműködik közvetlenül műveleti csoportokkal az Unión belül).

[90] Szentgáli Gergely: Az Európai Unió kiberbiztonsági törekvései és szervezetei II. (Hadmérnök, VIII. évfolyam 1. szám, 2013. március) 296.

3.6.2 ITU, azaz az International Telecommunications Union (ITU)

Az informatikai bűncselekmények elleni nemzetközi fellépés szükségessége, az internacionális együttműködés hatékonysága nem lehet kétséges a deliktumok országok határait átlépő jellege miatt. A digitális világ védelmében és biztonságának megőrzésében, azaz összefoglaló néven a kiberbiztonság eszközeinek tekinthető intézkedések megtételéhez relatíve egységes fogalmak kellenek. A kiberbiztonság jogi, technikai és szervezeti kihívásokat jelent és mivel ezek globális jellegűek, így szükségessé vált egy koherens, nemzetközi együttműködés keretein belüli stratégiának a kialakítása. Csak ilyen jellegű stratégia az, amely alkalmas az érintett országok szerepének meghatározására, illetve a már létező stratégiák számbavételére. A nemzetközi együttműködés szükségességét felismerve több internacionális szervezet foglalkozik a kiberbiztonság kérdésével. Ezek között is kiemelkedik az ITU az általa megalkotott Global Cybercrime Agenda, valamint az Európai Unió Kiberberbiztonsági Stratégiája.

Az ITU a kiberbiztonság fogalmát - a lényegi elemek meghatározásával - a következők szerint definiálja:[91] „*A kiberbiztonság azoknak az eszközöknek, politikáknak, biztonsági koncepcióknak, biztonsági intézkedéseknek, iránymutatásoknak, kockázatkezelési megközelítéseknek, cselekményeknek, képzéseknek, jó gyakorlatoknak, biztosítékoknak és technológiáknak a gyűjteménye, amelyeket fel lehet használni a kiberkörnyezet, valamint a szervezetek és a felhasználók eszközeinek védelmére*”[92].

Az Európai Unió Kiberbiztonsági Stratégiája[93] pedig következőképpen definiálja a fogalmat: „*A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket.”*

[91] „Recommendation X.1205 (04/08)”, Pub. L. No. X.1205 (é. n.), https://www.itu.int/rec/T-REC-X.1205-200804-I. letöltve: 2018. január 05.

[92] Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user’s assets

[93] „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.

Ezek a nemzetközi stratégiák a kiberbiztonságra vonatkozó fogalmi meghatározásukkal utat mutattak Magyarország nemzeti kiberbiztonsága fő irányainak kidolgozására, így került megalkotásra 2013-ban a Nemzeti Kiberbiztonsági Stratégiája.[94] A kormányhatározat a kiberbiztonság fogalmát az alábbiak szerint definiálta: „*a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez*."

Az említett stratégiákban a közös cél a kibertér, a virtuális környezet védelme az azt fenyegető támadásoktól, mind ezek a kiberbiztonság érdekében meghatározott eszközök és intézkedések alkalmazását jelentik.

3.7 Nemzetközi szervezetek a számítógépes bűnözés ellen

A nemzetközi és az uniós szervezeteket egy fejezetben, de nem egy alfejezetben gondoltuk tárgyalni, egymástól minimális mértékben elválasztva.

3.7.1 Egyesült Nemzetek Szervezete (ENSZ)

Az Egyesült Nemzetek Szervezete részéről több dokumentum foglalkozik az informatikai bűncselekmények megelőzéséről, kezeléséről, az információs technológiák elleni harcról[95]. Az 1994-ben kiadott kézikönyv - a számítógépes bűncselekmények megelőzéséről és kezeléséről a számítógépes bűncselekmény (computer crime), valamint a számítógéppel kapcsolatos bűncselekmény (computer-related crime) fogalmakat még nem határolja el. Felsorolja ugyanakkor a kézikönyv a leggyakoribb számítógépes bűncselekmény típusokat, mint a számítógép manipulációjával elkövetett csalás, a számítógépes hamisítás, a károkozás számítógépes adatokban vagy programokban, illetve a számítógépes adatok vagy programok

[94] „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. Letöltve: 2018. október 03.

[95] Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről (1994); Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról; Az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról.

megváltoztatása, a jogosulatlan hozzáférés számítógépes rendszerekhez és szolgáltatásokhoz, a jogi védelem alá eső számítógépes programok jogosulatlan reprodukálása.

A kézikönyv támaszkodik az 1989-ben született Európa Tanács által elfogadott Ajánlásra.[96] Felismerték, hogy a számítógépes környezetben elkövetett bűncselekményekkel szemben nem elegendő a területi védekezés, mivel az a deliktum jellege miatt egy kiterjedtebb kört veszélyeztet.

Ugyanakkor a gyermekpornográfia bűncselekménye vagy épp a cyberbullying, más néven elektronikus zaklatás miatt, kiemelést érdemel az 1989-es gyermekek jogairól szóló New York-i egyezmény, amely több szabályt is tartalmaz a gyermeknek a káros tartalmakkal szembeni védelméről.

Az ENSZ közgyűlése a 2000-ben elfogadott határozatában már az információs technológiák bűncselekményekhez való felhasználásával szembeni harcra hívja fel a figyelmet, és olyan intézkedéseket azonosított, amelyek segítenek az információs technológiákkal való visszaélés megelőzésében, illetve az információs technológiákkal való visszaélések elleni fellépés érdekében. Így pl. az államok jogszabályai és joggyakorlata számolja fel a védett zónákat az információs technológiákkal való visszaélések esetében. Az információs technológiákkal való nemzetközi visszaélések esetében koordinálni kell az érintett államok között a nyomozó hatóságok együttműködését a nyomozásban és a vádemelésben. Fontos, hogy információ megosztás legyen az államok között, a nyomozó hatóságok személyzetének kiképzése és felszereléssel ellátása, jogrendszereknek védeniük kell az adatok számítógépes bizalmasságát, integritását és elérhetőségét a jogosulatlan megkárosítástól, és biztosítaniuk kell, hogy a visszaéléseket büntetni rendelik, a jogrendszereknek lehetővé kell tenniük a bűnügyi nyomozásokkal kapcsolatos elektronikus adatok megőrzését, és az ezekhez való gyors hozzáférést. A határozat rámutat, hogy a nyilvánosság figyelmének felhívására, a személyes szabadságjogok és a magánélet védelmének, valamint a kormányzat cselekvési lehetőségeinek megőrzésére az ilyen jellegű visszaélések elleni küzdelemben.

[96] UN Manual on the Prevention and Control of Computer-Related Crime vagyis a Számítógépes Bűnözés megelőzéséről és szabályozásáról szóló tanulmány. http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf. Letöltve: 2018. október 22.

3.7.2 Bűnügyi Rendőrség Nemzetközi Szervezete (International Criminal Police Organization- Interpol)

Az Interpol[97] egyik célja, hogy globális szinten összefogja és koordinálja a számítógépes bűncselekmények felderítését. A feladataik ellátásához megalakították a Digital Crime Centert, amely leginkább a kutatással és az innovációval kapcsolatos teendőket látja el. Ezen központ mellett létrejött még a Cyber Fusion Center, amely a szervezet tagországainak nyújt segítséget a nyomozás kezdetétől annak befejezéséig. A két egysége létrehozta a forenzikus tevékenységével kapcsolatos szakértői laborját is, a Digital Forensic Laboratory-t.

Az Interpol feladata, hogy koordinálja és összehangolja a 190 tagállam közötti együttműködést a bűnüldözés területén, a technológiai és technikai fejlődés figyelemmel kísérése mellett a szakemberek folyamatos oktatása, felkészítése a számítógépes bűncselekmények változásainak megfelelően.

3.8 Konklúzió

A hazai, az európai és a nemzetközi nyomozást végző vagy az azzal összefüggő, de nem nyomozó szervek feladatai között szerepel a számítógépes bűncselekmények nyomozása, valamint a nemzetbiztonsági szervezetek. Mivel a nemzetbiztonsági szervek a 2017. évi XC. törvény szerinti klasszikus értelemben vett nyomozást nem folytatnak, így azokat a disszertációban nem kívánjuk megemlíteni, amely alól a Nemzeti Kibervédelmi Intézet kivételt képez.

Az Európai Unión belül működő szervezetek és az azon kívüli szervezetek számítógépes bűnözéssel kapcsolatos szerveit, szervezeteit és azok feladatai áttekintése révén megállapítottuk, hogy mind az Unió mind pedig azon kívül a jogalkotók a probléma kihívására igyekeznek reagálni, a legújabb technikai és technológiai felvetéseket a jog eszközével, így folyamatosan készített jelentésekkel, hatásvizsgálatokkal, a már meglévő szabályozások felülvizsgálatával, kiegészítésével hatályosítani.

A hazai gyakorlatban a számítógépes bűncselekmények területén is komolyabb előrelépés tapasztalható, amennyiben figyelembe vesszük, hogy már 2018-ban létrehozták az Országos

[97]Annual report 2017

Bírósági Hivatalon (továbbiakban OBH) belül a számítógépes bűnözéssel foglalkozó csoportot, akik szorosan együttműködnek szakosított intézményekkel és figyelemmel kísérik azokat a stratégiákat, amelyeket a digitális világ és kihívások negatívan érintenek.

A hazai ügyészség szervezetén belül is több ügyész foglalkozik a hagyományos bűncselekmények mellett a számítógépes bűncselekményekkel, részt vesznek képzéseken és továbbképzéseken Magyarországon és külföldön is[98].

[98] forrás: Fővárosi Főügyészség

4 A SZÁMÍTÓGÉPES BŰNCSELEKMÉNY ALANYAI

A számítógépes bűncselekmények nyomozásának problémáinak bemutatása a büntetőeljárásról szóló törvény felépítésének megfelelően ismertetjük, így a 4. fejezettől a statikus rész eljárási szabályait tárgyaljuk, míg a dinamikus részt nem vizsgáltuk, hiszen elsődlegesen a rendőrség által, a szó leghétköznapibb értelmében vett nyomozással kívántunk csak foglalkozni.

4.1 A különleges nyomozó szervek

A nyomozás feljelentéssel vagy a nyomozó hatóság, illetve az ügyészség hivatali hatásköréből kifolyólag tudomására jutott adatok alapján észleléssel indul[99]. Ezt követően a nyomozó hatóság vagy az ügyészség a rendelkezésre álló adatok alapján elrendeli a nyomozást, amelyről a sértettet haladéktalanul értesíti.

4.1.1 Készenléti Rendőrség Nemzeti Nyomozó Iroda

Magyarország egyik számítógépes bűncselekményekkel foglalkozó szervezete a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés elleni Főosztálya.

A Főosztály elődje 2007-ben alakult az akkor még Nemzeti Nyomozó Iroda Nyomozó Főosztály Csúcstechnológiai Bűnözés Elleni Osztályként, és jelenleg önálló főosztályként működik.

A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály 2017. január 1.-jén alakult, és három osztályra tagolódik. Az egyik osztály végzi a hatáskörükbe tartozó vagy magukhoz vont bűncselekmények nyílt nyomozását- így kihallgatásokat és a 2017.évi XC. törvényben felsorolt eljárási cselekményeket. A másik osztály a számítógépes bűncselekmények felderítését végzi a büntetőeljárásról szóló törvény, valamint az Rtv. alapján. A harmadik osztály a Forenzikus Osztály, feladata nemcsak a szervezetükön belüli, hanem más, hazai rendőri szervnek is a szakértői tevékenység elvégzése, támogatása, valamint egyéb

[99] 2017. évi XC. törvény a büntetőeljárás megindításáról

bűncselekmény során keletkezett adatok, elektronikus bizonyítékok mentése, értékelése, elemzése úgy, hogy azok alkalmasak legyenek a bíróság előtt a bizonyításra.

A KR Nemzeti Nyomozó Iroda a fent említett BM rendelet alapján a következőkben lehet röviden a feladatait meghatározni:

- büntetőeljárás lefolytatása
- operatív felderítés
- forenzikus tevékenység
- OSINT jelentések, elemzések készítése
- monitorozás
- rendezvény biztosítás
- hazai együttműködés
- nemzetközi együttműködés
- szakirányítás, segítségnyújtás
- a rendőri és igazságszolgáltatás egyéb területein dolgozók (ügyészek, bírók) oktatása

A Készenléti Rendőrség Nemzeti Nyomozó Irodának fontos szerepe van a nemzetközi bűnügyi jogsegélyek teljesítésével, a nemzetközi kapcsolattartásokban, nemzetközi nyomozó csoportokban való részvételben, hazai jogszabályok véleményezésében és szakmai fórumokon történő részvételben is.

A nemzetközi szervezetekkel való együttműködés és a nemzetközi bűnügyi jogsegélyek teljesítése mellett feladatuk szorosan összekapcsolódik többek között a hazai szervezetekkel, így a Nemzeti Kibervédelmi Intézet fentebb ismertetett feladataival és a forenzikus vizsgálatok és szakirányítási és oktatási feladataik révén valamennyi rendőr hatóság munkájával is.

4.1.2 Budapesti Rendőr-főkapitányság

A Készenléti Rendőrség Nemzeti Nyomozó Iroda mellett a Budapesti Rendőr-főkapitányságon is (röviden: BRFK) Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztály szintén a számítógépes bűncselekményekkel kapcsolatos nyomozásokat folytat, továbbá a BRFK kerületi rendőrkapitányságainak és más főosztályainak a forenzikus vizsgálatokat is elvégez.

Az általános szabály szerint, minden olyan deliktum esetében, amelynek tárgya vagy eszköze informatikai berendezés vagy információs rendszer és amennyiben nem éri el az elkövetési érték az 50 millió forintot, vagy egyéb minősítő körülmény nem merül fel, úgy az illetékességgel rendelkező kerületi rendőrkapitányság jogosult eljárni Budapest területén elkövetett jogellenes cselekmények esetén.

A bűncselekmény nyomozásának elrendelését követően vizsgálják az elkövetett cselekményt (a tényállás pontos tisztázása végett), az elkövetés helyét és idejét, amely alapján megállapítható, hogy a cselekmény bűncselekmény-e. Amennyiben bűncselekmény elkövetése megállapítható vagy egyszerű gyanú merül fel arra vonatkozóan, úgy a következő lépés annak megállapítása, hogy melyik hatóságnak van hatásköre az eljárás lefolytatására, illetve „kinek" az illetékességi területén történt. További fontos tényező, a bűncselekmény időpontjának megállapítása, amely az eljárás lefolytatásában vagy annak elutasításában is szerepet játszhat.

A számítógépes bűncselekményekkel kapcsolatos feljelentés esetében a fent említett vizsgálatok különösen fontos szerepet játszanak, hiszen éppen a számítógépes bűncselekmények jellemzői között felsorolt látencia és nemzetköziség miatt, előfordulhat[100], hogy

- A cselekmény már elévült
- Az eljárás lefolytatására a magyar hatóságok nem jogosultak.

[100] 2017. évi XC. törvény a büntetőeljárásról 381.§ c.), h.) a feljelentés elutasítása.

4.2 A hatáskörrel és illetékességgel kapcsolatos dilemma

A számítógépes bűncselekmények nyomozása szempontjából - az illetékesség megállapításának kérdésében - az elkövetés helyével, az ügyek oknélküli és értelmetlen áttételével, a hatóságoknak sokszor szándékukon kívül is sikerül a nyomozás hátráltatása. A nyomozás gördülékeny megindítása miatt szükséges tisztázni, hogy hogyan lehet megállapítani a kibertérben elkövetett bűncselekmények esetében az elkövetés helyét.

Az illetékesség az azonos szintű szervek közötti horizontális munkamegosztást jelenti. Azokat a szabályokat, amelyek a konkrét ügyben eljáró hatóságot Magyarország területi beosztásának megfelelően működő, azonos hatáskörű szervek közül jelölik ki az eljárásra, illetékességi szabályoknak nevezzük[101]. A már korábban említett BM rendelet 3.§-a alapján a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt - sorozat-bűncselekmények esetén a bűncselekmények többségét - elkövették. Amennyiben az elkövetés helye nem állapítható meg, vagy pedig a cselekmény jellegéből adódóan a több hatóság lenne jogosult lefolytatni az eljárást, akkor a megelőzés elve érvényesül, vagyis ott fogják az ügyet kivizsgálni, ahol korábban intézkedtek.

Az illetékesség tekintetében beszélhetünk:

- általános
- különös
- kizárólagos

illetékességről[102].

Az általános illetékességű nyomozó hatóságok a rendőrkapitányságok (így a kerületi és városi), a kiemelt illetékességű a megyei rendőrfőkapitányságok, a Budapesti Rendőr- Főkapitányság, valamint a Készenléti Rendőrség Nemzeti Nyomozó Iroda és a Reptéri Rendészeti Igazgatóság.

A számítógépes bűncselekmények esetében is első gondolatra sokakban az a válasz fogalmazódik meg, hogy ott követik el azokat, ahol maga az eszköz található.

[101] Fantoly Zsanett-Budaházi Árpád: Büntető eljárásjog I. Statikus rész (NKE Szolgáltató Kft., Budapest 2015.) 66.
[102] u.az

Ugyanakkor a válasz ennyire nem egyszerű ennél a deliktumnál, hiszen ma, amikor már az asztali számítógépek helyett laptopokat, tableteket és okostelefonokat használunk, amelyek mozgatása, helyváltoztatása nem ütközik nehézségbe, akkor már lehet érezni, hogy nem evidens a válasz. Például, amennyiben valaki útközben (két település között vagy éppen két ország között utazva követi el egy vállalkozás ellen a jogellenes tevékenységét, akkor annak megállapítása, hogy ki jogosult megindítani a nyomozást már ennyire nem egyszerű).

A nyomozó hatóság a hatáskörét és az illetékességét hivatalból vizsgálja[103], amennyiben valamelyik hiányát észleli, akkor átteszi a hatáskörrel és illetékességgel rendelkező nyomozó hatósághoz vagy ügyészséghez[104].

A büntetőeljárás megindulásakor jelentősége van, hogy az adott bűncselekmény hol „követődött el" és az eljárás lefolytatására melyik hatóságnak van hatásköre. Ez utóbbi meghatározását a nyomozó hatóság hatáskör-és illetékességével foglalkozó rendeletben[105] van lefektetve, annyi kitétellel, hogy késedelmet nem tűrő esetben bármely nyomozó hatóság végezhet eljárási cselekményt, azonban erről a hatáskörrel és illetékességgel rendelkező nyomozó hatóságot köteles haladéktalanul tájékoztatni[106].

Létezik az illetékesség megállapítására olyan nézőpont is, miszerint az elkövetés helye ott van, ahol maga a kibertérben elkövetett jogellenes cselekmény ténylegesen megvalósul (így fordulhatott elő az a probléma, amikor az elektronikus cégbejegyzés megjelent, akkor a cégbíróság székhelye szerinti kerületi kapitányságnál a közokirat-hamisítások miatt indított eljárások száma megsokszorozódott, mert valamennyi olyan ügyben, ahol cégbejegyzés, vagy cégváltozással kapcsolatban történt feljelentés vagy jogellenes cselekmény, azok a Fővárosi Cégbíróság helye szerinti kerületi kapitányságra lettek továbbítva).

A virtuális térben elkövetett cselekmények esetében jelenleg megszokott eljárás:

- azt, hogy hol követték el a bűncselekményt és a nyomozást lefolytatására jogosult szerv meghatározásával kapcsolatban jelenleg a 25/2013. (VI.24.) BM rendelet alapján: a

[103] „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 4.§ (1). letöltve: 2018. augusztus 18.
[104] 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről, 4.§ (2).
[105] 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről.
[106] Bánáti János és mtsai., *A büntetőeljárási törvény magyarázata - Az új, 2017. évi büntetőeljárási törvény magyarázata a kodifikációs bizottság korábbi tagjaitól* (Budapest: HVG-ORAC, 2018), 473.

nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt elkövették[107].

Problémaként merül fel, hogy kiberbűncselekmény[108] esetében az jogosult-e eljárni, akinek a területén észlelték a bűncselekményt vagy az a hatóság jogosult a nyomozást lefolytatni, akinek az illetékességi területén a jogellenes cselekményt elkövették, esetleg, ahol az elkövető bejelentett lakcímmel rendelkezik, életvitelszerűen tartózkodik?

Amennyiben elfogadjuk, hogy az elkövetés helye szerinti hatóság jogosult eljárni, akkor már csak azt kellene tisztázni, hogy számítógépes bűncselekmény esetében hol van az elkövetés helye?

Probléma az egyes bűncselekmény típusoknál, pl. az online hirdetéses csalások esetében, az hogy az elkövetés (tévedésbe ejtés) helye ott van, ahol az elkövető a szándékos megtévesztésre alkalmas dolgot vagy szolgáltatást feltöltötte és meghirdette, vagy ott van, ahol azt a sértett vagy sértettek megrendelték. A virtuális tér jellemzőit, az informatikai eszközök elterjedését, tulajdonságait figyelembe véve, ha annak megállapítása lehetetlen, hogy hol történt a tárgy hirdetésének feltöltése a hirdetési- vagy közösségi oldalra, akkor annak a hatóságnak kell lefolytatni az eljárást, ahol az elkövető lakik, ismeretlen tettes ellen folytatott nyomozás során, ahol a sértett él, több sértett esetén pedig a megelőzés szabályát kell alkalmazni vitás kérdésekben, azaz, ahol először tettek feljelentést egy adott bűncselekmény elkövetése miatt[109].

A számítógépes bűncselekmények jellemzői alapján el lehet mondani, hogy a virtuális térben elkövetett bűncselekmények esetében már problémát jelent az elkövetés helye, hiszen a világháló egy határok nélküli tér, amelyben az elkövetőnek és a sértettnek vagy áldozatnak még csak földrajzilag sem szükséges egy helyen tartózkodni, így annak megállapítása, hogy ki jogosult eljárni, a hatóságok között illetékességi vitát eredményez.

A hazai szakirodalom áttekintése során megállapítható, hogy a számítógépes bűncselekmények elkövetési helyének kérdéskörével kapcsolatban kevés tanulmány foglalkozik.

Az egyik ezzel foglalkozó szakirodalom Ibolya Tibor *A számítástechnikai jellegű bűncselekmények nyomozása című* tanulmányában[110] a sértett feljelentése nyomán az alábbi

[107] 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről 3.§ (1).
[108] A kibertérben elkövetett bűncselekményt értjük itt a kiberbűncselekmény alatt
[109]Ez a szabály természetesen csak a több sértett esetében érvényesül.
[110] Ibolya Tibor: *A számítástechnikai jellegű bűncselekmények nyomozása* (Budapest: Patrocinium, 2012), 37.

elkövetési helyeket és ezáltal feltételezem az illetékesség meghatározási problémáját is demonstrálja. A dilemma alapja szerint a vázolt jogeset, hogy a gyanúsított egy ismert aukciós portálon egy műszaki terméket hirdetett meg a bolti árnál jóval alacsonyabb értéken. A vételárat előre, egy meghatározott bankszámlaszámra kellett fizetni. A termékre több vidéki városból is érkezett megrendelés és pénzátutalás, amelyeket a gyanúsított egy budapesti bankfiókban felvette. Ez alapján Ibolya Tibor megállapításai a következők voltak:

- A cselekmény elkövetésének helye a gyanúsított lakóhelye, mert onnan töltötte fel a csalárd hirdetést,
- A cselekmény elkövetésének helye a bank budapesti fiókja, mert a gyanúsított ott vette fel a pénzt, „a kár ott következett be”
- A cselekmény elkövetésének helye a sértett számlavezető bankfiókjához igazodik, mert a sértett onnan utalta el a vételárat, a kár ott következett be
- A cselekmény elkövetésének helye a sértett lakóhelye, mert ott olvasta el a hirdetést
- A cselekmény elkövetésének helye az internetes honlap üzemeltetőjének székhelye, mert az elkövetési magatartást a gyanúsított az interneten tanúsította
- A „cselekmény elkövetésének helye az internet”, ezért az iratokat megküldik az ügyésznek állásfoglalásra.

Az említett dilemmák és lehetőségek a csalás (Btk. 373.§) tényállásával kapcsolatban kerültek bemutatásra, mégis valamennyi kibertérben elkövetett bűncselekmény esetében a hatóság számára problémát jelenthet, hogy ki illetékes az ügyben az eljárás lefolytatására. Az ügyészség álláspontja ugyanakkor, hogy az ügyek értelmetlen áttétele helyett azok gyors és eredményes lefolytatása legyen a cél és ne a kapitányságokon folyamatban lévő ügyek számának a csökkentése.

Az online csalásokkal kapcsolatban (nem az információs rendszer felhasználásával elkövetett csalás tényállása értendők ezalatt) a BH 2011/332. bírósági állásfoglalása szerint: az „*Internetes hirdetéssel megvalósított csalás esetén az elkövetési magatartás- a megtévesztés-akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot.*”

Ibolya Tibor ügyész úr továbbment az illetékesség fejtegetésekor, amikor azt írta, hogy fontos annak megállapítása, hogy a cselekményt a számítógép, mint célpont ellen vagy a számítógép, mint eszköz segítségével követték el[111].

A fent idézett BH esetében azonban érdemes megjegyezni, hogy azon bűncselekmények esetében alkalmazható, amelyik bár az internet felhasználásával valósul meg, de az csak közvetetten játszik szerepet a jogellenes cselekmény elkövetésében, de nem a kibertérben történik. Hiányossága, hogy az úgynevezett internetes hirdetéses csalások megvalósulása esetén, mivel nem célzottan egy személy sérelmére követik el (több sértett lehet az ügyben) úgy a megelőzés elve alapján célszerű a nyomozás lefolytatása, azaz ahol az adott deliktum esetén a feljelentés megtétele és a nyomozás indítása hamarabb történt meg.

Az Egyesült Államok szabályozásában ugyanakkor érdemes megfigyelni, hogy a joghatóság kérdése nem jelent ilyen problémát azon államaikban, ahol van a Cyber Crime-mal, azaz számítógépes bűncselekményekkel kapcsolatban külön törvény, azokkal az országokkal szemben, ahol nincs külön számítógépes bűncselekményekkel kapcsolatos törvény.

A külön „cyber" vagy „computer" crime-mal kapcsolatos törvényekkel rendelkező államokban, amennyiben a deliktum elkövetési magatartása épp abba az államba irányul, vagy pedig a támadás, vagy jogellenes magatartás onnan származik, akkor a joghatóság nem kérdéses[112], hiszen annak az államnak a hatósága jogosult eljárni.

Amennyiben a hazai szabályozást - beleértve, hogy a Számítástechnikai Bűnözésről szóló Egyezmény sem rendelkezik ezzel kapcsolatban - továbbá Ibolya Tibor ügyész úr álláspontját összehasonlítom az USA bizonyos tagállamainak szabályozásával, akkor a kibertérrel, valamint kiberbűncselekményekkel (vagyis a kibertérben elkövetett bűncselekményekkel) kapcsolatban az eljárás joghatóságának kérdése egyszerűbben eldönthető lenne.

A hatáskör és az illetékesség kérdésében az ügyek áttétele tekintetében elsősorban a szemléletmódbeli váltásra kellene koncentrálni, vagyis a megelőzés elve, alapján az jogosult eljárni, amelyik hatóságnál hamarabb tették meg a feljelentést. Amennyiben nem állapítható meg, hogy hol tettek először feljelentést- akár mert több sértett van, vagy éppen több elkövető,

[111] i.m.
[112] „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,. pl: Észak-Karolinának is van külön kiberbűnözéssel kapcsolatos törvényük: 2010 North Carolina Code, Chapter 14 Criminal Law. Article 60- Computer Related Crime.14-453.2.Jurisdiction

akik földrajzilag távol vannak egymástól- úgy ez utóbbiak tartózkodási helye szerinti illetékes nyomozó hatóságnak, a célszerűség szem előtt tartásával kellene lefolytatnia az eljárást. Célszerűség alatt pedig az ügyek oknélküli áttétele helyett, az együttműködésben látjuk a megoldást.

Az Európai Parlament és Tanács 2013/40 számú irányelvének 12. cikke a joghatóság kérdésében a tagállamokra bízza a döntést, így a direktívában említett bűncselekményeket

a) egészben vagy részben a területükön követték el; vagy
b) egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

A tagállamok biztosítják, hogy joghatósággal rendelkezzenek abban az esetben, ha:

a) az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e; vagy
b) a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön.

A joghatóság kérdése, sokszor nem tűnik az egyik legfőbb problémának, a nyomozás vagy felderítés gördülékenységének- így az adatkérések vagy adatgyűjtések végrehajtásának gördülékenysége, a jogszerűség fenntartása érdekében egységes szabályozás és gyakorlat létrehozása, kialakítása, mind nemzeti, mind pedig közösségi szinten elengedhetetlen.

Ugyanakkor felmerülhet annak a lehetősége is, hogy az a hatóság járjon el, akinek az illetékességi területén az internetes szolgáltatást végző elektronikus hírközlési szolgáltatást végző székhelye, esetleg az adott szolgáltatást igénybe vevő előfizető lakhelye található[113].

[113] Ennek értelmezésében segítséget nyújt az 2003. évi C. törvény az elektronikus hírközlésről szóló törvény (továbbiakban: Eht.)188.§ Értelmező rendelkezések 14.) pontja: *Elektronikus hírközlési szolgáltató:* elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy és a *22.) pontja Előfizető:* olyan természetes vagy jogi személy, vagy más szervezet, aki vagy amely a nyilvánosan elérhető elektronikus hírközlési szolgáltatás nyújtójával ilyen szolgáltatások igénybevételére vonatkozó szerződéses viszonyban áll.

4.3 A számítógépes bűncselekmények alanyi oldala

A bűncselekmények központi szereplői mindig az azt elkövető és a sértett, aki az elkövető miatt valamilyen joghátrányt szenvedett, vagy szenvedő fél.

A büntetőjog tudománya alanynak nevezi azt a személyt, akit az elkövetett bűncselekmény miatt felelősségre lehet vonni és emiatt vele szemben szankció alkalmazható. A törvénykönyv az alany kifejezést nem használja, rendelkezik azonban a bűncselekmény elkövetőiről[114].

A számítógépes bűncselekményekkel kapcsolatban sokáig tartotta magát az a nézet, hogy az elkövetők magasan iskolázott, informatikusok, de legalább az informatika iránt érdeklődő személyek, akik jó anyagi háttérrel és általában biztos munkahellyel rendelkeznek. Ez a felfogása az informatikai eszközök egyre szélesebb körű elterjedése és felhasználhatósága, az internet népszerűsége miatt megváltozott.

A köztudatban Kevin D. Mitnick óta, a „hacker", vagy hekker kifejezés terjedt el, akihez negatív érzések társulnak. A 2017-ben a BKK (Budapesti Közlekedési Központ) internetes jegy-és bérletértékesítő rendszerének sérülékenységét felfedő esemény óta, újabb kifejezést is megismerhetett a társadalom, az „etikus hekkert", akihez már kevésbé fűződik negatív érzés.

A hekkerek leginkább informatikai végzettséggel vagy ilyen irányú érdeklődés körrel rendelkező szakemberek, akik más számítógépébe vagy informatikai rendszerébe hatolnak be, azért, hogy az abban tárolt adatokat megismerjék, megszerezzék, a jelszavakat, bankszámla adatokat megszerezzék, a jogosultnak a rendszerbe történő bejutást, hozzáférést ellehetetlenítsék, megakadályozzák.

A hekkereket a feladataik és céljuk (ideológiájuk), képzettségük alapján az alábbi csoportokba lehet sorolni[115]:

- Fehér kalapos (etikus) hacker (White hat hacker): céljuk nem a károkozás. Megbízásból támadják a rendszert, annak sérülékenységének vizsgálata miatt. A megbízó által a szerződésben meghatározott rendszereket tesztelik.

[114] Balogh Ágnes, Tóth Mihály: Magyar büntetőjog. Általános rész (2010, Osiris Kiadó, forrás: https://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_520_magyar_buntetojog/ch03s05.html, letöltve: 2019. február 10)
[115] forrás:https://www.thefreelibrary.com, letöltve: 2019. február 15.

- Fekete kalapos hacker (cracker vagy Black-hat hacker): olyan személyek, akik bűnös magatartásukat a saját vagy mások megbízásából hajtják végre. Céljuk az anyagi haszonszerzés, a károkozás, a figyelemfelkeltés, demonstráció vagy politikai motiváció.

- Szürke kalapos hacker (Grey-hat hacker): tevékenységük a fehér és a fekete kalapos hekker közé tehető. Az általuk végrehajtott illegális támadások célja, hogy az adott rendszer üzemeltetőit a biztonsági résről értesítsék, amiért pénzt kér a vállalattól.

- Script kiddie: olyan szaktudással nem rendelkező „kölykök", akik tudásukat chat szobákban, fórumokon szerzik meg, úgy, hogy a valaki által előre megírt parancssor segítségével hatolnak be rendszerbe vagy törlik az adatokat. Motivációja az elismertség, de a tudásuk meg sem közelíti a hackerekét.

- Hactivista: ők az informatikai rendszerek segítségével, felhasználásával hozzák nyilvánosságra politikai nézetüket, radikális gondolkodásukat. Ilyen ismert hactivista az Anonymus csoport is.

A számítógépes bűncselekmények alanyai (elkövetői) nemcsak az előbb említett hekkerek lehetnek, hanem az egyes bűncselekmény típusoknál eltérő elkövetési magatartást elkövető személyek, akik speciális jellemzőit a 9. Fejezetben, a bűncselekményeknél részletesen tárgyaljuk.

A nyomozási problémák vizsgálata során nem az a lényeg, hogy az elkövetőt milyen névvel illetjük, sokkal inkább az elkövető motivációja, vagy az általa elkövetett célja a lényeges, hiszen a felderítését, a nyomozás lefolytatását, gyanúsítottként történő kihallgatását, a bizonyítékok beszerzését, a kényszerintézkedések foganatosítását annak szem előtt tartásával szükséges lefolytatni.

4.4 Az idő, mint a nyomozást nehezítő tényező a bizonyítékok összegyűjtése során

A büntethetőség tekintetében az elkövető cselekménye a jogellenes cselekménye törvényben meghatározott büntetési tételének felső határa, de legalább öt év, amelynek elteltével már nem lesz büntethető, kivéve egyes, törvényben tételesen meghatározott esetekben[116].

A bűncselekmény elkövetési idejének különös jelentősége van, hiszen főszabályként az az elkövetéskor hatályban lévő törvényt kell alkalmazni, ami az egy „mozzanatú bűncselekmény" elkövetésénél különös jelenősége van, de problémát okozhat több mozzanatú bűncselekmények elkövetésénél.

A számítógépes bűncselekmények nyomozása során további (objektív) kihívást jelenti az idő múlása az elkövetés, a nyomozás és a bizonyítékok összegyűjtése szempontjából is.

A számítógépes deliktumok esetében (is) az idő fontos tényező a sértettek, a hatóságok munkája és nyomozása szempontjából, valamint az elkövetők felderítése és a további cselekményeik megakadályozása érdekében.

A kibertéren keresztül elkövetett bűncselekmények egyik jellemzője, hogy nem feltétlenül a jogellenes cselekmény elkövetésekor észlelik a sértettek azt, hogy bűncselekmény áldozatai lettek, hanem egy későbbi időpontban vagy egy hosszabb időintervallumban, vagy akár soha (látencia) nem veszik észre.

Ugyanígy nehézséget vet fel a jogellenes tartalom újbóli, jellemzően más felhasználó által történő megjelenítése, az inkriminált tartalom visszakereshetősége.

A számítógépes deliktumok felderítése és az elkövetők elleni sikeres eljárás lefolytatásának egyik nagyon fontos tényezője, természetesen a megfelelő szakismeret mellett- az idő kérdése. A bűncselekmény elkövetési idejének meghatározása mind a kibertérből ki nem lépő jogellenes cselekmények esetén, mind pedig a kibertérből kiinduló, de a fizikai világba kilépő deliktum esetén nehéz.

Kiberbűncselekmények tekintetében viszont kérdésként merül fel, hogy mikor történt az elkövetés?

[116] Btk. 26.§ (1) bekezdés

A kibertérben elkövetett bűncselekmények közül a Btk. 423§ szerinti információs rendszer vagy adat megsértésének bűncselekményén (ransomware támadáson) keresztül érzékeltetjük a problémát. Ennek esetében a bűncselekmény befejezettségének problémája a következő[117]:

- a rosszindulatú szoftver vagy program megírása,
- a megírt szoftvert feltöltése a világhálóra,
- a rosszindulatú szoftver a felhasználó által történő telepítése a rendszerébe,
- a rosszindulatú szoftver a számítógépnek vagy rendszernek megfertőzése,
- a rosszindulatú szoftver a hatásának kifejtése (amikor az elérhetetlenné tette a rendszerben vagy eszközön tárolt adatokat vagy azokat illetéktelen számára hozzáférhetővé tette)
- amikor a zárolt adatokért cserébe bizonyos összegű pénz megfizetésének a követelése, vagy
- a sértettnek a követelés teljesítése, vagy
- annak észlelése, hogy a felhasználó bűncselekmény elkövetésének áldozata lett.

Ha összevetjük a jogtudomány szerinti elkövetési idő bekövetkezésével kapcsolatos elméleteket és a kibertérben elkövetett bűncselekmények lehetséges bekövetkezésének dilemmáját, akkor megállapíthatjuk, hogy valamennyi elmélettel azok összekapcsolhatók.

Ám kérdésként felmerül, hogy szükség lenne egy egységes álláspontra, már csak a fentebb említett inkriminált tartalom újbóli (akár a tartalom létrehozásának elévüléses utáni) feltöltésére vagy a tartalom visszakereshetőségére.

Álláspontunk szerint mivel az elkövetés idejének meghatározása a büntetőeljárás megindításakor bír jelentőséggel, hiszen az elévülés fennállása esetén, a nyomozást megszüntető ok, így az elkövető nem vonható felelősségre, a büntetőeljárás nem indítható meg. Éppen ezért a sokáig látenciában maradó számítógépes bűncselekmények elkövetőinek felelősségre vonása, hogy az elévülés miatti felelősségre vonást ne kerülje el, a sértett vagy a hatóság tudomására jutásának időpontja kellene, hogy a mérvadó legyen.

[117] egy viszonyleg egyszerűbb példán keresztül szemléltetem a dilemmát, de hasonló problémák vetődhetnek fel valamennyi számítógépes bűncselekmény esetében.

4.5 Konklúzió

A disszertáció címében megfogalmazott számítógépes bűncselekmények nem azonosak teljes mértékben a kiberbűncselekményekkel, egész pontosan a kibertérben elkövetett bűncselekményekkel.

Számítógépes bűncselekményként határoztuk meg azokat a bűncselekményeket, ahol magának a számítógépnek, mint elkövetés eszközének van jelentősége. Azaz azok a bűncselekmények, ami már létezett a számítógép megjelenése 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, amivel off-line módban is el lehet jogellenes cselekményt elvégezni.

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.

5 A SZÁMÍTÓGÉPES BŰNCSELEKMÉNYEK FELDERÍTÉSÉRE ÉS NYOMOZÁSÁRA VONATKOZÓ ELJÁRÁSI SZABÁLYOZÁS

5.1 A bizonyítás

A bizonyítás, mint büntetőeljárásjogi fogalom nem más, mint a büntető jogilag (anyagi jogilag és eljárás jogilag) releváns, múltbéli tények megismerése a törvényes bizonyítási eszközök és módszerek útján, illetve ezeknek a tényeknek az igazolása és rögzítése bizonyítási eszközökkel.[118]

A bizonyítás célja a büntetőjogi felelősség eldöntéséhez szükséges releváns tények, ismeretek megszerzése, feladata pedig a bűncselekmény vonatozásában a tényállás tisztázása[119].

Logikai értelemben a bizonyítás „valamely ítélet (tétel, hipotézis, elmélet) igazságának, helyességének kimutatása olyan ítéletek, tételek stb. segítségével, amelyeknek igazságát már kimutatták, igazolták, bebizonyították. A bizonyítás tehát következtetés alkalmazása amelynek célja hogy valamely már ismert tételről, ítéletről kimutassa, hogy az megfelel a valóságnak, visszatükrözi az objektív valóságot, más szóval: igaz."[120]

A bizonyítékok tekintetében megkülönböztetünk szabad- kötött és vegyes bizonyítási rendszert, míg Tremmel Flórián könyvében megemlíti „*A jogtörténeti bizonyítási rendszerek*"[121] között a négyes felosztást:

- pozitíve kötött
- negatíve kötött
- teljesen szabad
- nem teljesen szabad

Hazánkban a hatályos Be. alapján egyes tankönyvek szerint a szabad bizonyítás rendszer érvényesül, míg a fent említett Tremmel tanulmány szerint a *nem teljesen szabad* bizonyítási rendszer van érvényben; azaz minden, az eljárásjogi törvény alapján meghatározott bizonyíték

[118] Fantoly Zsanett és Gácsi Erzsébet Anett: *Eljárási büntetőjog – Statikus rész* (Szeged: Iurisperitus, 2013), 202.
[119] Budaházi Árpád és Fantoly Zsanett: *Büntető eljárásjog I. - Statikus rész* (Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, NKE Szolgáltató Kft., 2015), 144.
[120] 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).
121 Tremmel Flórián: Bizonyítékok a büntetőeljárásban (Dialog Campus, 2012) 61.

felhasználható, ugyanakkor jogszabály elrendelheti a bizonyítási cselekmények teljesítésének és lefolytatásának, a bizonyítási eszközök megvizsgálásának és rögzítésének meghatározott módját[122], továbbá rögzítik, hogy szabadon felhasználható a törvényben meghatározott minden bizonyítási eszköz, és szabadon alkalmazható minden bizonyítási cselekmény, ugyanakkor a törvény elrendelheti egyes bizonyítási eszközök- így a tanúvallomás, terhelt vallomása, szakvélemény, pártfogó felügyelői vélemény, irat, okirat, elektronikus adat- felhasználását[123].

A Be. a bizonyítás törvényességére vonatkozó szabálya biztosítja, hogy az eljárással érintettek jogait, jogainak védelmét a bizonyítás „kényszere" alatt ne sérthessék meg, az egyes eljárási cselekmények a törvényben meghatározott eljárási szabályok szerint hajtsák végre a hatóságok. A nem teljesen szabad bizonyítási rendszer alapján, egyes esetben a büntető eljárási törvény meghatározhatja az egyes bizonyítási eszközök igénybevételét.

Finszter Géza kriminalisztikai bizonyításelmélettel kapcsolatos gondolatai szerint „*A büntetőeljárás jogi- és a kriminalisztikai bizonyításelmélet - eltérő szemlélettel ugyan, de a kölcsönös tisztelet jegyében - ugyanarról, a büntetőeljárásban zajló, megismerési folyamatról fejti ki mondanivalóját. Az eljárás formáját meghatározó gondolkodás számol azzal, hogy csak az igazság megismerése töltheti ki a jogi formákat, míg a kriminalisztikai feltárás egész tevékenységét a tételes jog keretei közé helyezi, mert csak így biztosítható a büntetőigény egyetlen elfogadható érvényesítési módja, a törvényesség."*[124]

A kétféle megközelítés eltérő vonásait emeli ki az alábbiakban Finszter[125]:

- A processzuális bizonyításelmélet azt ragadja meg az eljárási folyamatban, ami szabályozható, ezért *fő kifejezési eszköze a jogi norma*. A kriminalisztika tárgya viszont a megismerésnek azok a mozzanatai, amelyek a tapasztalatokon, a hipotéziseken, a tervezhetőségen és az elemző-értékelő készségen alapuló szabad választással jellemezhetők. A kriminalisztikai megismerés *fő kifejezési eszköze az ajánlás*.

- Az eljárásjogi célokból adódik, hogy azok középpontjában *a végeredmény* áll, ami lehet a valóság megismerése, avagy olyan megállapítás, miszerint a releváns múlt a büntető döntés

[122] Be.166.§ (2) bekezdés
[123] Be. 167.§(1) bekezdés
[124] Finszter Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében, jegyzet, 43. oldal (forrás: users.atw.hu/be/letoltes/Krimjegyzet.doc)
[125] Uaz 43-44.

számára *a bizonyosság* erejével nem ismerhető meg. A kriminalisztika viszont nyomozás legfontosabb irányjelzőinek *a kiinduló adatokat* tekinti, ezért központi kategóriája *a gyanú*.

- Az eljárási szabály *szintetizálja* a lehetséges megismerési formákat és mindig *a jövőre tekintve* határozza meg a büntető igény érvényesítésének a rendjét. Ezzel szemben a kriminalisztika *analitikus módon* jár el és tekintetét *a múltra* szegezi, számára az a kérdés, hogyan lehetséges a büntetőjogi jelentőségű múltbeli eseményt az igazságszolgáltatási döntés érdekében *rekonstruálni.* A kriminalisztika a rekonstrukció érdekében vizsgálja a nyomképző mechanizmusoknak a működési törvényeit. Ezeket a törvényszerűségeket foglalja össze *a nyomtan elmélete.*

- A nyomtan útmutatást ad a bűncselekményre utaló tárgyi és személyi bizonyító tények felderítéséhez. Azokat a módszereket, amelyek segítségével feltárható a bizonyító tényeknek a bizonyítandó tényekkel meglévő kapcsolatait tartalmazza *az azonosítás tana*.

5.1.1 A bizonyítás büntetőeljárás jogi megközelítése

A bizonyítás egy átfogó és az eljárás más szakaszában is megjelenő cselekménysorozat. A büntetőeljárásban a bizonyítás egy emberi megismerő tevékenység, melynek elsődleges célja a múltban történt-jogilag releváns- tények megismerése, majd ezeknek megfelelően a helyes jogi minősítés megállapítása, és a büntetés kiszabása, vagy a vádlott felmentése[126].

A büntetőeljárásról szóló törvény 7.§ (4) bekezdése szerint továbbra is érvényesül az „in dubio pro reo" elv (ami a bizonyítási teher egyik formája), amely szerint „A kétséget kizáróan nem bizonyított tény nem értékelhető a terhelt terhére."

A bizonyítás tehát a jog- pontosabban a jogszabályban meghatározott tevékenység, amelyet a jogszabályokban, az abban felhatalmazott személyek vagy hatóságok folytathatnak le, az abban meghatározott eljárási cselekmények betartásával és a törvényben meghatározott jogok és kötelezettségek figyelembevétele mellett.

[126] Alföldi Ágnes Dóra: Gondolatok a büntetőeljárásbeli bizonyítás jelentőségéről és fogalmának elméleti megközelítéséről (in Jogelméltei Szemle 2/2011. Budapest, 2011. Jogelméleti Szemle online: http://jesz.ajk.elte.hu/alfoldi46.html, letöltve: 2019, 02.06)

Finszter Géza szerint a *bizonyítás* egy olyan tevékenység, amelynek révén a már megszerzett és közölt ismeret igaz volta felől a közlő a közlés címzettjében igyekszik meggyőződést kelteni. Hogyan jelennek meg ezek a gondolatok a gyakorlatban? A *nyomozó hatóság* a nyomozás során a megismerendő tények okozataiként keletkező, közvetlenül érzékelhető fizikai és pszichikai jelenségekből igyekszik megismerni a feltételezett bűncselekményt manifesztáló tényeket[127].

A bűncselekmények bizonyításával kapcsolatban Király Tibor úgy fogalmazott, hogy „A büntetőeljárásban egyedi tényekről mondanak ítéletet, arról, hogy a vádlott bizonyos helyen és időben lopott, erőszakoskodott, ölt vagy mást követett el. Az ilyenféle egyedi kijelentésekben kifejezett igazságok az abszolút igazságok csoportjába tartoznak, amelyeket szokás tényigazságnak is nevezni. Követelmény velük szemben, hogy teljesen, pontosan fejezzék ki a tényt, amelyre vonatkoznak”[128].

Tremmel Flórián szerint „a bizonyíték fogalma szerves alkotóeleme a bizonyításnak... Lényegében tehát minden egyes bizonyíték tulajdonképpen részbizonyítást jelent büntetőügyben”[129].De mit is ért a szerző a részbizonyítás fogalmán?

Mivel a bizonyítás egy olyan „tevékenység” kell, hogy legyen, amely során a nyomozó hatóság a bűncselekmény múltban bekövetkezett történéseit

A bizonyítás során csak olyan adat használható fel, melynek forrása és a beszerzési módja, rögzítése, feldolgozása megfelel az eljárásjogi szabályoknak, a hitelesség követelményének, valamint akkor használható fel, ha a beszerzett adat valóságtartalommal bír. A bizonyítás a felderítés során beszerzett adatoknak a valódiságát alátámasztó eljárás, mely igazolja a tények valódiságát, és a felderítés során szerzett adatok cáfolatlanságát[130].

A számítógépes bűncselekmények esetében a bizonyítás összetettebb, mint a hagyományos bűncselekmények esetében, hiszen azok sokszor online módon és akár az országhatárokon kívülről vagy épp az Európai Unió határain túlról szerezhetők csak be[131].

---

[127] Finszter Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében, jegyzet, 34. oldal (forrás: users.atw.hu/be/letoltes/Krimjegyzet.doc) Letöltve: 2019. január 02.
[128] Király Tibor: Büntetőítélet a jog határán (Tanulmány a perbeli valószínűségről, Budapest 1972) 174. o
[129] Tremmel Flórián: Bizonyítékok a büntetőeljárásban (Dialog Campus, 2012) 64. oldal
[130] Nyitrai Endre: A felderítés és a bizonyítás kriminalisztikai megközelítésből (forrás: http://www.dosz.hu/dokumentumfile/tsz2015_1.pdf, letöltve: 2019. január 02.)
[131] Európai Bizottság -Sajtóközlemény (forrás: http://europa.eu/rapid/press-release_IP-19-843_hu.htm, letöltve: 2019. március 27.)

5.2 Bizonyítékok a számítógépes bűncselekmények esetében

A bizonyítás azokra a tényekre kell, hogy kiterjedjen, amelyek a büntető és a büntetőeljárási jogszabályok alkalmazásában jelentősek. A bizonyítás a büntetőeljárás járulékos kérdéseinek elbírálásában jelentős tényekre is kiterjedhet[132].

A tárgyi bizonyítás eszközök tehát a számítógépes környezetből beszerzett eszközök a bizonyítandó tény megállapítását vagy kizárását, mint „nyomhordozó", „nyomképző" eszközök segítik; úgyszintén a számítástechnikai eszköz jelenléte vagy épp hiánya, továbbá helyszíni elhelyezkedése alapján vonható le következtetés a bizonyítás tárgyával kapcsolatban.

Nyomhordozóként értendő például a merevlemez, a számítógép háttértárolója, amennyiben azokon például zsarolólevelet rögzítettek.[133]

5.2.1 Bizonyítékok összegyűjtése a számítógépes bűncselekmények bizonyítása során

Az internetes környezetben elkövetett bűncselekmények esetében bizonyítékok összegyűjtése okozhatja az egyik legnagyobb problémát. A hagyományosnak[134] mondható deliktumokkal szemben a számítástechnikai környezetben elkövetett jogsértő cselekmények vonatkozásában nem csak fizikailag- megfogható bizonyítékok lefoglalása (pl.: desk top, laptop, tablet, CD/DVD, pendrive) válhat szükségessé, hanem az azokon lévő adatok, információk, valamint a kibertérben lévő elektronikus (elektronikus információs rendszerben tárolt) adat megszerzése, megismerése és bizonyítékként történő felhasználása is szükséges lehet.

A bizonyítékokkal kapcsolatban elemzésre kerül a Büntetőeljárásról szóló 2017.évi XC. törvény, valamint a Számítástechnikai Bűnözésről szóló Egyezményről szóló 2004. évi LXXIX. törvény és nemzetközi ajánlások.

[132] Be. 163.§ (1) bekezdés
[133] Matus Márk: Kutatás, lefoglalás, bűnjelkezelés (In: Kriminalisztika BM Duna Palota és Kiadó, Budapest 2004) 236-237.
[134] Fenyvesi Csaba: A kriminalisztika tendenciái- A bűnügyi nyomozás múltja, jelene, jövője (Dialóg Campus Szakkönyvek, Dialóg Campus Kiadó, Budapest, 2017) 242.

A nyomozás elrendelése és a kényszerintézkedés elrendelése során szükséges az esetlegesen felmerülő akadályok miatt a különböző forrásokból- így nyílt vagy nem nyílt forrásokból-származó információk beszerzése és mérlegelése.

Az elektronikus bizonyítékok, mint a digitális eszközökből vagy a kibertérből nyerhető bizonyíték magán viseli annak változékonyságát, manipulálhatóságát. Emiatt egyes tagállamokban az e-bizonyítékok összegyűjtésével és értrékelésével szemben különleges követelményeket támasztanak annak érdekében, hogy a bíróságok számára elfogadható legyen.

Nem mindegy ugyanakkor, hogy a bizonyítékként felhasználható adat hol található. Így az, egy vagy több fizikai adathordozón lelhető fel- amelynek nyomai lehetnek egy telefonon, számítógépen, nyomtatón vagy akár gépjárműben, okos (smart) eszközön (hűtőgép, hűtő-fűtő berendezés stb.) vagy azok a felhőben (cloud)[135] kerülnek eltárolásra?

Sok esetben, eltérően a fizikai térben található bizonyítékokkal, nem elég megtalálni a kérdéses „dolgot", hanem annak útját, mint egy bizonyíték láncolatot szükséges felderíteni és rögzíteni, ily módon alkalmas lehet a teljes bizonyításra.

A vizsgálatunk tárgyát képezte a bizonyítékok beszerzésével kapcsolatban, hogy a nyomozó hatóságok jellemzően milyen elektronikus vagy digitális bizonyítékokat/ bizonyítási eszközöket gyűjtenek be?

- a telekommunikációs eszközök és/vagy azok adattartalma,
- számítástechnikai eszközök/azok adattartalma,
- egyéb adathordozókat (pl. pendrive, merevlemez, memóriakártya) és/vagy azok adattartalma,
- elektronikus formában tárolt könyvelési iratok,
- elektronikuslevelezés,
- hangfelvétel,
- elektronikusan tárolt távközlési előfizetői és forgalmi adatok, illetve egyéb mobilkommunikációs adatok,

[135] cloud szolgáltatás: „A felhő alapú információtechnológiai rendszerek lényege, hogy olyan adatokkal, szoftverekkel dolgozunk, amelyek egy része, vagy akár a teljes egésze nem a saját információtechnológiai eszközünkön, hálózatunkon található, hanem valahol az Interneten." (Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél- Hadmérnök, VI. Évfolyam 4. szám-2011. december, 177. oldal, forrás: http://hadmernok.hu/2011_4_kovacsz.pdf, letöltve: 2018. október 11.)

- elektronikusan tárolt pénzintézeti, előfizetői és forgalmi adatok,
- ATM felvételek,
- mobilkommunikációs adatok,
- biztonsági kamerák és térfigyelő kamerák felvételei,

A beszerzett adatok tekintetében az ügyész asszony, dr. Losonczy-Molnár Melinda elmondta, hogy általában elégedettek a nyomozószervezetekkel. A hatóságok minden, az elektronikus, illetve digitális bizonyítékok körébe tartozó, általuk fontosnak ítélt „tárgyat" lefoglalnak, ugyanakkor nehéz annak megítélése, egy sikertelen felderítéssel vagy nyomozással záródó ügy esetén, hogy minden esetben sikerül-e valamennyi bizonyítékként felhasználni kívánt „tárgy" beszerzése, megfelelő értékelése.

A bizonyítékok összegyűjtésére vonatozóan az alábbi megállapítás tehető:

A bizonyítékok - így pl.: ATM felvételek, biztonsági-és térfigyelő kamerák felvételei tekintetében elsődlegesen a nyílt típusú adatszerzés lehetőségével éltek:

a) adatkérés
b) kényszerintézkedéssel, mint lefoglalás, információs rendszerbe tárolt adatok; megőrzésre kötelezés, az ügy megítélésétől, attól függően, hogy ismeretlen vagy nem ismeretlen tettes ellen folyt az eljárás vagy
c) OSINT (Open Source Intelligent, azaz nyílt forrású/típusú információgyűjtés) lehetőségével, amelynek jogi szabályozásával.

A nem nyílt adatszerzés tekintetében a nyomozó hatóság a nyílt eljárásban nem beszerezhető módon és lehetőségekkel szerezheti meg az ügy eldöntéséhez szükséges adatokat:

d) bírói és ügyészi engedélyhez nem kötött leplezett eszközök alkalmazása
e) ügyészi engedélyhez kötött leplezett eszközök
f) bírói engedélyhez kötött leplezett eszközök alkalmazása
g) g.) titkos információgyűjtés

A fent említett digitális bizonyítékok beszerzésénél ugyanakkor csak a törvényben felsorolt „csoportok" kerültek felsorolásra. Az információ technológia fejlődésével a bizonyítékok köre bővülhet, akár olyan mértékben is, hogy a törvény merev szabályai miatt azok törvényessége, változatlanságuk megőrzése nem lehetséges.

5.3 Digitális bizonyítékok és elektronikus bizonyítékok

A nyomozás során a múltban történt események megállapításához szükséges a bizonyítékok összegyűjtése, értékelése, a tanúk kihallgatása, azok értékelése, tények, következtetések levonása, megállapítás megtétele, majd mind ezekből a büntetőeljárás befejezése a gyanúsított ellen vádemelési, avagy az eljárást megszüntető javaslattal.

5.3.1 Van-e eltérés a digitális bizonyítékok és a hagyományos bizonyítékok között?

A digitális bizonyítékok koncepcionálisan ugyanazok, mint bármely más bizonyíték, vagyis az információ felhasználásával az azt vizsgáló hatóság igyekszik a személyeket és az eseményeket időben és térben elhelyezni annak érdekében, hogy a bűncselekmények okait, az elkövetés módszerét a lehető legpontosabban feltárják.

Az új Büntetőeljárási törvény külön nem rendelkezik a digitális bizonyítékokról (Digital Evidence[136]), hanem az elektronikus adatot, valamint az információs eszközt említi, nem határozza meg azok fogalmát, hanem felsorolás szerűen, a hagyományos bizonyítékok körébe vonva tárgyalja azokat.

A magyar és külföldi szakirodalom tanulmányozása és a digitális bizonyítékokra vonatkozó szabályok összegyűjtése kapcsán, kétféle megnevezést használnak, leginkább egymás szinonimájaként, a digitális és az elektronikus adat/bizonyíték fogalmát.

A következőkben a két elnevezés között kísérletet teszünk arra, hogy megtaláljuk a helyesebb kifejezést a számítógépes bűncselekményekkel kapcsolatos bizonyítékok elnevezésére, annak ellenére, hogy a büntetőeljárásról szóló törvény, továbbá a Büntető Törvénykönyvünk is az „elektronikus” kifejezést használja.

A digitális adat olyan adat, amely egy kódolási eljárással jön létre, és amely alkalmas az elektronikus dokumentum előállítójának és egyúttal a dokumentum tartalmának azonosítására. Digitalizálás alatt azt a folyamatot értjük, melynek során a korábban más (analóg) hordozón

[136] A digitális bizonyítékok kriminalisztikai értelemben: a bináris formátumban tárolt vagy továbbított információ, amely potenciális bizonyító erejű (Barry A.J. Fisher- William J. Tilstone- C. Woytowicz: Introduction to Criminalistics- The Foundation of Forensic Science (Elsevier Academic Press, 2009) 295.

rögzített tartalmakat valamilyen digitalizáló eszköz segítségével a számítógép által értelmezhető formában kódoljuk, illetve rögzítjük a gép által olvasható adattároló eszközre.

A digitális bizonyítékok egyik nagy területe a hagyományos keresőoldalak kutatása és azok elemzése. A bűncselekményekkel, például a gyermekpornográfiával és a szexkereskedelemmel kapcsolatos nyomozások a digitális bizonyítékokkal foglalkoznak; azonban új utak nyíltak meg az internet egyre növekvő kihasználásának, globális értelemben vett kommunikációs eszközként. Ilyen digitális bizonyíték lehet a közösségi oldalak (Facebook, Tweeter, Instagramm, stb.) vagy a különböző kommunikációra használt applikációk, oldalak (Messenger, Viber, Skype, e-mail stb).

A digitális bizonyítékok sokszor több információt hordoznak a hatóság számára, mint az elektronikus bizonyítékok, hiszen azok tartalmához történő hozzáférés (az említett nagyobb segítséget nyújthat a hatóság számára, mint a kizárólag elektronikus úton keletkezett evidenciák. Ugyanakkor nem lenne szakszerű, ha a két típusú bizonyítékot megkülönböztetnénk egymástól, hiszen azok több ponton összefüggnek, sokszor együtt említik őket.

Az elektronikus adat nem más, mint elektronikus úton rögzített adat. A Büntetőeljárásról szóló törvény szerint az elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja. Az elektronikus dokumentumokat keletkezésük szempontjából két részre oszthatjuk: egy részük eleve digitális formában jön létre (born digital), hiszen a szerzők nagy része – haladván a korral – számítógép segítségével, szövegszerkesztővel ír, a fotók is ma már egyre nagyobb számban készülnek digitális fényképezőgéppel; másik részük pedig digitalizálási folyamat eredményeként, papír (vagy egyéb analóg) formátumú nyomat számítógépes reprezentációjaként keletkezik, vagyis, mint a hagyományos személyazonosítás (kézi aláírás) modern, elektronizált változata olyan kódolási eljárás, amely alkalmas az elektronikus dokumentum előállítójának és egyúttal a dokumentum tartalmának azonosítására.

Ha Sorbán Kinga tanulmányában[137] említett Donn Parker által összeállított csoportosítását vesszük alapul, amely szerint:

- a számítógép fizikai valójában az elkövetés tárgya: ez a helyzet azoknak a bűncselekményeknek az esetében, amikor a számítógép fizikai komponensére követik el a bűncselekményt, pl. ellopják, vagy megrongálják azt. Az informatikai elem ezekben a bűncselekményekben valójában csak esetleges, így ezek a deliktumok nem számítanak számítógépes bűncselekményeknek;
- a számítógépes környezet az elkövetés tárgya azokban az esetekben, amikor az adott bűncselekményt, számítógépes rendszerre, programra, vagy számítógépben tárolt adatra követik el. Ezek a bűncselekmények a klasszikus számítógépes bűncselekmények pl. a hekkelés, a számítógép megfertőzése kártékony programokkal (malware) stb.
- a számítógépes környezet a bűncselekmény eszköze, amikor az elkövető olyan bűncselekményt követ el információtechnológiai környezetben, amely egyébként számítógép felhasználása nélkül is elkövethető lett volna. Ebbe a körbe tartoznak a tartalommal kapcsolatos bűncselekmények, mint a gyermekpornográfia, illetve a szerzői jog megsértésével kapcsolatos bűncselekmények
- a számítógép lehet az elkövetés szimbóluma: ez utóbbi esetben a számítógépnek nem kell feltétlenül jelen lennie a bűncselekmény elkövetése során, elkövető csupán arra hivatkozik. A szerző olyan csalást hoz fel példaként, amelyben az elkövető a megtévesztés során arra hivatkozott, hogy hozzáférése van bizonyos speciális számítógépes programhoz,

Akkor a fentiek fényében az elektronikus bizonyítékokat három nagy csoportba soroltuk[138]:

Az egyik csoportba tartoznak a kibertérből beszerezhető bizonyítékok, így például a felhőben található adatok, a közösségi oldalakon és az elektronikus levelező rendszerben található információk stb.

A másik csoportba a számítástechnikai eszközökön található digitális bizonyítékok tartoznak, míg a harmadik csoport az első két csoporttal összefüggő információkból levonható evidenciák.

[137] Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés az Amerikai Egyesült Államokban (forrás: https://docplayer.hu/47794558-Az-informatikai-buncselekmenyek-elleni-fellepes-az-egyesult-allamokban.html, letöltve: 2019. február 22) 155-156.
[138] Az alábbi megállapítások a saját véleményünket képviselik az elvégzett kutatás alapján

A felsorolt bizonyíték típusok közötti különbség abban áll, hogy míg az első esetben a digitális adat fellelhetősége például a felhőben vagy egy weboldalon lehet, addig az informatikai eszközön tárolt adatot magán a számítástechnikai eszközökön, adathordozókon lehet megtalálni (nem szükséges internet kapcsolat).

A harmadik eset, azaz az első kétfajta evidenciához kapcsolódik, vagyis azok keletkezését, módosítását, létrehozásának idejét, helyét, a létrehozó személyével stb. kapcsolatban hordoz információkat.

A digitális és az elektronikus bizonyítékokkal kapcsolatban a kérdés, hogy miként lehet bizonyítékot találni (pl. képeket, videókat) a forrástól, úgy, hogy a bíróság számára annak elfogadhatóságáról.

5.4 A bizonyítékok beszerzésével kapcsolatos nyílt adatszerzés lehetőségei

A bizonyítékok megszerzése a hatóságok részéről nem kizárólag valamelyik kényszerintézkedés foganatosítása vagy végrehajtása útján teljesülhet, hanem a rendőrségnek lehetősége van arra, hogy adatkéréssel forduljon egy másik nyomozószervhez vagy egyéb szervezethez, hogy adatokat, információkat kérjen, amelyeket egyébként az eljárás során nem tudna hitelt érdemlő módon megszerezni.

5.4.1 A megkeresés/ Az adatkérés

A hatályon kívül helyezett Büntetőeljárásról szóló törvényben 2018. június 30.-ig a hatóságnak lehetősége volt más hatóságoktól, önkormányzatoktól állami-és nem állami szervezetektől a nyomozáshoz szükséges információk megszerzésére. Ez az eljárási lehetőség a nyomozó hatóság számára alapot jelenthetett további nyomozati cselekmények elvégzésére a Be. 151.§-a alapján.

Az új Be. hatályba belépésével megszűnt a megkeresés jogintézménye és helyette bevezette a jogalkotó a 261.§-al az adatkérést, amelynek „keretében a büntetőeljárással összefüggésbe hozható:

a) a szervezet birtokában lévő adat továbbítása
b) a szervezet birtokában lévő elektronikus adat vagy irat továbbítása vagy
c) a szervezet által teljesíthető tájékoztatás adása kérhető”[139].

5.4.2 Az adatkérés jelentősége a bizonyítás során

A nyomozó hatóság, az ügyészség és a bíróság adatkéréssel élhet jogi személyt, jogi személyiséggel nem rendelkező gazdasági szervezet, állami vagy helyi önkormányzati szervezet felé is. Az eljárási törvény tételesen felsorolja az érintett szervezeteket.

Az adatkérésnek fontos szerepe van a bűncselekmény felderítésében és további szakaszokban is, ugyanakkor számtalan esetben volt arra példa, hogy a gyanúsított épp egy adatkérés során szerzett tudomást az őt érintő eljárásról.

A bizonyítás során a különféle adatok, információk (így például metaadatok[140]) ismerete, hozzáférése a nyomozás alkalmával sok esetben szükséges, azok beszerzése a Be. 261.§-a alapján lehetséges a szolgáltatótól az előkészítő eljárás során például az elektronikus hírközlési szolgáltatótól, banktitkokat, fizetési titoknak, értékpapírtitoknak vagy biztosítási titoknak minősülő adatot kezelő szervezettől, az egészségügyi és a hozzájuk kapcsolódó személyes adatot kezelő szervezettől. A feltételes adatkérésre a rendőrség vagy a terrorizmus kezelésével foglalkozó szervezet ügyészségi engedéllyel, három hónapra (amely egyszer még meghosszabbítható) állami, helyi önkormányzati stb szervezettől a Be. 266.§-a alapján. De adatkéréssel beszerezhető és felhasználható adatok a nyomozás szempontjából sokszor nélkülözhetetlen hírközlési szolgáltatóktól beszerezhető hívószám előfizetőjének neve és adatai, a telefon IMEI száma, a SIM kártya IMSI [141]száma, valamint ennek alapján a híváslista, és a hívások időtartama, valamint az úgynevezett kelő-fekvő pozíciók, a telefonpartner neve.

Az adatkérés során a hatóság a harmadik félről az alkalmazásszolgáltatótól szerzi be az információt. A szolgáltató az elektronikus kereskedelmi szolgáltatásokról, valamint az

[139] a Büntetőeljárásról szóló 2017. évi XC. törvény 261.§ (3)-(4).
[140] a metaadat fogalma: lásd a 71. oldalon
[141] IMSI szám: **(**International Mobile Subscriber Identity, magyarul: nemzetközi mozgó előfizető azonosító**):** ez a felhasználó azonosítására alkalmas kód, mely tartalmazza az előfizetőre vonatkozó összes információt. Ha az előfizető mozgásnál van, minden azonosítási területváltáskor szükség van ennek kiadására, azonban biztonsági okokból ilyenkor nem ez, hanem a TMSI kerül felhasználásra. (forrás: https://mobilarena.hu/teszt/amit_a_sim_kartyakrol_tudni_erdemes/azonositok_kodok_szamsorok.html, letöltve: 2018. október 11.)

információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény alapján, titkosított kommunikációt biztosító szolgáltatást nyújt, köteles az ilyen alkalmazás igénybevételével továbbított küldeményekkel, közlésekkel kapcsolatosan keletkező vagy kezelt[142] adatokat, beleértve a metaadatokat, azok keletkezésétől számított 1 évig megőrizni[143]. Így az alkalmazásszolgáltatók tekintetében a kért adatok vonatkozásában a hatóság megkereséssel kell, hogy éljen.

A külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén a titkosított kommunikációt biztosító szolgáltatást nyújtó alkalmazásszolgáltató

a) a szolgáltatás típusát
b) a szolgáltatás előfizetőjének vagy felhasználójának
    ba) a szolgáltatás igénybevételéhez szükséges azonosító adatait, a szolgáltatás igénybevételének dátumát, kezdő és záró időpontját
    bb) a regisztrációhoz használt IP-címét és portszámát
    bc) az igénybevételnél használt IP-címét és portszámát a felhasználói azonosítót köteles átadni.[144]

5.4.3 Az elektronikus bizonyítékokhoz történő hozzáférés

Gyakorlati tapasztalatunk alapján állíthatjuk, hogy a legtöbb problémát a nyomozó hatóság számára azt jelenti, amikor a számítástechnikai rendszerben tárolt adathoz hozzá kell férni vagy, amikor az ügy szempontjából olyan lényeges adatra van szükség, amely valamelyik közösségi oldalon a felhasználó fiókjában vagy felhőben kerül elhelyezésre.

Ezt a két esetet, illetve szabályozást tekintve az alábbiak szerint történik az eljárás:

1. eset, amikor akár a levelezési rendszer, akár pedig valamelyik közösségi háló fiókjába a belépéshez nem kell sem a felhasználónevet sem a jelszót megadni, mivel az adott informatikai eszközön a kényszerintézkedést elszenvedő be van jelentkezve, vagy a beállítások

[142] „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 13/B.§ (1). letöltve: 2018. október 20.
[143] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről 13/B.§ (1).
[144] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről 13/B.§ (1).

úgy vannak megadva, hogy a felhasználónevet és a jelszót az adott számítógépen vagy IP címen megjegyzik, és az automatikus belépési funkció be van rajta állítva.

A nyomozó hatóság számára az eljárás lefolytatása szempontjából a büntetőeljárásról szóló törvény alapján a következő eljárási cselekmény lefolytatása válhat szükséges:

Bár a belépés akadályok nélkül végrehajtható, főleg abban az esetben, amikor a kényszerintézkedést elszenvedő fél együttműködik, mégis a Be. 302.§-a szerint kutatás a lakás, az, egyéb helyiség vagy jármű átkutatása, valamint az információs rendszer, illetve adathordozó átkutatása, a büntetőeljárás eredményességének érdekében. Ebből az eljárásjogi szabályból következik, hogy az informatikai rendszerben tárolt elektronikus adat- függetlenül attól, hogy a kutatás elszenvedő fél abba beleegyezik-e vagy sem, illetve az adott rendszert (ergo számítógépet, adattároló eszközt) védik-e jelszóval vagy nem, lefoglalható, átvizsgálható, az azon tárolt adat rögzíthető, megismerhető, az bizonyítékként felhasználható.

A Be. alapján a kutatást az érintett- tehát nem feltétlenül a gyanúsított- jelenlétében kell lefolytatni. A kutatás megkezdése előtt az érintettet fel kell szólítani, hogy a keresett dolgot adja elő vagy pedig az információs rendszeren tárolt adatokat tegye a hatóság számára hozzáférhetővé. Amennyiben a kért bizonyítékot a hatóság részére átadja, vagy az adatot önszántából hozzáférhetővé teszi - azaz a belépéshez szükséges jelszót megmondja, átadja- úgy a kutatás nem folytatható (az erre vonatkozó részletes eljárás menete a későbbiekben kerül kifejtésre).

Ugyanakkor amennyiben a hatósággal nem működik együtt az eljárással érintett, úgy a nyomozó hatóságnak más módon kell az információs rendszerben tárolt adatot megszerezni, megismerni, olyan formában, hogy az bizonyításra alkalmas legyen. Ugyanez a szabály vonatkozik arra az esetre is, ha a gyanúsított eleve be van lépve a levelezési rendszerébe vagy pedig a közösségi fiókjába és a hatóságnak „csak” a belépés gombra kell kattintania vagy az automatikus belépés van a böngészőjébe beállítva.

Ezekben az esetekben is érvényben van a Számítástechnikai Bűnözésről szóló Egyezmény 32. cikke, a „Tárolt számítástechnikai adathoz való hozzáférés” határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén kimondja, hogy: A Szerződő Fél a másik Szerződő Fél engedélye nélkül:

a) a nyilvánosság számára elérhető módon (nyílt forrású) tárolt számítástechnikai adathoz hozzáférhet, függetlenül az adat földrajzi elhelyezkedésétől; vagy
b) a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását.

A helyzet bonyolultságát adja, hogy nem minden állam írta alá, így az eljárás végrehajtása csak az aláíró államokban lehetséges.

Amennyiben az aláíró országok/felek területén kell az eljárást végrehajtani, kérdés, hogy az Egyezmény implementálása megtörtént-e a saját büntetőeljárási törvényükben.

A számítógépes bűncselekmények nyomozása során a legnagyobb jelentősége egyrészt magának a felhasználó által „megadott" adatoknak van, másrészt a felhasználó által hagyott úgynevezett „internetes lábnyomnak", vagy digitális nyomnak van, amely a webes böngészési előzményeket, a készített és a tárolt, feltöltött dokumentumainkat jelenti.

A felhasználók „nyomokat" hagynak az interneten, a különböző informatikai eszközökön, akár levelezésekkel, (családi) fényképek, - videók megosztásával, internetes rendeléssel, vásárlással, a különböző online piaci műveletekkel vagy pedig az elektronikus közigazgatási rendszerek (ügyfélkapu) igénybevételével.

A nyomozó hatóság feladatát a régi Be. a következőkben határozta meg: a bizonyítási eljárás során, hogy a Be. rendelkezéseit betartva bizonyítsa a jogellenes cselekmény elkövetését, felderítse és értékelje az eljárás során összegyűjtött bizonyítási eszközöket[145], a törvényesség betartása mellett a szükséges nyomozati cselekményeket elvégezze.

Az új büntetőeljárási törvény a nyomozó hatóság feladatát már másképp határozta meg; a bűncselekmények felderítés érdekében előkészítő eljárást és nyomozást végez[146].

Az informatikai eszközök és rendszerek terjedése, azok széleskörű használata során új kihívásokkal szembesülnek a rendészeti és nemzetbiztonsági szervek, amelyek sok esetben megkönnyíthetik cselekmény, illetve az elkövető megállapítását, ugyanakkor a jogi

[145] a(korábbi) büntetőeljárásról szóló 1998. évi XIX. törvény 77.§ (1)-(2) .
[146] Be. 31.§ (1)

szabályozásra figyelemmel, sokszor indokolatlanul van megkötve a kezük a bizonyítékok beszerzése és értékelése tekintetében.

Érdekes módon, amennyire mind az Alaptörvényünk, a jogalkotók szándékainak ismeretében a hatóságokat sokkal szigorúbb szabályok kötik az internetes környezetben elkövetett eljárási cselekményének szabályozása tekintetében és a figyelem nagyobb eséllyel irányul rájuk, mint a felhasználók által hanyagul kezelt jelszavak, adatvédelmi beállítások esetében.

A digitális bizonyítékok keletkezésével kapcsolatban a legfontosabb annak megértése, hogy valamennyi nyom egyedi, annak keletkezésével, értékelésével kapcsolatban nem szabad egy sémát felállítani, hiszen a bűncselekmények jellegétől, az elkövetők számától, informatikai tudásától és jellemzőitől függően változhatnak.

5.5 Bizonyítékok a fizikai térben

A kibertérrel összefüggésbe hozható deliktumokkal kapcsolatban a kutatás során a fizikai térben is keletkezhetnek bizonyítékok, az azokkal kapcsolatos cselekmények a kényszerintézkedés foganatosítása során dilemmát jelenthetnek.

1. Számítógép: Az egyik legfontosabb nyomhordozó eszköz lehet a számítógép, amely fajtáját tekintve vagy PC (Personal Computer) vagy laptop. A számítógép a kutatás során általában a legkézenfekvőbb tárgy, ami szinte valamennyi bűncselekmény esetében hordozhat olyan nyomokat, bizonyítékokat, amelyek bizonyítékként
2. Mobiltelefon: A mobiltelefont ma már a legtöbb használó mini számítógépként, személyi asszisztensként használja. Sokszor több adatot és információt tartalmaz, és több mindent lehet megtudni a tulajdonosáról, mint a rendelkezésre álló rendszerből, a személyről elvégzett információgyűjtésből. A mobiltelefonok egyrészt telekommunikációs eszközök, másrészt dokumentumok, fényképek, egyéb adatok tárolására alkalmasak. Ugyanolyan vagy talán több információt hordozhatnak, ezért a bizonyítás során kiemelkedő szerepük van.
3. Perifériák: A perifériák azok a számítógéphez csatlakoztatható eszközök, ami nem egy további eszköz illesztését oldja meg. A perifériát általában- de nem feltétlenül- a külvilággal történő kapcsolattartásra használja a számítógép. Tipikus periféria a

nyomtató, a billentyűzet, az egér és a monitor.[147] A perifériák már nemcsak egyszerűen kiegészítik a számítógépet, hanem sok esetben olyan információt is hordoznak, amelyek digitális bizonyítékok nyomait hordozza, így kényszerintézkedések során lefoglalásuk és vizsgálatuk nélkülözhetetlen.

4. Tartós adathordozók: A 2011/83/EU irányelv79 – a fenti határozatnak megfelelően – kimondja, hogy a tartós adathordozóknak „*lehetővé kell tenniük a fogyasztó számára az adattárolást mindaddig, amíg […] érdekei védelmének érdekében szükségesnek tartja*" továbbá, hogy az „*ilyen adathordozók közé sorolandók különösen a papír, az USB-kulcsok, a CD-ROM-ok, a DVD-k, a memóriakártyák vagy a számítógépek merevlemezei, illetve az elektronikus levelek*".

5.6 Bizonyítékok a virtuális térben

A nyomozás sikeres lezárásának érdekében, a hatóságnak szükséges annak mérlegelése, hogy mit lehet bizonyítéknak tekinteni, valamint azokat hogyan, milyen eszközökkel és milyen taktika keretében lehet beszerezni.

A bizonyítékok megszerzése még a hagyományosnak nevezhető bűncselekmény (így a lopás, csalás, vagy akár emberölés) esetében is gondos mérlegelést igényel. Mérlegelni kell, hogy mit kell bizonyítéknak tekinteni, valamint annak átgondolása is nélkülözhetetlen, hogy az evidenciákat milyen módszerrel szerzik meg és tárolják annak érdekében, hogy azok minden kétséget kizáróan az eljárás végéig alkalmas legyen a bíróság előtti bizonyításra.

A „hagyományosnak" nevezhető bűncselekmények esetében- emberölés, közokirathamisítás, csalás, lopás, stb- a bizonyítás az elkövetés eszközének maradéktalan megszerzése, a helyszínen rögzíthető nyomok biztosítása, rögzítése (fénykép-, video vagy akár hangfelvétel formájában) esetlegesen oly módon, hogy azok alkalmasak legyenek arra, hogy szakértő vagy szaktanácsadó a hatóság által feltett kérdéseket minden kétséget kizáróan meg tudjon válaszolni.

[147] „Periféria", https://pcforum.hu/szotar/perif%C3%A9ria, elérés 2018. július 30., https://pcforum.hu/szotar/perif%C3%A9ria. Letöltve: 2018. október 10.

5.7 Bizonyítékok és az elektronikus adatok

A számítógépes bűncselekményekkel kapcsolatban a bizonyítékok, azok beszerzése, rögzítése rendhagyónak is tekinthető. A nyomozás során nem feltétlenül a fizikai térben behatárolható bizonyítékok észlelése nehéz, hanem az azokból összegyűjthető digitális bizonyítékokról, amikre eltérő végrehajtási szabályok vonatkozhatnak.

A további részletezés előtt szükséges tisztázni, hogy mit is ért a jog az adat és az elektronikus adat fogalma alatt.

5.7.1 Az adat és az elektronikus adat fogalma

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információs szabadságról szóló törvény (továbbiakban: Infotv.) nem határozza meg az adat fogalmát, csak a személyes adat és a különleges adat meghatározását tartalmazza.

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságát szabályozó jogszabály (továbbiakban: Ibtv.) értelmező rendelkezéseiben található meg az adat jogi fogalma.

Az Ibtv. 1.§ (1) bekezdés 1. pontja alapján adatnak tekinthető az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

A régi Be. nem határozta meg az elektronikus adat fogalmát- sőt sok esetben nem is használja ezt a kifejezést, így a hatság a más jogszabályban található fogalomra támaszkodott. A 2018. július 01.-től életbe lépett új büntető eljárási törvény már külön nevesíti azt:

„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja”.[148]

[148] 2017. évi XC. törvény a büntetőeljárásról 205.§ (1)

A jogi szabályozás ugyanakkor nem áll meg ennél a fogalomnál, mivel a bizonyítékok értékelése, összegyűjtése és lefoglalása előtt- mindenekelőtt a (ház)kutatás megkezdése előtt- nem árt a hatóságoknak ismerni és szem előtt tartani az adat osztályozását, hiszen a büntetőeljárásról szóló törvény alapján bármilyen eljárás megkezdése és lefolytatása előtt többek között a törvényesség és az arányosság elvének betartásával kell az eljárást végrehajtani. Éppen ezért külön eljárási szabályok szem előtt tartásával kell a lefoglalás foganatosítást végezni, amennyiben a nyomozás szempontjából szükségessé válik, hogy a kutatást ügyvédi- vagy közjegyzői irodába folytassák le.

5.8 Tárgyi bizonyítási eszközök és a metaadatok

A tárgyi bizonyítási eszközök minden olyan tárgy vagy dolog, amely a bizonyítandó tény bizonyítására alkalmas, értve ezalatt azokat, amelyek a bűncselekmény elkövetésével összefüggésben az elkövető nyomatit hordozza.

Az informatikai eszközök, -rendszerek használata során keletkeznek ilyen digitális nyomok vagy, ahogyan fentebb is említettük, a digitális lábnyomok, amelyeket bizonyítékként lehet használni a nyomozás során. Ilyen digitális nyomok keletkeznek akár egy dokumentum létrehozásakor (vagy akár annak módosításakor, törlésekor), fájlok megnyitásakor, az internetről történő böngészéskor. Ezek a számítógépben a megfelelő helyre mentődnek el és azok bármikor visszakereshetők.

Illési Zsolt a digitális nyomokat, mint bizonyítékforrást kriminalisztikai értelemben az alábbiakként határozta meg: *„A digitális nyom minden olyan adat, amely a vizsgált ügy szempontjából releváns informatikai rendszer szubjektumai és objektumai kölcsönhatása révén keletkezett, továbbítódott, tárolt, módosult vagy törlődött.”*[149]

Hogyan gyűjthetők be a metaadatok és a bizonyítás során milyen jelentőségük van?

A digitális eszközök használata során a keletkezett adatokhoz történő hozzáférés jogi megítélése bonyolult, hiszen önmagában a metaadat megítélése sem egységes.

[149] Illési Zsolt: Az igazságügyi informatikai szakértés modellezése (forrás: http://robothadviseles.hu/pres/Illesi_Zsolt10.pdf, letöltve: 2019. február 23.)

Adatvédelmi szempontból minősülhet személyes adatnak, technikai szempontból pedig olyan adatnak értelmezhető, amely egy másik adat létrejöttével együtt keletkezik, és amelyik módosítható, törölhető, megváltozható.

5.8.1 A metaadatok

A metaadat „*olyan azonosító vagy leíró adat vagy adatcsoport, amely az iratkezelési folyamat egyes részeihez, valamint a munkafolyamat elemeihez kerül generálásra, és az irathoz vagy ügyirathoz történő hozzárendelése és rögzítése által elősegíti egyedi irat és ügyirat kezelését Tágabb értelemben a metaadat olyan strukturált adat, amely egy információs erőforrást ír le, magyaráz, tár fel, vagy más módon könnyíti meg visszakeresését, felhasználását és kezelését"*[150]. A metaadat által megismerhető információk személyes adatok körébe tartoznak, hiszen annak tartalma alapján az egyén beazonosítható, személyes profilja elkészíthető.

Egy-egy fájlhoz az alábbi információk tartoznak:

- A fájl létrehozásának dátuma
- A fájl módosításának dátuma
- A fájlhoz történő hozzáférés dátuma
- A fájl mérete (fizikai és logikai).

A metaadatok keletkezése kétféle módon történhet:

- automatikusan
- intellektuálisan.

Minden egyes informatikai eszköz, rendszer, számítógépes program használata, készítése során keletkeznek metaadatok. Vagyis: dokumentum létrehozásakor, weboldal megtekintésekor, -azok letöltésének alkalmával, e-ügyintés alkalmával az űrlapok, nyomtatványok, kérelmek kitöltése, letöltése esetében, a közösségi oldalak, levelezések használata során, az informatikai eszközök bekapcsolásakor, beállításakor automatikusan keletkeznek metaadatok.

[150] Munk, Sándor: Szemantika az informatikában, *Hadmérnök* IX., sz. 2. (2014): 1–21.letöltve: 2018. október 01.

A létrejövő adatnál, így többek között hangfájl, képfájl esetében is ehetőség van arra, hogy átnevezzük, egyéni tulajdonságokat adjunk meg (intellektuális).

Ahogy említettük a metaadat személyes adat is lehet, hiszen egyes esetekben az azt létrehozó személyre vonatkozó információkat- így név, felhasználóneve, IP címe alapján stb. következtetni lehet az érintettre, ezért annak összegyűjtése, felhasználása során az Infotv. egyes rendelkezéseit is figyelembe kell venni.

A személyes adat fogalmát a 2011. évi CXII. törvény, az információs önrendelkezési jogról és az információs szabadságról szóló törvény határozza meg. Ez alapján az érintettel kapcsolatba hozható adat- különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai vagy fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret, - valamint az adatból levonható, az érintettre vonatkozó következtetés.[151]

A 2018. májusban életbe lépett Európai Unió adatvédelmi rendelet 30. pontja alapján „*A természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a természetes személyes profiljának létrehozására és az adott személy azonosítására.”*[152]

5.8.2 A (meta)adatokkal kapcsolatos bizonyítékok beszerzése

A hazai jogrendszerben az ügyészség és a bíróság szabadon értékeli a bizonyítékokat, vagyis az ügyekben egyéni mérlegelés alapján dönti el, hogy az eljárás során mi az, amit elfogadnak bizonyítéknak és mi az, amit nem. Egy megkötés van: a bizonyítékok beszerzése során az azt beszerző hatóság nem követhet el bűncselekményt vagy más törvénybe ütköző dolgot[153].

[151] „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 3.§ . letöltve: 2018. október 01.
[152] 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).
[153] A büntetőeljárásról szóló 2017. évi XC. törvény 78.§ (4)

Az informatikai környezetben, sőt magában a kibertérben keletkező adatok beszerzésére, értékelésére sokszor más szabályok vonatkoznak, mint a „hagyományos”, nem virtuális bizonyítékok esetében.

5.9 A bizonyítékok értékelése

Magyarországon szabadon felhasználható minden bizonyítási eszköz, így a tanúvallomás, a terhelt vallomása, a szakvélemény, a pártfogó felügyelői vélemény, a bizonyítási eszközök- így az irat és az okirat, valamint az elektronikus adat is. Ez utóbbi az új Be-vel került be az eljárási rendben.

Az elektronikus adatok értékelhetősége tekintetében majd a metaadatokkal kapcsolatban kerül részletesen kifejtésre, hogy milyen jellemzői vannak, illetve a felhasználhatóság és a bizonyítékként történő felhasználás eseteiben milyen nehézségei vannak.

A külföldi és a magyar szakirodalom is kiemeli, hogy a digitálisan beszerezhető bizonyítékok egyenlő értékűek a fizikai bizonyítékokkal, vagyis az elektronikus szerződések értékelése ugyanannyit ér, mint a papír alapú szerződések, okiratok, ugyanarra a joghatás kiváltására alkalmas.[154]

A már hatályon kívül helyezett Be. és a hatályos Be. törvényben nem változott a jogalkotó álláspontja abban a tekintetben, hogy nem értékelhető bizonyítékként az olyan bizonyítási eszközből származó tény, amelyet a bíróság, az ügyészség, a nyomozó hatóság, illetve a (2) bekezdésben meghatározott hatóság bűncselekmény útján, más tiltott módon vagy a résztvevők büntetőeljárási jogainak lényeges sérelmével szerzett meg- annyi különbséggel, hogy míg az 1998. évi XIX. törvényben a „korlátozás” kifejezés szerepelt.[155]

Az elektronikus adat, tehát bizonyítási eszköznek számít, így az új eljárási törvényünk szerint, ha „*ahol e törvény tárgyi bizonyítási eszközt említ, azon e törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell*”[156].

[154] Dr. Anamaria Cristina Carcel: Criminologie (Editura Hamangiu, Bucuresti 2009. p. 101. (ISBN 9787-606-522-099-7)
[155] A büntetőeljárásról szóló 2017. évi XC. törvény 167.§.
[156] A büntetőeljárásról szóló 2017. évi XC. törvény 205.§ (2) .

Az okos telefon használatnál alapvetően – azaz beszélés, illetve üzenetküldésen kívül- népszerűek az applikációk használata (bankolási, egészség-figyelési, sportolási és más aktivitási, helymeghatározási céllal) valamint internet használata a különböző ügyintézésre, e-mail küldésre, a különböző okos eszközök (óra, tablet, otthoni és munkahelyi IoT88-k) csatlakoztatása, amely szintén értékelhető bizonyítékként használható.

Az internettel kapcsolatban az elektronikus közszolgáltatások fejlesztése és terjedése miatt a személyes szolgáltatások használata helyett megjelent az elektronikus ügyintézés, amely során lehetőség van arra, hogy az e-közigazgatást, ügyfélkaput használó személyek belépési időpontjait, a belépésekkor használt IP címeket megismerjük, az általuk igénybe vett szolgáltatásokról, a feltöltött és letöltött (számukra érkezett dokumentumokról) tájékozódjunk megkeresés formájában. A hatósági megkeresést a NISZ Zrt. teljesíti, amely többek között a metaadatok segítségével képes a teljeskörű válaszadásra.

Speciális szabály, hogy a rejtjelezett vagy más módon megismerhetetlenné tett adatot a megkeresett köteles az átadás vagy a közlés előtt eredeti állapotába visszaállítani, illetőleg a megkereső számára az adat tartalmát megismerhetővé tenni[157].

Metaadatok keletkezése és típusai:

- Amennyiben digitális eszközzel (így telefon vagy fényképezőgéppel készítenek felvételt), úgy annak az eszköznek a típusa, gyári száma, a kép GPS koordinátái
- A dokumentumok: a készítőjének a neve, a készítés időpontja, a karakterszámok, a különböző változások
- Hang-fájlok, megismerhető, hogy azt milyen programmal készítették, zenei tartalom esetén az előadó vagy zenekar neve, a készítés éve, védett-e, stb.
- Videó-fájlok: a készítő program neve, vágási adatok, szerző, műfaj, kiadási év.

Szinte minden fénykép tartalmaz EXIF adatot, amiből megismerhető, hogy milyen körülmények között, milyen szoftver használatával és módon készültek az adott fotók. Ez tartalmazza a fényképezőgép sorozatszámát, amennyiben azt menti a metaadatok közé. A keletkezett adatokat nem törli a felhasználó, úgy akár egyes weboldal segítségével az eltulajdonított eszköz által készített és az internetre feltöltött kép segítségével, annak

[157] Gyaraki Réka és Simon Béla: Biztonsági események rendészeti szempontból – A kiberbűncselekmények kezelése", in *Incidensmenedzsment - éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára*, Krasznay Csaba (Budapest: Dialóg Campus Kiadó, 2017).

megtalálása is lehetséges. Az EXIF adatok hasznosak a büntetőeljárás során, de épp adatvédelmi okból a közösségi oldalak ezeket az adatokat eltávolítják.[158]

A metaadatok megismerésével kapcsolatban az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII törvény (továbbiakban Ekertv) módosítása történt a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016.évi LXIX. törvénnyel, így már nemcsak a metaadatokat kell biztosítani a szolgáltatóknak, hanem a tartalmat is.[159]

5.10 A hagyományosnak tekinthető és a nem hagyományos bizonyítékok közötti különbség problémája

Az elektronikus vagy digitális bizonyítékok értékelése és felhasználhatósága a változékonyság miatt kérdéses. Hibásnak tartom azt, hogy a jogalkotó tárgyként kezeli és eltárgyiasítja azt a kényszerintézkedések végrehajtása során.

Ahogy már említettem a Be. az elektronikus irat fogalmát meghatározza, amelybe beletartozik a papír alapon készült dokumentum digitalizált változata (szkennelés, pdf., vagy jpeg., stb. kiterjesztéssel) és épp úgy beleértendő az elektronikusan elkészített dokumentum időbélyeggel ellátva, amelyeket ugyanannak elnevezve nem épp szerencsés.

További segítséget nyújtott Erdei Árpád, aki az új Be.-vel kapcsolatban, a tárgyi bizonyítási eszköz és az elektronikus adat közti problémát érzékelteti, amikor is kifejti a következő gondolatait:

„A tárgyi bizonyítási eszközt meghatározó 204.§ (2) bekezdése szerint *irat minden olyan tárgyi bizonyítási eszköz*, amely bármilyen eljárással adatokat rögzít, „így különösen a papíralapú vagy *elektronikus adatként létező szöveg, rajz ábra*". A rendelkezés ekként félreérthetetlenül tárgyi bizonyítási eszköznek minősíti az elektronikus adatot. Az elektronikus adatról szóló 205.§ (2) bekezdése szerint viszont, ahol a Be. „tárgyi bizonyítási eszközt említ, azon [...] az elektronikus adatot kell érteni, „kivéve, ha a Be. másként rendelkezik.

[158] KR NNI KBEFŐO egyik főnyomozója által készített módszertani útmutató alapján
[159] A GDPR életbelépését követően sem ad megfelelő szabályozást a metaadatokra.

Mindezt jelzi, hogy a tárgyi bizonyítási eszköz és az elektronikus adat közötti különbséget a törvény nem tudja megragadni vagy pontosan kifejezni."[160]

Azaz a fentiekből is látható, hogy az elektronikus iratot tárgyi bizonyítási eszközként kezeli, így összemosódik, pedig a digitálisan (elektronikusan) keletkezett bizonyítékok kevésbé statikusak, a bizonyítási eljárás során a hatóságokok vagy az eljárásban bevont szakértő által nem könnyen reprodukálhatók, ugyanakkor könnyen manipulálhatók.

A hagyományos bizonyítékoktól eltérőek, alapvető tulajdonságaik sokszor nehezen meghatározhatók. *A digitális bizonyítékok változékony és átmeneti természete ellentétben áll az egyéb tudományágakban alkalmazott tartós fizikai jellemzőkkel – pl.: az ujjnyomatkészítés gerincmintáival...*[161].

Az elektronikus bizonyítékok esetében annak vizsgálata menetének pontos dokumentálása már a bíróság előtti hitelesség megkérdőjelezhetetlenségéhez elég kell, hogy legyen. A pontos dokumentálás legalább a képrögzítő (pl.: videó felvétel készítése) eszközzel biztosíthatja a vizsgálat valódiságát.

A bizonyítékok hitelességének (azaz változatlanságának) bizonyítása a kibertérből származó bizonyítékok esetében nem mindig biztosítható. Megoldást jelenthet a problémára az e-aláírás vagy a bitcoin alfejezetben ismertetett blockchain technológiának a fejlesztése, amely biztosítaná és közvetlenül az ügyészség részére továbbíthatná az elektronikus adatokat.
A bizonyítékok beszerzése során felmerül a terhelt együttműködési kötelezettsége és figyelemmel kell lenni adatvédelemre is.[162]

5.11 A bizonyítékok értékelése és bemutatása

Az intézkedésekről szóló jelentést a hatóságnak olyan módon kell megírni, hogy a technikailag laikus közönségnek is érthető legyen, valamint a digitális bizonyítékokat világosan és pontosan kell bemutatni, egyértelműen beazonosítva a tényleges bizonyítékok jelentőségét a

[160] Bánáti-Belegi-Belovics-Erdei-Farkas-Kónya: A büntetőeljárási törvény magyarázata (Hvgorac kiadó, Budapest 2018, 290. oldal)
[161] Eva A. Vincze (2016) Challenges in digital forensics, Police Practice and Research, 17:2, 183-194, DOI: 10.1080/15614263.2015.1128163 letöltve: 2018. október 01
[162] Dr. Ulrich Sieber: Computerkriminalität und Information Data Recht. Computer und Recht 11. 1995, s-109-110.

vizsgálatban. A jelentésnek összpontosítani kell arra, illetve igazolnia kell azt, hogy a bemutatott bizonyítékok hitelesek, megbízhatóak és alkalmazhatóak, valamint kellően részletesnek kell lennie ahhoz, hogy egy független harmadik fél is meg tudja ismételni a következtetéseket. A törvényszéki vizsgálat megkívánja, hogy a jelentés megírását részletes, egyidejűleg történt jegyzetek támogassák. A vizsgálatvezetőnek pontosan meg kell határozni azt, hogy milyen törvényszéki eszközök kerültek felhasználásra a vizsgálat a során, ezzel segítve azt, hogy minden recenzens megértése az eredményeket és a következtetéseket.

Casey szerint „*ahhoz, hogy a vizsgálati folyamat átláthatóságát megadja, a zárójelentések tartalmaznia kell fontos részleteket minden egyes lépésről, tartalmazva a követett referencia protokollokat és módszereket, hogy így megragadják, dokumentálják, összegyűjtsék, megőrizzék, rekonstruálják, rendezzék és megkeressék a kulcsfontosságú bizonyítékokat*."[163]

Mielőtt hivatalosan benyújtja az írásos jelentést vagy bemutatja a vizsgálat eredményeit, a vizsgálatvezetőnek érvényesíteni kell ezeket az eredményeket. Bevált gyakorlat az eredmények ellenőrzésére, hogy lefuttatnak egy második megbízható törvényszéki eszközt, vagy kézzel ellenőrzik a bizonyítékok eredeti helyét, megerősítve azt, hogy az megegyezik az eredeti eredményekkel.

Ha egy digitális törvényszéki nyomozó bemutatja a leleteket, gyakran hasznos lehet világosan leírni a jelentésben, hogy a bizonyítékokat hogyan kezelték és elemezték, hogy így bemutassák és ellenőrizzék a felügyeleti láncot, valamint az összes vizsgálati folyamatot, amit elvégeztek a bizonyítékokon.

A „Bevezető a digitális kriminalisztikai jelentés megírásához" és „Útmutató a jelentés íráshoz" használható útmutatók arról (a 7.7. alfejezetben található a magyar fordítása), hogy milyen elemeknek kell lennie egy számítógépes bűncselekmény esetében a hatóság által írt jelentésben. Természetesen a jelentés formátuma függ a vizsgálathoz tartozó kezdeti elvárásoktól is. Ha lehet, előzetesen meg kell állapodni erről.

[163] Eoghan Casey, *Digital Evidence and Computer Crime.* (Burlington: Elsevier, 2004), http://public.eblib.com/choice/publicfullrecord.aspx?p=288741.letöltve: 2018. október 01

5.12 Az ENISA által kiadott gyakorlati útmutató az elektronikus bizonyítékok összegyűjtése és értékelése esetében

Az ENISA gyakorlati útmutatójában találhatók olyan hasznos információk, tanácsok, amelyek a kevésbé jártas nyomozóknak is segíthetnek a kényszerintézkedés- így a házkutatás és lefoglalás- végrehajtásában. Az útmutató a hazai jogszabályokkal, rendeletekkel kiegészítve sok eljárásjogi kérdést megoldhatna[164].

„*A nyomozó szervek számára a tetthelyre történő érkezést követően fontos, hogy alaposan átvizsgálják a helyszín közvetlen és közvetett környezetét és azonosítsanak olyan kulcsfontosságú tényezőket és személyeket, akik összefüggésbe hozhatók a feltételezett bűncselekménnyel. Amennyiben nem a rendőrség érkezik meg elsőként a helyszínre, törekedniük kell arra, hogy kapcsolatba lépjenek azokkal a személyekkel, akik először voltak ott a tetthelyen. Amikor ezt megteszik, megállapíthatják a digitális eszközök kilétét, és a helyszínen történt bármilyen tevékenységet a gyanúsítottak között.*"

Javaslatunk az, hogy a nyomozó szervek az elkövetéssel összefüggésbe hozható helyszínre érkezés előtt már tájékozódjanak azért, hogy a szükséges kényszerintézkedéseket, eljárási cselekményeket rugalmasan el tudják végezni, ezzel is kevesebb időt hagyva arra a kényszerintézkedéssel érintett személyek számára, hogy bizonyítékot tüntessenek el, semmisítsenek meg vagy módosítsanak. Az elektronikus bizonyítékok jellemzőinek és a bizonyítékokhoz fűződő elvárások szem előtt tartásával kezdje meg a hatóság a cselekmények végrehajtását. Amennyiben a helyszínre a nem bűnügyi munkát végzők érkeznek először - pl. a helyszín biztosítását, körül zárását a közrendvédelmi feladatokat ellátó osztállyal együtt kívánják megvalósítani- úgy azok a személyek a helyszínt a lehetőség szerint hagyják érintetlenül, változatlanságát biztosítsák.

„*Mielőtt belépnek a bűncselekmény helyszínére, meg kell állapítani a megfelelő egészségügyi és biztonsági követelményeket. Nagyon fontos azonosítani a még meglévő veszélyforrásokat, legyenek azok a még helyszínen lévő személyek vagy környezeti tényezők. Az első válaszadónak és a helyszínen lévő egyéb tisztviselőknek a biztonsága kiemelkedően fontos, és meg kell tenni minden lépést ahhoz, hogy ne kerüljenek veszélybe*."

Javaslat: a helyszín külső és belső adottságainak felmérése már a kiérkezés előtt, a kutatás tervezése előtt történjen meg a rendelkezésre álló eszközökkel, információkkal. A kutatást, lefoglalást úgy kell végrehajtani, hogy sem az ott tartózkodó személyek, sem a nyomozó

[164] Az ENISA angol nyelvű szövegének magyar fordítását dőlt betűvel írom, a saját javaslatokat, véleményeket pedig egy-egy részlet után fejtjük ki

hatóság tagjai ne sérüljenek. Továbbá valamennyi eljárási cselekmény a helyszínen található vagyontárgyak sérelme nélkül kerüljön végrehajtásra, amennyiben lehetséges, úgy a lehető legrövidebb idő alatt.

„Az is bevált gyakorlat, hogy a rendőrök soha nem mennek egyedül ismeretlen helyre (például az otthoni felhasználók lakásába, ügyfelek irodájába stb.). Egyes esetekben az is szükséges lehet, hogy elmagyarázzák az ügyfélnek, hogy pontosan mit fognak tenni (pl. a rendszerben lévő malware azonosítása, megállapítása), illetve még ennél is fontosabb, hogy elmagyarázza a helyszínen lévő nyomozó hatóság, mi nem fog történni ottlétük során. Hasznos lehet még megkérdezni ezt a személyt, hogy eddig mit csinált, és hogy észrevett-e valamilyen furcsa dolgot a rendszer viselkedésében. Ez az információ segíthet elvezetni a szükséges következő lépéseket megtételéhez.

A jegyzetek kiegészítése képpen, a nyomozónak érdemes digitális fényképezőgépet és videó felvevő készülék használni annak érdekében, hogy pontos ábrázolja a kutatás helyszínét.
A nyilvántartásnak tartalmaznia kell többek között:

- *a helyszín alaprajzát, mely dokumentálja az eszközök és a környező tárgyak helyét is*
- *a jelenlévő személyeket*
- *a belépéskor készített fényképeket*
- *fényképeket az eredeti helyükön lévő digitális bűnjelekről.”*

Javaslat: A rendőrök soha nem mennek egyedül helyszínre, így már a kutatás tervezésekor a helyszín adottságait, méretét, elhelyezkedését, a tervezéskor figyelembe kell venni. Tekintettel kell lenni arra, hogy minimum hány fő tudja végrehajtani a kényszerintézkedést és maximum hány fő, akik az adott helyen tudnak tartózkodni és esetleg milyen szakértelemmel kell, hogy rendelkezzen az eljárás gyors és precíz végrehajtásához.
Az adott technikai felszereléseket- így a berendezések, gépek vizsgálatához szükséges laptopok, eszközök, az adatok mentéséhez szükséges eszközök, a végrehajtott cselekmények kép-és hangrögzítésére alkalmas eszközök működőképességének ellenőrzése történjen meg.
A lehető legtöbb részletet az arra alkalmas eszközzel rögzíteni kell, ami mellett természetesen írásban is dokumentálni kell a fontosabb történéseket, adatokat, információkat.

Érdemes a helyszínen már megkezdeni a kihallgatásokat, amennyiben a törvényi feltételek adottak, amiket kézzel a helyszínre vitt jegyzőkönyvön rögzíteni kell. Kívánatosnak tartjuk, hogy az ehhez szükséges eszköz is álljon a rendelkezésre mindig.

„A nyomozó szervnek a tett helyszínére való belépése után egyidejű jegyzeteket kell készítenie arról, hogy mit is csinálnak, mi is történik. Az ennek elvégzésére vonatkozó iránymutatást az első válaszadó alkalmazójának vagy a bizonyíték összegyűjtését kérelmező testületnek kell biztosítani. Két példa a fent említett iránymutatásokra, a Brit ACPO Gyakorlati Útmutató a Számítógép-alapú Elektronikus bizonyítékokhoz[165] és az Iránymutatás az OLAF személyzetének a digitális törvényszéki eljárásokhoz[166]tartalmazza.

Minden digitális bizonyítékot azonosítani és biztosítani kell, és gondoskodni arról, hogy engedély nélkül senki nem nyúlhat hozzá ezekhez az eszközökhöz. A nyomozó szerveknek meg kell próbálniuk összeállítani a lehető legtöbb információt a részletekből. A jelszavas bejelentkezési adatok, a hálózati topológia (mind fizikai és virtuális), a számítógépes rendszerek felhasználói, az internetes kapcsolatok és a biztonsági rendelkezések mind hasznos útmutatást adhatnak a bűnjel vizsgálata során. Fontos megjegyezni, hogy az első válaszadóknak nem kellene foglalkozniuk a gyanúsítottakkal."

Javaslatunk az, mivel Magyarországon még nem alkottak meg arra vonatkozóan semmilyen iránymutatást, útmutatót, hogy milyen minimum szabályokat kell betartani, így érdemes lehet a nem vagy kevésbé jártas hatóságnak a nyomozati cselekmények előtt tájékozódni, szükség esetén szakértőt vagy szaktanácsadót igénybe venni ahhoz, hogy a számítástechnikai eszközök, rendszerekbe változtatást, arra illetéktelenek ne tudjanak elvégezni, az adatok, elektronikus bizonyítékok ne sérüljenek és ne váljanak hozzáférhetetlenné, azok eredeti állapota megmaradjon.

„Az elkobzással kapcsolatos előírások:

Mint a fentiekben, ahogyan már említésre került, sok esetben az elsőként helyszínre érkező hatóságnak szüksége lehet arra, hogy bizonyítékokat gyűjtsön az ügyfélnél (például egy bankban, cégnél vagy magánszemély otthonában). Mivel ezen adatok elemzése a legtöbb

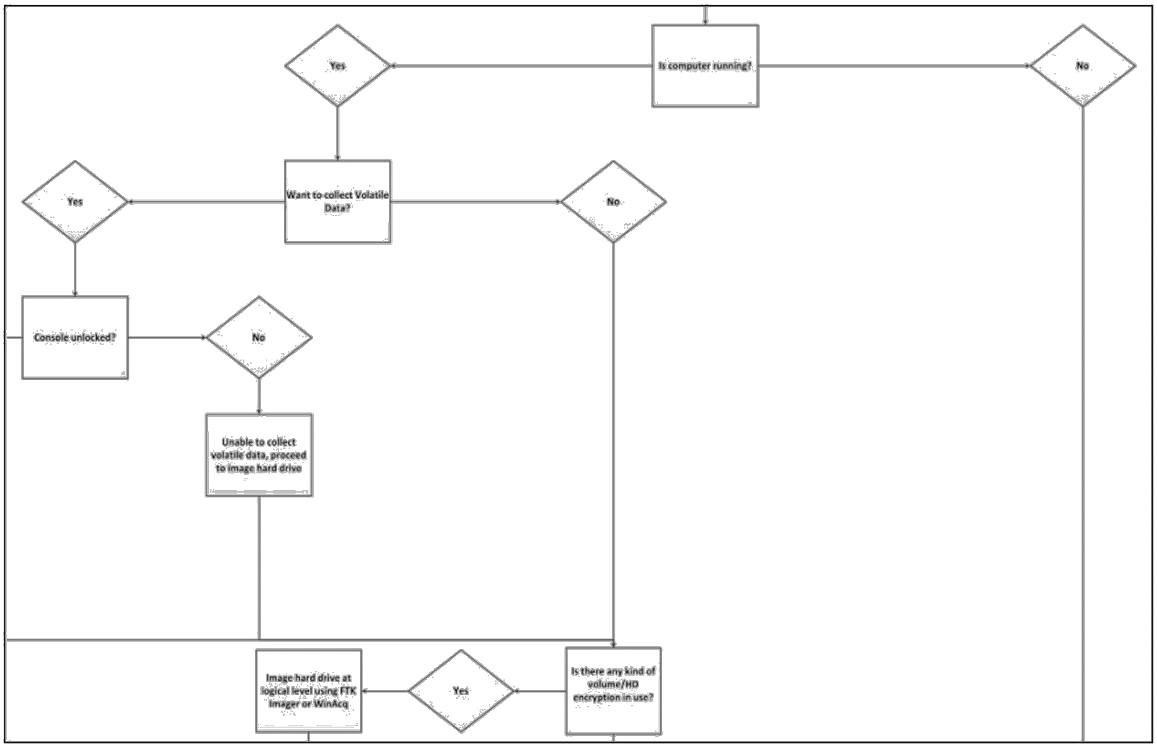
[165] Janet Williams, szerk., *ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence* (Metropolitan Police Service, 2012), https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. Letöltve: 2018. október 20.

[166] OLAF, „Guidelines on Digital Forensic Procedures for OLAF Staff", 2016. február 15., https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf. Letöltve: 2018. október 21.

esetben elég időigényes, gyakran érdemes elkészíteni a rendszerek tükörképét és a képeket a laborban elemezni, nem pedig a helyszínen.

Az ENISA javaslata, hogy a nyomozó szervnél legyen kéznél egy táblázat arról, hogy hogyan kell eljárni a különböző esetekben. Rendkívül fontos, hogy ez a táblázat kiterjedjen szinte minden lehetséges esetre. Fontos kérdések lehetnek a következők:

- *Működik-e a számítógép?*
- *Hálózathoz van kapcsolva a számítógép?*
- *Meg kell-e őrizni a változó (felejtő) adatokat?*
- *Alkalmazva van-e a teljes merevlemez titkosítása? Nyitva van-e a konzol?"*



1. ábra Mueller, L.,'Computer Forensic Hard Drive Imaging Process Tree with Volatile Data Collection', 11 December 2010147.

Javaslatunk az, hogy a helyszínen érdemes az elsődleges vizsgálatokat elvégezni és mérlegelni, hogy:

- lehetséges-e az adott eszköz, rendszer helyszínen történő átvizsgálása, vizsgálata, a helyben történő mentés
- szükséges-e a számítástechnikai eszközök lefoglalása vagy egyébként biztosíthat-e a rajta lévő bizonyítékok változatlansága

Az ENISA által tett javaslat ugyanakkor teljes mértékben érdemes lenne a hazai gyakorlatba történő átvételre, hiszen az a „jó gyakorlat” kialakításához megfelelő alapot nyújthat.

5.13 Elektronikus bizonyíték gyűjtése, tárolása:

Az elektronikus bizonyítékok gyűjtésének módja attól függ, hogy milyen bűncselekmény miatt folyik az eljárás, milyen típusú bizonyítékok lelhetők fel az adott adathordozón vagy információs rendszeren találhatók, és a (bizonyítási) eszközök vagy a kényszerintézkedést elszenvedő milyen pozíciót tölt be a büntetőeljárásban.
Az Európai Unió 2017-ben publikált, de már azt megelőzően a tagállamok nyomozó szerveit, ügyészségeit, kibervédelemmel foglalkozó szervezeteit egy több pontból álló kérdéssorral megkereste, amelynek összesítései alapján a számítógépes bűnözéssel kapcsolatban jelentést készített, ezt a tavalyi évben publikált is. Ez a Genval jelentés vagy Hetedik körös jelentés. A hazai tapasztalatok alapján a helyszíni adatgyűjtéssel kapcsolatos végrehajtás a következőképpen néz ki[167]:

A helyszínen történő adatgyűjtés két kategóriába sorolható: közvetlen és közvetett. Az első „közvetlen” kategória, amikor az adathordozó maga kerül lefoglalásra, ilyenkor nincs szükség külön műveletre az adatok begyűjtéséhez. Az adatok beszerzésének alapfeltétele, hogy biztosítani kell az adatok változatlanságát (írásvédő eszköz, hash), valamint az adatokat tartalmazó adathordozó fizikai sértetlenségét, épségét és a bűnjel azonosítását (megfelelő csomagolás, bűnjelcímke használatával). A lefoglalt adathordozóról fénykép- vagy videofelvétel készül, ha kiszerelésre került sor (pl. merevlemez) akkor a kiszerelés előtti állapotról is, hogy milyen berendezésben (laptop, számítógép, szerver, egyéb célhardver), hogyan és hol helyezkedett el.

A második, „közvetett” kategória, amikor valamilyen előzetes tevékenység szükséges az adatok lefoglalásához. A teljesség igénye nélkül ilyen tevékenység lehet például egy adatbázis backup/export, de akár a titkosítás feloldása, adott könyvtárról image készítése is ide tartozik. Többnyire vállalatok/cégek szerverei esetében kerül rá sor, de előfordulnak olyan esetek is,

[167] „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. Letöltve: 2018. október 01.

amikor magánszemély által használt informatikai eszköz esetében is alkalmazni kell. A tevékenység természetesen fényképfelvételekkel dokumentálásra kerül. Abban az esetben, amikor együttműködést igénylő esetre kerül sor, például cég informatikusa által átadott adat, akkor az a jegyzőkönyv mellett az átadott adatfájlról hash érték generálására kerül sor. Az ilyen esetek jellemzője, hogy „ismert adat" lefoglalására kerül sor. Az általánosabb, „közvetlen" módon beszerzett adatok „ismeretlen adat" jellemzővel bírnak és utólagosan, elemző tevékenység során állapítható meg, hogy az adott adathordozó milyen adatokat tartalmaz, továbbá azok mit és milyen módon bizonyítanak.

A kutatás és lefoglalás során azonban az időhiány miatt nincs mindig lehetőség a bűncselekmény nyomait esetleg viselő adathordozókról történő adatmentésre, az eszköz vagy rendszer átvizsgálására a helyszínen. Ilyen esetben csak bűnjelként történő lefoglalásra történhet, aminek vizsgálatát hivatali helyiségben hajtják végre, vagy szakértőnek/ szakértői intézetnek adják át meghatározott módon és a vizsgálatot kirendelő határozattal teljesítik.
Ez előbbi történhet akár az eljárás alá vont személy, vagy annak képviselője jelenlétében és ezt követően kerül sor az adatmentésre. Az adatmentéshez szükséges adathordozók minden esetben üres, vagy ha korábban már felhasználásra került, akkor többször felülírással törölt (wipe) adathordozóra történik.
Az adatok mentése oly módon történik, hogy a bizonyítékul szolgáló adathordozóról készített bit azonos adatmentést, valamint az adott ügyben szükséges és kinyert adatokat külön adathordozón ügyirathoz csatoljuk bizonyítékként, az adatmentésről, illetve elemzésről készült jelentéssel együtt.

Helyszíni (live forensic) adatmentés: Igazságügyi szakértő, a nyomozó hatóság tapasztalt és erre kiképzett tagjai, illetve más speciális adatmentő szerv által biztosított szaktanácsadó a helyszínen, működés közben vizsgálja meg az adott információs rendszert. A működés közben történő vizsgálat ma már azért elkerülhetetlen, mivel egyrészt az adatok egy részét külső hálózati eszközökön, felhő rendszerekben, egyéb internetes helyeken tárolhatják, amelyekhez a hozzáférés kizárólag a helyszínen biztosított. Másrészt a titkosítási technikák gyors fejlődése miatt nem lehet tudni, hogy egy számítógép leállítása után mely fájlok, könyvtárak vagy meghajtók adattartalma válik elérhetetlenné. A helyszíni adatmentést hitelesen a számítógép releváns adattartalmának megváltoztatása, programok telepítése nélkül, megfelelően dokumentálva kell végrehajtani. Az adatok mentése szintén „imag-fájlokban", „HASH-kulccsal" verifikálva, külső adathordozókra történik.

5.14 Konklúzió és javaslatok

Az e-bizonyítékok jellege olyan kérdéseket vethet fel az elfogadhatóság tekintetében, amelyek más típusú bizonyítékokkal nem merülnek fel. Ezért egyes tagállamokban az e-bizonyítékok összegyűjtésére vonatkozó konkrét követelmények a bíróságok számára elfogadhatóak. Az értékelés azonban kimutatta, hogy a legtöbb tagállamban az eljárási jog elsősorban technológiai szempontból semleges, ami azt jelenti, hogy a bizonyításgyűjtés általános szabályait és elveit alkalmazzák, és hogy az eljárási rendszer nem tartalmaz konkrét formális szabályokat az elfogadhatóságról és az értékelésről.
A számítógépes bűncselekmények nyomozása során alkalmazott kényszereszközökkel kapcsolatban a Belügyminisztériumhoz, valamint az Országos Rendőr-főkapitánysághoz fordultam statisztikai adat szolgáltatása végett, de ezzel kapcsolatban nem rendelkeznek számokkal, a RobotZsaru rendszerben ezek nem kerülnek felvezetésre az adatszolgáltatás miatt kötelezően kiállítandó úgynevezett statisztikai lapokra.

A számítógépes bűnözés elleni hatékony fellépéshez sok nyomozó megjelölte a gyenge vagy egyáltalán nem jó együttműködést az ügyészséggel, illetve az iránymutatásuk hiányát.
Ugyanakkor a számítógépes bűncselekményekkel foglalkozó szervezeteket részéről többször elhangzott a nyomozások sikeressége érdekében a kreativitás, amelyet a túl merev szabályok néhány esetben megakadályoznak. A kényszerintézkedésre végrehajtásra vonatkozó ajánlások száma kevés vagy teljes mértékben hiányozik.
Az elméleti képzések mellett szükség lenne megfelelő gyakorlati képzésre, olyan gyakorlati laborok kialakítására, amely biztosítana alapvető technikai eljárások rutin szerűvé válását.
A 100/2018. (VI.8) Korm. rendeletben az elektronikus adatokra és információs rendszerekre vonatkozó előírások, szabályok újragondolása is szükséges lenne.

Az ENISA gyakorlati útmutatójához fűzött javaslatok segítséget adnának nemcsak a bűnügyes állomány részére, hanem valamennyi olyan, a nyomozásban részt vevő személynek, akiknek bár nem feladata és nem is a tevékenységének része, de bármikor találkozhat számítógépes bűncselekménnyel összefüggő helyszínnel, így nekik is segítség lenne, ha van mihez fordulni.

6 AZ ELEKTRONIKUS BIZONYÍTÉKOKKAL KAPCSOLATOS EURÓPAI UNIÓ TAGÁLLAMAINAK SZABÁLYOZÁSA

Az elektronikus bizonyítékok külföldi államok szabályozásának kiválasztásával kapcsolatban több szempontot is figyelembe vettem. Ilyen szempont volt, hogy olyan országok szabályait vizsgáljam, amelyekről eddig nem vagy kevés magyar nyelvű tanulmány született, valamint a magyar szabályozástól annyira eltérő, hogy akár még példaként is szolgálhat a jogalkotás számára.

A következőkben szükségesnek éreztem, hogy megvizsgáljam több Európai Unió tagállamának e-bizonyítékokra vonatozó eljárását, valamint azokat a szervezeteket, amelyek a bizonyítékokkal kapcsolatos tevékenységet végzik.

A külföldi szakirodalom áttekintése során feltűnt, hogy ott sem található arra válasz, hogy elektronikus vagy digitális jelző a helyes a kibertérből származó bizonyítékok megnevezésére, de leginkább az elektronikus bizonyíték kifejezést használata a jellemző.

Egyes tagállamok az elektronikus bizonyítékok összegyűjtése céljából követik az Európa Tanács a Számítógépes Bűnözésről Szóló Egyezményében vagy a nemzetközi iránymutatásokban meghatározott „legjobb gyakorlatokat”, mint az ACPO[168] iránymutatásait, amelyek az e-bizonyítékok tárolására és átadására is vonatkoznak.

Az Európai Unió számítógépes bűncselekmények elleni küzdelem elleni komoly szándékát fejezte ki azzal, hogy valamennyi tagállamot felkérték arra, hogy az általuk feltett kérdésekre a saját szabályozásuk tekintetében válaszolják meg, amelyet aztán a Genval munkacsoporthoz 2017. június 13-i ülésén elő is terjesztették előzetes véleménycserére.

A küldöttségeket felkérték, hogy 2017. július 3-ig nyújtsanak be írásbeli észrevételeket a zárójelentés tervezetéről.

[168] The Association of Chief Police Officers

A COREPER felkérést kapott arra, hogy nyújtsanak be meghatározott, a kölcsönös értékelés hetedik fordulójáról szóló zárójelentést annak érdekében, hogy a Tanács tájékoztatást kapjon az értékelés eredményeiről, amit aztán értékelés céljából továbbítottak az Európai Parlamentnek.

Mindazonáltal, mivel a számítástechnikai bűncselekmények kiterjed a bűncselekmények széles skálájára, egyetértettek abban, hogy az értékelés olyan bűncselekményekre összpontosít, amelyekre a tagállamok különös figyelmet szenteltek. Ebből a célból az értékelés a következőkre terjedt ki: számítógépes támadások, gyermek ellen elkövetett szexuális visszaélés / pornográf online és online kártya-csalás, valamint átfogóan vizsgálta a számítógépes bűnözés elleni küzdelem jogi és működési szempontjait, a határokon átnyúló együttműködést és az érintett uniós ügynökségekkel való együttműködésről.

A Genval jelentés értékelésének szempontjából különösen fontos a 2011/92 / EU irányelv a gyermekek szexuális bántalmazása és szexuális kizsákmányolásáról, valamint a gyermekpornográfia elleni küzdelemről és az információs rendszerek elleni támadásokról szóló 2013/40 / EU irányelv.

A megállapított főbb hiányosságok a számítógépes bűnözésről és a számítógépes biztonságról szóló külön statisztikák gyűjtésével kapcsolatosak, mivel a rendelkezésre álló adatok nem elégségesek, széttöredezettek, és nem teszik lehetővé az összehasonlítást sem ugyanazon tagállam különböző régiói között, sem a különböző tagállamok között. A Munkacsoport megállapítása szerint „megbízható statisztikákra van szükség ahhoz, hogy áttekintést nyerjenek, nyomon kövessék és elemezzék a számítógépes bűnözés tendenciáit és fejleményeit, annak érdekében, hogy megfelelő lépéseket tegyenek, és értékeljék a jogrendszer hatékonyságát az ilyen bűncselekmények elleni küzdelemben. A tagállamoknak ezért a szabványosított megközelítés alapján ajánlották az eljárások különböző szakaszaiban a számítógépes bűnözésre vonatkozó konkrét és átfogó statisztikák gyűjtését."[169]

Az Európai Unió tagállamai közül kutatást végeztünk Észtország, Hollandia, Írország és Spanyolország számítógépes bűnözéssel kapcsolatos szabályozásában.

[169] A Tanács határozata az Európai Tanács számítástechnikai bűnözésről szóló egyezményének (185.sz.CETS) második kiegészítő jegyzőkönyvére vonatkozó tárgyalásokon való engedélyezésről (Brüsszel, 2019.2.5.)

6.1 Észtország

Észtországot a számítógépes bűncselekményekkel kapcsolatban leginkább az 2007-ben történt orosz-észt kibertérrel összefüggő eseményekkel összefüggésben említik. Azzal azonban már kevésbé foglalkoznak, hogy azt követően az ország komoly védelmi intézkedéseket hajtott végre, amely során mind a számítógépes bűncselekmények nyomozásával, mind pedig a kibervédelem és kiberbiztonság területén komoly, példaértékű lépéseket tettek. A kiberbiztonság-oktatása és a digitális fejlesztése az Európai Unión belül jelenleg utolérhetetlen[170].

Az észt rendőrség (Politsei- ja Piirivalveamet) és határőrség a fő bűnüldöző hatóság a számítógépes bűnözés területén. Néhány kiválasztott bűncselekményt a rendőrség is foglalkozik. A rendőrség feladata az Észtország ellen irányuló, annak alkotmányos rendjének és a területi integritásának megváltoztatására irányuló tevékenységek megelőzése és leküzdése[171].

A rendőrség és határőrség igazgatósága különböző prefektúrákban, valamint a nyomozással foglalkozó bűnügyi rendőrség központjában kiépítettek egy számítógépes bűnözés „vizsgálati kapacitásával" foglalkozó egységet fejlesztettek ki[172]. A központi bűnügyi rendőrségnél a számítógépes bűnözéssel az úgynevezett III. egység foglalkozik, amelyik felelős a számítógépes bűncselekmények elleni eljárások előzetes vizsgálatáért, összegyűjti és elemzi a bűncselekményekre vonatkozó eljárási hatásköröket.

Ezenkívül a szolgálat támogatja a bűnmegelőzés, a bűnözés blokkolása és a tárgyalás előtti eljárás további egységeit, szolgálatait, amelyek különleges ismeretekkel rendelkeznek az információs technológiákban. A bűnügyekkel foglalkozó rendőri egység további feladata a számítógépes bűnözés területén folytatott nemzetközi együttműködés előmozdítása[173].

Az észt prefektúrákban (északi, déli, nyugati és keleti prefektúrák) létrejöttek a bűnügyi hírszerző szolgálatok, amelyek többek között felelősek a számítógépes bűnözés megelőzéséért, blokkolásáért és előzetes eljárásáért, valamint az internetes monitoring elemzésért.[174] A

[170] Sandra Sarev-Tanel Kerikmae-Kasper Ágnes: Az e-polgárság mint virtuális migráció eszköze Észtországban (Információ és Társadalom, 2016., 2. szám) 8-31.
[171] forrás: https://cyberpolicyportal.org, letöltve: 2019. március 29.
[172] 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) 67-74.
[173] Genval 7. körös jelentés
[174] Genval 7. körös jelentés

prefektúrák magukban foglalják a gyermekek szexuális zaklatásával kapcsolatos internetes és gyermekpornográfiai súlyos bűncselekményeket vizsgáló gyermekvédelmi szolgáltatásokat is.

Elektronikus bizonyítékokkal kapcsolatos észt szabályozásnál a Genval 7. körös értékelésében az ország a következőket válaszolta az ezzel kapcsolatos kérdésekre: „*Eddig nem volt szükség az e-bizonyíték fogalmának meghatározására az észt jogszabályokban. Az Európa Tanács számítógépes bűnözéséről szóló egyezmény és az információs rendszerek elleni támadásokról szóló, 2013. augusztus 12-i 2013/40 / EU európai parlamenti és tanácsi irányelv és a 2005/222 / IB tanácsi kerethatározat helyébe lépő 2013/40 / EU irányelvek a következők: referencia*

Észtországban nincsenek külön szabályok az e-bizonyítékok elfogadhatóságára vonatkozóan. Jogszabályai szerint az e-bizonyítékok elfogadhatósági szabályai ugyanazok, mint más bizonyítékok esetében. Emellett nincsenek külön rendelkezések az e-bizonyítékok összegyűjtésére vonatkozóan, és nem alkalmazzák a bizonyításgyűjtés általános szabályait és elveit."

Az észt számítógéppel foglalkozó szervezetek vonatkozásában továbbá megjegyzik, hogy az országban a bizonyítékokat olyan módon kell összegyűjteni, hogy a bizonyításfelvételi eljárás ne sértse az abban részt vevő személyek becsületét és méltóságát, nem veszélyezteti életüket vagy egészségüket, vagy indokolatlan tulajdonjogot okoz.

A bizonyítékok összegyűjtése során konkrét rendelkezések vannak az eszközök és szakértelem használatáról.

A Genval jelentésben írt válasz szerint Észtországban, amennyiben a bizonyítékot külföldi államtól szerezték be egy eljárás során (megkeresés), annak használata megengedett, feltéve, hogy a bizonyítékot a külföldön hatályos jogszabályok alapján megfelelően meghozták, és a bizonyítékok beszerzése érdekében végrehajtott eljárási cselekmények nem ütköznek egymással az észt büntetőeljárások elveit. Rendszerint jogi segítségnyújtás iránti megkereséssel történik[175].

[175] Eneli Laurits: Criminal procedure and digital evidence in Estonia (forrás: journals.sas.ac.uk/deeslr/article/download/2301/2254, letöltve: 2019. március 23.)

6.2 A holland e-bizonyítékra vonatkozó szabályozás

A holland szabályozás vizsgálatára többek között Fantoly Zsanett egyik tanulmánya miatt esett a választásunk[176], amelyben követendő példaként említi a holland büntetőjogi rendszert. Ezt alapul véve igyekeztünk a holland büntetőjog számítógépes bűncselekményekkel kapcsolatos szabályozásban dokumentumkutatást végezni.

Hollandia számára a jogszabályok folyamatos frissítése és megerősítése létfontosságú a számítástechnikai bűnözésre vonatkozó nemzetközi megközelítés megerősítéséhez. Hollandiában a nyomozásokat az Államügyészséget képviselő ügyész látja el, aki teljes felelősséggel tartozik a nyomozásokért.

A holland rendőrség általános feladata - a magyar rendőrség feladataihoz hasonlóan - a kihallgatások foganatosítása, letartóztatás és bizonyítékok összegyűjtése, amelyekről hivatalos jelentést készít. Sok rendőrhatóság vagy „alapegység" végez saját nyomozást ugyanakkor. Az ún. „Inrichtingsplan politie" a hollandiai rendőrségnek egy regionális egysége, amely több kerületben is található (összesen 25 kerületben) és amely egy Regionális Bűnügyi Nyomozási Egységgel is rendelkezik.

Hollandiában a Központi Bűnüldözési Egység két alegységre tagozódik[177]:

- Nemzeti Csúcstechnológiai Bűnüldözési Egység (National Hightech-Misdaadeenheid vagy National High Tech Crime Unit NHTCU)
- Nemzeti Csoport a gyermekpornográfia és a gyermekek szexuális kizsákmányolása ellen (The National Team Against Child Pornography and Traveling Child Sexual Abuse (TBKK).

Hollandiában, a hazai joggyakorlathoz hasonlóan a büntetőeljárásról szóló törvény (Nederlands wetboek van strafvordering vagy Dutch Code of Criminal Procedure-továbbiakban DCCP)[178] szabályozza a nyomozások során a kényszerintézkedésekre vonatkozó szabályokat.

[176] Fantoly Zsanett: A jogi személyek büntetőjogi felelőssége Hollandiában (Acta Juridica Et Politica, Szeged, 2003) 16-18.
[177] Oerlemans, Jan-Jaap Title: Investigating cybercrime (Lay-out: AlphaZet prepress, Waddinxveen Printwerk: Amsterdam University Press, 2017)
[178] Eoghan Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the internet 3rd (Academic Press, 2011, pp 125-126

Általánosságban a DCCP szabályozza az elektronikus bizonyítékgyűjtést. A DCCP 350. cikke mondja ki azt, hogy a bíróság „rechtbank" (általában egy három bíróból álló testület) ítéli meg az állítólagos bűncselekmény bizonyíthatóságát, valamint azt, hogy valóban vádlottnak tulajdonítható-e. A bíróknak meg kell győződniük arról, hogy az alperes a bűncselekmény elkövetésében valóban bűnös a törvényes bizonyítási eszközök alapján (DCCP 338. cikk). A törvényes bizonyítási eszközök a bíró saját megfigyelései és észrevételei, az alperes, tanúk és szakértők bíróság előtt tett kijelentései és írásos dokumentumok (DCCP 339. cikk).

Az írásos dokumentumok magukba foglalják a különböző hivatalos iratokat, amelyek önmagukban is rendelkeznek bizonyító erővel és minden „további dokumentumok", amelyek csak abban az esetben számítanak, amennyiben kapcsolatban állnak a bizonyíték további értelmezésének tartalmával (DCCP 344. cikk (1)). A nyomozó tiszt hivatalos jelentése speciális bizonyítási értékkel bír- ellentétben a hazai gyakorlattal, ahol bár a törvény szerint a jelentés, mint közokirat bizonyító erővel rendelkezik, azonban ténylegesen kevésbé szokták figyelembe venni; alá tudja támasztani azt, hogy az alperes elkövette-e az állítólagos cselekményt (DCCP 344. cikk (2)). Az DCCP 344. cikkének (1) bekezdésében említett „egyéb dokumentumok" függetlenek a közegtől és tartalmazhatnak elektronikus dokumentumokat[179].

A forenzikus digitális bizonyíték a bíróságon számos módon felhasználható: szakértő által írt hivatalos dokumentumként, a szakértő bírósági vallomásaként, a nyomozást végző tiszt hivatalos jelentéseként, amely tartalmazza a megfigyeléseket vagy bírói észrevételként amikor a bizonyíték a bíróságon számítógépen van bemutatva.

Az elektronikus bizonyítékot a rendőrség gyűjti be és tárolja. A DCCP és a rendőrség adatvédelmi törvénye szabályozza az elektronikus bizonyítékok összegyűjtését, tárolását és megsemmisítését. Az elektronikus bizonyíték elemzésének lehetősége azok számára van biztosítva, akiket a bírósági eljárás során bevontak, a büntetőeljárás részeként.

A holland joghatóságon kívül szerzett elektronikus bizonyítékokra nincs további szabályozás. A bíróságon egyéb bizonyítékként kezelik, a teljes nyilvánosságra hozatal alapján. Mégis, ha a nyomozati eljárás nem felel meg a DCCP által előírtakkal, a bizonyítékokat a bíró elfogadhatatlannak ítélheti meg. Ha a bizonyítékok összegyűjtését segítő ország speciális

[179] Algemene Rekenkamer(Prestaties in de strafrechtketen (2012, Uitgevers)

feltételeket szab, akkor a rendőrség és az ügyész tiszteletben fogja tartani ezeket a feltételeket. Mindazonáltal ez akadályozhatja a bizonyítékok bíróságön történő felhasználását.

6.3 Az írországi szabályozás elektronikus bizonyítékokkal kapcsolatban[180]

A számítógépes bűncselekmények nyomozása Írországban elsődlegesen a Számítógépes Bűnügyi Nyomozóegység (Computer Crime Investigation Unit-CCIU) feladata.

Az An Garda Síochána[181]-n belül a Számítógépes Bűnügyi Nyomozóegység (CCIU) az az elsődleges rendőri szerv, amelynek feladata a számítógépes bűncselekmények megelőzése és vizsgálata.

Feladatai a súlyos bűncselekmények kivizsgálása, így például:

- A számítógépes hálózati behatolások vagy -támadások a vállalati, magán- vagy kormányzati tulajdonú rendszerekben
- a komplex számítógépes bűncselekmények kivizsgálása
- valamennyi típusú bűncselekmény során lefoglalt informatikai eszköz igazságügyi vizsgálata, beleértve az internetes hálózatokat is
- a rendőröket összekötő és tanácsadó szervként működik a helyszíni vizsgálatok során
- az egyetlen kapcsolattartó a nemzetközi ügynökségek és partnerek részére, mint az EC3, Europol, FBI stb.
- képzést tart a rendőrségnek, a kormányzati szerveknek, a Szövetségi Banknak mind a kiberbiztonság, mind a számítógépes bűnözés területén
- képzést nyújt például az OLAF-fal vagy IACIS-szel együtt a rendőri szerveknek.

Az 1991-es írországi büntetőtörvénykönyv az adatot úgy definiálja, mint bármely „*olyan formátumban lévő információ, amelyhez számítógéppel (beleértve a programot) lehet hozzáférni*”. A 2011-es Távközlési (Adatok Megőrzése) Törvény az adatot úgy determinálja, mint forgalmi adatok vagy helyadatok, valamint az előfizető vagy felhasználó azonosításához

[180] Gordana Buzarovska - Lazetik és Olga Kosevaliska, „Digital Evidence in Criminal Procedures - A comparative approach”, *Balkan Social Science Review* 2, sz. 1 (2013): 66–83.
[181] Az An Garda Síochána az ír Nemzeti Rendőrség, amely általános rendészeti feladatokat, így közrendévédelmi, közlekedésrendészeti, bűnüldözési és bűnmegelőzési feladatokat lát el.

szükséges kapcsolódó adatok. A 2001-es büntető igazságszolgáltatásról szóló (lopással és csalással kapcsolatos bűncselekményekkel foglalkozik) törvény nem tartalmaz meghatározást az adatról, de az „információ nem olvasható formáját" olyan információként írja körül, amely mikrofilmen, mágnesszalagon vagy lemezen, vagy egyéb, nem olvasható formátumban van tárolva (elektronikus vagy más egyéb módon). A 2016-os büntető igazságszolgáltatás (Információs Rendszerrel Kapcsolatos Bűncselekmények[182]) törvényjavaslata az adat átfogó meghatározását teszi lehetővé, úgymint bármely tény, információ vagy koncepció olyan formában, amely lehetővé teszi feldolgozását egy információs rendszerben, beleérte az olyan programot is, amellyel az információs rendszer a folyamat elvégzésére képes lesz. Az ír jogban nincsen különleges definíció a tartalom, a helyadat vagy számítógépes adat fogalmaira.

Az információs rendszer a büntető igazságszolgáltatás (Információs Rendszerrel Kapcsolatos Bűncselekmények) törvényjavaslatban úgy van meghatározva, mint:

a) Egy eszköz vagy összekapcsolt, vagy összefüggő eszközök egy csoportja, amelyek közül az egyik egy program felhasználásával az adatok feldolgozását végzi és
b) az adat bármilyen célból kifolyólag az eszköz vagy eszközcsoport által van tárolva, feldolgozva, visszanyerve vagy továbbítva.

A törvényjavaslat rendelkezésében ez lesz az információs rendszerre vonatkozó egyetlen meghatározás az ír jogban. Egyéb definíció a fentebb említett többi kifejezésre nincsen. Az, hogy mégis mi alkot meg egy parancsot és annak formáját a számos bevont ügynökség között, a normál gyakorlat és a megegyezés szerinti formátum kérdése.

Az e-bizonyíték magába foglalja, de nem korlátozódik le, a regisztrációs információkra[183], az internetes böngészési előzményekre, tartalmakra, képekre és egyéb fájlokra és IP címekre. Az 1997-es büntető igazságszolgáltatás törvény (Vegyes Rendelkezések) 10. szakasza alapján általános meghatalmazást lehet szerezni az állítólagos bűncselekmény bizonyítékainak megszerzésére – olyan bűncselekményekére, amelyek 5, vagy annál több év börtönbüntetéssel sújttatandók. Az e-bizonyítékokat, amelyek üzleti felvételekből származnak a 6. szakasz által előírt módon kell szolgáltatni.

[182] Offences Relating to Information Systems
[183] Elektronikus levelezés szükséges felhasználónév, közösségi oldalak stb.

6.4 A spanyolországi e-bizonyítékokra vonatkozó szabályozás

Spanyolország számítógépes bűncselekményekkel kapcsolatos vizsgálat indoka leginkább a nyelvismeret és a Magyarországhoz hasonló gazdasági helyzet volt. Továbbá a rendőrség és az ahhoz szorosan kapcsolódó rendőrhatóság- a La Guardia Civil- szerepe miatt érdemel figyelmet.

Spanyolországban két típusú „rendőrhatóság" létezik a bűncselekmények megelőzésére és felderítésére, amelyek egyaránt rendelkeznek jogosítványokkal a számítógépes bűncselekményekkel(ciber delicto vagy crimen informatico) kapcsolatos nyomozó hatósági feladatokkal.

Az egyik hatóság a Nemzeti Rendőrség (National Police-NP), míg a másik a La Guardian Civil. Mind a két hatóság a spanyol Belügyminisztérium része és az úgynevezett Biztonsági Titkárság része[184].

A nemzeti rendőrséghez tartozik a Technológiai Nyomozó Egység (Technological Investigation Unit- UIT), ami egy olyan központi szervezet, akik a technikai jellegű felderítésért felelősek Spanyolország területén belül. Szerepük van továbbá a nemzetközi együttműködésekben, a képzésekben és a technikai segítségnyújtásokban.

Az UIT két egységgel rendelkezik. Az egyik egység a forenzikus vizsgálatok elvégzésére (a nyílt, online hálózatok vizsgálatával, valamint a gyermekpornográf tartalmú oldalak vizsgálata, az OSINT-tal stb), míg a másik egység az IT biztonsággal (kiberbiztonsággal) foglalkozik. Az IT biztonsággal foglalkozó egységen belül is további két szervezetet alakítottak ki, úgy, mint a logikai védelemmel továbbá a kibertámadásokkal foglalkozó szervezet[185].

La Guardia Civilnek is szerepe van a számítógépes bűncselekmények vizsgálata során. A számítógépes bűncselekményekkel foglalkozó további egység Spanyolországban a La Guardia Civil, ami nyers fordításban a hazai polgárőrségnek feleltethető meg, ám a hazai szervezettel ellentétben, a La Guardia Civil rendelkezik nyomozati jogkörrel[186].

[184] Solano, Miller Soto: El crimen on-line. Una mirada a la responsabilidad del proveedor de servicio de Internet. (Spanish) Akadémiai folyóirat, *Justicia Juris* , ene-jun2012, Vol. 8 Issue 1, p75-83, 9p;
[185] Andrea Giménez-Salinas Framis, José Luis González Álvarez: Investigación criminal- Principios, técnicas y aplicaciónes (Madrid, LID Editorial, 2016)
[186] Genval 7. körös jelentés

A helyes meghatározásuk a rendes rendőri egységek és a különleges bűnügyi egységek között található.

Spanyolországban található továbbá egy úgynevezett EMIMEs (Equipos Mujer Menor), akik a gyermekpornográfiával és a kiskorúak elleni bűncselekményekkel (mint a grooming) is foglalkozik.

A spanyol jogalkotók a büntető törvénykönyvben meghatározták az elektronikus bizonyíték fogalmát: bármilyen információ, amit generáltak/készítettek vagy tartottak, vagy átküldtek bármilyen elektronikus eszközzel, és amely képes tényeket megerősíteni a vizsgálat (nyomozás) során.

Az (elektronikus) bizonyítékokra vonatkozó eljárási szabályozás szerint, ugyanúgy kell eljárni, mint a hagyományos bizonyítékok esetében. Ugyanis azt a lefoglalás során le kell zárni és bíróság rendelkezésére bocsátani, aminek vizsgálatára a Bíróság saját hatáskörben vagy a rendőrség kérésére, szakértői vizsgálat alá vethető. A szakértő feladata az elektronikus bizonyítékok elemzése.

Ahhoz, hogy az elektronikus bizonyíték bizonyítékként felhasználják, csak abban az esetben lehetséges, ha annak hitelességéhez nem fér kétség, valamint egyértelműen alátámasztja azt egy hiteles dokumentumot vagy feltételezést.

Fontos kritérium, hogy a hitelességét semmilyen formában ne lehessen megkérdőjelezni.

6.5 Az Európai Unió digitális bizonyítékokra vonatozó szabályozása

Az Európai Parlament és a Tanács felismerte, hogy a számítógépes bűncselekmények során a digitális bizonyítékokra vonatkozó szabályozás ez idáig nem elégséges, hogy a nyomozó hatóságok hatékonyan tudjanak fellépni a bűnözőkkel szemben. A Bizottság 2018. április 17-én új szabályokat és rendeleteket javasolt, így létrehoz egy European Production rendeletet, ami lehetővé teszi egy tagállam igazságügyi hatóságai számára, hogy közvetlenül egy szolgáltatótól elektronikus bizonyítékokat szerezzenek (például e-maileket, szövegeket vagy üzeneteket alkalmazásokban, valamint információkat az elkövető első lépésként történő azonosításához), amelynek jogi képviselője 10 napon belül, vészhelyzet esetében pedig 6 órán belül köteles

válaszolni, ezzel is megszüntetve a tartalomszolgáltatók „privilégiumát”, hogy a hatósági megkeresésekre egyáltalán nem vagy csak jóval később válaszolnak.

A hatóság tapasztalata, hogy a szolgáltatók e-mail tartalmak megismerésének végett megkereséssel fordulnak hozzájuk, ám sokszor arra való hivatkozással, hogy a kért adat nem a megkeresett székhelyen található, hanem egy másik országban vagy földrészen található „felhőben”, ez a bizonyítékok beszerzésében, adatok megismerésében és további felhasználásában késlekedést okoz[187].

További probléma a határokon átnyúló bűnözés tekintetében, hogy még az Unión belül sem értékelik egyformán a bizonyítékokat, ami sokszor harmadik országoktól történő adatkérés tekintetében hatványozottan érvényesül.

A rendelet előkészítésnek tekinthető a Budapesti Számítástechnikai Bűnözésről szóló Egyezmény évek óta szükséges módosításához.

6.6 Konklúzió

Az európai unió valamennyi tagállamaiban az 1997. december 5- i 97/827/IB együttes fellépés a Tanács és az Európai Unióról szóló szerzése cikke alapján a szervezett bűnözés elleni nemzetközi kötelezettségvállalásokkal összhangban az általános ügyekkel és értékelésekkel foglalkozó munkacsoport a Genval, 2013. október 3-án határozott arról, hogy a kölcsönös értékelések hetedik fordulóját a számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet során a tagállamoktól meghatározott kérdésekre a tagállamoknak 2017. július 3-ig határidőt szabva kell válaszolniuk. Az elkészített jelentések alapján az európai államok válaszai alapján igyekeztem az elektronikus digitális bizonyítékokkal kapcsolatos holland, spanyol és írországi rendőrségi szervezetek valamint az e-bizonyítékok szabályozásával kapcsolatban megállapítható, hogy hasonlóságát mutatnak egymással, de leginkább a nemzeti rendőrségek szervezetein belül található egységek a törvényben meghatározott felhatalmazással és az Európai Unió irányelveivel- így például a 2013/40/EU irányelv az információs rendszerek

[187] „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. Letöltve: 2018. október 01.

elleni támadásokról, a Miniszteri Bizottság R (91) 11. számú ajánlása[188], az Európai Unió Kiberbiztonsági Stratégiája stb.

Az elektronikus bizonyítékokkal kapcsolatban az Európai Tanács 2017 október 18-i következtetései leszögezik, hogy „*Megoldásokat kell találni az elektronikus bizonyítékokhoz való, határokon átnyúló gyors és hatékony hozzáférés biztosítására a terrorizmus, valamint a súlyos és szervezett bűnözés más formái elleni hatékony uniós, illetve nemzetközi szintű küzdelem érdekében; a jogalkotási ciklus végéig meg kell állapodni az elektronikus bizonyítékokra, a pénzügyi információkhoz való hozzáférésre, valamint a pénzmosás elleni hatékonyabb küzdelemre vonatkozó bizottsági javaslatokról. A Bizottságnak sürgősen be kell nyújtania az elektronikus bizonyítékokkal kapcsolatos nemzetközi tárgyalásokra vonatkozó tárgyalási megbízásokat is.*”[189].

A Számítástechnikai Bűnözésről szóló Egyezmény második kiegészítő jegyzőkönyvében megfigyelhető többek között, hogy több ponton is sürgetik az elektronikus bizonyítékokkal kapcsolatos szabályozások kölcsönös elismerését és a büntetőeljárási szabályozások közelítését, amely segítséget jelentene nyomozó hatóságok a határok nélküli kibertérből összegyűjthető elektronikus bizonyítékoknál.

[188] Lanzarotte - egyezmény
[189] A Tanács határozata az Európai Tanács számítástechnikai bűnözésről szóló egyezményének (185. sz. CETS) második kiegészítő jegyzőkönyvére vonatkozó tárgyalásokon való részvétel engedélyezéséről

7 SZAKÉRTŐ

A szakértővel kapcsolatos kérdések érintésére csak olyan mértékben kerül sor, amennyire a kutatás során szükségesnek éreztük, hiszen egyik fontos eleme a büntetőeljárás statikus részének valamint szerepe az informatikai ismerek szükségességének világában megkérdőjelezhetetlen.

A kutatás során nem kívántunk olyan mértékben vizsgálódni, mint ahogy a doktori értekezésében tette azt Dr. Nogel Mónika[190] vagy Dr. Máté István[191], sokkal inkább a nyomozó hatóság munkájának folytatása során betöltött feladatait vizsgáltuk,

A szakértő szerepének vizsgálata szorosan összefügg a bizonyítás kérdésével, hiszen szerepük többek között a múltban történt események, tények vizsgálata. Szerepük funkcionális oldala tekintetében Tremmel kiemeli, hogy akkor kerül sor szakértői vizsgálatra és szakértői vélemény adására, ha az ügy eldöntéséhez szükséges tény megállapításához vagy megítéléséhez különleges szakértelem szükséges[192]. Továbbá kiemeli, hogy hatályos jogunk akkora bizalmat helyez a szakértőbe, hiszen a szakértői vizsgálatot a hatóság távollétébe is elvégezheti.

„A szakértőnek tudós bíróként, tények bírájaként való felfogása a bírói hatalom gyengítését, a szabad mérlegelés, az ügy összes körülményeinek megvizsgálásán alapuló, benső bírói meggyőződés elve elleni támadást jelentett[193]” jegyzi meg Székely János.

Milyen kapcsolat van a szakértő és a bizonyítás között? A szakértői vizsgálat olyan közvetett és összetett megismerési folyamat, amelynek során a szakértő nyomozást végez, szakmai tényeket állapít meg és következtetéseket von le. A szakértő tevékenysége átfogja többé-kevésbé a nyomozó szerepkörét is, igaz tevékenysége ténykérdésekre korlátozódik.[194]

Ahogyan Tremmel Flórián a bizonyításfogalommal kapcsolatos tanulságokat levonja:

a. A bizonyítás bonyolult, sokoldalú jelenség, ezért csak az egy oldalát kiemelő, metafizikus meghatározás nem lehet teljes.

[190] Nogel Mónika: Igazságügyi szakértői vélemények hiteltérdemlősége a büntetőeljárásban (Pécs, 2018)
[191] Máté István: Az igazságügyi informatikai szakértő szerepe és feladata (Pécs, 2017)
[192] Tremmel: Bizonyítékok a büntetőeljárásban (Dialog Campus, 2006) 129.
[193] Székely János: Szakértők az igazságszolgáltatásban (Közgazdasági és Jogi Könyvkiadó, Budapest, 1967) 61-62 o.
[194] Vö.. Székely János: Szakértők az igazságszolgáltatásban…62.o.

b. Ha a bizonyításnak nem tárjuk fel a döntő lényegét, akkor az egyes- egyébként lényegi ismérveket- nem tudjuk összefogni, egységbe vonni.
c. A bizonyítás döntő lényege csak dialektikus módon ragadható meg a bizonyítás sajátos viszony-és folyamatjellegének feltárásával.
d. Végül a lényegi ismérvek funkcionális (teleologikus) és strukturális (genetikus) kisegítő módszerrel is kifejthetők[195].

A szakértő bevonásának, szerepének fontossága, a szakértő igénybevétele egy büntetőeljárás során mindig is kérdéses. A szakvéleménynek egyre nagyobb szerepe van bizonyítási eszközök között, hiszen a technika, technológia fejlődésének köszönhetően a korábban meg sikertelenül befejezett ügyekben szerzett bizonyítékok értékelhetővé váltak és a bizonyítás és az elkövető felderítése is egyre sikeresebb lett.

A büntetőeljárási törvény alapján, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni[196].

Szakértelmet igénylő kérdésnek, vagyis szakkérdésnek minősíthető minden olyan releváns kérdés, ami nem minősül jogkérdésnek, és a bizonyításhoz szükséges felhasználhatósága szakértemet kíván.

A hatályos Be. (de más jogszabályok) ismét nem határozta meg a különleges szakértelem fogalmát, így az áttekintett jogirodalomban a következő, releváns meghatározást találtam: a jogi szakmától különböző, valamely más tudományos, technikai szakterületet, esetleg művészeti ágra vonatkozó ismereteket takarja. A szakértő a bíróság különleges szakértelmét pótolja, feladata a releváns szakkérdések megvilágítása és értékelése. Ebből következik, hogy a szakértő jogkérdésekben nem nyilváníthat véleményt [197].

A bizonyítás egyik eszköze, a szakvélemény elkészítésével, a szakértő kirendelésével összefüggésben, a jó-illetve rossz gyakorlattal kapcsolatban kerestem a választ a számítógépes bűncselekmények nyomozása során.

[195] Tremmel: Bizonyítékok a büntetőeljárásban (Dialog Campus 2006) 59.
[196] A büntetőeljárásról szóló 2017. évi XC. törvény 188.§ (1).
[197] 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. Letöltve: 2018. július 20.

A bizonyítás eszközei közé tartozik a szakvélemény, amelynek elkészítése csak az igazságügyi szakértői tevékenységről szóló törvényben meghatározott feltételek alapján végezhető[198].

Az igazságügyi szakértő feladata a hatóság kirendelése vagy megbízása alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel ...döntse el a szakkérdést[199]. Szakkérdésnek minősülnek azok a vizsgálatok, amelyek elvégzéséhez különleges szakértelem szükséges (pl.: halott személy esetében DNS vizsgálat, mérgezéssel összefüggő toxikológiai vizsgálat stb.)

A szakértő feladata, hogy az adott ügyben a hatóság által történt kirendelés alapján, a legjobb tudása szerint, pártatlanul, a szakértői kirendelő határozatban feltett kérdésekre, a törvényben meghatározott határidő alatt befejezze a vizsgálatot.

De: a szakértőnek nem feladata, hogy jogkérdésben döntsön, hiszen Erdei Árpád is kiemelte, hogy „a nem jogi természetű szakmai ismeretek alkalmazásának szükségessége jogi kérdések megítélése során azt a veszélyt idézi elő, hogy a büntetőjogi felelősség megállapítása- ha az a „szakkérdés" mikénti eldöntésétől függ-legalábbis részbe kikerül a hatóság kezéből. Nem bízhatunk abban, hogy e veszély csupán néhány tilalom felállításával kizárható[200].

7.1 Szakértő, szaktanácsadó és eseti szakértő

Szakértő alkalmazására akkor van szükség, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges.[201]

A meghatározás nem is feltétlenül szükséges, hiszen a különleges szakértelem szubjektív fogalom, ráadásul azt sem fejti ki a jogalkotó, hogy az adott szakértelem valamilyen különleges eszköz felhasználásával vagy pedig a szakember különleges tudásával függ össze.

[198] „2016. évi XXIX. törvény az igazságügyi szakértőkről", Pub. L. No. XXIX. törvény (é. n.), https://net.jogtar.hu/jogszabaly 5.-10.§§.
[199] Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3.§ (1) . letöltve: 2018. július 20.
[200] Erdei Árpád. i.m. 263.
[201] A büntetőeljárásról szóló 2017. évi XC. törvény188.§ (1) .

Általánosan azt a tudást értik alatta, hogy a büntetőeljárásban bíróként, ügyészként vagy nyomozóként részt vevő szakemberek általános szakmai ismeretének szintje, amibe értelemszerűen nem tartozik a jogi ismeret[202].

Ugyanakkor az informatikával kapcsolatos ismeretek igen széles körben mozognak, ezért azt, hogy pontosan mit is jelent a szakkérdés fogalma ebben az informatika tudományában, nehéz meghatározni.

Kezdve azzal, hogy a jogalkalmazók körében az, hogy melyik mobil eszköz, számítógép milyen típusú operációs rendszerrel működik, vagy melyik futtatható rajta, egészen a komoly informatikai tudást igénylő programozáson át eltérést mutat, amely összefügg az életkorral, a tanulással és a nyitottsággal az új tudás felé.

A rendőrségen dolgozó nyomozók tudása tekintetében is erős eltérések mutatkoznak, amit még nehezít is, hogy az informatikai eszközök szinte valamennyi bűncselekmény vagy szabálysértés esetében megtalálhatóak, mint bizonyítékot hordozó eszközök, így az sem teljesen egységes, hogy milyen esetekben elég egy egyszerű megállapítás.

Ehhez még hozzátartozik, hogy semmilyen iránymutatás, állásfoglalás nem született arra vonatkozóan, mely típusú vizsgálatok esetében szükséges a szakértő kirendelése és mely esetekben elég, ha az rendőri jelentés formájában (amely teljes bizonyító erejű okirat) az ügy gazdája végzi el.

A szakértő szerepe a büntetőeljárás során a rendelkezésre bocsátott adatok, eszközök vizsgálata a feltett kérdésekre, ezáltal a bizonyítékok szolgáltatása.

Az eseti szakértő olyan - az eljárásban megállapítandó vagy megítélendő jelentős tény vagy egyéb körülmény megállapításához vagy megítéléséhez - megfelelő szakértelemmel rendelkező természetes vagy jogi személy, aki nem igazságügyi szakértő; valamint olyan igazságügyi szakértő, aki az igazságügyi szakértői szakterületekről, valamint az azokhoz kapcsolódó képesítési és egyéb szakmai feltételekről szóló rendeletben meg nem határozott szakterületen ad szakvéleményt.[203]

[202] Bánáti és mtsai., *A büntetőeljárási törvény magyarázata - Az új, 2017. évi büntetőeljárási törvény magyarázata a kodifikációs bizottság korábbi tagjaitól*, 264.
[203] Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 2.§ (2).

A szakértői törvény szerint eseti szakértő is igénybe vehető, ha

a) az adott szakterületen nincs bejegyzett igazságügyi szakértő

b) az adott szakterületen - időszakos hiány vagy egyéb szakmai ok miatti hiány okán - a bejegyzett igazságügyi szakértők egyike sem tud eleget tenni a kirendelésnek, vagy

c) az adott szakterület nem szerepel a miniszter rendeletében felsorolt szakterületek között.

A szaktanácsadó szerepe ugyanakkor hasonló a szakértőjéhez, de valamilyen érthetetlen okból- feltételezzük az elfogultság látszatának elkerülése miatt- már nem rendelhető ki ugyanabban az ügyben szakértőként a korábban kirendelt szaktanácsadó.

Az igazságügyi szakértők a 9/2006. (II.27.) IM rendelet mellékleteiben határozza meg azokat a területeket és az ahhoz tartozó felsőfokú végzettséget, amelyek igazságügyi szakértői tevékenység végzésére jogosít:

- a tűzvédelmi, valamint személy- és vagyonvédelmi területeken
- orvosi, továbbá egyes pszichológiai és biológiai területeken
- munkabiztonsági területen
- mező- és erdőgazdálkodási, valamint az élelmiszer-ipari területeken
- közlekedési és az ipari területeken
- informatikai és hírközlési területeken
- környezetvédelmi, a természetvédelmi és a vízügyi területeken
- kulturális területen
- gyógypedagógiai és egyes pszichológiai területeken
- közgazdaság, vám- és egyes pénzügyi területeken
- lakás- és építésügyi, településrendezési, valamint az idegenforgalmi területeken
- kriminalisztikai területeken

- audiovizuális média területén

- titokvédelmi területen.

A szakértővel kapcsolatban a túlbizonyítással kapcsolatban Nogel Mónika doktori értekezésében foglalkozik és hivatkozik Erdei Árpádra.

Erdei szerint „Evidensnek látszik, hogy a szakszerű és racionális tevékenységben irreleváns tényekre nem lenne szabad energiát fektetni.[204]”.

A túlbizonyítással kapcsolatban megemlíthető az „alkalmatlan bizonyítási eszköz” vagy az az eset is, amikor a büntetőjogi felelősség megállapításakor kevesebb bizonyítási eszköz is elegendő lenne, az ügyben, amelyben bármilyen számítástechnikai eszköz vagy az adott bizonyítási eszközből az adott tényállás megállapítása tekintetében nem várható érdemi bizonyíték[205].

7.2 Az igazságügyi szakértői kirendelésének szükségessége

Összességében a szakértő kirendelésével kapcsolatos dilemmának az alapja az elkészített interjúk alapján sokszínűséget mutat. A megkérdezett nyomozók válaszaiból kitűnik, hogy a kibertérrel összefüggő bűncselekmények esetében azért rendelnek ki szakértőt, mert vagy félnek attól, hogy a digitális bizonyítékot nem ismerik fel, eljárási hibát követnek el a kényszerintézkedés végrehajtásakor, az ügy fajtája ténylegesen indokolja vagy az ügyben eljáró ügyészség csak a „pecsétes” papírt fogadja el és a hatóság tagja által készített jelentést, amely egyébként közokiratnak minősül, nem fogadják el, hanem szakértő kirendelését írják elő. A szakértőtől várják el azt a szaktudást, amivel nem rendelkeznek.

[204] Erdei Árpád: Tény és jog a szakvéleményben (Közgazdasági és Jogi Könyvkiadó, 1987) 162.
[205] Nogel Mónika: Igazságügyi szakértői vélemény hiteltérdemlősége a büntetőeljárásban, forrás: https://ajk.pte.hu/files/file/doktori-iskola/nogel-monika/nogel-monika-muhelyvita-ertekezes.pdf, (letöltve: 2019. február 08.)

7.3 Igazságügyi informatikai szakértő kirendelés

Az igazságügyi szakértő kötelezettségeivel kapcsolatban a 2016. évi szakértői törvényben foglaltak az irányadóak. Ez alapján a szakértő közreműködésre és véleményadásra kötelezett, ez a legalapvetőbb szakértői kötelezettség, ami nem más, mint a szakértői ténykedés formális lényege- fejti ki Dr. Idzigné dr. Novák Marianna Csilla a doktori értekezésében[206]. A szakértői ténykedés érdemi lényege, hogy a vizsgálatot valós, korszerű tudományos és szakmai ismereteknek megfelelően köteles a legjobb tudása szerint elvégezni.

A kirendelésre vonatkozóan általában a szokásjog játszhat szerepet, pedig egyes esetben az adott kérdés megválaszolása saját hatáskörben is megoldható lenne.

A nyomozás és a bizonyítás szempontjából elvárható magatartás az igazságügyi szakértővel, hogy ugyanolyan alapossággal, pártatlansággal járjon el, mint ahogyan az őt kirendelő személy (az ügy előadója) tenné, amennyiben rendelkezne azzal a különleges szakértelemmel, melyre vonatkozóan szakértő bevonását látta szükségesnek.

Szakértőtől elvárható tehát az az ismeret és jártasság, mely biztosítja számára, hogy a kirendelésekor birtokába került informatikai eszközök vagy elektronikus adatok vizsgálata, úgy történjen, hogy azok egyrészt a kirendelő határozatban megadott tényállásnak megfelelően a feltett kérdésekre teljes mértékben válaszoljon, kétség se férjen hozzá, hogy azok megőrizték eredetiségüket, változatlanságukat. Az elkészített szakértői véleménynek érthetőnek, világosnak kell lenni, hogy az alkalmas legyen a büntetőeljárásban a további felhasználásra.

Nem utolsó sorban pedig a szakértő kötelessége a számára átadott tárgyak, eszközök, adatok eredetiségének a megőrzése és a szakértői vélemény elkészítésével együtt a hatóság számára történő visszaadása.

A kirendelt szakértő köteles és jogosult mindazokat az adatokat megismerni, amelyek a feladatának teljesítéséhez szükségesek, e célból

a) az eljárás ügyiratait - a törvényben meghatározott kivételekkel

b) az eljárási cselekményeknél jelen lehet

[206] Dr. Idzigné dr. Novák Marianna Csilla: A szakértő státuszváltozása a hazai büntetőeljárásban- különös tekintettel a kizárásra vonatkozó szabályokra (Széchenyi István Egyetem, 2018.)

c) a terhelttől, a sértettől, a tanútól, a vagyoni érdekelttől, az egyéb érdekelttől és az eljárásban kirendelt szakértőtől felvilágosítást kérhet

d) a kirendelőtől újabb adatokat, ügyiratokat és felvilágosítást kérhet

e) a kirendelő felhatalmazása alapján a neki át nem adott tárgyi bizonyítási eszközt, elektronikus adatot megtekintheti, megvizsgálhatja, mintavételt végezhet.

A szakértő a vizsgálat során személyt és tárgyi bizonyítási eszközt, elektronikus adatot tekinthet és vizsgálhat meg, a személyhez kérdéseket intézhet[207].

Ha a szakértő olyan tárgyi bizonyítási eszközt vagy elektronikus adatot vizsgál meg, amely a vizsgálat folytán megváltozik vagy megsemmisül, annak egy részét lehetőleg az eredeti állapotban úgy kell megőriznie, hogy az azonosság, illetve a származás megállapítható legyen. A kirendelő meghatározhatja azokat a vizsgálatokat, amelyeket a szakértőnek a kirendelő jelenlétében kell elvégezni, ezáltal biztosítva van annak lehetősége, hogy a nyomozó hatóság a vizsgálatok során aktívan részt vegyen, ezáltal folyamatosan figyelemmel kísérje a szakvéleményének menetét.

7.4 A szakértői vélemény

A bizonyítékok értékelésénél Gödöny a szakértőkkel és a szakvéleménnyel szemben támasztott követelmények közül a hiteltérdemlőséget, a valósággal való egyezőséget, azaz az igaz voltának megállapítását emeli ki[208].

A szakértői bizonyítás kriminalisztikai szempontjából az alábbi tulajdonság emelhetők ki:

a.) a validitás vagy a vizsgálatok érvényességi foka, ami a levont következtetések és a valóság megfelelésének arányát jelenti. Annál magasabb a módszer érvényességi foga, minél nagyobb arányban esnek egybe a segítségével tett megállapításai a szakértőnek a valósággal,

[207] Büntetőeljárásról szóló 2017. évi XC. törvény 192.§.
[208] Gödöny József: Bizonyítás a nyomozásban (Közgazdasági és Jogi Könyvkiadó, Budapest, 1968) 212.

b.) reliability- megbízhatóság, annál megbízhatóbb egy adott eljárás, minél nagyobb azoknak a szakértőknek a száma, akik egymástól függetlenül ugyanarra a következtetésre jutnak a vizsgálati eredmények alapján,

c.) confidence- hitelesség, ami egy akkreditálási, minőségbiztosítási, minőségellenőrzési rendszer fenntartása. Ezek biztosítják az érvényes és megbízható módszerek alkalmasságának követelményeit.[209]

Ahogy Tremmel Flórán is rámutat a szakértői véleményre, hogy az részbizonyításnak is felfogható, hiszen az ügy bizonyításához szükséges szakértői vizsgálatra és -vélemény adásra, ha az ügy eldöntéséhez szükséges tény megállapításához vagy megítéléséhez különleges szakértelem szükséges[210]. A szakértői tevékenység során a szakértő különleges szakértelemmel rendelkezik, ami mind a ténymegállapításhoz mind pedig a következtetések levonásához szükséges (Tremmel).

Ugyanakkor a nyomozás során a szakértő által készített szakvélemény-más bizonyítási eszközhöz hasonlóan- részbizonyításnak, azaz „makrobizonyításnak" minősül, hiszen az ő feladata a rendelkezésre bocsátott bizonyítékok, valamint az őt kirendelő határozatban feltett kérdésekből levonható következtetések megállapítása, azok alapján a vélemény elkészítése.

A részbizonyításnak van funkcionális és strukturális aspektusa. Amíg az előbbi alatt azt értjük, hogy akkor kerül sor szakértői vizsgálatra és szakértői vélemény adására, amennyiben az ügy eldöntéséhez szükséges tény megállapításához vagy megítéléséhez különleges szakértelem szükséges. Addig az utóbbi oldal esetében a szakértés önmagában véve olyan közvetett és összetett megismerési folyamat, amely esetében a szakértő vizsgálatot végez és a különleges szakértelme segítségével szakmai tényeket állapít meg és következtetést von le[211].

Az Amerikai Egyesült Államokban a szakvéleménnyel kapcsolatban szükséges pozitív példakánt említeni a Daubert-ügyet, amelyben a Legfelsőbb Bíróság összeállította azokat a legfontosabb szempontrendszereket, amelyeket vizsgálni kell:

- A szakértői technika vizsgálata, illetve az annak alapjául szolgáló elméleteket tesztelték-e már vagy tesztelhető-e

[209] Kertész Imre: A szakértői bizonyítás (In:Kriminalisztika 1., BM Duna Palota és Kiadó, 2004) 231-232.
[210] Tremmel: Bizonyítékok a büntetőeljárásban (Dialog Campus, 2012) 129.
[211] Tremmel: uaz. 129.

- A szakértői vélemény alapjául szolgáló elméletet publikálták-e már lektorált szaklapban?

- Meghatározták-e a technika vagy a módszer hibaszázalékát annak alkalmazása során és vannak-e a technikai folyamat ellenőrzésének standardjai,

- Milyen az adott szakmai terület elfogadottsága a tudomány képviselői részéről[212]?

A felsorolt szempontok a szakértői vélemény megbízhatóságát garantálja.

Az új szakértői törvény a szakértői vélemények tartalma vonatkozásában az alábbi kötelezettségeket fogalmazza meg[213].

„*A szakvéleménynek tartalmaznia kell*

a) *a leletet*

b) *a vizsgálat módszerének rövid ismertetését*

c) *a szakmai ténymegállapításokat*

d) *a szakértő véleményét*

e) *ha az ügyben korábban vizsgálat lefolytatására került sor és a kirendelés erre kiterjed, a korábbi vizsgálatra vonatkozó adatok és megállapítások értékelését*

f) *a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokai*."

A szakértő- valamennyi típusú igazságügyi szakértőt értve alatta[214]- részvételének szükségessége a számítógépes bűncselekmények nyomozás vagy bármelyik eljárási cselekmény során vita tárgyát képezheti.

Nincs egységes álláspont sem a hatóságok, sem a büntetőeljárás egyéb résztvevői- így az ügyészség, bíróság- között annak tekintetében, hogy van-e szükség szakértő kirendelésére és

[212] Forrás: https://www.theexpertinstitute.com/the-history-of-daubert-v-merrell-dow-pharmaceuticals/ letöltve: 2019.01.30.
[213] 2016. évi XXIX. törvény az igazságügyi szakértőkről 47 § (1).
[214] Az igazságügyi szakértők típusát, ahol szükséges pontosan meg fogom határozni. Amikor a szakértő kifejezést használom, akkor, mint gyűjtőfogalmat értem alatta

ha igen, mikor szükséges a kirendelése, vagy pedig fölösleges pénzkidobás a legtöbb esetben, hiszen azokat a vizsgálatokat, amelyeket elvégez, azt akár a helyi informatikus vagy rendszergazda is el tudja végezni.

A szakértő vagy szaktanácsadó igénybevételével kapcsolatban:

A korábbi büntetőeljárásról szóló törvény alapján csak abban az esetben szükséges a szakértő kirendelése, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges[215], ennek szabályozása a 2017. évi XC. törvényben sem változott.

A különleges szakértelem fogalma Kertész szerint: *olyan tudományos (orvosi, vegyészi) ismeret vagy gyakorlati tapasztalat bármely szakma területéről, amely az adott korban és társadalomban kívül esik az általános műveltséghez tartozó ismeretanyagon és a jogi szakértelmen. Ezekben a kérdésekben szakértőt kell bevonni az eljárásba, még abban az esetben is, ha az eljáró személy maga is rendelkezik azzal a különleges szakértelemmel*[216].

Amíg például egy DNS vizsgálat, egy testi sértés súlyosságának, nemi erőszak megtörténtének megállapításához elmeállapot eldöntéséhez orvosszakértő kirendelése-, és a szakértő véleménye elengedhetetlen, addig lehetséges lenne-e, hogy az egyes számítógépes bűncselekmények nyomozása során az ügy típusa és a hatóság eljáró tagja elvégezzen-e bármilyen „szakértői" vizsgálatot, amely alkalmas lehet az adott bűncselekmény elkövetésének rekonstruálásához és minden kétséget kizáró ténymegállapításhoz?

Kertész gondolatai alapján *„Ha az eldöntendő kérdés megoldása különleges szakértelmet igényel, akkor a szakértő bevonása még akkor is kötelező, ha az eljáró nyomozó, ügyész vagy bíró rendelkezik ezekkel a szakismeretekkel. A szakértői vizsgálatokkal megállapítható kérdések köre áttekinthetetlen és a tudomány, valamint a technika haladásával egyre tovább bővül. A jog nem határozza meg ezt a kört, de ugyanakkor egyes esetekben kötelezővé teszi a szakértő igénybevételét."* [217].

A szakértő alkalmazása kötelező, ha

[215] A régi büntetőeljárásról szóló 1998. évi XIX. törvény 99.§ (1)
[216] Kertész Imre: A szakértői bizonyítás (In: Kriminalisztika, BM Kiadó, 2004) 200.
[217] Kertész: uaz. 201.

a) a bizonyítandó tény, illetőleg az eldöntendő kérdés személy kóros elmeállapota, illetőleg kábítószer függősége

b) a bizonyítandó tény, illetőleg az eldöntendő kérdés kényszergyógykezelés szükségessége

c) a személyazonosítást biológiai vizsgálattal végzik

d) elhalt személy kihantolására kerül sor.

A számítógépes bűncselekmények esetében a szakértő kirendelése, mint az eddig ismertetett eljárási szabályok során, eltérő.

Az igazságügyi szakértőkről szóló törvény alapján tehát „*Az igazságügyi szakértő feladata, hogy a hatóság által kirendeléssel vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményének felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását”*[218]

A szakterületek elkülönítése a Szaktv.2005 3. § (1) / Szaktv.2016 5. § (5) bekezdésében foglalt felhatalmazás alapján a 9/2006. (II. 27.) IM rendeletben történik meg. A rendelet az informatika vonatkozásában az alábbi (szak)területeket határozza meg:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
- informatikai biztonság
- informatikai rendszerek tervezése, szervezése
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
- számítástechnikai adatbázis, adatstruktúrák
- szoftverek[219]

[218] Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1.

[219] 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. letöltve: 2018. október 01.

Az informatikai szakértő kirendelésével kapcsolatban fontos, hogy ne azért történjen meg annak igénybevétele, mert a hatóság a jogszabályok és/vagy alapvető informatikai tudás birtokában nem képes az ügyben dönteni, hiszen magának a szakvéleménynek az elkészítése időigényes és esetleg fölösleges bűnügyi költséget generálhat. A szakértő kirendelése mellett szóló érvek:

- Mivel a digitális nyomok változó környezetben keletkeznek, így annak változatlanságának biztosítására az átlagosnál magasabb szakértelemre is szüksége lehet

- (Ház)kutatás és lefoglalás során a szakértő igénybevétele a nyomok rögzítésénél hasznos lehet

- A tiszta, világos megfogalmazás

- A bíróság előtt sokszor nagyobb érvényt lehet szerezni a vádnak.

A szakértő kirendelése ellen szóló érvek:

- A nem alapos vagy nem érthető szakértői vélemény nehezítheti a nyomozást, vagy nem megfelelő bizonyítékot eredményezhet.

- Esetlegesen a szakértő elfogulatlansága megkérdőjelezhető, mint ahogy a nyomozó elfogultsága, az ügy sikerességének siettetése is kétséget ébreszthet.

- A szakértés elvégzésére nyitva álló határidő a 60+30 nap, egyes esetben hosszú, indokolatlanul késlekedhet annak befejezésével.

- Sokszor indokolatlanul magas a szakértő díjazása.

- A hatóság nem mindig szakkérdésben veszi igénybe, sokkal inkább az általános ismeretek hiánya miatt rendelhet ki szakértőt.

A szakértő alkalmazása kirendeléssel – határozattal- történik, amelyben meg kell jelölnie

a) a szakértői vizsgálat tárgyát és azokat a kérdéseket, amelyekre a szakértőnek választ kell adnia

b) a szakértő részére átadandó iratokat és tárgyakat, ha az átadás nem lehetséges, az iratok és a tárgyak megtekintésének helyét és idejét

c) a szakvélemény előterjesztésének határidejét.

Ha a szakvélemény elkészítéséhez sürgős részvizsgálatra van szükség, e vizsgálat kirendelő határozat nélkül, az ügyész vagy a nyomozó hatóság szóbeli rendelkezése alapján is elvégezhető.[220]

A szakértő a szakvéleményét két hónapon belül kell, hogy előterjessze. Ez a határidő a szakértő kérelmére egyszer, legfeljebb egy hónappal hosszabbítható.

Az eljárási törvény szerint általában egy szakértőt kell alkalmazni egy eljárásban az adott szakkérdésben. Ha a vizsgálat jellege szükségessé teszi, több szakértő is kirendelhető. Ez úgy is történhet, hogy a kirendelés csak a szakértői csoport vezetőjét jelöli ki, és feljogosítja őt arra, hogy a többi szakértőt bevonja.

7.5 A szakértő kirendelésének lehetősége

A bíróság, az ügyész, illetőleg a nyomozó hatóság a szakértői névjegyzékben szereplő igazságügyi szakértőt, illetőleg szakvélemény adására feljogosított gazdasági társaságot (a továbbiakban: gazdasági társaság), szakértői intézményt, vagy külön jogszabályban meghatározott állami szervet, intézményt, szervezetet (a továbbiakban: szervezet), ha ez nem lehetséges, kellő szakértelemmel rendelkező személyt vagy intézményt (a továbbiakban: eseti szakértő) rendelhet ki szakértőként.

A kérdések alapján a rendőrségnél a következő általános gyakorlatokról szereztünk tudomást: A bűnügyi állomány tekintetében a házkutatás és lefoglalás eljárása a bűncselekmények típusától függ. Amennyiben feltehetőleg elektronikus adat kerül lefoglalásra, úgy egy CD-t vagy DVD-t esetleg külső merevlemezt visznek magukkal, amelyre a vizsgálni kívánt adatokat kimentik. A saját maguk által vitt eszközöket lefoglalják a büntetőeljárási törvényben előírtaknak megfelelően, majd ezt követően szakértőt rendelnek ki, amelynek feladata az adathordozó átvizsgálása, a kirendelő határozatban feltett kérdések megválaszolása. Ugyanakkor, amennyiben nagyobb adat lefoglalása és vizsgálata válik szükségesség, úgy az egész számítógép, illetve informatikai eszköz lefoglalása mellett szoktak dönteni. Arra a kérdésre, hogy milyen módon hozzák el a számítógépeket, informatikai eszközöket, meglepő

[220] A büntetőeljárásról szóló 2017. évi XC. törvény 189.§ (1)-(2) .

válasz született: az áramforrásból és a hálózatból eltávolítják, majd ezt követően valamennyi ki-és bemeneti egységet leragasztják és a rendeletnek megfelelően bűnjelezik majd szállítják be a kapitányságra vagy közvetlenül az igazságügyi informatikai szakértőhöz.

A lefoglalás tekintetében nincs protokoll, hanem az ügy előadója, sokszor saját elgondolása szerint, dönt arról, hogy kell-e, mikor és milyen módon történjen meg annak végrehajtása.

7.6 Szakértő vs. szaktanácsadó

A szaktanácsadó, hasonlóan a szakértőhöz, különleges szakértelemmel rendelkezik, de az eljárás során segítségéhez, tudásának igénybevételéhez kirendelés nem szükséges, ellentétben a szakértővel.

Felkérése történhet írásban és szóban, a feladatának ismertetése mellett. Ő szakvéleményt nem készít, csak felvilágosítást ad, mégis egy helyszínen elvégzendő feladata, segítsége semmivel sem csekélyebb, mint a szakértőnek.

Amíg a szakértő a rendelkezésre álló adatokból, az eljárás személyeitől adatokat, felvilágosítást kérhet, egyes eljárási cselekményeknél jelen lehet, addig a szaktanácsadó, mint a hatóság segítőjeként kihallgatható tanúként[221], jogosult olyan jellegű technikai tevékenység elvégzésére, amelyet a hatóság önmaga is elvégezhetne[222], esetleg akár a technikai felkészültsége, modernebb eszközök megléte az, ami miatt segítsége különösen fontos lehet egyes esetben.

7.7 A szakértő kirendelésével kapcsolatos tapasztalat

A Fővárosi Főügyészségtől kapott tájékoztatás szerint nem volt jellemző az elmúlt években, hogy a szakértő túlterjeszkedett volna a kompetenciáján. Ugyanakkor nem megengedhetőnek értékelik, ha a nyomozó hatóság tagja a kirendelő határozatban arra kéri a szakértőt, hogy a

[221] BH 165. számú állásfoglalás
[222] Kertész: A szakértői bizonyítás (In: Kriminalisztika, BM Kiadó, 2004) 200.

bűncselekménnyel kapcsolatban keressen adatokat, ugyanis ez már a saját kompetenciáján, feladatán történő túlterjeszkedés.

Az ügyészségen elfogadhatónak ítélik meg, ha bizonyos esetekben az ügyben eljáró hatóság végzi el az adatállomány elemzését, értékelését, de arra vonatkozóan ők sem tudták meghatározni, hogy pontosan milyen kérdésnél húzható meg a határ.

A helyszínen igénybe vett szakértő vagy szaktanácsadó feladata, a számítógép átvizsgálása a hatóság irányítása alatt nélkülözhetetlen lehet. Ugyanakkor, ahogy a táblázatban is megtekinthető az informatikai szakértők is specializálódnak, így amennyiben nem a szakterületének megfelelő területről ad ki szakvéleményt, úgy azt a bizonyítékok értékelésénél nem vehető figyelembe.

Ugyanúgy aggályos, ha a szakértő nemcsak az adatok átvizsgálását végzi el, hanem egyes esetben kijelenti, hogy annak tartalma alapján milyen bűncselekmény elkövetése állapítható meg.

Példa:

Amennyiben egy elektronikus adat tartalmával kapcsolatban a szakértő megjegyzi, hogy egyes adatokon 18. életévet be nem töltött személy látható és ezáltal a kényszerintézkedést elszenvedő vagy az adat tulajdonosa elkövette a gyermekpornográfia bűncselekményét, úgy a saját kompetenciáján túlterjeszkedett. Amennyiben a hatóság ezen túl nem rendel ki a feltételezés megállapítására orvosszakértőt, úgy a gyanúsítás nem megalapozott, azt a bíróság nem veszi figyelembe.

7.8 Konklúzió

A fejezetben a szakértőkre, a szakvéleményre, szaktanácsadóra vonatkozó a büntetőeljárásjogi és kriminalisztikai szabályozást, rendelkezést igyekeztünk a legteljesebb mértékben számba venni, áttekinteni.

A kutatás során a Legfőbb Ügyészségen is a szakértő kirendeléssel és szakvélemény elkészítésével kapcsolatos kérdéseket és azokra adott választ valamint az elvégzett kérdőíves kutatást összevetettük.

A szakértő kirendelésének szükségessége a jelen helyzetben sokszor elengedhetetlen, ugyanakkor a hatóságok több esetben is a szakvélemény elkészülésétől, a szakértőtől várják az ügyek megoldását. A kérdésben állást foglalni ténylegesen csak akkor lehetne, ha a hazai viszonylatban megszületne egy olyan egységes állásfoglalás, útmutató, amely akár tételesen felsorolná azokat a bűncselekményeket, ahol szükséges a szakértő (itt igazságügyi informatikai szakértőt értek) kirendelése, vagy amiben egységes álláspont vélemény születne arra vonatkozóan, hogy melyek azok a nyomozó hatóság által is elvégezhető cselekmények, amiket a szakértelemmel (de nem Katona Imre által meghatározott különleges szakértelmet értve alatta) akár a bűnüldözéssel foglalkozó szervek is végre tudnak hajtani, és amelyek minden kétséget kizáróan hitelesnek fogadnak el a bírósági eljárás során.

Az informatikai tudás és eszközök fejlődése, szélesebb körben történő használata miatt a nyomozó hatóság körében szükséges lenne mind a továbbképzés, amely következtében elkerülhető lenne a felesleges kirendelések és nem a ténykérdésre vonatkozó szakértői kirendelésben feltett kérdések, ezáltal a fölösleges szakértői díjjak kifizetése.

Ugyanakkor a folyamatos konzultáció, megbeszélés a nyomozó hatóságok, a Magyar Igazságügyi Szakértői Kamara, a bíróságok és ügyészségek közötti rendszeres kommunikáció az oknélküli és értelmetlen kirendelések elejét venné.

Milyen vizsgálatok végezhetők el a szakértő igénybevétele nélkül?

1. Egy adott informatikai- vagy mobileszköz típusának, IMEI, IMSI számának megállapítását a nyomozó hatóság bármely tagja el tudja végezni, még abban az esetben is, ha a készüléken nem látható ez az információ.

2. Annak megállapításához sem szükséges szakértő kirendelése vagy a szakértőt kirendelő határozatban annak a kérdésnek a feltétele, hogy az adott eszköz mobiltelefon-e, számítógép-e stb.

3. Amennyiben a mobiltelefonon lévő információk hozzáférhetők, úgy az abban tárolt fényképek, telefonkönyv, kimenő-, bejövő, nem fogadott hívások mind a telefon menüjéből, mind pedig a szolgáltatótól beszerezhetők, az ügy előadója önállóan képes megnézni. Ugyanez vonatkozik az üzenetekre is.

4. Amennyiben a számítástechnikai rendszer hozzáféréséhez szükséges jelszó rendelkezésre áll, arról természetesen feljegyzést kell készíteni, az abban tárolt

adatok tulajdonságaihoz, kiterjesztésükhöz, típusának megállapításához szintén nem kell szakértő kirendelése.

8 KÉNYSZERINTÉZKEDÉSEK SORÁN BESZEREZHETŐ ADATOK

A hatályos Be. alapján a kényszerintézkedések közül két szabályozással foglalkoztunk ebben a fejezetben, a házkutatás és a lefoglalás, mivel a kibertérben történt elkövetés esetében szintén speciális eltéréseket mutatnak a végrehajtás tekintetében.

8.1 A kutatás és lefoglalással kapcsolatos szabályozás

A kényszerintézkedések közül a kutatás és a lefoglalás a számítógépes bűncselekmények tárgyi bizonyítási eszközeinek beszerzésénél egy „hagyományos tárgytól" kriminalisztikai módszerét tekintve Matus Márk, programozó szerint *nem különbözik, mégis a számítástechnikai berendezések egy része rendelkezik bizonyos egyedi tulajdonságokkal (pl.: az adathordozó és az adatok sérülékenysége), amelyek a bizonyításra való alkalmasság megóvása érdekében az általános kriminalisztikai ajánlások sajátos alkalmazási módját igénylik*.[223]

A számítástechnikai eszközök berendezések használata, az említett digitális lábnyomok keletkezése során szintén nyomról beszélünk kriminalisztikai értelemben, hiszen a nyom olyan fizikai elváltozás, amely a bűncselekmény elkövetésével kapcsolatban keletkezett és így lehetővé teszi a bűncselekmény elkövetésével kapcsolatban keletkezett és így lehetővé teszi a bűncselekmény megvalósulására, illetve az elkövetőre vonatkozó következtetések levonását[224].

8.1.1 A kutatás

Nem új eljárási cselekményként, hanem a házkutatás kifejezés helyett alkalmazza a jogalkotó a kutatást, mint kényszerintézkedést. Annak végrehajtásakor a hatóság beleavatkozik az Alaptörvényben meghatározott kutatást elszenvedő személy(ek)alapvető jogaiba, azáltal, hogy a bűncselekmény gyanúja esetén annak bizonyítására, a bizonyítékok felkutatására, az elkövető

[223] Matus Márk: Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben (In: Kriminalisztika könyv, BM Duna Palota, BM Kiadó, 2004) 286.- Matus Márk, egykori rendőrségi - és igazságügyi informatikai szakértő
[224] Tremmel Flórián-Fenyvesi Csaba-Herke Csongor: Kriminalisztika (Dialóg Campus, 2009) 47.

kilétének megállapítására, valamint az információs rendszer illetve adathordozó átvizsgálása érdekében hajtja végre.

A kutatás a büntetőeljárás eredményes lefolytatása érdekében a lakás, az egyéb helyiség, a bekerített hely vagy a jármű átkutatása. A kutatás információs rendszer, illetve adathordozó átvizsgálására is kiterjedhet.

A kutatásra vonatkozó eljárási szabálynál nincs lényegi változás annak elrendelése tekintetében. Így akkor kerül az elrendelésére, ha:

a) bűncselekmény elkövetőjének elfogására
b) bűncselekmény nyomainak felderítésére
c) bizonyítási eszköz megtalálására
d) elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására, vagy
e) információs rendszer, illetve adathordozó átvizsgálására vezet[225].

A kutatást a bíróság, az ügyészség vagy a nyomozó hatóság saját hatáskörében eljárva rendelheti el az új eljárási törvény életbelépése után.

Ha a kutatás elrendeléséhez szükséges bírósági határozat meghozatala olyan késedelemmel járna, amely a kutatással elérni kívánt célt jelentősen veszélyeztetné, a kutatás a bíróság határozata nélkül is végrehajtható. Ilyen esetben a bíróság határozatát utólag haladéktalanul be kell szerezni. Ha a kutatást a bíróság nem rendeli el, annak eredménye bizonyítékként nem használható fel[226].

A kutatást elrendelő határozatnak tartalmaznia kell a kutatás célját és az elrendelését megalapozó tényeket.

Ha ez lehetséges, a kutatást elrendelő határozatban meg kell jelölni azt a személyt, bizonyítási eszközt, elkobozható vagy vagyonelkobzás alá eső dolgot, információs rendszert vagy adathordozót, aki vagy amely megtalálására a kutatás irányul.

A kutatást az érintett ingatlan vagy jármű tulajdonosának, birtokosának vagy használójának a jelenlétében kell végrehajtani.

[225] Be. 302.§ (1).
[226] Be. 303.§ (3).

A kutatásra vonatkozó lényeges változások nem történtek, így annak megkezdése előtt ismertetni kell a kutatást elrendelő határozat tartalmát, és a határozatot a helyszínen kézbesíteni kell[227].

Ha a kutatás meghatározott személy, bizonyítási eszköz, dolog, információs rendszer vagy adathordozó megtalálására irányul, akkor fel kell szólítani az érintett ingatlan, illetve jármű tulajdonosát, birtokosát vagy használóját, illetve az általa megbízott személyt, hogy a keresett tárgyi bizonyítási eszköz vagy személy hollétét fedje fel, illetve a keresett elektronikus adatot tegye hozzáférhetővé. A felszólítás teljesítése esetén a kutatás csak akkor folytatható, ha megalapozottan feltehető, hogy a kutatás során más bizonyítási eszköz, dolog, információs rendszer vagy adathordozó is fellelhető.

A Be. 305.§ (4) bekezdés szerint amennyiben a hatóság felszólítására az elektronikus információs rendszer vagy adat önkéntes hozzáférhetővé tétele megtörténik, a kutatás nem folytatható tovább, kivéve, ha feltehető, hogy további bizonyítási eszköz, tárgy dolog, illetve információs rendszer vagy adathordozó is fellelhető.

Mennyire tekinthető eredményesnek az a kényszerintézkedés végrehajtása, ha az azt elszenvedő fél a biometrikus adatokkal, jelszavakkal védett rendszert úgy teszi hozzáférhetővé, hogy azokat nem bocsájtja a hatóság rendelkezésére? A jogalkotó itt ismételten figyelmen kívül hagyta azokat a technikai megoldásokat, amelyekkel lehetővé teszik azt a felhasználók számára, hogy a rendszereiket a lehető legbiztosabb megoldásokkal védjék és amelyek kikerülése által a bizonyítékok megőrzéséhez, sérthetetlenségének és hitelességnek kétsége, a hatóság vagy szakértő által történő változatlanságának követelménye sérülhet.

A kutatás, lefoglalás és bűnjelkezelés során a hitelesség folyamatos biztosítása jelenti az egyik legkomolyabb gondot tehát[228].

A kutatás végrehajtását egy tervezésnek kell megelőznie, amely során a nyomozók adatkéréssel információgyűjtéssel, tanúkihallgatással, szaktanácsadó igénybevételével beszerezhetik azokat az adatokat, információkat, amelyekre szükség van, illetve azok feltalálható milyen eszközöket kell keresni. Annak tudatában lehetne előre tervezni, hogy hogyan hajtják végre a kényszerintézkedést. De, nem minden információ szerezhető meg az eljárási törvényben

[227] Be.303.§ (3).
[228] Vö. MatusMárk: Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben (Kriminalisztika, I) 292. o.

meghatározott lehetőségekkel. Így tervezés során nem deríthetők fel azok az eszközök (pl.: pendrive, SSD kártya), amelyek a kereskedelmi forgalomban bármikor és bárhol beszerezhetőek és amelynek mérete alkalmassá teszi a könnyű elrejtésre.

Fontosnak tartottuk annak hangsúlyozását, hogy ma már bármilyen bűncselekményről legyen szó- akár számítástechnikai térhez kötött, akár számítástechnikai térhez nem kötött bűncselekményről van szó - a gyanúsított vagy sértett birtokában lévő az informatikai eszközöknek szerepük van a bizonyítás tárgya vagy eszköze tekintetében,[229] így azok rejtekhelyét, az azzal kapcsolatos teendőket szükséges megtervezni, az adathordozókra történő esetleges rögzítésre felkészülni.

Az ügyészség az interjú során - amely még 2018. július 1.-je előtt az alábbi eseteket, nyomozási eljárásokat emelte ki:

- A számítástechnikai és telekommunikációs eszközök vonatkozásában a hatóságok a Nyor[230]. alapján, valamint a lefoglalt eszköz tekintetében az arra vonatkozó BM-PM rendeletnek megfelelően járnak el.
- Tapasztalatként említik, hogy amennyiben felmerül annak lehetősége, hogy számítástechnikai eszköz átvizsgálása válhat szükségessé, úgy informatikai szakértőt rendelnek ki, akik esetleg már a (ház)kutatás alkalmával is megjelennek, elvégzik az adatok és eszközök szakszerű átvizsgálását, szükség esetén az adatok mentését
- Bizonyos esetekben szakirányítást kérnek az KR NNI-től vagy a BRFK KGBEFO-tól, esetleg igénylik, hogy a szakirányítóként megjelölt szervezet segítsen a helyszínen a végrehajtásban vagy a bizonyítékok értékelésében, elemzésében.

A tapasztalat ugyanakkor, hogy nem minden kapitányság rendelkezik megfelelő eszközökkel és a rendőrség állománya a szaktudás hiányossága vagy hiánya miatt sokszor vesznek igénybe külső segítséget. A külső segítség, a szakértő vagy szaktanácsadó, aki a helyszínen elvégzi azokat a teendőket és rendelkezik azokkal az eszközökkel, amik a sikeresen végrehajtott kutatáshoz elengedhetetlen.

Az információs rendszerben létrejönnek olyan információk, amelyek a különböző alkalmazások, szoftverek segítségével keletkeznek- dokumentumok, táblázatok, az internetről

[229] Dr. Ruxandra Raducanu: Aspects of legislative novelty in the domain of office offences. Noutăţi legislative în spaţiul juridic penal european. Ed. Universitaria, Craiova, 2008, p. 260-262. (ISBN 978-606-510-041-1)
[230] A Nyor.-t felváltott a 100/2018. (VI.8) Korm. rendelet

letöltött képek, stb, (digitális lábnyom) amelyek háttérinformációval szolgálhatnak a hatóság számára és amelyek egyébként nem beszerezhetőek, csak az informatikai eszköz és a rajtalévő adat átvizsgálásakor.

Ha csak egy bizonyos információra van szükség, amelynek szolgáltatására az állami, önkormányzati szerv egyébként is köteles, és az információ kinyeréséhez nem szükséges speciális ismeret, akkor a nyomozó hatóságok a megkeresés eszközéhez nyúlnak, azaz küldenek egy átiratot. Erre példa lehet annak lekérdezése, hogy adott időszakban mely munkatársak végeztek munkát az állami, önkormányzati szerv adott épületében.

Ha a beszerzendő információ az eljárás szempontjából kiemelten fontos, vagy annak kinyeréséhez speciális információ szükséges, esetlegesen tartani lehet attól, hogy az adatokat törlik vagy felülírják, akkor egy erőforrás-igényesebb és gyorsabb eljárási cselekmény következhet: a lefoglalás. Erre példa lehet, amikor a nyomozó hatóság akár az állami, önkormányzati szerv épületében önálló cselekményként, akár egy nyilatkozattételre jogosult személy tanúkénti kihallgatása alkalmával lefoglalja a munkatársak rendszerhasználatáról szóló logfájlokat tartalmazó adatokat és az azokat rögzítő adathordozót.

A kutatás az eljárás alá vont személy jogaiba történő egyik legerősebb beavatkozás a fentebb említettek közül. Tipikusan akkor alkalmazható, ha más intézkedés nem biztos, hogy eredményre vezetne, vagy a nyomozás érdekében ez tűnik a legcélszerűbbnek. Jellemzően akkor kerül foganatosításra, ha az eljárás alá vont személy nem együttműködő, vagy a beszerzendő adat, információ nem egyszerűen körülírható, annak kigyűjtéséhez speciális ismeret szükséges. Példaként jelölhető, amikor az állami, önkormányzati foglalkoztatott a hivatali informatikai eszközöket használja fel illegális tevékenységre például zsaroló, fenyegető e-mailek küldésére, gyermekeket ábrázoló pornográf felvételek tárolására[231].

Az eljárásjog szerint tárgyi bizonyítási eszköz alatt értendő minden olyan tárgy - ideértve az iratot és az okiratot is -, amely a bizonyítandó tény bizonyítására alkalmas, többek között:

a) amely a bűncselekmény elkövetésének, vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza
b) amely a bűncselekmény elkövetése útján jött létre

[231] Gyaraki és Simon, „Biztonsági események rendészeti szempontból – A kiberbűncselekmények kezelése”.In: Incidensmenedzsment 2017- éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára (Budapest, 2017 Dialóg Campus)

c) amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy
d) amelyre a bűncselekményt elkövették.

Irat minden olyan tárgyi bizonyítási eszköz, amely műszaki, vegyi vagy más eljárással adatokat rögzít, így különösen a papíralapú, vagy elektronikus adatként létező szöveg, rajz, ábra. Ebben az értelemben az elektronikus ügyintézés során – így például: okirat az az irat, amely valamilyen tény, adat valóságának, esemény megtörténtének, vagy nyilatkozat megtételének bizonyítására készül, és arra alkalmas. Az okiratra vonatkozó rendelkezések irányadók az okiratból készült kivonatra is.

A belügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól szóló 100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól a kutatásról és a lefoglalásról felvett jegyzőkönyvvel összefüggésben az alábbi rendelkezéseket tartalmazza:

„*Az információs rendszer átvizsgálása során biztosítani kell az információs rendszer útján- védelmi eszköz vagy informatikai megoldás megkerülése vagy kijátszása nélkül- hozzáférhető adatok megismerését és rögzítését.”*

Eset:

Egy 2014-ben végrehajtott házkutatás során, amely szerzői jogok megsértése miatt indult büntetőeljárásban vált szükségessé, az eljáró hatóság a kényszerintézkedés során a helyszínen lévő gyanúsítottat a helyiségben lévő számítástechnikai eszköztőöl kis távolságra ültette le. A kényszerintézkedést elszenvedő fél arra hivatkozva, hogy fel szeretné hívni az ügyvédjét, a nyomozó miközben tárcsázta a számot, pillanatnyi figyelmetlenségét kihasználva, a számítógépet kihúzta az áramforrásból és a továbbiakban megtagadta az együttműködést.

A lefoglalt számítógépeken és adathordozókon kívül a helyszínen lévő szakértő a gyanúsított mobiltelefonjának tartalmáról képernyőfotót készített, de az eszköz lefoglalásra nem került. Egyéb adatmentés az eszközön azért nem történt mert a szakértő nem hozott magával megfelelő eszközt annak végrehajtásához.

Az ügyészség a következőket emelte ki a (ház)kutatás végrehajtása során:

- Az ügyek többségében megfigyelhető, hogy előre tervezett információgyűjtést követően hajtják végre a kényszerintézkedést, amely nemcsak a helyszín tekintetében, hanem az ott tartózkodó személyekre is kiterjed.
- Szakértő kirendelése és eszközök biztosítása egy-két esetet leszámítva előre tervezetten történik
- Amennyiben a (ház)kutatás során a terhelt nem együttműködő vagy olyan eszköz kerül feltalálásra, amely a nyomozás szempontjából releváns adatokat, információkat tartalmazhat, akkor azt elsődlegesen az intézkedés során a helyszínen át kell vizsgálni.

A korábbiakban leírtak alapján álláspontunk szerint: indokolt lenne, hogy a helyiség vagy gépjármű kutatásától elválasztva, külön szakaszban kidolgozni az információs rendszerrel kapcsolatos kutatás szabályozását. Amennyiben ugyanis ténylegesen betartja a hatóság, hogy az informatikai eszköz tulajdonosát vagy kezelőjét az eljárás megkezdésekor felszólítja, hogy a keresett adatot tegye hozzáférhetővé és amennyiben az az eszköz, vagy csak egyes dokumentumok jelszóval vagy biometrikus azonosítóval védettek, akkor annak a hatóság rendelkezésére bocsátása nehézkes lehet. Szükséges lenne, hogy a jogalkotó valamennyi változtatás lehetőségét a szükséges mértékig engedélyezze, úgy, hogy a bizonyíték alapvetően ne változzon meg.

8.1.2 Szemle

A bűncselekmény elkövetésével érintett rendszernek az alaposabb vizsgálata lehet szükséges a bűncselekmény elkövetője által hátrahagyott nyomok összegyűjtése és rögzítése érdekében. A vizsgálat a szemle szabályai szerint hajtható végre.

Igaz, hogy a szemle nem a kényszerintézkedések közé, hanem önálló bizonyítási cselekmény, de az egyes mozzanatai miatt, inkább itt szerettem volna megemlíteni.

A korábban hatályos Be. alapján a szemlét a bíróság, illetőleg az ügyész rendel el, és tart, ha a bizonyítandó tény felderítéséhez vagy megállapításához személy, tárgy vagy helyszín megtekintése, illetőleg tárgy vagy helyszín megfigyelése szükséges[232].

[232] A (régi) büntetőeljárásról szóló 1998. évi XIX. törvény 119.§ (1).bekezdés

A szemle, mint bizonyítási cselekmény lehetőséget biztosít a nyomozó hatóságnak, az ügyészségnek, illetve a bíróságnak arra, hogy a bizonyítandó tény megállapítása érdekében vagy amennyiben a bizonyítás szempontjából indokolt tárgyat, személy vagy helyszínt megfigyeljen.

A szemlénél, ha a hatóság úgy ítéli meg, vagy valamilyen körülmény indokolja– szakértőt is lehet alkalmazni, vagy amennyiben az információs rendszer vagy adathordozó átvizsgálása valami miatt különleges szakértelmet igényel, az elektronikus bizonyítékok összegyűjtésére szaktanácsadó vehető igénybe, aki a későbbiekben már nem rendelhető ki szakértőként[233].

A szemle alkalmával a bizonyítás szempontjából jelentős körülményeket részletesen rögzíteni kell. A szemlén fel kell kutatni és össze kell gyűjteni a tárgyi bizonyítási eszközöket, és gondoskodni kell a megfelelő módon történő megőrzésükről. A szemle tárgyáról, ha lehetséges és szükséges, kép- vagy hangfelvételt, illetve képet és hangot egyidejűleg rögzítő felvételt, rajzot vagy vázlatot kell készíteni, és azt a jegyzőkönyvhöz kell csatolni.

Gárdonyi Gergely a szemle végrehajtásánál pozitív feltételként említi, hogy a szemle tárgyait kriminál technikai módszerekkel, eljárásokkal indokolt a helyszínen talált személyekhez, tárgyakhoz kötni, a számítógépes bűncselekmények nyomozásánál, az egyes eszközökben tárolt adatok megismerésénél, vagy azok adott személyhez köthetőségénél az ezredes úr megállapítása mindenképpen figyelmet érdemel[234].

Az interneten található bizonyítékok mentése általában „online” szemle keretében történik. Az adatmentésben az eljáró nyomozók végzik az ügyben releváns adatok keresését és rögzítését, így az internetes kereséseket, a letöltött fájlokat. Az adatmentés folyamatáról jegyzőkönyv vagy jelentés készül, amelynek részletesnek kell lennie, a folyamatokat, megállapításokat rögzíteni kell. Az adatokról érdemes un. „image-fájlt”, amit „HASH-kulccsal” kell azonosítani, amelyet egy adathordozón rögzítenek (ez utóbbi lehet CD/DVD/BR-disk, vagy winchester). Ezen mozzanat részleteit is jegyzőkönyvben kell rögzíteni.

Amennyiben az információs rendszer vagy adathordozó részletes átvizsgálása a nyomozó hatóság részéről nem szükséges, bizonyos esetekben az elektronikus bizonyíték adatkérés útján is beszerezhető.

---

[233] Az erre vonatkozó álláspontunk a szakértőkkel foglalkozó a 8. fejezetben fejtem ki

[234] 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) 134.

8.2 Lefoglalás

A lefoglalás egy olyan kényszerintézkedés, amely során a dolgot, azaz a bizonyítékot elvonják a birtokos rendelkezése alól. A régi, büntetőeljárásról szóló 1998. évi XIX. törvényben a lefoglalás a bizonyítás érdekében vagy az elkobzás, illetőleg a vagyonelkobzás biztosítására a dolognak a bíróság, az ügyész, illetőleg a nyomozó hatóság általi őrzésbe vétele vagy megőrzésének más módon történő biztosítása[235].

Kriminál technikai szempontból *a számítógépes felszerelés biztosítását, lefoglalását követően ebből az adatforrásból kell kigyűjteni a releváns adatokat*[236].

Az új büntetőeljárási törvény a lefoglalás céljával kapcsolatban a korábbi eljárási szabályhoz képest nem sokat változott: a bizonyítási eszköz, illetve az elkobozható dolog vagy a vagyonelkobzás alá eső vagyon biztosítása a büntetőeljárás eredményes lefolytatása érdekében. A lefoglalás a lefoglalás tárgya feletti tulajdonjogot korlátozza.[237]

A lefoglalás az ingó dolgot-így bármilyen számítástechnikai eszközt, berendezést-, számlapénzt, az elektronikus pénzt vagy az elektronikus adatot érinthet,[238] amelyeknél minden esetben a hitelesség megőrzése elengedhetetlen.

A lefoglalás, mint kényszerintézkedés nemcsak 18. életévet betöltött természetes személy ellen foganatosítható, hanem olyan személy ellen is, aki a gyermekkora vagy kóros elmeállapota miatt egyébként nem büntethető, de a birtokában lévő eszköz, tárgy, elektronikus adat vagy eszköz a bűncselekmény vagy szabálysértés során bizonyítás nyomait hordozza vagy hordozhatja.

8.2.1 A lefoglalás menete

A lefoglalás megkezdésekor a lefoglalással érintett felet, vagy az információs rendszerben tárolt adat vagy adathordozó birtokosát, illetve kezelőjét fel kell szólítani, hogy a keresett dolgot adja át, illetve tegye hozzáférhetővé (a jelszót vagy az elérési módot tegye lehetővé). Amennyiben

[235] korábbi Be.151.§ (1).
[236] Tremmel Flórián-Fenyvesi Csaba-Herke Csongor: Kriminalisztika, Tankönyv és Atlasz (Dialóg Campus, Budapest-Pécs 2005)276.
[237] A büntetőeljárásról szóló 2017. évi XC. törvény 308.§ (1) .
[238] Wolfgang Bär: Beschlagnahme von Computerdaten (II.) Computer und Recht 12. 1996. s. 752.

azt megtagadja, úgy rendbírsággal sújtható. Ez a szabály nem vonatkozik arra a személyre, akire egyébként a tanúkihallgatás megtagadására vonatkozó jogával élhet vagy aki tanúként nem hallgatható ki.

A kibertérben elkövetett bűncselekmények esetében a lefoglalás speciálisan hajtható végre figyelembe véve azt, hogy az adat nem kézzel megfogható dolog. Ennek lefoglalásának kérdései miatt szükségesnek érzem együtt tárgyalni a szakértővel kapcsolatos szabályokat is ezen kényszerintézkedéssel együtt.

Lefoglalt eszközökről történő adatmentés: a szakértő, vagy a hatóság megfelelően kiképzett tagja a lefoglalt számítógépekről, telefonokról elvégzi az adatmentést és arról az adatokat tartalmazó riportot készít, egyben a bizonyítékként felhasználható adattartalomról a hiteles adattartalmat külső adattárolóra menti[239].

A szolgáltató cégektől (telekommunikációs cégek, tárhely szolgáltatók, pénzügyi intézmények, hatóságok stb.) megkeresés útján beszerzett adatokat külső adathordozókon csatolják a nyomozati iratokhoz.

Két típusú lefoglalást különböztethetünk meg:

1. amikor maga az informatikai eszköz a bűncselekmény elkövetésével van összefüggésben, ezáltal annak külső vagy belső része a nyomhordozó
2. amikor az informatikai eszközön vagy rendszerben található adat a bizonyítás tárgya.

Az első eset, amikor az informatikai eszköz (dolog) a bizonyítás tárgya. Ebben az esetben a lefoglalás általános szabályai szerint kell eljárni, (PC, telefon, tablet stb.) lefoglalása mennyire arányos és szükségszerű (figyelembe véve azt, hogy egy vagyoni jellegű dolog kerül lefoglalásra). Az eszköz lefoglalásánál mérlegelni kell, hogy az mennyire szükséges intézkedés.

A Fővárosi Főügyészség azonban rávilágított arra, hogy sokszor azzal kapcsolatban sincs egységes gyakorlat, amikor egy bűncselekmény miatt közterületen vagy a magánterületen elhelyezett kamerafelvétel megismerése és lefoglalása szükséges vagy elegendő a tartalom lementése, amelyet egy adathordozóra másolnak át és azt a hatóság lefoglalja, bűnjelként kezeli. A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya által kiadott

[239] „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".

útmutató szerint, ha a cselekmény jellege nem indokolja, akkor elegendő csak az adat lefoglalása, de amennyiben az adat mellett szükséges egyéb más vizsgálat pl.: a metaadat megismerése, akkor az egész eszköz lefoglalása válik szükségessé.

Ezzel kapcsolatban érdemes megemlíteni a bűnjel fogalmát. Azt a lefoglalt dolgot (továbbiakban bűnjelet) amely az eljárás során a bizonyítás eszközéül szolgál, valamint, amelyet az eljárás során azonosítani, megvizsgálni, valamint megtekinteni szükséges.[240]

A számítástechnikai eszközök lefoglalásakor jelentkező nehézségek.

Az eszközt úgy kell lefoglalni, vagy letétbe helyezni, hogy azt vagy azokat már a helyszínen, az eljáró hatóság tagja külön-külön becsomagolja és gondoskodik arról, hogy annak tartalmáról illetéktelenek ne szerezzenek tudomást, valamint a lefoglalt dologban sérelem ne keletkezzen. A számítástechnikai eszközök lefoglalása során a kutatásnál említett tervezés szükséges, hiszen a különböző eszközökön futó operációs rendszerek vizsgálata más és más eljárást igényelhetnek, tovább a mobileszközök folyamatos működésükhöz szükséges töltő vagy power bank (hordozható külső akkumulátor), kábelek nem mindig állnak rendelkezésre a helyszínen.

A nyomozó hatóságoknak az eljárási törvény lehetőséget ad, hogy a kutatás és/vagy lefoglalás alkalmával az esetlegesen különleges tudást igénylő esetekben szakértőt vagy szaktanácsadót vegyen igénybe.

A második eset, amikor az informatikai eszközön vagy rendszerben tárolt adatok lefoglalása szükséges. Az adat megismerése az, amit bizonyítékként kívánnak felhasználni. Így nem feltétlenül szükséges magának a gépnek a lefoglalása, sokkal inkább annak elérése, a belépéshez szükséges jelszó megismerése fontos.

A hatóságnak abban az esetben, ha nem adják át a felhasználáshoz, megismeréshez szükséges jelszót vagy kódot (lásd fentebb), akkor lehetősége van megkeresés útján azokat megismerni nyílt eljárásban.

[240] „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.), 20, https://net.jogtar.hu/jogszabaly?docid=a0300011.im 1.§ (1). letöltve: 2018 október 01

Amennyiben az adat birtokosa nem támaszt nehézséget annak megismeréséhez, úgy a lefoglalást olyan módon kell végrehajtani, hogy annak keletkezéséhez, eredetéhez, tartalmának változatlanságához kétség ne férjen.

Az új Be. az elektronikus adatok lefoglalásával már foglalkozik. A jogalkotó nem tartotta azt elegendőnek, hogy a szakmai szabályok határozzák meg a lefoglalás folyamatát, hanem azt törvényi szintre kívánják emelni az egységes végrehajtás érdekében. További fontos szabályozás, hogy csak arra az adatra terjedjen ki a lefoglalás, amelyik a bizonyítás tárgya, az egyéb adatra pedig ne terjedjen ki.

Ennek kivitelezése azért nehéz, mert adathordozó esetén a bűncselekménnyel kapcsolatban hozható adaton kívül más, a nyomozás szempontjából érdektelen adat is megtalálható. Az adathordozó átvizsgálásának végrehajtását pedig azt követően akár a szervezet helyiségében, akár szakértő igénybevételével kívánják elvégezni.

Ebben az esetben is lehetőség van arra, hogy akár az adott fájl kiterjesztése vagy mérete alapján nem foglalják le- de ez nagyon időigényes. Vagy lefoglalást követően az eljárással érintett személy jelenlétében az ügy szempontjából irreleváns adatokkal kapcsolatban a lefoglalást megszüntetik, azokat másolással visszaadják.

A 2017. évi XC. törvény, az új Be. alapján az elektronikus adat lefoglalására[241] vonatkozóan, amely végrehajtható

- az elektronikus adatról másolat készítésével
- az elektronikus adat áthelyezésével
- az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével
- az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy
- jogszabályban meghatározott más módon.

A fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.[242]

[241] Be. 315.§ (1) a.]-d.)
[242] Ebben az esetben a jogalkotó a decentralizált virtuális fizetőeszközökkel, kriptovalutával, elektronikus fizetési eszközökkel kapcsolatos szabályozást érti.

A jogalkotó már rendelkezik az elektronikus adatként létező irat lefoglalására vonatkozóan, mint az e-kereskedelem és e-ügyintézéssel kapcsolatban (pl.:2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, a 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről, 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről által szabályozott esetekben) keletkező és a papír alapú dokumentumokkal egyenértékű közokiratok tekintetében az irat lefoglalására vonatkozó szabályokat kell alkalmazni.

Az elektronikus adat lefoglalását úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse.

Az elektronikus adatot tartalmazó információs rendszer vagy adathordozó akkor foglalható le, ha

a) az elkobozható, illetve vagyonelkobzás alá esik
b) az tárgyi bizonyítási eszközként bír jelentőséggel, vagy
c) a bizonyítás érdekében az abban tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség.

Mi történik abban az esetben, ha az adatok nagyobb mennyisége miatt a kutatás helyszínén nem vizsgálható át az informatikai eszköz, illetve az azon található adat, és a nyomozás szempontjából nem releváns adat vagy esetleg a lefoglalást szenvedő fél számára kényes adat kerül lefoglalásra?

Egy informatikai eszközön, akár személyi számítógép, laptop, tablet vagy mobiltelefonról van szó, rengeteg olyan információ található, amelyek mennyisége, kiterjedése vagy a hatóság rendelkezésére álló idő rövidsége miatt a helyszínen nem vizsgálható át. Úgy szintén előfordulhat az is, hogy a szükséges információk a nyomozás további szakaszában vagy az adatok egymás relációjában értelmezhetők. Ilyen esetben két megoldás lehetséges. Az egyik, amikor a merevlemezt vagy azt az adathordozót foglalják le, amely a bizonyítékot hordozhatja, illetve a másik eset, amikor a helyszínen hiteles másolat készül és azt követően a hatóság épületében vagy a szakértői intézetben esetleg a szakértőnél kerül sor annak átvizsgálására. Ilyen esetben alapvetően – ahogyan az eljárás későbbi szakaszában is- megfelelő mennyiségű

hiteles másolat készítése szükséges az elektronikus bizonyítékról. Megfelelő mennyiségnek tekinthető, hogy mind a hatóság részére, amennyiben szakértő kerül kirendelésre, úgy részére és mindenképpen az ügyészi, illetve bírósági szakban is az ügy aktájában legalább egy példány legyen.

Mivel a helyszínen a fentebb ismertetett okok miatt az adathordozó egész tartalmáról készülhet mentés, így értelemszerűen azokról az adatokról is, amelyek nem képeznek bizonyítékot az adott ügyben.

A vizsgálat során- az ügy típusától és a lefoglalást szenvedő féltől függetlenül- kényszerintézkedési eljárással érintettek lehetnek családi képek, videók, privát üzenetek, de akár üzleti titkot, üzleti levelezést vagy szabadalmat is érintő információk, know-how, amellyel kapcsolatban az arra jogosultat anyagi vagy erkölcsi veszteség érheti, amennyiben azokat késlekedés miatt- jelen esetben a hatóság általi lefoglalás következtében- nem teljesít.

Ilyen esetben a lefoglalást követően, az arra jogosult félnek írásban jeleznie kell azt, hogy milyen adat található az adathordozón, van-e minősítése az adatnak, illetve védett-e valamilyen jelszóval.

Ezen adatok is a nyomozó hatóság által a lefoglalás végrehajtásához igénybe vett adathordozón maradnak, de a kirendelésről szóló jegyzőkönyvben tételesen fel kell sorolni, hogy melyek azok a fájlok (nevük, keletkezésük ideje, kiterjesztése stb..) amelyek a vizsgálat tárgyát képezik. Ezzel lehet biztosítani a másolat hitelességének megkérdőjelezhetetlenségét.

Amennyiben olyan adat is található a lemásolt elektronikus bizonyítékok között, amelyek nem képezik azok tárgyát, de a lefoglalást szenvedő félnek ahhoz üzleti, anyagi vagy jóhírnevéhez fűződő érdeke sérülne, úgy a bizalom elvének megfelelően, arra a lefoglalás megszüntetésére kerül sor, amelyet megszüntető határozatban közölnek az érintett-tel.

„*Ha ez az eljárás érdekét nem veszélyezteti, információs rendszer vagy adathordozó lefoglalása esetén az elektronikus adattal rendelkezni jogosult kérésére másolatot kell készíteni az általa megjelölt elektronikus adatról.”*[243]

Az IM-BM-PM együttes rendelete a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól,

[243] Be. 315.§ (6).

valamint az elkobzás végrehajtásáról elektronikus adat lefoglalását az azt tartalmazó adathordozó vagy információs rendszer teljes tartalmáról történő másolat készítésével kell végrehajtani, ha az informatika eszköznek az érintett őrizetében hagyásának feltételei fennállnak és az adat eredeti helyen való további tárolása a büntetőeljárás érdekeit nem veszélyezteti (a rendelet 67.§ (1) bekezdés), továbbá a bizonyítás szempontjából az adatot tartalmazó információs rendszer vagy adathordozó teljes tartalmának jelentősége van illetve előre nem meghatározható vagy jelentős mennyiségű adat átvizsgálására van szükség.

Nem hajtható végre a lefoglalás azokra az adatokra, adathordozóra, amelyek a terhelt és a védő közötti levelezések, feljegyzésekkel vagy egyéb, az üggyel összefüggő levelezéseket tartalmazza. Továbbá nem foglalható le az olyan elektronikus adat, amelyet a tanúvallomás megtagadására jogosult személy birtokában van.

A lefoglalás csak a szükséges ideig tarthat, azt meg kell szüntetni és a tárgy visszaadásáról, értékesítéséről, megsemmisítéséről vagy végleges törléséről határozatban rendelkeznie kell a lefoglalást kezdeményező félnek.

Az említett egységes rendelet rendelkezik az elektronikus adattal kapcsolatos eljárásról[244], ami szerint az elektronikus adat lefoglalását másolat készítésével kell végrehajtani.

Másolat készítése indokolt, ha a lefoglalt dolognak az érintett őrizetében hagyásának feltételei fennállnak, és a másolat készítését követően az adat eredeti helyen való további tárolása a büntetőeljárás érdekeit nem veszélyezteti.

Ugyanakkor nemcsak az adat másolásával szerezhetik meg annak tartalmát, hanem amennyiben az ügy érdekei indokolják, az adat eredeti helyen történő további tárolása a büntetőeljárás érdekeit veszélyezteti, akkor az elektronikus adat lefoglalását áthelyezéssel kell végrehajtani.

A lefoglalás végrehajtásához indokolt esetben szaktanácsadót kell igénybe venni.

(2) Az elektronikus adat lefoglalásakor az átmásolás lehetőség szerint utólag meg nem változtatható adathordozóra történhet. Az átmásolást megelőzően a lefoglalás helyszínén ellenőrizni kell, hogy a hatóság által az átmásoláshoz használt adathordozó adatokat nem

[244] 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 67.§.

tartalmaz. Az átmásolás során biztosítani kell azt, hogy az eredeti adatok ne változzanak meg.

(3) A hatóság a jegyzőkönyvben az átmásoláshoz használt adathordozó típusát, gyártási számát, illetve a rajta tárolt adat jellegét és tartalmát feltünteti. Ha az átmásolás utólag megváltoztatható adathordozóra történik, biztosítani kell az adatok változatlanságát, vagy azt, hogy a megváltoztatás nyomon követhető legyen.

(4) A fizetésre használt elektronikus adat vagyonelkobzás érdekében történő lefoglalását követően haladéktalanul fel kell hívni az érintettet, hogy a bűnjel előzetes értékesítése vagy megváltása kérdésében nyilatkozzon.

(5) Ha az érintett kéri a fizetésre használt elektronikus adat értékesítését, ez csak abban az esetben mellőzhető, ha arra a bizonyítás érdekében is szükség van.

(6) Ha a hatóság az adat birtokosát, illetve kezelőjét az új Be. 316. § (1) bekezdése szerint az adat megőrzésére kötelezte, a (2) bekezdést megfelelően alkalmazni kell.

A lefoglalt elektronikus adatot adathordozón vagy a hatóság rendelkezése alatt álló tárhelyen kell őrizni.

Ha a fizetésre használt elektronikus adat lefoglalását a 67. § (5) bekezdésében meghatározott módon hajtják végre, és annak a bírósági bűnjelkezelő rendelkezésére bocsátása szükséges, azt az ügyészség vagy a nyomozó hatóság a bírósági bűnjelkezelő e célból rendszeresített számláján történő jóváírással teljesíti.

A lefoglalással kapcsolatban általában a következők megállapítások tehetők:

- nincs egységes gyakorlat azzal kapcsolatban, hogy milyen esetekben szükséges magát az adatot, valamint az adathordozó eszközt lefoglalni.

A lefoglalás során azonban törekedni kell, hogy amennyiben csak magának az adat lefoglalásának nincs semmilyen akadálya (technikai vagy az eljáró hatóság részéről megoldható), úgy az informatikai eszközt nem kell lefoglalni, ezáltal biztosítható a legkisebb érdeksérelem.

- nincs arra vonatkozóan egységes álláspont, hogy a lefoglalás megkezdése előtt szükséges-e vagy sem előzetes tájékozódás, információgyűjtés a bizonyítási eszközökről (azok feltalálási helyéről, fajtájáról…)

Az elektronikus adatok vizsgálata vagy másolása során fontos szabály, hogy az elektronikus információs rendszerben tárolt adatok könnyen megváltoztathatók.

A bekapcsolt állapotú számítógép külső beavatkozás nélkül is folyamatosan végezhet előre tervezett műveleteket, így vírus ellenőrzést, biztonsági mentést, operációs rendszer frissítést, amelyek változásokat eredményeznek az adatállományban.

Az adatoknak a beszerzése kétféleképpen lehetséges:

- a működő – bekapcsolt állapotú – rendszer vizsgálatával
- a nem működő – kikapcsolt állapotú – rendszer adatainak vizsgálatával.

A bekapcsolt állapotú rendszer vizsgálatához olyan szoftveres és hardveres eszközök állnak rendelkezésre, amelyek megakadályozzák, hogy a rendszer áttekintése változást eredményezzen.

A kikapcsolt állapotú rendszerek esetében lehetséges az adattároló fenti módszerrel, írásvédővel történő csatlakoztatása és ellenőrzése, vagy az adatok digitális formában történő lemásolása.

Ennek egyik módszere a klónozás, amikor azonos kapacitású adathordozóra készít másolatot a hatóság. A másik módszer a lemezkép készítés, amikor az adathordozó tartalmát egy nagyobb kapacitású tárolóba, egyetlen nagy adatfájlban rögzítik. A létrehozott lemezkép-adatfájlok alkalmasak arra, hogy azokat speciális adatelemző szoftverekkel elemezzék.

A digitális másolat készítése kizárólag csak nemzetközileg elfogadott tanúsítvánnyal rendelkező és ellenőrzött eszközre lehetséges, ami ezáltal garantálja az eredetivel történő egyezőséget.

Az informatikai eszközök az adatokat kettes számrendszerben, „0” és „1” helyiértékek hosszú sorozataként tárolják[245].

[245] Egy ilyen érték a „bit”, ami a legkisebb informatikai tárolási mértékegység.

A tanúsított másolatot készítő eszközökkel készített adat az úgynevezett „bitazonos” másolat, ami mindenben megegyezik az eredetivel. Ezen megtalálhatóak a töredékes és törölt adatokból hátramaradt adatrészek és az operációs rendszer működése során keletkezett adatok is, nem csak a felhasználó által létrehozott dokumentumok.

A digitális másolat készítése után a másolatról erre szolgáló alkalmazással úgynevezett „hash” érték készítése szükséges. Ez az érték olyan algoritmus futtatását jelenti, ami a teljes adattartalmat veszi figyelembe, ami alapján alkot egy jelentősen rövidebb számsort. Ezen számsorból ugyanakkor nem fejthető vissza az eredeti adattartalom, a művelet visszafelé nem végezhető el.

Teljesen más „hash” érték keletkezik azonban a legminimálisabb változtatás esetén is. Például egy szöveges dokumentumról készül hash érték változásához elegendő egy további betű hozzáírása a szöveghez, vagyis a másolatról a másolás időpontjával egy időben készített hash érték tanúsítja, hogy az eredeti adattartalomról készített másolattal egyező a később elvégzett tartalommal, ami által a hatóságok tudják bizonyítani, hogy a vizsgálat során nem módosították azt.

A hash érték használata nemzetközileg elfogadott, gyors és automatikus művelet, ami sokkal hatékonyabb, mint a kézi ellenőrzés, ráadásul megmarad a bizonyíték zárt láncolata és a későbbiekben visszaellenőrízhető, ami a további eljárás tekintetében nélkülözhetetlen.

A számítógépeken kívül a mobiltelefonok, tabletek is tartalmaznak elektronikus adatokat, amelyek bizonyítékként felhasználásra kerülnek. A mobil eszközökön tárolt adatokhoz történő hozzáférés esetenként bonyolultabb, mert ezek az eszközök többségében csak a felhasználó által megadott kódokkal (a SIM kártya PIN vagy PUK kódjával, két lépéses belépési azonosítóval, jelkóddal vagy biometrikus adatokkal) érhetőek el. Ezen kívül titkosítást is alkalmazhatnak a felhasználók, ami miatt azok vizsgálata úgy, hogy az adattárolót az eszközből eltávolítják és más eszközhöz közvetlenül csatlakoztatják, lehetetlen lesz.

Ettől függetlenül a legtöbb esetében lehetséges az adatok megismerése célzottan az adott eszköz típushoz a gyártó vagy más cég által fejlesztett hardver és szoftver eszközök segítségével.

8.2.2 E-mail lefoglalása

A hagyományos bűncselekmények esetében a bizonyítékul szolgálhat a postai levelezés, a szolgáltatók által küldött számlák, határidőnaplóban történő bejegyzés stb.

Az informatika terjedése és a digitális világ fejlődése lehetővé tette, hogy a hagyományos postai szolgáltatás igénybevétele helyett az írott kommunikáció elektronikus levelezés útján történjen. Az e-mail, hasonlóan a postai levélküldeményekhez, szintén rendelkezik olyan adatokkal, amelyek bizonyítékként szolgálhatnak, így annak feladója, az elküldésének ideje, a levél címzettje elolvasta-e az e-mailt, és annak milyen tartalma van- esetleg milyen csatolmányt tartalmaz. Ugyancsak népszerű, hogy egy adott e-mail fiókot több személy használ és az egymásnak szánt közléseket nem levélként továbbítják, hanem piszkozatként mentve tudatják egymással.

A lefoglalás, mint kényszerintézkedés kiterjedhet szintén- az elektronikus adathoz hasonlóan- magára az e-mail fiókra és annak tartalmára, anélkül, hogy az annak tartalmát a gyanúsítottak tudnák törölni, változtatni vagy hozzáférhetetlenné tenni.

Az elektronikus postafiók esetében a hatóság megváltoztatja a jelszót és annyi változtatást végez, hogy a fiókhoz történő megosztást letiltja, így lehetősége lesz a továbbiakban annak tartalmát megismerni és a nyomozás során bármikor felhasználni.

8.2.3 A bitcoin mint bizonyíték lefoglalása[246]

Bár a disszertáció leginkább a számítógépes bűnözés jogszabályi kereteit vizsgálja, ennek ellenére, a most leginkább mindenkiből ellentétes érzéseket és gondolatokat kiváltó kriptovaluták szabályozásáról és az eddig említett kényszerintézkedések végrehajtást egyik legjobban szemléltető technikai lehetőségeket ismertetem.

Azért tartottam továbbá fontosnak a kissé részletesebb ismertetését, mivel a legtöbb bűncselekmény nyomozása során elsődleges elv: a kövesd a pénz útját! Ezzel a fizetőeszközzel történő fizetés új kihívásokat jelent mind a nyomozó hatóság, mind pedig a jogalkotó számára.

[246] A Bitcoinnal kapcsolatos kutatásban a KR NNI Kiberbűnözés Elleni Főosztály egyik főnyomozója által készített útmutató segített

Az egyik legismertebb virtuális fizetőeszköz a bitcoin (továbbiakban: BTC), amely az online térben történő legális és illegális kereskedelem egyik fizetőeszköze.[247]

Amiért a tanulmány megírásakor fontosnak éreztem, hogy megemlítésre kerüljön, részben azért, mert sok kibertámadás vagy gazdasági jellegű deliktum esetében, mint bizonyíték szükséges lehet annak lefoglalása (vagy legalábbis a BTC pénztárca feltalálása már jelentőséggel bírhat) valamint mert sok helyen tartja magát az a nézet, hogy a bitcoin összefügg a pénzmosás bűncselekményével.

A BTC egy kriptovaluta, vagyis egy olyan független pénzforgalmi rendszer, amely lehetővé teszi a felhasználók számára, hogy közvetlen utaljanak egymással az interneten keresztül, harmadik fél - azaz egy pénzintézet közvetítése nélkül.

Akkor mégis, miért alkalmasabb a bűnözőknek az ezzel történő fizetés és miben nehezíti bűnüldöző szerveknek a bizonyítást a kriptovalutákkal történő teljesítés és a pénz útjának nyomon követése?

A kriptovaluták esetében nem beszélhetünk azt vezető pénzintézetről, azaz a tranzakciók nem ellenőrzöttek. Azok valós időben mindenki számára követhetőek, amit blokkláncnak, azaz blockchain-nek neveznek, így nyomon lehet követni, hogy egy BTC cím mekkora fedezettel rendelkezik, valamint ugyanazt az összeget csak egy címre lehet elutalni[248].

A blockchaint vagy blokkláncot a bitcoin rendszerhez csatolt számítógépek összessége tartja nyilván, amivel kapcsolatos műveletek tulajdonképpen matematikai műveletek és ehhez számítógépek szükségesek.

A blokklánc ellenőrzi a „pénz” mozgását, vagyis ő veszi át a pénzintézet szerepét, míg a BTC kifizetés, utalás tekintetében a számítógépek járnak el, akik az ún. bitcoin bányászattal biztosítják a számítási kapacitást.[249]

---

[247] The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. 53ePublishing LLC (USA), 2014. pp. 9-33.

[248] Amennyiben a kriptovaluták helyett elektronikus adatot tennénk be a leírásban, azok hitelessége és megváltoztathatatlansága is biztosítható lenne a technológia és a jog megfelelő alakítása és fejlődése mellett (a szerz.)

[249] M. Antonopoulos, Andreas Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media; 2 edition, 2017. pp. 211-228.
Gerard, David: Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts. CreateSpace Independent Publishing Platform, 2017. pp. 69-78.

A bitcoin pénztárcának több verziója ismert. Az egyik a mobil applikációs bitcoin wallet- vagy pénztárca, ami a felhasználó mobil telefonjára kerül letöltésre. Második, a szoftver bitcoin pénztárca, ahol a wallet szoftver a számítógépen van telepítve. Erre példa a Bitcoin Core. Továbbá ott van az online pénztárca, amellyel a számlát egy online szolgáltatással nyitja meg. Ezt gyakran a www.blockchain.info. weboldalról töltik le.

Van még egy „hardveres" pénztárca is, amely a privát kulcsot külön, megfelelően rögzített hardvereszközön tárolja.

Végül ott van a papír tárca: amikor a felhasználó kinyomtat egy magánkulcsot és a nyilvános kulcsot, aminek egyik előnye, megakadályozza azt, hogy a bitcoinok rossz kezekbe kerüljenek (például a számítógépes bűnözőkébe). A hátránya a papír pénztárcának, hogy elveszíthető[250].

A bitcoin jellemzői:

- virtuális fizetőeszköz, vagyis a valós világban nem lehet vele találkozni
- decentralizáltság, de csak a szükséges mértékig
- nyilvánosság
- anonimitás.

8.2.4 A rendszer működése:

Minden egyes pénzügyi művelet nyilvános, az bárki számára megtekinthető. Ezt az „egyszerű szabályt" úgy sikerül betartatni, hogy a rendszer minden tranzakción végigfuttat egy hash algoritmust. A hash algoritmusok egyirányú kódolási módszerek, melyet a számítógépes adatok titkosításánál is használnak. Az algoritmus a számítógépes adatokat konvertálja számokká, amit hash értéknek hívunk. Ha ez a szám elég hosszú, akkor teljesen azonosíthatóvá tesz valamilyen egyedi adatot. A hash-szám egyértelműen utal a titkosított adatra, azonban belőle nem állítható elő visszafejtéssel az adat, amit titkosított[251].

[250] How to Make a Paper Bitcoin Wallet, 208i. sz., https://www.coindesk.com/information/paper-wallet-tutorial/. Letöltve: 2018. október 01.
[251] 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.

Tehát ez azt jelenti, hogy nem a tranzakciók lesznek titkosak, hanem a felhasználók azonosítása lesz nehéz vagy egyenesen lehetetlen. A nevek és a bankszámlaszámok helyett az ügyletek hosszúak, értelmetlen karaktersorozatból álló számsorok vannak, ami az egyes pénzügyleteknél változhat. Ez lehetővé teszi, hogy a rendszerben nehezen visszakövethetően, akár teljesen anonim módon tudunk vásárolni[252].

8.2.5 Anonimitás és a bitcoin

A bitcoin használók névtelenségét biztosítja az IP-cím elrejtésének lehetősége a Tor hálózat használatával. A Tor hálózat használatával a felhasználó IP-címe anonim, így nem lehetséges a személy személyazonosságának és helyének nyomon követése. A Tor hálózata felhasználói ugyanis névtelenül böngészhetnek az interneten, az IP-címet nem rögzítik. A bitcoin tranzakciókat nem lehet az IP-címhez kötni, ezért nem kapcsolható a felhasználó személyéhez. A nyilvános Wi-Fi hálózatok használata vagy a VPN-szolgáltatás használata is anonimitást jelent az interneten.

Anonimitást biztosíthatja továbbá egy harmadik személy (úgynevezett stróman) bevonása, a bitcoin-mixer[253] használata, az érmegyűjtés és a bitcoin kereskedő

A Bitcoin értékesítési lehetősége:

- online csereprogramok és cserék;
- személyesen kontaktussal a kereskedővel készpénzben.

8.2.6 BTC alkalmazási területe:

Az internet böngészése közben, akár a bitcoin használatára vonatkozóan, akár az alkalmazási területeit keresve, szinte csak pozitív véleményeket lehet róla találni. Nincs tranzakciós díj, ráadásul nagyon gyors is, és közvetlenül lehetséges az utalást végrehajtani. Mindezt amellett,

[252] „Bitcoins.hu az első magyar bitcoin portál”, http://bitcoins.hu/, elérés 2017. december 6., http://bitcoins.hu/. Letöltve: 2018. október 01.
[253] A bitcoin mixer egy olyan online szolgáltatás, amit "mixer vagy keverési szolgáltatásnak" neveznek. A bitcoinokat más bitcoinnal kicserélik, az azt végző számára jutalék kifizetése mellett, ami a bitcoinok teljes összegének csak néhány százaléka (2% vagy 3,5%)

hogy megmarad a felhasználók anonimitása is, amely bizonyos programokon keresztül teljes mértékben biztosítható.

Egyrészt, ahogyan az elején is írtam, semmilyen hatóságtól vagy pénzintézettől nem függ, ugyanakkor lehetőség van arra, hogy a bitcoinnal különböző árukért, szolgáltatásokért fizetni lehessen, de arra is lehetőség van, hogy a különböző számítógépes játékokban a felhasználók ennek segítségével virtuális fegyvert, életet, bónuszokat vásároljanak.

A számítástechnikai játékokba történő felhasználásán túl lehetőség van ma már arra is, hogy egyes légitársaságoknál akár repülőjegyet is lehessen vele vásárolni, vagy kávézóban fizetni.

8.2.7 A BTC jogi szabályozása Magyarországon

Magyarországon a bitcoin, mint fizetőeszköz még nincs semmilyen törvény által szabályozva, annak megvásárlása, az azzal történő fizetés, kereskedés nem is tiltott. A Magyar Nemzeti Bank (MNB) ugyanakkor egy figyelmeztetést tett közé, amelyben arra hívja fel a bitcoint vásárolni szándékozókat, hogy *„… a fizetésre használható virtuális eszközöket szervező és a kereskedést lebonyolító intézményeket a jegybank nem felügyeli, a szervező fizetésképtelensége esetén a magyarországi garanciaalapok kártalanítási felelőssége nem terjed ki rájuk.*”

Az MNB szerint kiemelt kockázattal jár egy befektetés az ilyen típusú eszközökbe, mivel ezek olyan külföldi társaságok és magánszemélyek által kibocsátottak, amelyek mind a Magyar Nemzeti Bank (MNB) mind az Európai Unió felügyeleti intézményeinek joghatóságán kívül esnek. Azaz, amennyiben egy ilyen „befektetéssel” kapcsolatban a fogyasztókat (számomra a felhasználó helyesebb kifejezés, lévén, hogy teljes mértékben egy virtuális pénzről beszélünk) vagyoni hátrány érne, úgy abban az esetben senki nem kártalanítja őket. Ez azt jelenti, hogy sem az Országos Betétbiztosítási Alap felé (OBA), sem pedig a Befektető-védelmi Alap (Beva) felé nem tudnak kártérítésért folyamodni az esetleges károsultak. Magyarországon a hatályban lévő 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény értelmező rendelkezésében sincs olyan meghatározás, amely lehetővé tenné, hogy a bitcoint, mint fizető eszközt besorolják, így az nem tekinthető hivatalos fizetőeszköznek.

Ugyanakkor a bitcoin-nal való kereskedést nem zárja ki a MNB, de adójogi vonatkozásai vannak.

Magyarországgal ellentétben ugyanakkor már egyes országokban megjelent egyfajta szabályozása a bitcoinnak.

8.2.8 A Bitcoinnal kapcsolatos kényszerintézkedések

A bitcoin, bár fizetőeszköz, mégsem lehet ugyanazokat a szabályokat alkalmazni rá, mint a hagyományos pénz esetében, mivel nem kézzel fogható, annak értéke erősen ingadozó, és a lefoglalt pénzzel ellentétben az letéti számlára nem fizethető be.

A BTC nem más, mint egy vagyoni értéket megtestesítő elektronikus adat, amelyre speciális szabályok vonatkoznak.

Annak ellenére, hogy elektronikus adatról beszélünk, fontos eltérések vannak a rá vonatkozó intézkedések tekintetében.

A régi büntetőeljárásról szóló 1998. évi XIX. törvény 151.§ (2) bekezdése szerint a lefoglalás „a bíróság, az ügyész, illetve a nyomozó hatóság elrendeli - az ingatlan kivételével - annak a dolognak, információs rendszernek, ilyen rendszerben tárolt adatokat tartalmazó adathordozónak vagy adatnak a lefoglalását, amely

a) bizonyítási eszköz,
b) a törvény értelmében elkobozható, vagy amelyre vagyonelkobzás rendelhető el.”

A hatályon kívül helyezett Be. törvény nem említi a virtuális fizetőeszköz lefoglalását, míg a hatályos Be. már a lefoglalás tárgyaként említi az elektronikus pénzt, így a lefoglalásának törvényben lefektetett lehetősége megvan[254]. Kérdéses ugyanakkor, hogy milyen gyakorlati problémák merülhetnek fel?

A bitcoin nem kézzel fogható dolog, hanem egy karaktersor (ami egy tetszőlegesen megadott és tetszőleges számú cím), ami a blokkláncban tárolt adatok szerint derül ki, hogy mennyi bitcoin van azon, ami mindenki számára nyilvános (a nyilvánosság nem azt jelenti, hogy ismerjük név szerint, hogy kié a BTC!).

[254] Bár a korábban hatályos jogszabály szerint is mindenféle törvényes módszerrel lefoglalható volt, még ha maga a kriptovaluta vagy elektronikus pénz nevesítve nem is volt

Ahogyan már említettem a bitcoin egy pénztárcában tárolódik, ami a bitcoin program által létrehozott fájl. Ha a fájl megsemmisül, annak a privát kulcsának és címének ismerete mellett, újra létre lehet hozni egy másik fájlt és további tranzakciókat lehet végrehajtani.

Épp ez okozza a nehézséget a lefoglalással kapcsolatban. Ugyanis, mivel az elektronikus adat esetében a lefoglalás nem kézzel fogható, a rendelkezésre jogosulttól történő elvonással hajtható végre, így az bármikor újra létrehozható (hiszen annak címe, akármilyen bonyolult, megjegyezhető) és a bitcoin elvonható a hatóság lefoglalását követően. Ennek tudható az be, hogy a zár alá vételnek, valamint az információs rendszerben tárolt adat megőrzésre kötelezésnek, mint kényszerintézkedésnek értelme ennél a fizetésre alkalmas eszköznél nincs. Ráadásul az alap bűncselekmény büntetési tétele sokkal magasabb is lehet- a bizonyítás ellehetetlenüléséről ne is beszéljünk- mint a zár alá vételnek a megsértése.

Másik lehetőség lenne, magának a tárca fájlnak a lemásolása és az azt tartalmazó informatikai eszközön történő törlése, de a fentebb vázolt okok miatt, illetve mert nem zárható ki, hogy az eljárást elszenvedőnek még egyéb, fel nem talált informatikai eszközén van róla másolata, szintén nem lenne értelme.

8.2.9 A kriptovalutákkal kapcsolatban felmerülő probléma:

Fő problémaként jelentkezik, hogy a hagyományos pénzzel, értékpapírral ellentétben a kriptovalutáknak nem egyértelmű a létezése a kiberbűncselekmények során, hiszen, ahogyan fent is írtam nem kézzel fogható, materiális fizetőeszköz, hanem azzal kizárólag a virtuális térben, az arra alkalmas rendszer segítségével lehet tranzakciókat elvégezni. Így jellegénél fogva nem köthető személyhez, sem helyhez, sem pénzintézethez, így amennyiben biztos információ nem keletkezik arra vonatkozóan, hogy a bűncselekmény során bármilyen kriptovaluta, mint bizonyíték, szerepet játszik az eljárásban, sokszor csak a véletlenen és a szerencsén múlik, hogy a hatóságok tudomást szerezzenek róla.

A hatóság számára a bitcoin lefoglalásának módja az lenne, ha létrehoznának egy „hatósági pénztárcát”, amelyre ráutalnák az összes bitcoint. A jelenleg hatályos rendelet szerint:

> *„1.§ (3) Ha a bűnjel magyar pénz - kivéve az (1) bekezdésben foglalt esetet - a hatóság huszonnégy órán belül, de legkésőbb a lefoglalást követő első munkanapon befizeti a bűnjelkezelője letéti számlájára. Ebben az esetben a postai befizetési lap feladóvevényét az*

eredeti ügyiratban elhelyezett bűnjeljegyzékhez kell csatolni, ami aztán befizetésre kerül a Magyar Államkincstár felé a hatóság székhelye szerint illetékes területi szervének (továbbiakban: Kincstár területi szerve), amely azokat az eljáró hatóság további intézkedéséig hatósági letétként kezeli. Ebben az esetben a bűnjelkezelő kötelezettségei a Kincstár külföldi pénzt kezelő területi szervét terhelik."[255]

Ugyanebben a rendeletben az elektronikus adat lefoglalására és kezelésére vonatkozóan is ad iránymutatást:

„67. § (1) Az elektronikus úton rögzített adatot a hatóság adathordozóra történő rögzítés (átmásolás) útján foglalja le, vagy a helyszínen lefoglalt adathordozóról az adatokat szakértő vagy szaktanácsadó bevonásával menti le.

(2) Az (1) bekezdésben meghatározott lefoglaláskor az átmásolás utólag meg nem változtatható adathordozóra történhet. Az átmásolást megelőzően a lefoglalás helyszínén ellenőrizni kell, hogy a hatóság által az átmásoláshoz biztosított adathordozó adatokat nem tartalmaz. Az átmásolás során biztosítani kell azt, hogy az eredeti adatok ne változzanak meg. A hatóság a jegyzőkönyvben a rögzítésre használt adathordozó típusát, gyártási számát, illetőleg a rajta tárolt adat jellegét és tartalmát feltünteti."

A KR Nemzeti Nyomozó Iroda bitcoin lefoglalással kapcsolatos útmutatója szerint:

1. Nem elegendő egy olyan adathordozóra átmásolni a bitcoin walletet, amit aztán írásvédetté tesznek, mert azzal az érdemleges lefoglalás nem valósul meg. Szükséges, hogy a hatóság egy saját számítógépen hozzon létre egy pénztárcát- program telepítésével-, amely a bitcoin fogadására alkalmas és amely ismeri a teljes blokkláncot.
2. A létrehozott pénztárca tartalmazza azt a címet, amelyre a lefoglalt bitcoint utalni akarjuk. Ehhez BTC-nak a hatósági címre történő beérkezéséig internetes kapcsolatra van szükség, ezért az NNI főnyomozója kiemelte, hogy mindenképpen legalább két számítógépre van szükség, amellyel biztosítani lehet, hogy bitcoin fogadásra alkalmas fájllal együtt letöltött esetleges adathalász vagy más rosszindulatú vírusok képesek legyenek megszerezni a privát kulcsot, ezzel esetleg megszerezni a lefoglalt BTC-t. Emellett lehetőleg egy internetes kapcsolattal nem rendelkező számítógépre is

[255] 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, 200.

szükséges a bitcoin programot feltelepíteni és a tárcát itt létrehozni. Amennyiben a BTC-nal kapcsolatban a lefoglalást meg kell szüntetni, úgy az internetkapcsolat újból szükséges lehet.

Az IM-BM-PM együttes rendelete meghatározza a pénz lefoglalására és bűnjelkezelésére vonatkozó szabályait, ami az új büntetőeljárásban bevezetett szabályok miatt módosult az alábbiak szerint:

Az elkobzás vagy vagyonelkobzás alá eső fizetésre használt elektronikus adat lefoglalását az elektronikus adat lefoglalásában és megőrzésre kötelezés eljárásjogi szabályozásnak megfelelően a meghatározott művelet elvégzésével, a fizetésre használt elektronikus adat áthelyezésével vagy az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával kell végrehajtani, akkor, ha az vagyonelkobzás alá esik, és a zár alá vétel feltételei nem állnak fenn, vagy az nem lenne végrehajtható, illetve ha az adat elkobzás alá esik, és az elektronikus adat ideiglenes hozzáférhetetlenné tételének vagy az elektronikus adat ideiglenes eltávolításának a feltételei nem állnak fenn.

Az új Be. 315. § (2) bekezdésében meghatározott művelet elvégzése végrehajtható olyan művelettel is, amely alapján a fizetésre használt elektronikus adat értéke a bűnjelkezelő e célból rendszeresített számláján kerül jóváírásra[256].

A bitcoin felkutatása és lefoglalása szükséges az eljárás során. Az új Be. által kínált megoldás szerint: A fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.[257]

Az elektronikus adatként említett kriptovaluták esetében a bírósági bűnjelkezelő rendelkezésére bocsátása szükséges, azt az ügyészség vagy a nyomozó hatóság a bírósági bűnjelkezelő e célból rendszeresített számláján történő jóváírással teljesíti.[258]

[256] 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 67.§ (5)-(6).
[257] 2017. évi XC. törvény a büntetőeljárásról 315.§ (2).
[258] 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 67/B. §.

A bitcoin esetében a rendeletben foglaltakra tekintettel, bár annak árfolyama folyamatosan változik, de a pénz lefoglalásával ellentétben, ahol annak a jogosult részére történő visszaadását követően kamatot kell fizetni, a kriptovaluták esetében meg sem említi annak lehetőségét.

8.3 Az elektronikus adatok megőrzésére kötelezés

A nyomozások során alapvető fontosságú, hogy az adatok tárolását, továbbítását végző kisebb-nagyobb szervezetek azonnal, haladéktalanul és maradéktalanul végre tudják hajtani a hatóság által elrendelt kényszerintézkedést, ezáltal megakadályozva annak törlését, felülírását addig, amíg a nyomozó hatóság tagjai azokat meg nem vizsgálják, vagy le nem foglalják.

Információs rendszerben tárolt adatok megőrzésére kötelezést az 1998. évi XIX. törvény 158/A.§ szabályozta, ami a bűncselekmény felderítése és a bizonyítás érdekében a számítástechnikai rendszer útján rögzített adat birtokosának, feldolgozójának, illetőleg kezelőjének az információs rendszerben tárolt meghatározott adat feletti rendelkezési jogának ideiglenes korlátozása volt.

A megőrzésre kötelezett feladatait, konkrét tevékenységét is meghatározta a korábbi eljárási törvényünk.

Az új, 2017.évi XC. törvény a megőrzésre kötelezést már nem külön szakaszban tárgyalja, hanem az elektronikus adat lefoglalásával együtt, mintegy lefoglalással egyenlő, de legalábbis azt kiegészítő kényszerintézkedést. A Be. 316.§ alapján a megőrzésre kötelezett lehet:

- az elektronikus adat birtokosa,
- az elektronikus adat feldolgozója
- az elektronikus adat kezelője.

Ebben a személyi körben közös, hogy mindnek határozat vele történő közlésének időpontjától köteles a határozatban megjelölt információs rendszerben tárolt adatot változatlanul megőrizni, és − szükség esetén más adatállománytól elkülönítve − biztosítani annak biztonságos tárolását.

A megőrzésre kötelezett köteles az információs rendszerben tárolt adat megváltoztatását, törlését, megsemmisülését, valamint annak továbbítását, másolat jogosulatlan készítését, illetőleg az adathoz való jogosulatlan hozzáférést megakadályozni.

A megőrzésre kötelezést elrendelő a megőrzéssel érintett adatot fokozott biztonságú elektronikus aláírással láthatja el. Ha az adat eredeti helyen történő megőrzése az érintettnek az adat feldolgozásával, kezelésével, tárolásával vagy továbbításával kapcsolatos tevékenységét jelentősen akadályozná, az elrendelő engedélyével az adat megőrzéséről annak más adathordozóra vagy más információs rendszerbe történő átmásolásával gondoskodhat. Az átmásolást követően az elrendelő az eredeti adatot tartalmazó adathordozóra és számítástechnikai rendszerre vonatkozóan a korlátozásokat részlegesen vagy teljesen feloldhatja.

Ahhoz az adathoz, amelyet a megőrzésre kötelezés érint, az intézkedés tartama alatt kizárólag az elrendelő bíróság, ügyész, illetőleg nyomozó hatóság, valamint az elrendelő engedélyével az adat birtokosa vagy kezelője jogosult hozzáférni. Arról az adatról, amelyet a megőrzésre kötelezés érint, az adat birtokosa vagy kezelője az intézkedés tartama alatt csak az elrendelő kifejezett engedélyével adhat más részére tájékoztatást.

A megőrzésre kötelezett köteles haladéktalanul tájékoztatni az elrendelőt, ha a megőrzésre kötelezéssel érintett adatot jogosulatlanul megváltoztatták, törölték, átmásolták, továbbították, megismerték, vagy, ha ezek megkísérlésére utaló jelet észlelt.

A megőrzésre kötelezést követően az elrendelő haladéktalanul megkezdi az érintett adatok átvizsgálását, és ennek eredményéhez képest az adatnak az információs rendszerbe vagy más adathordozóra történő átmásolásával az adat lefoglalását kell elrendelni, vagy a megőrzésre kötelezést meg kell szüntetni.

A megőrzésre kötelezés az adatot tartalmazó adathordozó lefoglalásáig, illetve az adat átmásolásáig, de legfeljebb három hónapig tarthat. Ez megszűnik, ha a büntetőeljárást befejezték. A büntetőeljárás befejezéséről a megőrzésre kötelezettet értesíteni kell.

Előfordul, hogy a számítástechnikai adatok kizárólag egy belső rendszeren vannak, amelyet a munkáltató üzemeltet. Ebben az esetben ezzel a rendszergazdával szemben kell elrendelni a kényszerintézkedést. Az ezt elrendelő hatóság az őrzés biztonságának fokozása érdekében további biztonsági intézkedést épít be, amikor előírja, hogy a megőrzéssel érintett adatot elektronikus aláírással láthatja el.

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól a 2015. évi CCXXII. törvény 1. § 22. pontja rendelkezik, eszerint fokozott biztonságú elektronikus aláírás: az eIDAS Rendelet 3. cikkének 11. pontja szerinti aláírás.[259]

A jogintézmény létrehozásának az egyik legfőbb indoka, hogy kiterjedt nemzetközi nyomozásokban sok esetben az egyes államok nyomozó hatóságainak jogsegélykérelmet kell küldeni a másik állam nyomozó hatóságai felé, ami több hónapot is igénybe vehet. Ezek az átmeneti időszakok gyakran oda vezettek, hogy a jogsegélykérelem megérkezésekor az adatok már nem voltak fellelhetők. A jogintézmény alkalmazásával az ilyen jellegű problémák csökkenthetők lennének.

8.4 Az internetes tartalom blokkolása

Az internet, mint a határok nélküli világháló az adatok korlátozások nélküli elérhetőségét, megoszthatóságát és hozzáférhetőségét biztosítja. Ennek köszönhetően a bűncselekmények széles palettájának és az elkövetőknek lehetőséget ad arra, hogy nemcsak rejtve tudjanak maradni, hanem a bűnös tevékenységüket véghez tudják vinni.

Egy új jogintézmény jelent meg a 2012. évi C. törvényben, a Büntető Törvénykönyv újragondolásakor: „Az elektronikus adat hozzáférhetetlenné tétele”., amellyel együtt megjelent az eljárásjogi szabályozása is már a régi Be.-be, amely a kényszerintézkedések közzé került be: „Az elektronikus adat végleges hozzáférhetetlenné tétele”, és „Az elektronikus adat ideiglenes hozzáférhetetlenné tétele”.

Ez a szabályozás egyébként egy uniós kötelezettségnek is eleget tesz - a 2011/93/EU irányelv 25. cikkében foglaltaknak -, amely szerint a tagállamoknak meg kell tenniük a szükséges intézkedéseket annak érdekében, hogy a gyermekpornográfiát tartalmazó vagy azt terjesztő, a területükön üzemeltetett weboldalak eltávolíthatók legyenek. Ezzel együtt a jogalkotónak biztosítékot kellett nyújtani azzal kapcsolatban, hogy ennek a korlátozásnak a szükségesség és

[259] Az Európai Parlament és a Tanács 910/2014/Eu rendelete szerint (3.cikk 11.) „fokozott biztonságú elektronikus aláírás”: olyan elektronikus aláírás, amely megfelel az a 26. cikkben meghatározott követelményeknek; 26. cikk: A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie: a) kizárólag az aláíróhoz köthető; b) alkalmas az aláíró azonosítására; c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat; d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

arányosság tekintetében garanciát nyújtson a felhasználóknak. Ez a jogintézmény a büntetőeljárási törvényben rögzített kényszerintézkedés, amely a törvény eredeti szövegében még nem szerepelt.[260]Ez tehát egy eljárási cselekmény, amely a tényállás tisztázásáig kíván egy speciális helyzetet teremteni, addig, amíg nem dönthető el kétséget kizáróan, hogy jogellenes vagy sem, valamint az elektronikus adat jellegéből fakadóan az elkobzásnak, mint eljárási cselekménynek végrehajtása nem lehetséges.

Érdekes tekintettel lenni arra, hogy az eddig ismertetett kényszerintézkedésekkel ellentétben ezt bíróság rendeli el, aminek az a feltehető oka, hogy a jogalkotó is látta azt a veszélyt, hogy a szólásszabadság korlátozására is alkalmas lehet annak kontroll nélküli alkalmazása.

Az adatok lefoglalásával ellentétben itt nem a nyomozás érdekeinek előmozdítása az elsődleges cél, hanem a vélhetően jogsértő állapot megszűntetése, ideiglenes jelleggel.

Az új Be. lényegében nem változtat a korábbi Be. 158/B. § szabályozáson, vagyis az elektronikus adat ideiglenes hozzáférhetetlenné tételét, mely az elektronikus hírközlő hálózat útján közzétett adat (e cím alkalmazásában a továbbiakban: elektronikus adat) feletti rendelkezési jog ideiglenes korlátozását, és az adathoz való hozzáférés ideiglenes megakadályozását jelenti. Ha az eljárás olyan közvádra[261] üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének[262] van helye, és ez a bűncselekmény folytatásának megakadályozásához szükséges, akkor ideiglenes hozzáférhetetlenné tétel rendelhető el. Az ún. tartalom bűncselekmények esetében - ilyen a gyermekpornográf, vagy szerzői jogot sértő deliktumok - már rögtön megvalósul a jogellenes cselekmény, és szükségessé válhat az elektronikus adat elszeparálása.

A törvény megfogalmazása szerint az elektronikus adat ideiglenes hozzáférhetetlenné tétele az elektronikus hírközlő hálózat útján közzétett adat (e cím alkalmazásában a továbbiakban: elektronikus adat) feletti rendelkezési jog ideiglenes korlátozása, és az adathoz való hozzáférés ideiglenes megakadályozása. Bármilyen közvádra üldözendő bűncselekmény útján keletkezett jogsértő tartalmak esetén, amennyiben az elektronikus adat (végleges) hozzáférhetetlenné tételének van helye, valamint a bűncselekmény folytatásának megakadályozásának úgy

[260] Az intézkedés nem csak a büntetőeljárási törvényben, hanem az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ektv) 12/A. §-ban is rögzítésre került 2012-ben.
[261] A nem közvádra üldözendők a magánvádas bűncselekmények (könnyű testi sértés, magántitok megsértése, levéltitok megsértése, rágalmazás, becsületsértés, kegyeletsértés)
[262] A Büntető Törvénykönyvről szóló 2012. évi C. törvény 77. §.

ideiglenes hozzáférhetetlenné tétel rendelhető el. Azaz, az olyan weboldalak, melyek tartalma illegális, lehetségessé válik az ideiglenes hozzáférhetetlenné tétel, amely a büntetőeljárás alatt alkalmazható. A hatályos Be. szerint ez az eljárás egyrészt preventív célú, vagyis ne lehessen a továbbiakban az adott tartalmakhoz hozzáférni, másrészt megakadályozhatja az ilyen bűncselekmények eszkalálódását.

Feltételezésünk szerint a prevención túl az ideiglenes hozzáférhetetlen tétel egy olyan köztes állapotot teremthet, amely amennyiben a bűncselekmény elkövetése esetleg nem bizonyítható, úgy az ideiglenes blokkolással az eljárás befejezését követően az eredeti állapot visszaállítható. Az eljárásban a bíróság, pontosabban a nyomozási bíró jogosult eljárni. Az intézkedésnek két formáját különbözteti meg a törvény:

a) a bíróság mérlegelésétől függ:

Amikor az eljárás közvádra üldözendő deliktum miatt indult meg, amellyel kapcsolatban helye van a végleges hozzáférhetetlenné tételének és ezáltal megakadályozhatják a bűncselekmény tovább folytatását.

b) kötelező a hozzáférhetetlenné tétel elrendelése, ha:

a) a tárhelyszolgáltató az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettséget nem teljesítette, vagy az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresése a megkeresés kibocsátásától számított harminc napon belül nem vezetett eredményre, és

b) b) a büntetőeljárás gyermekpornográfia (Btk. 204. §) vagy állam elleni bűncselekmény (Btk. XXIV. Fejezet) vagy terrorcselekmény (Btk. 314-316. §) miatt indult, és az elektronikus adat e bűncselekménnyel áll összefüggésben.[263]

Ezt követően a bíró (mint fentebb említettem a nyomozási bíró) határozatot hoz, amelyet a Nemzeti Média-és Hírközlési Hatóságnak elküld, akik a tárhelyszolgáltatót az eljárásról és az ügyirat számáról értesítik.

A hozzáférhetetlenné tételi eljárás során tulajdonképpen két folyamatot lehet megkülönböztetni. Az egyik esetben az elektronikus adat eltávolításáról beszélünk. Ezt a

[263] A (korábbi)büntetőeljárásról szóló 1998. évi XIX. törvény158/D.§ (1) a.] és b.).

bíróság jogosult határozatban elrendelni. A kötelezett a tárhelyszolgáltató. Ebben az esetben a Nemzeti Média-és Hírközlési Hatóság az eljárás megszervezésében nem vesz részt.

A másik esetben az elektronikus adat hozzáférésének megakadályozása történik, amiben szintén a bíróság jogosult eljárni. Az eljárás kötelezettjei az internet-szolgáltatók, a keresőszolgáltató és a gyorsítótár szolgáltató. Ebben az esetben az NMHH-nak viszont már van szerepe.

Az elektronikus adat hozzáférhetetlenné tétele elrendelhető ideiglenesen, az adat ideiglenes eltávolításával vagy a hozzáférés ideiglenes megakadályozásával.

Az eljárás alanyai tehát a hírközlési szolgáltató, a keresőszolgáltató, a gyorsítótár- szolgáltató, a nyomozó hatóság, az ügyészség, a bíróság, a Nemzeti Média és Hírközlési hatóság és természetesen a sértett(ek), az elkövető(k), esetleg szakértő, stb….

Erre a kényszerintézkedésre akkor kerül sor, ha a tárhelyszolgáltató a felszólítás ellenére nem távolította el a jogsértő adatot, vagy a külföldi hatóság jogsegély iránti megkeresése a megkeresés kibocsátásától számított 30 napon belül nem vezetett eredményre, illetve az elektronikus adat gyermekpornográfia, terrorcselekmény vagy állam elleni bűncselekmény miatt indult büntetőeljárással van összefüggésben.

A bíróság az ideiglenes hozzáférhetetlenné tételről értesíti a Nemzeti Média-és Hírközlési Hatóságot, akik ellenőrzik annak végrehajtását, valamint annak tényét bevezetik a KEHTA-ba. Ezt tehát a bíróság rendelheti el két módon: elektronikus adat ideiglenes eltávolításával, vagy elektronikus adathoz való hozzáférés ideiglenes megakadályozásával.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének teljesítésére kötelezett a bíróság megnevezésével és a határozat számának a megjelölésével tájékoztatja a felhasználókat a tartalom eltávolításának vagy a tartalomhoz hozzáférés megakadályozásának a jogalapjáról.

Az ideiglenes hozzáférhetetlenné tétel és az információs rendszerben tárolt adatok megőrzésére kötelezés együttesen is elrendelhető.

Az elektronikus adat ideiglenes eltávolítására az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló

törvényben[264] meghatározott tárhelyszolgáltatót kell kötelezni. A kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására. Ebben az esetben tehát a vélhetően jogsértő adat magyar joghatóság alatt van, azaz a magyar bíróságok döntése kikényszeríthető magyar hatóságok által.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság megszünteti, és az elektronikus adat visszaállítását rendeli el, ha az ideiglenes hozzáférhetetlenné tétel elrendelésének oka megszűnt, vagy a nyomozást megszüntették (kivéve, ha a Btk. 77. § (2) bekezdése alapján az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye).

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a büntetőeljárás befejezésével megszűnik. Ha a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét nem rendelte el, az elektronikus adat visszaállítására kötelezi a tárhelyszolgáltatót.

Az ideiglenes hozzáférhetetlenné tétel megszüntetéséről és az elektronikus adat visszaállításáról szóló határozatot a kötelezettel haladéktalanul közölni kell. A tárhelyszolgáltató a határozat vele történő közlésétől számított egy munkanapon belül köteles az elektronikus adat visszaállítására.

Az elektronikus adat ideiglenes eltávolítására és visszaállítására vonatkozó kötelezettség teljesítését a bírósági végrehajtó foganatosítja.

A bíróság hivatalból vagy az ügyész indítványára a tárhelyszolgáltatóval szemben az elektronikus adat ideiglenes eltávolítására vagy visszaállítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki, ami ismételten is kiszabható.

A bíróság a határozatával az elektronikus hírközlési szolgáltatókat kötelezi az elektronikus adathoz való hozzáférés ideiglenes megakadályozására.

Ha az elektronikus adat feletti rendelkezésre jogosult ismeretlen, az elektronikus adat ideiglenes hozzáférhetetlenné tételéről szóló határozatot hirdetményi úton kell kézbesíteni. A hirdetményt

[264] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

tizenöt napra ki kell függeszteni a bíróság hirdetőtáblájára, továbbá közzé kell tenni a bíróságok központi internetes honlapján.

A bíróság az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendeléséről elektronikus úton haladéktalanul értesíti a Nemzeti Média- és Hírközlési Hatóságot (továbbiakban: NMHH)

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének a végrehajtását az NMHH szervezi és ellenőrzi. Az NMHH a bíróság elektronikus úton megküldött értesítése alapján az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába,[265] ezzel egyidejűleg a bíróság határozatáról elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására. Ha valamely elektronikus hírközlési szolgáltató a kötelezettséget nem teljesíti, az NMHH erről haladéktalanul értesíti a bíróságot.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság megszünteti, ha a tárhelyszolgáltató teljesíti az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettségét, az elrendelésének oka egyébként megszűnt, vagy a nyomozást megszüntették (kivéve, ha a Btk. 77. § (2) bekezdése alapján az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye).

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének megszüntetéséről a bíróság elektronikus úton haladéktalanul értesíti az NMHH-t, amely az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget törli a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést.

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a büntetőeljárás befejezésével megszűnik. Ha a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét nem rendelte el, az ideiglenes hozzáférhetetlenné tétel megszűnéséről elektronikus úton haladéktalanul értesíti az NMHH-t, amely az elektronikus adathoz való hozzáférés ideiglenes

[265]Bővebben:http://nmhh.hu/cikk/160577/Kozponti_elektronikus_hozzaferhetetlenne_teteli_hatarozatok_adatbazisa_KEHTA letöltve: 2017. április 20.

megakadályozására vonatkozó kötelezettséget törli a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést.

Ha valamely elektronikus hírközlési szolgáltató a hozzáférés újbóli biztosítására vonatkozó kötelezettséget nem teljesíti, az NMHH erről haladéktalanul értesíti a bíróságot.

A bíróság hivatalból vagy az ügyész indítványára az elektronikus hírközlési szolgáltatóval szemben az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vagy a hozzáférés újbóli biztosítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki, ami ismételten is kiszabható.

A nyomozás során az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelésére a nyomozó szerv vezetője teszi meg az előterjesztését az ügyészhez, aki ezt továbbítja a bírósághoz. Pozitív döntés esetén a bíróság a végrehajtón keresztül kötelezi a tárhelyszolgáltatót az ideiglenes eltávolításra.

Az esetek meglehetősen nagy számában a tárhelyszolgáltató nem rendelkezik magyarországi képviselettel, vagy sok esetben nem fellelhető, vagy honossága szerinti jogrendszerben a szólásszabadság megnyilvánulásának értelmezi azt, amit a magyar bíróság jogsértőnek talál.

Ha a bírósági döntés nem vezet eredményre, és a törvényben meghatározott súlyos bűncselekmények elkövetésének gyanúja áll fenn, a bíróság az NMHH-n keresztül tájékoztatja az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására, azaz például a külföldi szervereken a vélelmezhetően jogsértő tartalom elérhető, de azt a magyar szolgáltatók szűrik és elérhetetlenné teszik.[266]

E jogintézményhez hasonló az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ektv) 13. §-ban rögzített „Értesítés a jogsértő információs társadalommal összefüggő szolgáltatásról" jogintézményéhez. A jogalkotó ebben az esetben a jogsértő tartalmak

[266] Ez a rendszer sokban hasonlít a NAV által betiltott szerencsejáték oldalakra, de ott a jogalapot a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény 36/H. § adja és nem a büntetőeljárás. Bővebben: www.nav.gov.hu/nav/szerencsejatek/blokkolt_honlapok letöltve: 2017. április 20.

eltávolítására kötelezés kezdeményezését a jogaiban sértett személy közvetlen lehetőségévé teszi az információs társadalommal összefüggő szolgáltatást nyújtó természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet irányába.

Itt viszont a sérelem a szellemi tulajdonában sértett jogokra, illetve kiskorú személy személyiségi jogaira vonatkozik, és nem szükséges hozzá bűncselekmény megvalósulásának gyanúja.[267]

Az új Be.-ben az elektronikus adat hozzáférhetetlenné tétele, mint kényszerintézkedés szinte változatlan formában megmaradt. A különbség leginkább a korábbi Be.-ben meghatározott, (1998. évi XIX. törvény 158/B.§-ban) szabályozás óta- eltelt időszak tapasztalatai tekintetében változik, egyszerűbbé teszi az eljárást.

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a jogalkotó szerint[268]: az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozása és az adathoz való hozzáférés ideiglenes megakadályozása.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelésével kapcsolatban nincs változás, eszerint, a közvádra üldözendő bűncselekmény miatt folyó eljárások esetében, amellyel kapcsolatban az elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény megszakítása érdekében szükséges, amelyet határozattal a bíróság rendeli el (ez szintén nem változott az 1998. XIX. törvény szabályozásához képest).

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendelhető a továbbiak szerint az

a) az elektronikus adat ideiglenes eltávolításával, vagy
b) az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával. történhet meg.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének teljesítésére kötelezett tájékoztatja a felhasználókat a tartalom eltávolításának vagy a tartalomhoz hozzáférés megakadályozásának a jogalapjáról.

[267]Be. 335.§ (2).
[268]Be 336.§ (1)

8.4.1 Az elektronikus adat ideiglenes eltávolítása

Az elektronikus adat ideiglenes eltávolításával kapcsolatban a fokozatosság elve érvényesül a szólás-és sajtószabadság tekintetében. Az eljárásjogi szabályozás szerint „*Az elektronikus adat ideiglenes eltávolítására az érintett elektronikus adatot kezelő, az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvényben meghatározott tárhelyszolgáltatót, illetve tárhelyszolgáltatást is végző közvetítő szolgáltatót (a továbbiakban együtt: eltávolításra kötelezett) kell kötelezni. Az eltávolításra kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására”*[269].

Az ideiglenes eltávolításra a közvádra üldözendő bűncselekmények gyanúja esetében van lehetőség, amelyet a bíróság rendel el, és amelynek az említett Elkertv. alapján a tárhelyszolgáltató a kötelezett.

Az elektronikus adat ideiglenes eltávolítását a bíróság megszünteti és az elektronikus adat visszaállítását rendeli el, ha

- az elrendelésének oka megszűnt, vagy
- az eljárást megszüntették, kivéve, ha a Büntető Törvénykönyvben meghatározott feltételek alapján az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye.

Az elektronikus adat ideiglenes eltávolítása a büntetőeljárás jogerős befejezésével megszűnik. A bíróság hivatalból vagy az ügyészség indítványára az eltávolításra kötelezettet az elektronikus adat ideiglenes eltávolítására vagy visszaállítására vonatkozó kötelezettség elmulasztása miatt rendbírsággal sújthatja.

8.4.2 Az elektronikus adathoz való hozzáférés ideiglenes megakadályozása

Az elektronikus adathoz való hozzáférés megakadályozása akkor történhet, amennyiben az elektronikus adat ideiglenes megakadályozása nem vezetett eredményre és a büntetőeljárás kábítószer-kereskedelem, kóros szenvedélykeltés, kábítószer készítésének elősegítése,

[269]Be 337.§ (1).

kábítószer-prekurzorral visszaélés, új pszichoaktív anyaggal visszaélés, gyermekpornográfia, állam elleni bűncselekmény, terrorcselekmény vagy terrorizmus finanszírozása miatt folyamatban lévő büntetőeljárásban a bíróság elrendeli a felsorolt bűncselekménnyel összefüggő elektronikus adathoz való hozzáférés ideiglenes megakadályozását, ha

- az eltávolításra kötelezett az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettséget nem teljesítette
- az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresése a megkeresés bíróság általi kibocsátásától számított harminc napon belül nem vezetett eredményre,
- az eltávolításra kötelezett azonosítása lehetetlen vagy aránytalan nehézséggel járna, vagy
- az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresésétől eredmény nem várható vagy a megkeresés aránytalan nehézséggel járna.[270]

A bíróság az elektronikus adathoz való hozzáférés ideiglenes megakadályozásának elrendelését haladéktalanul közli a Nemzeti Média- és Hírközlési Hatósággal (a továbbiakban: NMHH), amely a kényszerintézkedés végrehajtását szervezi és ellenőrzi.

Az NMHH az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába, ezzel egyidejűleg a bíróság határozatáról elektronikus úton haladéktalanul tájékoztatja az elektronikus hírközlési szolgáltatókat, amelyek a tájékoztatástól számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására. Ha valamely elektronikus hírközlési szolgáltató a kötelezettséget nem teljesíti, az NMHH erről haladéktalanul tájékoztatja a bíróságot.

c) a nyomozást megszüntették, kivéve, ha a Btk. 77. § (2) bekezdése alapján az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye.

(7) Az elektronikus adathoz való hozzáférés ideiglenes megakadályozása a büntetőeljárás jogerős befejezésével megszűnik.

[270] Be. 337.§ (1).

(8) Ha a bíróság a (6) bekezdés c) pontjában vagy a (7) bekezdésben meghatározott esetben nem rendelte el az elektronikus adat végleges hozzáférhetetlenné tételét, az elektronikus adathoz való hozzáférés ideiglenes megakadályozásának megszüntetését vagy megszűnését elektronikus úton haladéktalanul közli az NMHH-val, amely az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget törli a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton haladéktalanul tájékoztatja az elektronikus hírközlési szolgáltatókat, amelyek a tájékoztatástól számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést.

(9) A bíróságnak az elektronikus adathoz való hozzáférés ideiglenes megakadályozása megszüntetéséről vagy megszűnéséről szóló határozatát akkor kell kézbesíteni az elektronikus adat felett rendelkezésre jogosultnak, ha az eljárás addigi adatai alapján személye és elérhetősége ismert. A bíróság e határozata ellen kizárólag az ügyészség élhet fellebbezéssel.

(10) Ha valamely elektronikus hírközlési szolgáltató a hozzáférés újbóli biztosítására vonatkozó kötelezettséget nem teljesíti, az NMHH erről haladéktalanul tájékoztatja a bíróságot.

(11) A bíróság hivatalból vagy az ügyészség indítványára az elektronikus hírközlési szolgáltatót az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vagy a hozzáférés újbóli biztosítására vonatkozó kötelezettség elmulasztása miatt rendbírsággal sújthatja.

A törvénnyel, mint sok kényszerintézkedéssel kapcsolatban a TASZ, azaz a Társaság a Szabadságjogokért- írt észrevétele során észrevételként jegyzi meg, hogy nem csak egy szűk körben hajtható végre, hanem bármilyen közvádra üldözendő bűncselekmény esetén alkalmazható[271].

[271] A Társaság a Szabadságjogokért álláspontja az elektronikus adat hozzáférhetetlenné tételével kapcsolatban (forrás: https://tasz.hu/files/tasz/imce/2011/tasz_velemeny_20121026.pdf letöltve: 2018. április 20.)

8.4.3 Felhívás az elektronikus adat önkéntes eltávolítása érdekében

Bár a kényszerintézkedések köréhez tartozik majd ez az új eljárásjogi szabály, mégis egyfajta választási lehetőséget ad arra, hogy a hatósági felhívásban foglaltaknak eleget tegyenek. Egyetlen probléma jelentkezhet ebben az esetben, ha az adat előállítója, az azt közzé tevő valamint a tárhelyszolgáltató személye nem egy és ugyanaz. Erre az esetre a szabályozás nem nyújt egyelőre iránymutatást. A joggyakorlatra vár a processzus részleteinek tisztázása. Azt gondoljuk, hogy maga a hirdetmény útján (is) történő kézbesítés megoldás lehet a gyakorlat kialakulásáig.

Amennyiben a büntetőeljárás érdekeit nem sérti, az ügyészség vagy a nyomozó hatóság az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelését megelőzően felhívhatja az elektronikus adat önkéntes eltávolítása érdekében a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény szerinti azon médiatartalom-szolgáltatót, illetve azon tárhelyszolgáltatót vagy tárhelyszolgáltatást is végző közvetítő szolgáltatót, amelyik képes megakadályozni az elektronikus adathoz való hozzáférést. A felhívás teljesítése nem kötelező, annak célja az elektronikus adathoz való hozzáférés megakadályozásának a gyorsabbá tétele.

8.5 Konklúzió

A számítógépes bűncselekmények során alkalmazható kényszerintézkedések hazai szabályozásánál megfigyelhető, hogy a jogalkotó szándéka sokkal inkább a számítógépen vagy információs rendszerben tárolt adatokra vonatkozik, mintsem arra, hogy azok végrehajtása során mindenképpen maguknak a számítástechnikai eszközöknek a lefoglalását értik.

Annak ellenére azonban, hogy az eljárási szabályokban megemlíti az információs rendszert, illetve adathordozót, véleményünk szerint ismét túlságosan leszűkíti a lehetőségeket, nem gondolva arra az informatika folyamatos változására, fejlődésére.

9 SPECIÁLIS LEHETŐSÉGEK A SZÁMÍTÓGÉPES BŰNCSELEKMÉNYEK FELDERÍTÉSÉBEN

A disszertáció címének kiválasztásakor tulajdonképpen a nyomozó hatóság lehetősége a (számítógépes) bűncselekmények (is) esetében a nyomozási szakaszban és a vizsgálati szakaszban elvégezhető eljárások voltak. A nyomozási során lehetett nem nyílt eljárás keretében a felderítést végrehajtani. Az új Be.-t követően azonban a törvényben feketén-fehéren megjelent a nyomozás részeként a leplezett eszközök alkalmazásának különböző formái is.

A fent nevesített kényszerintézkedések mellett a másik legcélravezetőbb megoldása a nyomozó hatóság kezében a leplezett eszközök alkalmazása, amelyek különösen alkalmasak lehetnek a szervezett bűnözés, a terrorcselekmény megállapítása, a korrupcióval összefüggő bűncselekmények és a számítógépes bűnözés felderítésére, megelőzésére.

A büntetőeljárási törvényben és a Rendőrségről, továbbá a 2010. évi CXXII. törvény a Nemzeti Adó-és Vámhivatalról szóló törvényben, a 100/2018. (VI.8.) Korm. rendeletben meghatározzák a leplezett eszközök alkalmazásának lehetőségeit, az ügyészi- és bírói engedélyhez kötött, valamint ahhoz nem kötött lehetőségeket.

A szabályozás említését azért tartom fontosnak, mivel az egyik olyan lehetőség a nyomozó hatóság kezében, amellyel a kibertérben elkövetett jogellenes cselekményeket és az azt elkövetőket jóval nagyobb eséllyel lehet tetten érni, mint a nyílt eljárásban meghatározott módszerekkel.

Fenyvesi Csaba véleményét osztjuk a „*titkos eszközök és módszerek felértékelődnek a világ bűnözésében az elmúlt évtizedekben bekövetkezett változásaira tekintettel... és a hagyományos, nyílt nyomozási módszerek nem elegendőek az eredményes bűnüldözés megvalósításához. A titkos felderítési lehetőségek alkalmazásának az is az előnye lehet, hogy segíthet már a büntetőeljárás előtti időszakban is az adatgyűjtésben, utána pedig a büntetőeljárás ideje alatt is.*” [272]

[272] Fenyvesi Csaba: A kriminalisztika tendenciái, A bűnügyi nyomozás múltja, jelene, jövője (Dialóg Campus, Budapest, 2017) 219-220.

9.1 A leplezett eszközök igénybevételének általános szabályai

A számítógépes bűncselekmények az egyik olyan, atipikusnak nevezhető, a társadalmat, gazdaságot és nemzetállamokat veszélyeztető cselekmények, amelyek az elkövetés jellege, annak hatása miatt nemcsak a nyomozószervekre, hanem a nemzetbiztonsági szervezetekre is ró feladatot.

A leplezett eszközök alkalmazása olyan a magánlakás sérthetetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő alapvető jogok korlátozásával járó, a büntetőeljárásban végzett különleges tevékenység, amelyet az erre feljogosított szervek az érintett tudta nélkül végeznek[273].

A leplezett eszközök alkalmazása során az azt igénybe vevő szervezetnek be kell tartania:

- A szükségesség
- Az arányosság
- A célszerűség elvét

Azaz, a leplezett eszközök akkor alkalmazhatóak, ha:

- megalapozottan feltehető, hogy a hatóság által megszerezni kívánt információ az eljárás során bizonyítékként felhasználható adatok beszerzése szükséges, és a leplezett eszköz alkalmazása nélkül nem lenne megismerhető.
- A leplezett eszköz alkalmazása nem jár az érintett(ek) alapvető jogainak aránytalan sérelmével

A leplezett eszközök alkalmazásának lehetősége és a módszerek a számítógépes bűncselekmények felderítésének talán egyik legfontosabb lehetősége, ugyanakkor nem minden esetben olyan egyszerű, mint a hagyományos bűncselekmények esetében.

A következőkben kiemelem az úgynevezett online házkutatást, amelyet a német büntetőtörvénykönyv nevezett el és annak a hazai megfelelőjét, megemlítve a nehézségeket is.

[273] Be. 214.§ (1) bekezdés

9.2 Online házkutatás a magyar és a német büntetőeljárásjogban[274]

A leplezett eszközök közül a kutatás során érdekesnek és ezért érdemesnek tartottam foglalkozni azokkal a lehetőségekkel, amikor az egyes felhasználók személyes, kibertérben zajló életét, akár bűnmegelőzés, felderítési, nemzetbiztonsági célból a technika adta lehetőségekkel ellenőrzik és gyűjtik be az adatokat, a digitális lábnyomokat ezáltal bizonyítékot gyűjtenek a jogellenes cselekmény elkövetésének igazolására vagy elvetésére.

Az online házkutatás elnevezést sem az 1998. évi XIX. eljárási törvény, de még a 2017. évi XC. törvény sem használja ebben a formában és a magyar jogban önmagában a kifejezés is értelmezhetetlen jelenleg[275], de ha a Be. 231.§ (1) bekezdése szerinti szabályozást nézzük, mint „az információs rendszer titkos megfigyelése" kifejezést, már értelmezhetőbbé válik a fogalom.

Ha nagyon keresnénk a hazai eljárásban a megfelelőjét, akkor az tulajdonképpen az internet és különböző szoftverek segítségével elvégezhető titkos adatszerzés, viszont jogértelmezési szempontból a (ház)kutatás szabályait figyelembe véve értelmezhetetlen és eljárásjogilag törvénybe ütköző lenne, hiszen a kutatást meg kell előznie egy felszólításnak, miszerint a keresett dolgot adja át vagy az elektronikus adatot tegye hozzáférhetővé.

Az értelmezéshez segítségül hívtam a német szabályozást, amit majd összehasonlítok az új Be. szabályozásával.

9.2.1 Az információs rendszer titkos megfigyelése Németországban- az Online-Durchsuchung

A német jogrendszerben, büntetőeljárásjogi törvénybe azonban bevezetésre került az „online házkutatás" vagy „Online-Durchsuchung[276]".

A német büntetőeljárásjogi szabályozás alapján az online-kutatást érintett személy tudomása nélkül kell végrehajtani. Az eljárás során technikai eszközzel beavatkoznak a gyanúsított által

[274] Az elektronikus információs rendszerben tárolt adatok, információk titkos adatszerzés
[275] Először talán dr. Romhányi Gergely: Az Online házkutatás helye és szükségessége a magyar büntetőeljárásban című tanulmányában találkoztam ezzel a kifejezéssel, amit most gyakorlati szempontból értelmezek. (http://www.jogiforum.hu/publikaciok/433 letöltve: 2018. október 12.
[276] „StPO (Strafprozessordnung)" (é. n.), https://dejure.org/gesetze/StPO/100b.html §100b.

használt információtechnológiai rendszerbe, amelyből az általa online tevékenysége során keletkezett adatok gyűjthetők (digitális lábnyom), ha:

- alapos annak gyanúja, hogy az elkövető vagy a résztvevő személyében az eljárási törvényben meghatározott különösen súlyos bűncselekményt követték el, vagy próbált elkövetni vagy

- a cselekmény különösen súlyos és

- a tényállás vizsgálata érdekében vagy a gyanúsított hollétének meghatározása lényegesen nehezebbé vagy lehetetlenné válna.

Az intézkedés csak a vádlott (gyanúsított) ellen irányulhat. Más személyek informatikai rendszereibe történő beavatkozás csak akkor megengedett, ha az bizonyos tények alapján feltételezhető, hogy egy másik személy információs rendszereit használja, és a vádlott információs rendszereivel való interferencia végrehajtása önmagában nem vezet a tények kivizsgálásához vagy a vádlott tartózkodási helyének meghatározásához.

Az online házkutatás akkor is megvalósítható, ha más személyeket elkerülhetetlenül érint. Ennek kivitelezése megvalósulhat akár úgy, hogy közvetlenül a hatóságok (esetleg szaktanácsadó) telepítik fel a számítástechnikai eszközre, vagy akár maga a megfigyelni kívánt személy részére- akár a social engineering[277] lehetőségét alkalmazva- maga a célszemély telepíti a programot tudta nélkül a saját informatikai eszközére. Ez utóbbi végrehajtásának sikeressége kérdésesebb, mint amikor a hatóság végzi el a feladatot, hiszen a kontroll és a sikeresség lehetősége eshetőleges.

A Német Köztársaságban az online házkutatásnak a 2008-ban történt bevezetése óta nem feltétlenül volt pozitív visszhangja, hiszen több nagy vírusírtó cég (Avira, Kaspersky) is magának a „Polizeitrojan" azaz rendőrségi trójainak nevezett szoftver alkalmazásával kapcsolatos aggályainak adott hangot, az ismert trójai vírusok hatásai miatt, amelyeket egyébként a bűnözők is képesek lennének manipulálni, ezáltal hamis adatokat, eredményeket kapnának a bűnüldöző szervek.

[277] A social engineeringet pszichológiai manipulációnak nevezik magyarul és az emberi jellemre, annak befolyásolhatóságát használják ki vele

Az online házkutatással kapcsolatban leginkább a titkos információgyűjtés szabályai (lesznek) irányadóak, hiszen az érintett tudta nélkül és jogai korlátozásával hajtható végre. Az online házkutatással összegyűjtött adatok vonatkozásában nem feltétlenül hajtható végre sikeres nyomozás, hiszen:

- előfordulhat, hogy a megfigyelt személy több informatikai eszközt használ, több helyen (akár internet kávézóban);

- nem biztos, hogy egy informatikai eszközt csak egy személy használja és ebben az esetben az esetlegesen keletkezett adatok „szétválogatása" aránytalan nehézséggel járna vagy nem érné el a kívánt eredményt.

Ugyanakkor a másik félnek, azaz az azt elrendelő számára is veszélyt hordozhat, hiszen a kémszoftverről a felhasználó tudomást szerezhet akár az eszközének átvizsgálása révén, így fennállhat a dekonspiráció veszélye.

Az információs rendszer titkos megfigyelése során alkalmazhatnak olyan szoftvert, amely alkalmas az adott számítógépen elhangzott kommunikáció megfigyelésére és rögzítésére, hang- és képfelvétel készítésére, de alkalmas lehet a billentyűzet leütések figyelésére és annak rögzítésére is. Azokban az esetekben, amikor egy adott munkaállomást (nem közösségi használatra gondolok) többen is használnak, a leplezett eszközök általános szabályainál ismertetett elvekre tekintettel, a megfigyelt számítógépet használókkal szemben (amennyiben több személyről beszélünk) az engedély kiadásánál figyelemmel kell lenni arra, hogy:

- az arányosság, a szükségesség és a célhoz kötöttség elvei ne sérüljenek
- a több felhasználó esetén szét lehet-e választani azok tevékenységét – különböző felhasználónév, felhasználói fiókok bejelentkezésével
- amennyiben nehéz megállapítani az adott számítógép használóját, úgy további leplezett eszköz igénybevételének lehetőségét is kell vizsgálni
- folyamatosan vizsgálni kell egyébként is más leplezett eszközök használatának lehetőségét.

Az engedélyt ezen, leplezett eszköz használatára is a bíróság végzésben engedélyezi, így a kérelem előterjesztésénél figyelemmel kell lenni valamennyi olyan tényezőre, amelyek az engedély megadásához elengedhetetlenek.

Előnye az online házkutatás lehetőségének, hogy olyan adatok is megismerhetők valós időben, amelyeket törölt az elkövető (ahogy fentebb írtam már, a törölt adatok sem törlődnek teljesen az adathordozókról, mert azok automatikus mentése- digitális nyoma, megmarad, az visszanyerhető), továbbá kétséget kizáróan utalhatnak a jogellenes cselekmény elkövetésére, a elkövető személyére és a módszerre, továbbá olyan bizonyítékok beszerzését is lehetővé teszi, amelyek e nélkül nem volna lehetséges.

Az online házkutatás szabályai Németországban erősen korlátozottak, és ma már azt csak a titkosított kommunikáció megfigyelésére engedélyezik[278].

9.2.2 Az információs rendszer titkos megfigyelése

A XXI. századra szinte teljes mértékben az informatikai és infokommunikációs eszközökre helyeződött át a titkos információgyűjtés esetében a hangsúly.

A bűnszervezetek, az elkövetők nemcsak ezeken keresztül kommunikálnak egymással, hanem az elkövetéshez szükséges eszközöket, adatokat, információkat az interneten keresztül szerzik meg, ismerik meg.

Sőt, már maga az információgyűjtés is alapvetően technikai eszközökkel történik, így :

- *hagyományosnak számító eszközök, mint rejtett kommunikációs eszközök, a miniatürizált kamerák;*
- *adatgyűjtéseket biztosító optikai, elektronikai, akusztikus, esetleg térinformatikai érzékelők;*
- *számítógépek, hálózatok, szoftverek, amelyek részint szolgáltatják, részint gyűjtik, tárolják és elemzik az információt.*[279]

A bírói engedélyhez kötött leplezett eszközök egyike - ahogyan az előzőekben is említettem- az információs rendszer titkos megfigyelése. Az eszköz alkalmazása során az arra feljogosított szerv bírói engedéllyel az információs rendszerben kezelt adatokat titokban megismerheti, az

[278] 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 letöltve: 2018. október 22. 154-155.oldal)

[279] Országgyűlés Hivatala: Titkos Információgyűjtés, forrás:http://www.parlament.hu/documents/10181/1479843/Infojegyzet_2018_3_titkos_informaciogyujtes.pdf/367c5fc7-36fa-32f9-5baf-06289973f235 Letöltve: 2019. február 15.

észlelteket technikai eszközzel rögzítheti. A rögzítés módját a Be. nem határozza meg, így az a megfigyelt személytől, a bűncselekmény jellegétől és a helyszín adott tulajdonságaitól kiterjedhet:

- A rendszerben tárolt adatok tartalmára, esetleg a metaadatokra.
- A rendszerhez történő hozzáféréshez szükséges jelszavakra, felhasználó azonosítókra.
- A rendszeren keresztül történő kommunikáció megfigyeléséhez, megismeréséhez
- A rendszert használók megismeréséhez (hang-és képrögzítéshez).

Az információs rendszer titkos megfigyelése történhet közvetlenül és közvetetten. A számítástechnikai eszközön egy kívülről feltelepített program segítségével, valamint a számítógépet megfigyelő kép- és/vagy hangrögzítésre alkalmas eszköznek (Be. 232.§ (3) a hely titkos megfigyelése) elhelyezésével, illetve ennek a két rendszernek a kombinációjával együttesen.

Az Országgyűlés Hivatala által megjelent dokumentum szerint az információgyűjtési módszerek- a lakás átkutatása, levelek felbontása- mellett az informatikára, távközlésre épülő eljárások váltak meghatározóvá:

- *a megfigyelt személy számítógépére telepített kémszoftver segítségével jutnak hozzá a gépen tárolt információkhoz, de a szoftver akár hang-és kép rögzítésére és továbbítására is alkalmas (ún. online házkutatás); vagy*
- *megfigyelést végző a kommunikációs csatornába helyezi be az adathalász eszközt, amelyen így minden információ áthalad; esetleg a kommunikációs szolgáltatóval való együttműködés révén jutnak az információt gyűjtők a szükséges adatok birtokába.*

Ugyanakkor fontos emlékeztetni arra, hogy a titkos információgyűjtés kétarcú folyamat, nemcsak hasznos lehet a bűncselekmények felderítése szempontjából, hanem zaklatást, beavatkozást jelenthet az emberek intimszférájába, sérthet személyiségi jogokat."[280]
A titkos adatgyűjtésnek – annak jellegére tekintettel - csak utólag van védői kontrollja, szemben pl. a gyanúsított együttműködését kívánó nyomozati cselekményekkel.[281]

[280] vö. Dr. Fenyvesi Csaba – Dr. Herke Csongor – Dr. Tremmel Flórián: Új magyar … 293.l.
[281] Fenyvesi Csaba: A védőügyvéd. Dialóg Campus. Budapest – Pécs, 2002. 218.l.

9.2.3 Előkészítő eljárás

A hatályos büntetőeljárásról szóló törvény a nyomozásokban nagyobb szerepet szán az ügyészségnek, mint közvádlónak, mind a vizsgálati, mind pedig a felderítési szakban. A törvény szerint az ügyészség nyomoz, felügyeli a felderítés törvényességét, valamint irányítja a vizsgálatot.

Az ügyészség előkészítő eljárást végez és a más szerv által végzett előkészítő eljárásban ellátja az e törvényben meghatározott feladatait.[282]

A kibertérben elkövetett deliktumok során az előkészítő eljárásnak kiemelt jelentősége van, hiszen a hagyományos bűncselekményekkel ellentétben magasabb a látencia, valamint a bizonyítást is sokban nehezíti a nemzetközi és technikai jellege is.

Az előkészítő eljárást a nyomozó hatóság vagy az ügyészség folytathat le, annak érdekében, hogy a megállapítsák, hogy a bűncselekmény gyanúja fennáll-e[283].

Maga az előkészítő eljárás nem más, mint a leplezett eszközök alkalmazására feljogosított szerv által folytatható eljárás, valamint nyílt eszközökkel is folytatható adatszerzés. Amit a törvényben meghatározott szervezetek és azok megsegítésére, a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, illetve a rendőrség terrorizmust elhárító szerve is végezhet.

Az előkészítő eljárás az egyik legalkalmasabb jogintézménye lehet annak, hogy a hatóságok a saját monitorozó tevékenységet végezve, az egyszerű gyanú esetén, a törvényben meghatározott eljárás lehetőségével éljen és a rendelkezésre álló idő- 6 hónapig, egyes esetben 9 hónapig- a bűncselekmény elkövetésének fennállását bebizonyítsa vagy épp elvesse. Bármely bűncselekmény miatt folytatható (így nincs megkötés, sem a büntetési tétel, sem pedig típusánál), így a kibertérben elkövethető valamennyi deliktum miatt, saját hatáskörben eljárva a nyomozó hatóságok vagy az ügyészség megkezdheti az eljárást.

Az előkészítő eljárás esetében elvégezhető adatszerző tevékenység a rendelkezésre álló és a törvényben meghatározott szervezetek nyilvántartásaiból és a törvényben még nem szabályozott OSINT-tal is elvégezhető.

[282] Be. 25. § (1)-(3) .
[283] Be 340.§ (1)

Az OSINT tevékenység törvényben történő szabályozásával kapcsolatban nem vagyok meggyőződve annak szükségességéről, ugyanakkor az azáltal szerzett bizonyítékok hitelességének, felhasználhatóságának kérdései viszont időszerű lenne már.

A leplezett eszköz is igénybe vehető az előkészítő eljárás során, de csak azzal a gyanúsítottal szemben, aki a bűncselekmény elkövetőjeként szóba jöhet, és az ő tartózkodási helyének megállapítása, elérhetőségének megismerése céljából. A kiberbűncselekmények esetében az elkövetők megismerése, felderítése mindig nehézséget okoz az internetes felhasználók anonimitása miatt. A bűnözők számára egyre népszerűbb a kibertér, mivel az azon keresztül folyó kommunikáció ténye a hatóságok számára sokszor nehézségekbe ütközött. Az új eljárás segítségével a leplezett eszközzel folytatott addigi eszköz alkalmazása tovább folytatható. Amennyiben az Unió kívánságát figyelembe veszük, miszerint a kibertér ne a bűnözők menedéke legyen, úgy további szabályozásokra még szükség lenne, anélkül, hogy a szólás- és véleménynyilvánításhoz fűződő jogok sérülnének.

A német StPo (Strafprozessordnung, azaz Büntető Perrendtartás) §163.-a rendelkezései szerint [284]az előkészítő eljárás során az ügyészség is lefolytathatja- hasonlóan a magyar eljárási törvény 347.§ (3) bekezdéséhez- a nyomozást a rendőrség mellett, de lehetőséget ad arra is, hogy a nyomozó hatóságot bízza meg a benyújtott információk alapján az eljárás lefolytatására.

Az ügyész (der Staatsanwalt) dönt a benyújtott bizonyítékok alapján, hogy az előkészítő eljárás lefolytatásáról vagy annak elutasításáról.

9.3 Az előkészítő eljárás során alkalmazható ügyészi engedélyes leplezett eszközök

A leplezett eszközök alkalmazásának előnye, hogy a bűncselekményt elkövetővel szemben, az annak végrehajtására feljogosított szerv, azért, hogy az eljárás célját titokba tartsa, a bűncselekményre vonatkozóan információkat, adatokat gyűjthet, anélkül, hogy arról az adott személy értesülne.

[284] https://dejure.org/gesetze/StPO/163.html. Letöltve: 2018. október 12.

A számítógépes környezetben elkövetett gazdasági illetve tartalombűncselekmények, valamint a terrorcselekmények bizonyítása esetében a rendelkezésre álló leplezett eszközök alkalmazása nagyobb sikerrel kecsegtethet, mint a korábbi Be.-ben szabályozott lehetőségek.

9.3.1 A fizetési műveletek megfigyelése

A fizetési műveletekre vonatkozó új eljárásjogi szabályozás különösen alkalmas lesz az információs rendszer felhasználásával elkövetett gazdasági bűncselekmények felderítésére és vizsgálatára. Bármelyik bűncselekmény elkövetésének legfontosabb bizonyítása lehet, a pénz útjának nyomon követése, az illegális forrásból származó jövedelmek felderítése, de a kibertérben elkövetett bűnözésnél, ahol sokszor csak egy bankszámlaszám ismert és esetleg egy fiktív vagy hajléktalan személy, ahol a számlák közötti átvezetések a netbankolásnak köszönhetően bárhonnan és bármikor intézhetők. A fizetési műveletek határozott időtartamra történő megfigyelésének köszönhetően a pénz mozgása, a számlák birtokosainak tevékenysége valós időben válik nyomon követhetővé és nem napokkal vagy esetleg később beszerezhető adatokból ismerhető meg.

Fizetési művelet megfigyelésének számít:

- A pénzforgalmi számlával kapcsolatos valamennyi fizetési művelet
- A fizetési műveletekre vonatkozó adatok rögzítése, továbbítása.

A fizetési műveletek legfeljebb 3 hónapra rendelhetők el, amelyet az ügyészség egy alkalommal legfeljebb további 3 hónappal hosszabbíthat meg. A megfigyelés alatt a fizetési műveletek felfüggeszthetők legfeljebb 2 napig, de ennek tényéről a pénzintézet, - a szolgáltató- tájékoztatást sem az érintettnek, sem harmadik félnek nem adhat.

A kriptovalutákkal kapcsolatos műveletek, mint a fizetési műveletek megfigyelésének szabályai jelenleg még nem kivitelezhetőek.

A probléma okai:

- a fizetési művelet nem függeszthető fel, hiszen nincs számlavezető bank a digitális pénz mögött

- a 100/2018. (VI.8.) Korm.rendeletben meghatározott szabályok szerint a szolgáltatót tájékoztatni kell az eljárásról, ami a kriptovaluták esetében nem lehetséges.

9.3.2 Álvásárlás

Az ügyészség engedélyével a bűncselekménnyel feltehetően összefüggésbe hozható dolog vagy annak mintája megszerzésére vagy szolgáltatás igénybevételére, az eladó bizalmának erősítése céljából a bűncselekményre vonatkozó tárgyi bizonyítási eszközt eredményező dolog megszerzésére vagy szolgáltatás igénybevételére, az elkövetés elfogásának elősegítésére irányuló színlelt megállapodás köthető és teljesíthető.[285]

Az álvásárlás tehát nemcsak kézzel fogható dolog, hanem bármilyen szolgáltatás igénybevételére alkalmazható (feltételezhetően a Darkneten Bitcoinért, vagyis kriptovalutáért megszerezhető illegális szolgáltatás vagy dolog is érthető alatta). Az álvásárláshoz fedett nyomozó vehető igénybe.

9.3.3 Fedett nyomozó alkalmazása[286]

Mészáros Bence tanulmányában[287] a fedett nyomozóval, mint a titkos információgyűjtés egyik lehetőségéről ír, de a kibertérben elkövetett bűncselekmények felderítésében történő alkalmazásukról nem esik szó. A fedett nyomozó feladata a kibertérben elkövetett bűncselekmények esetén speciálisabb lehet, mint a fizikai térben végzett munkájuk, hiszen amellett, hogy a technikai eszközök sokszor a segítségükre lehet egy-egy feladat elvégzése során, ugyanakkor hátráltató tényező is az, hogy ismerniük kell a kibertérben alkalmazott nyelvezetet, a szakzsargont és nem utolsósorban nehezítésként előfordulhat, hogy személyesen a bűnözővel nem kerülnek kapcsolatba.

A fedett nyomozó az a személy:

[285] Be. 221.§.
[286] Be. 222.§.
[287] 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. Letöltve: 2018. október 01

- A leplezett eszközök alkalmazására feljogosított szerv a szervhez tartozását, illetve kilétét tartósan leplező, kifejezetten ilyen feladat ellátása érdekében foglalkoztatott tagja (új Be.).

- A rendőrséghez tartozását, illetve kilétét tartósan leplező, kifejezetten ilyen feladat ellátása érdekében foglalkoztatott rendőr (Rtv.).

- A NAV-hoz tartozását, illetve kilétét tartósan leplező, kifejezetten ilyen feladat ellátása érdekében foglalkoztatott pénzügyi nyomozó (Navtv.)[288].

Az új Be.-ben a fedett nyomozó alkalmazására legfeljebb hat hónapra van lehetőség, az ügyészség engedélyével, amely alkalmanként hat hónappal meghosszabbítható, a büntetőeljárás céljának végrehajtása érdekében

a) „...a) bűnszervezetbe történő beépülés,
b) terrorista csoportba vagy terrorcselekmény feltételeinek biztosításához anyagi eszközt szolgáltató vagy gyűjtő, továbbá terrorcselekmény elkövetését vagy terrorista csoport tevékenységét anyagi eszközök nyújtásával vagy egyéb módon támogató szervezetbe történő beépülés,
c) álvásárlás,
d) rejtett figyelés végrehajtása,
e) ..... az információ továbbítása, vagy
f) *a bűncselekménnyel összefüggő információk és bizonyítékok megszerzése érdekében alkalmazható*."[289]

Fedett nyomozó különösen alkalmas lehet olyan bűncselekmények elkövetésének az előkészítő eljárás során vagy a felderítés[290] során, amikor az ügy bonyolultsága, az abban résztvevő személyek összetartása miatt egyébként lehetetlen lenne a bizonyítékok megszerzése vagy azok biztosítása. Ilyen bűncselekmény lehet különösen a kritikus infrastruktúrák elleni támadások malware-kkel vagy a gyermekpornográfia bűncselekmény bizonyítása, amikor is, az elkövetők zárt csoportokban kommunikálnak egymással titkosított csatornákon, így a szervezetbe történő

[288] Mészáros Bence: Fedett nyomozók alkalmazása a bűnüldözésben, forrás: https://www.uni-nke.hu/document/uni-nke-hu/5-meszaros-bence.original.pptx
[289] Be.222.§ (2) bekezdés.
[290] A nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI.8.) Kormányrendelet 133.§-a alapján a felderítés: a nyomozó hatóság a felderítés során különösen a bűncselekmény tárgyi és alanyi oldalához tartozó tényeket, az elkövető kilétének és tartózkodási helyének megállapításához szükséges tényeket, valamint a joghátrány alkalmazása szempontjából különös jelentőséggel bíró tényeket vizsgálja.

beépülés, a tagok megismerése, a bűncselekmény helyének lokalizálása során lehet kiemelkedő jelentősége a munkájuknak.

„*Nem büntethető a fedett nyomozó:*

- *az alkalmazása során elkövetett bűncselekmény, szabálysértés vagy közigazgatási bírsággal sújtandó szabályszegés miatt, ha annak elkövetése*

a) a fedett nyomozó alkalmazásának eredményességéhez, az alkalmazással elérni kívánt bűnüldözési célhoz szükséges, és az alkalmazással elérni kívánt bűnüldözési érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek,

b) a fedett nyomozó biztonságának biztosítása, lelepleződésének megakadályozása érdekében szükséges, és a fedett nyomozó biztonságával, lelepleződésének megakadályozásával kapcsolatos érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek, illetve

c) *más bűncselekmény elkövetésének megelőzése vagy megszakítása érdekében szükséges, és a bűncselekmény megelőzéséhez vagy megszakításához fűződő érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek*”[291]

A fedett nyomozó szerepét a leginkább a számítógépes bűncselekmények közül a gyermekpornográfia nem követhet el, ugyanakkor a bűncselekmény elkövetőinek felderítésében alkalmazásuk elengedhetetlen.

9.3.4 A fedett nyomozó feladata a gyermekpornográfia bűncselekményének felderítésében

A fedett nyomozó bevezetése a gyermekpornográfia bűncselekményének felderítésénél elengedhetetlen.

e olyan számítógépes bűncselekmény, amelynél 18. életévet be nem töltött személyről olyan felvételt-kép vagy videofelvételt- készítenek, amely szeméremsértő és alkalmas a nemi vágy felkeltésére.

[291] Be. 224.§ (1).

Btk. 204. § *„Aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt*

a) megszerez vagy tart,

b) készít, kínál, átad vagy hozzáférhetővé tesz,

c) forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz bűntettet követ el, aki az (1) bekezdés b) pontjában meghatározott bűncselekményt az elkövető nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére, illetve a sértettel kapcsolatban fennálló egyéb hatalmi vagy befolyási viszonnyal visszaélve követi el.

.....büntetendő, aki az (1) bekezdés c) pontjában meghatározott bűncselekményhez anyagi eszközöket szolgáltat.

(4) Aki tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban

a) szereplésre felhív,

b) szerepeltet,

Büntetendő, aki

a) tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf felvételen való szereplésre felhív,

b) olyan pornográf műsoron vesz részt, amelyben tizennyolcadik életévét be nem töltött személy szerepel vagy ilyen személyek szerepelnek,

c) tizennyolcadik életévét be nem töltött személy vagy személyek pornográf műsorban való szerepeltetéséhez anyagi eszközöket szolgáltat.

(6) Aki tizennegyedik életévét be nem töltött személyről vagy személyekről pornográf felvétel készítéséhez, forgalomba hozatalához vagy az azzal való kereskedelemhez szükséges vagy azt könnyítő feltételeket biztosítja, vétség miatt .... büntetendő."

A gyermekpornográfia- vagy gyermekek elleni szexuális abúzus- bűncselekményét az követi el, aki gyermekről (azaz a 18. életévet be nem töltött személyről vagy személyekről) pornográf felvételt megszerez vagy tart, készít, kínál, átad, vagy hozzáférhetővé tesz. Mindezen cselekményekhez pedig az internet számos lehetőséget kínál, hiszen egy tapasztalatlan, óvatlan gyermektől könnyedén csalhatnak ki idegenek olyan felvételeket, melyek nemiségüket súlyosan szeméremsértő nyíltsággal, célzatosan a nemi vágy felkeltésére irányuló módon ábrázolja. Ez pedig kimeríti a törvényben szereplő pornográf felvétel fogalmát.

A deliktum elkövetési tárgyai a 18. életévet be nem töltött személyek, valamint azok a felvételek, amelyek alkalmasak a nemi vágy felkeltésére.

A bűncselekmény elkövetési magatartásai:

A tényállás (1) bekezdés a) pontjaiban szereplő megszerzés és tartás tekintetében irreleváns, hogy az elkövetés tárgya hogyan került az elkövető birtokában- vásárlással, az internetről történő letöltés során ingyen, illetve a felvétel birtokosa beleegyezett-e a felvétel más számára történő megszerzésébe.

Az (1) bekezdés b) pontja szerint készít, kínál, átad vagy hozzáférhetővé tesz, amely magatartások tekintetében a nemi vágy felkeltésére alkalmas képet előállít, vagy annak továbbítását ingyen vagy pénzért esetleg egyéb előnyért más számára felajánl, vagy más számára ingyen vagy pénzért, esetleg más előnyért átad, illetve megteremti annak lehetőségét, hogy az információs rendszerben tárolt gyermekekről készített felvételt más is megismerje, akár úgy, hogy a szükséges belépést, jelszót, URL címet elérhetővé tesz.

Az (1) bekezdés c.) pontja szerint az elkövetési magatartás megvalósulása megtörténhet ingyenesen, vagy bármilyen előnyért, pénzért cserébe, akár haszonszerzési céllal, de mindenképpen más személyekhez történik a felvétel eljutása.

A „nagy nyilvánosság számára hozzáférhetetlenné tételének" fogalmát a Btk. 459.§ határozza meg. Ezen szakasz alapján: a sajtótermékek, a médiaszolgáltatás, sokszorosítás vagy elektronikus hírközlő hálózaton való közzététel útján történő elkövetést" érti[292].

Az elkövetési magatartások esetében: egy (kép)felvétellel kapcsolatban csak egyféle elkövetési magatartás követhető el. Azaz ugyanarra a felvételre nem állapítható meg a készítés, a tartás, mint elkövetési magatartás.

A nyomozás során felmerülő nehézségek:

Az elkövetők titkosított csatornákon kommunikálnak, zárt közösséget alkotnak. Ennél a bűncselekménytípusnál a legjellemzőbb a határok nélkülisége, a nemzetközi jelleg.

[292] BH 2005.133 alapján a hozzáférhetővé tétel olyan szándékos magatartást feltételez, amelynél több személy számára van lehetőség az adott felvétel(ek) megismerésére.

A kommunikáció és a csoporthoz tartozás jellemzői, hogy sajátos nyelvezetet használnak. Az új tagnak a csatlakozási feltétele legtöbbször egy csoporthoz, hogy 18. életévet be nem töltött személyről saját készítésű pornográf felvétel készítése és megosztása a csoport tagjaival.

Az ilyen típusú csoportok, szerveződések nem egykönnyen találhatóak meg, így igazából a hatóság tudomására jutása komoly kutatómunka eredménye, feljelentés, bejelentés útján lehetséges. A nemzetközi jellege miatt a sértettek beazonosítása szintén aprólékos nyomozói munka eredményeként teljesülhet és a felderítésnél a nemzetközi együttműködésnek kiemelt jelentősége van, hiszen az országhatárokon átnyúló bűnözés esetében is csak a saját állam rendőrsége teljesítheti és folytathatja le az eljárást és a kényszerintézkedések végrehajtását.

Nehézséget jelenthet, hogy az online világ elterjedése miatt, hogy maguk az elkövetők sem töltötték be a 18. életévüket. Jellemző, hogy a tinédzser korú személyek között kialakult kapcsolat során egymásnak erotikus tartalmú képeket küldenek, amelynek önmagában a tartása is már megvalósítja a törvényi tényállásra vonatkozó részt: „*tart*” vagy amennyiben egymásról készítik, úgy a „*készít*” elkövetési magatartásokat. Sajnálatosan egyre gyakoribb, hogy az előbb említett formában keletkezett képeket, felvételeket, bosszúból vagy pedig más, indokból, szándékosan megosztják egymás között vagy pedig a különböző internetes fórumokon, oldalakon elérhetővé teszik.

Ugyanakkor nemcsak a beállított, nyíltan erotikus, szeméremsértő felvételek tartozhatnak a gyermekpornográf „anyagok” közé, hanem a játszótereken gyanútlanul játszó, szórakozó gyermekekről készült olyan felvételek is, amelyeken az azon szereplő gyermekek olyan pozícióban, testhelyzetben vannak, játszanak (például a homokozóban széttett lábbal játszó kislány vagy egy bokor mögött pisilő kisfiú/kislány), ami épp amiatt miatt fotóznak le és töltenek fel pedofil oldalra az elkövetők.
Hasonló a helyzet a gyermeküköről (csecsemőről)meztelen vagy olyan helyzetben felvételt készítő szülőkről, akik ezeket a képeket a közösségi oldalukra a rokonoknak, barátoknak töltik fel, és amelyek alkalmasak lehetnek a pedofilok számára a nemi vágy kielégítésére.

A Kúria 2/2018. BJE. szerint: „*A gyermekpornográfia bűntettének a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 204. § (1) bekezdésében írt eseteiben nem eredményez halmazatot önmagában az, hogy az elkövetési magatartás – az azokon szereplő tizennyolcadik életévét be nem töltött személyek számától függetlenül – több pornográf felvételt érint. Ugyanakkor bűncselekményegységet csak az azonos törvényi tényállásba ütköző*

magatartások képeznek. E bűncselekmény tekintetében nem azonos, hanem külön-külön törvényi tényállást tartalmaznak a Btk. 204.§ (1) bekezdésének a), b) és c) pontjai.
II. Amennyiben az elkövető ugyanazon felvétellel kapcsolatban különböző pontokban írt elkövetési magatartásokat valósít meg, egységesen a legsúlyosabb büntetési tétellel fenyegetett bűncselekmény valósul meg.
III. Ha az elkövető különböző felvételekkel kapcsolatban valósítja meg a Btk. 204. § (1) bekezdésének különböző pontjaiba ütköző elkövetési magatartásokat, az azonos törvényhelyen belül egységként minősülő cselekmények egymással valóságos halmazatban állnak.
IV. A gyermekpornográfia Btk. 204. § (2) bekezdése szerinti minősített esetének rendbelisége a felvételeken szereplő, a törvényhelyben meghatározott feltételeknek megfelelő személyek számához igazodik."

A gyermekpornográfia bűncselekményének nyomozása során külön kihívást jelent az internet sötét oldalaként emelgetett Dark Net, amin keresztül folytatott illegális kereskedelem, a gyermekek áruként szexuális célból történő kihasználása és az ilyen célú kereskedelme külön kihívást jelent és amelyre jelenleg még a jogalkotók egységes fellépést nem tudtak kitalálni.

9.4 Konklúzió

A leplezett eszközök alkalmazása a számítógépes bűncselekmények felderítése során elengedhetetlen, hiszen az elkövetők, így például a hackerek, életüket leginkább a négy fal között töltik, a számítógépükön élik mindennapjaikat és azon követik a jogellenes cselekményüket. A megállapítása és felderítése, kapcsolataik és kommunikációjuk megismerése az IT fejlődésének köszönhetően a leplezett eszközök bevezetése nélkül ellehetetlenül.

A leplezett eszközök alkalmazása, bár az érintett személyek Alaptörvényben lefektetett jogait sértik, ugyanakkor a feltételek fennállása esetén a legcélravezetőbb megoldást is jelentheti a bűncselekmény megelőzés és felderítése érdekében.

Ennek ellenére a titkos információgyűjtés alkalmazásával összefüggésben, osztom Fenyvesi álláspontját, miszerint az „*éppen a bűncselekményektől védendő- polgár folyamatosan*

„megfigyelés„alatt van, virtuális és valóságos látókörben mozog... amelyek folyamatosan láthatóvá, felügyeltté és ellenőrzötté teszik a digitális dzsungel világában."[293]

Ugyanakkor Nyeste Péter a tanulmányában is említi, hogy *a titkos információgyűjtés és titkos adatszerzés különleges eszközeinek és módszereinek eredménye a továbbiakban a bizonyítási eszközök és cselekmények katalógusát gazdagíthatják*[294], mindemellett azok alkalmazása sokkal nagyobb eséllyel vezethet a számítógépes bűncselekmény elkövetőinek a nyomára.

[293] Fenyvesi: uaz. 220.
[294] Nyeste Péter: A leplezett eszközök hatékonysága (Pécsi határőr Tudományos Közlemények XIX. 2017) 157.

10 A BÜNTETŐ TÖRVÉNYKÖNYVBEN SZEREPLŐ SZÁMÍTÓGÉPES BŰNÖZÉSSEL KAPCSOLATOS EGYES TÉNYÁLLÁSOK NYOMOZÁSI PROBLÉMÁI

A büntetőeljárásjogi szabályozás mellett szerettem volna egyes büntető törvényi tényállásokat is megvizsgálni.

A törvényi tényállások szükséges mértékig említésre kerülnek, mindamellett a kérdéses részek, esetleg jogesetek alátámaszthatják a már említett flexibilitás hiányát a számítógépes bűncselekményekkel foglalkozó törvényeinkben.

10.1 Információs rendszer felhasználásával elkövetett csalás

A hatályos büntetőjogi szabályozás alapján az követi el az információs rendszer felhasználásával elkövetett csalást, „aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz.” A bűncselekmény által védett jogi tárgyak a számítástechnikai rendszer integritásához fűződő jogi érdeket, a vagyoni viszonyok, az elektronikus készpénz-helyettesítő fizetési eszközök forgalmának a biztonsága.

A bűncselekmény elkövetési tárgya egyrészt az információs rendszer/ maga a számítógépes adata, program, illetve másrészt a hamis, a hamisított, illetve jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz.

A bűncselekmény elkövetési magatartásai: a törvényi tényállás elnevezésében jogtalan haszonszerzés végett a számítástechnikai rendszerbe elektronikus adatot bevitele, az abban kezelt adatot megváltoztatása, törlése vagy hozzáférhetetlenné tétele. A tényállás ezen része a haszonszerzés végett végrehajtott, célzatos cselekményeket foglalja magába. A haszonszerzésre való törekvés. Az elektronikus adat bevitele történhet ún. off-line módban vagy akár online módban is.

A deliktumnál hiányoznak a klasszikus értelemben vett tényállási elemek, azaz a tévedésbe ejtés vagy a tévedésben tartás, így sokszor a csalás tényállásával- amennyiben azt például internetes hirdetési oldal segítségével követik el - sok esetben összetévesztik az elektronikus információs rendszer felhasználásával elkövetett csalással.

A sértett kárának bekövetkezését az információs rendszerben az elkövető(k) jogtalan befolyásolása okozza. Azaz amennyiben valaki az információs rendszerbe bármilyen valótlan vagy a jogosultsága kereteit túllépve adatot bevisz, bármilyen adathordozóról (pl.: CD, DVD, Pendrive) feltölt, a már bevitt adat tartalmát megváltoztatja műszaki úton, a törléssel az a rendszerben tárolt adatot megsemmisíti, úgy, hogy azt visszaállítani már nem lehet.

A hozzáférhetetlenné tétellel történő elkövetés azt jelent, amikor is az adat megszerzésére, kezelésére jogosult személy –akár csak ideiglenesen (a törvényalkotó nem említi azt az időtartamot, amíg is- gátolva van az adat elérhetőségében.

A jogosulatlanul többszörözés szintén bűncselekménynek számít**.**

A hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával történő károkozás, vagyis a készpénz-helyettesítő fizetési eszköz hamisítása.

A 2012. évi C. törvény , a Btk. 459.§-a alapján „*készpénz-helyettesítő fizetési eszköz a hitelintézetekről szóló törvényben meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett.”*[295]

Jogosulatlannak minősül a fizetőeszköz megszerzése, ha azt az elkövető lopással (akár fizikailag veszi magához a bankkártyát vagy pedig erre készített eszközzel megszerzi az azon

[295] Készpénz-helyettesítő fizetőeszköznek minősül a csekk, hitelkártya, a csekk-kártya, a debit- és hitelkártya, a kereskedelmi kártya, a váltó, a Széchenyi Pihenő Kártya (SZÉP-kártya), az Erzsébet-utalvány, továbbá a takarékbetétkönyv vagy az ilyen betétről kiállított más okirat és elnevezésétől függetlenül minden más, a fent felsoroltakkal azonos rendeltetésű okmány.

szereplő adatokat) vagy erőszakkal, fenyegetéssel, megtévesztéssel, illetőleg más jogellenes módon veszi birtokba.

Informatikai környezetben a bankkártyák felhasználása, használata:

- ATM-en (Automatic Teller Machine) keresztül történő készpénz felvétel, lekérdezés, azon keresztül történő befizetés, feltöltés stb.
- POS terminálon keresztül történő fizetés, vagy szolgáltatás/vásárlás kiegyenlítése bank- vagy hitelkártyával
- virtuális térben interneten történő áruvásárlás, vagy szolgáltatás kiegyenlítése (elektronikus kereskedelem vagy online kereskedelem).
- Az interneten a hamis, hamisított kártyák elfogadása tipikusan pénzmosásra utalhat.
- A bűncselekmény elkövetője bárki lehet. Csak szándékosan, pontosabban egyenes szándékkal elkövethető bűncselekmény.
- A bűncselekmény sértettje lehet természetes és jogi személy és tipikusan az, akinél a kár keletkezik.

Jogos kérdésként merül fel ennél a bűncselekmény típusnál, hogy milyen szerepe van annak a személynek, aki rosszindulatú szoftvert ír, amelyet egy ismeretlen személy megvásárol Bitcoinért, és amellyel a káros programot író iránymutatásai alapján, az ATM biztonsági burkolatát eltávolítva, egy pendrive-val feltelepítik és az automatában lévő pénzt eltulajdonítják. Milyen szerepe van a bűncselekményt elkövetőknek? Hogyan lehet bizonyítani a bemutatott kényszerintézkedésekkel, hogy ki volt az a személy, aki a programot írta?

10.2 Tiltott adatszerzés

A tiltott adatszerzés törvényi tényállása: „Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti,

c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,

d) elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti.[296]

Az (1) bekezdés szerint büntetendő, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

a) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiséget vagy területet, továbbá - a közösségi közlekedési eszköz kivételével - járművet titokban átkutat,

b) nyilvános vagy a közönség részére nyitva álló helyen kívül más helyiségben vagy területen, továbbá - a közösségi közlekedési eszköz kivételével - járművön történteket titokban technikai eszköz alkalmazásával megfigyeli vagy rögzíti."

Az deliktum alanya azok a személyek lehetnek, akik a személyes adat, a magántitok, a gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja, más lakásában, egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy azt rögzíti, más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti, elektronikus hírközlő hálózat - beleértve az információs rendszert is - útján másnak továbbított, vagy azon tárolt adatot kifürkészi, és az azon észlelteket technikai eszközzel rögzíti.

„*A Legfőbb Ügyészség – a Fővárosi Főügyészség által az un. MTVA-s megfigyelési ügyben hozott részmegszüntető határozat kapcsán – 2017 februárjában hivatalból eljárva megvizsgálta a Btk. 422.§-ának (1) bekezdésében szabályozott tiltott adatszerzés bűncselekménye szabályozását."*[297]

A Legfőbb Ügyészség (továbbiakban: LÜ) álláspontja szerint a tiltott adatszerzés bűncselekményt dogmatikailag helyes megközelítésben csak olyan helyen lehet elkövetni, ami

[296] Btk.422.§ (1) .

[297] „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.

a magánlaksértés bűncselekmény kapcsán kialakult joggyakorlat szerint megfelel a más lakása, egyéb helyisége vagy az azokhoz tartozó bekerített hely fogalmának.

Ilyen módon azonban nem vonható a törvényi tényállás alá az a magatartás, amikor munkahelyi irodákban, egyéb helyiségekben kerül sor az ott történtek technikai eszköz alkalmazásával való megfigyelésére vagy rögzítésére, pedig- ahogy az LÜ is rámutat- indokolt lenne az elkövetés helyének bővebb maghatározásával a bűncselekménnyel fenyegetett magatartások körét kibővíteni."[298]

A LÜ által benyújtott felülvizsgálati kérelem alapján a Kúria megállapítása... *„jelenleg hatályos szabályozás szerint a tiltott adatszerzés bűncselekményét csak olyan helyen lehet elkövetni, ami a magánlaksértés bűncselekmény kapcsán kialakult joggyakorlat szerint megfelel a „más lakása, egyéb helyisége vagy az azokhoz tartozó bekerített hely" fogalmának*".[299]

10.3 Az információs rendszer vagy adat megsértése

A bűncselekmény tényállása: „Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétséget követ el. Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz bűntettet követ el."

A tényállásban több jogi tárgy is megtalálható.

Az (1) bekezdés szerint a jogi tárgy: a számítástechnikai rendszerek integritása, biztonsága.

A tényállás további jogi tárgyai: a Btk. 423.§ (1) bekezdés b) pontjában az információs rendszerek biztonságos működése, azaz a jogosultság kereteinek megsértése, ezáltal a számítógépen vagy az információs rendszeren tárolt adat megváltoztatása (a rendszerhez

[298] „Tiltott adatszerzés bűncselekmény - A Legfőbb Ügyészség által tett intézkedésekről", http://www.jogiforum.hu/hirek/37269, 2017. február 17., http://www.jogiforum.hu/hirek/37269.
[299] „A tiltott adatszerzés bűncselekmény - A Kúria is osztja a Legfőbb Ügyészség jogi álláspontját".

jogosult személy olyan szándékos magatartása értendő ez alatt, amikor a magatartása az adat rosszindulatú megváltoztatására irányul.)

A bűncselekmény elkövetési tárgyai: az információs rendszer (a számítógép vagy számítástechnikai rendszer) és az abban tárolt számítógépes programok és elektronikus adatok. Az Információs rendszer fogalmát a Btk. 459.§ (1) bekezdés 15. pontja határozza meg: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

Az informatikai hálózat esetében megkülönböztetünk belső hálózatot (intranet) vagy az internet részét képező hálózat (pl. egy bank, biztosító hálózata), vagy a szerver feltalálási helye a valós térben vagy a virtuális térben (mint pl. az ún. cloud-szerverek esetében). A hálózatok egy része publikus, azaz minden felhasználó által, céljának megfelelően használható, a hálózatok másik része azonban a nyilvánosság elől elzárt és csak a beavatottak által ismert jelszóval, egyéb azonosítóval használható.

A bűncselekmény elkövetési magatartásai:

1. A jogosulatlan belépés, ami megtörténhet, egy más által jogszerűen birtokolt, használt számítástechnikai rendszerbe, úgy mintha az jogosult használó lenne (színlelés) vagy a számítástechnikai rendszeren keresztül egy védett hálózatba.

Szükséges az, hogy a számítógép vagy az informatikai hálózat, számítástechnikai hálózat bármilyen biztonsági és/ vagy védelmi megoldásokkal aktívan (vagyis a belépéskor minden egyes felhasználó legalább külön-külön felhasználónévvel és jelszóval illetve egyéb azonosítóval tudjon csak jogszerűen belépni) védve legyen.

Ezen feltételek fennállása esetén, az aktív védelem ellenére, aki jogosulatlanul belép, az (az aktív) védelemmel ellátott számítógépet vagy számítástechnikai rendszert vagy védett hálózatot a jogosultsága kereteit túllépve

- a biztonsági rendszer hiányosságait kihasználva jogosulatlanul belép vagy
- más felhasználó nevével és annak belépési kódjával lép be.

A bűncselekmény elkövetése szempontjából lényegtelen ugyanakkor, hogy hogyan jut a belépéshez szükséges adatokhoz, vagyis a megszerzésének módja lényegtelen.

Azaz megtévesztéssel (social engineeringgel, kifürkészéssel, a felhasználó hanyagságának köszönhetően- a clean desk (tiszta asztal szabályának megszegésével) a monitoron vagy munkaasztalon, vagy egyéb elérhető/látható helyen hagyott felhasználónév és jelszó otthagyása következtében-, illetve az világhálón is elérhető kódmegismerő program segítségével[300].

A belépés nem tekinthető jogosulatlannak, ha a számítástechnikai rendszer nincs ellátva semmilyen védelemmel (hálózati ,illetve fizikai), vagy a védelem nem aktivált.

A belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével történő bennmaradása:

2. Amikor az elkövető a saját felhasználónevével és jelszóval lép be az adott információs rendszerbe, de:
- a felhasználói jogosultságát túllépve, olyan műveleteket akar folytatni, amire a jogosultsága már nem terjed ki.

Ennek megállapítása nem igényel különleges szakértelmet, hiszen az információs rendszerekhez történő hozzáférés előre meghatározott, így annak véletlenszerű elkövetése szinte kizárt[301].

Az információs rendszer elleni támadásokról szóló 2013/40/EU irányelvben sem és a Btk.-ban sem található annak pontos meghatározása, hogy mit is értenek pontosan a jogosultság kereteinek túllépésén és milyen helyzetben rendeli büntetni a törvényben és milyen esetek képezhetik ez alól a kivételt. Így előfordulhat olyan vis major eset egy rendszerben, amikor a kár elhárítás érdekében történt jogosultság kereteinek túllépése is büntethető.

10.4 Az információs rendszer védelmét biztosító technikai intézkedés kijátszása

Aki a 375. §-ban, a 422. §-ban vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

[300] De: ha a belépéshez szükséges a jelszavakat, kódokat fizikai erőszak vagy fenyegetés alkalmazásával szerzik meg, akkor megvalósul a Btk. 195.§-a, vagyis a kényszerítés tényállása állapítható meg.
[301] A tényállás eleget tesz a Számítástechnikai Bűnözésről szóló Egyezménynek, valamint az Európai Parlament és a Tanács 2013/40/EU irányelvében foglaltaknak.

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve
b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétséget követ el.

Az információs rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekménye az információs rendszer vagy adat megsértésének és az információs rendszer felhasználásával elkövetett csalásnak az előkészülete.

Ezzel a szabályozással a jogalkotó az informatikai rendszerbe való jogosulatlan vagy a jogosultság kereteit túllépve a belépést lehetővé tevő (illegális) program, jelszó, belépési kód, más adat készítését, mások számára hozzáférhetővé tételét bünteti, amivel a védett rendszerek ezáltal feltörhetők. A védett számítástechnikai rendszerekbe történő jogosulatlan belépés teszi lehetővé a rendszer és az adatok elleni legkülönfélébb bűncselekmények elkövetését.

A bűncselekmény jogi tárgya: az elektronikus adatfeldolgozás- és átvitel integritása, biztonsága, mely magában foglalja a számítástechnikai rendszert és annak működését, valamint a feldolgozásra rendelt adatok, mint elektronikus impulzusok biztonságát.

A deliktum elkövetési tárgya: az elektronikus adatfeldolgozó- és adatátviteli rendszer védelmi-biztonsági megoldásainak kijátszására alkalmas program, belépési kód, jelszó, vagy egyéb adat, amely a védett rendszerbe történő jogszerű belépést biztosítja.

Belépési kód: a felhasználónév, amely a hozzárendelt jelszóval együtt teszi lehetővé valamely hálózatba, számítógépbe a belépést a jogosult számára.

Jelszó: a hálózat (Internet, intra- és extranet) valamint adatállomány hozzáféréséhez szükséges azonosító kulcsszó. Általában jelszavak védik a BIOS-t, különböző operációs rendszerekben pl. a megosztott erőforrásokat, a szövegszerkesztő programokban a dokumentumokat stb.

A bűncselekmény elkövetési magatartásai: számítástechnikai program készítése, átadása, megszerzése, forgalomba hozatala.

A készítés alatt a jogalkotó a program írását, az adott elektronikus információs rendszer védelmére szolgáló jelszó generálását, a jelszó felülírását stb. értendő. Átadás: az adott számítástechnikai rendszer vonatkozásában a program készítőjétől stb. különböző személynek

a birtokba adása. Közömbös, hogy ez ingyenesen, visszterhesen, megtévesztéssel vagy más módon történt. A megszerzés módja legfeljebb büntetéskiszabási szempontként értékelhető.

Hozzáférhetővé tétel: a program, jelszó, adat eljuttatása egyéb módon, akár aktív, akár passzív magatartással (pl. többek által használt helységben, irodában, gépteremben a belépési kód, jelszó stb. asztalon, képernyőre ragasztott papírdarabon történő otthagyása).

A forgalomba hozatal: több személy számára hozzáférhetővé teszi a feltörésre alkalmazható programot.

A számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismeret másnak a rendelkezésére bocsátása.

Kódfeltörő program írásához, jelszógeneráláshoz, ezek megszerzéshez, forgalomba hozásához szükséges elméleti vagy gyakorlati ismereteket, programrészleteket másnak továbbad, kapcsolatrendszert megoszt.

Nem tartozik ide a szakirodalomban ilyen programok megnevezése, a program működésének, hatásmechanizmusának leírása.

Ugyanakkor nem büntethető az, aki program, jelszó, adat készítő tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

A büntethetőséget megszüntető ok akkor jöhet szóba, ha a bűncselekmény elkövetéséhez szükséges, vagy ezt megkönnyítő számítástechnikai programot, jelszót, belépési kódot, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adatot,

- az elkövető azelőtt hozza a hatóság tudomására, vagy adja át a hatóságnak stb. mielőtt a hatóságnak erről ismerete lett volna.

A bűncselekmény elkövetője mindkét esetben bárki lehet. A szakismeret, a tudás szintje a büntetéskiszabási szempontjából lehet releváns.

A bűncselekmény célzatos, emiatt csak egyenes szándékkal (dolus directus) valósítható meg.

10.5 Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése

Btk. 385.§ „Aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait vagyoni hátrányt okozva megsérti, vétséget követ el.

Vétség miatt büntetendő, aki a szerzői jogról szóló törvény szerint a magáncélú másolásra tekintettel a szerzőt, illetve a kapcsolódó jogi jogosultat megillető üreshordozó díj, illetve reprográfiai díj megfizetését elmulasztja".

A bűncselekmény védett jogi tárgya a szerzői jogi védelem alá tartozó alkotásokhoz fűződő vagyoni jogok, vagyis az irodalmi, a tudományos és a művészeti alkotások szerzőinek és a kapcsolódó jogi teljesítmények jogosultjainak önálló jogai[302]. A tényállás háttér szabályozása az 1999. évi LXXVI. törvény a Szerzői jogról szóló törvény (továbbiakban Szjt). A tényállás elkövetési magatartásai:

- a szerzői vagy szerzői joghoz kapcsolódó jogok megsértése, ami jellemzően felhasználással valósul meg. Így a többszörözés, a terjesztés, a nyilvános előadás, a nyilvánossághoz közvetítés sugárzással vagy másként, átdolgozás stb.
- az üreshordozó díj, valamint reprográfiai díj megfizetésének elmulasztása[303].

A szerzői joggal kapcsolatos bűncselekmények közül említést érdemel még mindig a szoftverhamisítás. Ez egy „speciálisan" elkövetett szerzői jogi jogsértés, lévén, hogy a szoftverek esetében (kivéve a freeware) már a magáncélú letöltés is bűncselekménynek számít. Itt a most már hatályos büntető törvénykönyv szerint, amennyiben a szoftver értéke nem haladja meg a 100.000 forintot, úgy csak szabálysértés elkövetéséről beszélhetünk. Viszont az is tény, hogy akár egy szoftverrel is el lehet követni a deliktumot, amennyiben annak forgalmi értéke meghaladja a szabálysértési értékhatárt. Itt újabb probléma merül fel, mert a jogalkotónak - mint fentebb említettem- az a szándéka, hogy a …" *a büntetőjog, mint végső eszköz szempontjából indokolatlannak tűnik a nem jelentős mennyiségű szerzői mű vagy kapcsolódó jogi teljesítmény vonatkozásában megvalósuló, személyes célokat szolgáló felhasználások tömeges kriminalizálása. A szerzői jog területén fennálló nemzetközi kötelezettségeink, így különösen a …TRIPS egyezmény csupán a szándékos és a kereskedelmi mértékű „szerzői jogi*

[302] a Büntető Törvénykönyvről szóló 2012. évi C. törvény 385.§ .
[303] BH 2003.301.- a bűncselekmény megvalósul, amennyiben egy vendéglátó egységben a rádiókészülékkel szolgáltatják a zenét, de ezután a hely üzemeltetője a zeneszolgáltatásért járó díjat nem fizeti meg

kalózkodásra" nézve teszi kötelezővé a büntetőjogi szankciók előírását, a kereskedelmi mértéket el nem érő cselekmények esetén nincs olyan körülmény, amely ezen a területen a nemzetközi normáknál szigorúbb büntetőjogi szabályozást indokolná."[304]

2011. január 1-je óta a szellemi alkotásokat sértő bűncselekmények nyomozása kizárólag a Nemzeti Adó-és Vámhivatal hatáskörébe került. Így a rendőrségen az addig még folyamatban lévő nyomozások áttételre kerültek a NAV-hoz. Ennek az eljárások szempontjából célszerűségi okai is voltak, hiszen előfordult, hogy ugyanabban az ügyben vagy ugyanazon személy ellen párhuzamos nyomozás folyt a rendőrség és a vám-és pénzügyőrség bűnügyi nyomozói között, ami erősen megnehezíthette a felderítést.

Mivel illegálisan feltöltött filmekről, zenékről, játékokról és szoftverekről van szó, nyilvánvaló, hogy az elkövetők nem adóznak ezen bevételek után, vagy pedig fiktív cégek, társaságok állnak mögöttük.

A szerzői jogokat sértő bűncselekmények elkövetése, illetve az elkövetői is folyamatos és gyors változáson mentek át. Kezdetben még csak az otthon másolt video- illetve hangkazettákat lehetett piacokon vagy hirdetési újságokban megvásárolni. Ahogy az internet egyre népszerűbb lett, ahogy a számítógépek is hozzáférhetőbbek lettek, úgy változott a hamisítás is.

A hamis DVD-és CD lemezek árusítása esetében viszonylag egyszerűbb volt a felderítés, hiszen a különböző piacokon, közterületeken történő ellenőrzés során a papírdobozokból történő árusítás tetten éréssel és lefoglalással megoldódott. A másolt lemezekről egyszerűen lehetett megállapítani, hogy az azokat árusító személy vagy személyek nem fizették meg a jogdíjat (sokan a kihallgatás alkalmával hallották ezt a szót először) így már a hatóságnak csak a darabszámot kellett megállapítani, illetve már csak a jogtulajdonosokat esetleg az őket képviselő ügyvédi irodákat kellett megkeresni és nyilatkoztatni őket - ahogyan már fentebb is említettem -, hogy az elkövetőkkel szemben kívánják-e a polgári jogi igényeket érvényesíteni. A következő fejlődési lépcsőfok a DC és a DC++ technológia. Ezek olyan internetes oldalak, ahonnan szerzői joggal védett műveket lehetett közvetlenül vagy egy tároló helyről belinkelni. Egyszerű program, amelyhez nagy sávszélesség kellett. Lehetővé tette, hogy világszerte nagyszámú felhasználók az otthoni gépeiken tárolt tartalmakat egymás között megosszák. A DC-k üzemeltetői –kb.3-5 fő- üzemelteti és felügyeli a rendszert. Ez a technológia elavult.

[304] Btk. 385.§ .

A következő fejlődési fok a FTP-technológia, illetve a torrent oldalak. Ez a két technológia a büntető eljárásban is nehézséget okozhat. Nemcsak a nyomozó hatóságoknak, hanem az ügyészségnek, illetve a bíróságnak (büntetés kiszabások miatt) is megnehezítheti a munkáját, mivel a bizonyítékok összegyűjtése és azok értékelése sok esetben bonyolult.

Az FTP és a torrent technológia is igen népszerű és elterjedt a világon. Ezek képesek hatalmas károkat okozni a jogtulajdonosoknak, a szerzőknek és a forgalmazóknak is.

Megvizsgálva a technológiát, elmondhatjuk, hogy a legjobban az azokat üzemeltetők járnak, hiszen vagy emelt díjas SMS –szolgáltatással és regisztrációval lehet elérni az illegális tartalmakat vagy banki átutalással, internetes fizetéssel kapja meg a felhasználó a letöltéshez szükséges jelszót és felhasználónevet. Ezekről a honlapokról SPAM-ek útján vagy mostanában a népszerű közösségi oldalakon keresztül lehet értesülni, illetve meghívót kapni. Akármennyire tűnik hihetetlennek, de az FTP szerverek üzemeltetői több tízmilliós haszonra tesznek szert, még úgy is, hogy az emelt díjas SMS-szolgáltatók felé a szerződésben megállapodott százalékot kifizetik.

A torrent technológia lényege, hogy aki letölt, az fel is tölt egyben. A felhasználók a tracker szerveren egy torrent fájlt helyeznek el a torrent kliensbe, amelyet a felhasználók le tudnak tölteni. A rendszer automatikusan kis részletekben elkezdi letölteni a tartalmat azoktól a felhasználóktól, akik szintén megosztják vagy töltik le a fájlt. Ezek eleinte ingyenesen működtek, majd ezt fizetős rendszerré tették.

A torrent üzemeltetőjét nem lehet vagy nehéz „megfogni”, ezért sok esetben eddig gyakorlat alapján a feltöltőket és a szolgáltatókat derítették fel először, majd rajtuk keresztül próbáltak az elkövetőkhöz eljutni.

A szerzői jogok megsértésének bűncselekménye nehéz feladatok elé állítja a hatóságot, hiszen a technológia folyamatosan fejlődik és ezzel együtt, minden az interneten elkövethető bűncselekmények köre is szélesebbé válik.

E miatt fontossá vált nemcsak a jogalkotók részéről, hanem a jogalkalmazókéról is, hogy az eddig hatályos Büntető Törvénykönyv megreformálásra kerüljön.

A nyomozó hatóság részéről az eddig jelentkező nehézségeket:

- sokszor nem létező személyek, vagy nem létező cégek kötnek szerződést a szolgáltatókkal, vagy a bankszámlaszámok hajléktalan emberek nevén van
- az illegális tartalom nem feltétlenül a szerveren található, hanem egy proxy szerveren, éppen ezért egy házkutatás során nehezen található meg. Az IP cím, ami alapján esély lenne az elkövetők megtalálására, manipulálva van, így előfordulhat, hogy azok külföldre mutatnak vagy olyan személy számítógépére, aki egyáltalán nem érintett az ügyben.
- a kutatás amennyiben nem elég hatékony vagy gyors, előfordulhat, hogy az elkövetők az adatokat megpróbálják törölni vagy módosítani.
- a sértettek megállapítása, megkeresése, illetve a vagyoni hátrány megállapítása
- Ezek a felsorolások nem teljes körűek, hiszen az internet folyamatos fejlődése miatt ennél több akadályba is ütközhet a hatóság.

A bűncselekmény jogi tárgya a szerzői jogi védelem alá tartozó alkotásokhoz fűződő vagyoni jogviszonyok, azaz az irodalmi, a tudományos és a művészeti alkotások szerzőinek és a kapcsolódó jogi teljesítmények jogosultjainak önálló jogai[305]. Mivel továbbra is megmaradt ez a tényállás keretdiszpozíciónak, így azt az 1999. évi LXXVI. törvény a Szerzői jogról szóló törvény (továbbiakban Szjt) tölti ki tartalommal.

Eddig gyakorlat volt, hogy a letöltőket, amennyiben saját célra történt a letöltés, nem vonták felelősségre, épp azért, mert egyrészt sokszor azzal védekeztek, hogy nem volt tudomásuk arról, hogy az illegálisan feltöltött tartalomról van szó, másrészről magát a nyomozást is bonyolította és a határidőt indokolatlanul meghosszabbította.

A szerzői joggal kapcsolatos bűncselekmények közül említést érdemel a szoftverhamisítás. Ez egy „speciálisan" elkövetett szerzői jogi jogsértés, lévén, hogy a szoftverek esetében (kivéve a freeware) már a magáncélú letöltés is bűncselekménynek számít. Itt a most már hatályos Büntető Törvénykönyv szerint, amennyiben a szoftver értéke nem haladja meg a 100.000 forintot, úgy csak szabálysértés elkövetéséről beszélhetünk. Viszont az is tény, hogy akár egy szoftverrel is el lehet követni a deliktumot, amennyiben annak forgalmi értéke meghaladja a szabálysértési értékhatárt. Itt újabb probléma merül fel, mert a jogalkotónak - mint fentebb említettem- az a szándéka, hogy a …" *a büntetőjog, mint végső eszköz szempontjából indokolatlannak tűnik a nem jelentős mennyiségű szerzői mű vagy kapcsolódó jogi teljesítmény*

[305] Btk. 385.§ .

vonatkozásában megvalósuló, személyes célokat szolgáló felhasználások tömeges kriminalizálása. A szerzői jog területén fennálló nemzetközi kötelezettségeink, így különösen a …TRIPS egyezmény csupán a szándékos és a kereskedelmi mértékű „szerzői jogi kalózkodásra" nézve teszi kötelezővé a büntetőjogi szankciók előírását, a kereskedelmi mértéket el nem érő cselekmények esetén nincs olyan körülmény, amely ezen a területen a nemzetközi normáknál szigorúbb büntetőjogi szabályozást indokolná."[306]

Nyomozási nehézségek:

Az általános felderítési elv a szerzői jogokkal kapcsolatos bűncselekmények esetében is a „a kövesd a pénz útját". Ennél a bűncselekménynél könnyebbséget jelent a pénz útjának nyomon követésekor, hogy nem jellemző a kriptovalutákkal történő fizetés. A hatóságnak továbbá tudomással kell bírnia, hogy mely művek részesülnek védelembe, esnek oltalom alá és melyek nem.

A legnehezebb ugyanakkor sokszor a bűncselekmény társadalmi megítélése, hiszen a filmek, zenék stb. legális megszerzéséért fizetni kell, sokszor a zene-és filmkedvelők szerint irreálisan nagy összeget, míg egy-egy illegális oldalról azok töredékéért korlátlan mennyiségben lehet hozzájutni a legújabb művekhez. Így a feljelentés és bejelentés, egyúttal az állampolgári együttműködés csekély, míg a társadalom megítélése a jogvédő szervezetek által tett hatósági együttműködések miatt lesújtó.

A leplezett eszközök alkalmazásának lehetősége pedig- bár a büntetési tétel és az, hogy jellemzően szervezett bűncselekménynek minősíthető- az arányosság elve miatt, sokszor a kisebb súlyú jogsértések miatt megkérdőjelezhető[307].

[306] Btk. 385.§ .

[307] 2018. szeptemberben az EU elfogadta a szerzői jog reformját (linkadó), amelynek lényege, hogy minden információ átvételéhez licencszerződést kell kötni. Ezáltal a közösségi oldalakon felhasznált zene, kép stb. beleütközik a szerzői joghoz fűződő érdekekbe.

10.6 Információs rendszer felhasználásával (is) elkövethető bűncselekmények

Az eddig felsorolt kiberbűncselemények mellett szükséges az információtechnológia fejlődését kihasználó terroristák, illetve szélsőségesekről is szót ejteni.

Ahogyan Jonathan Barker: A terrorizmus című könyvében kifejtette, a terrorizmusnak három alapvető ismérve van:

1. az erőszak alkalmazása vagy az azzal való fenyegetés
2. a terrortámadások hátterében legyen megfogalmazott politikai cél
3. a terrorakciók során civilek személyi és vagyoni biztonsága kerüljön veszélybe.[308]

Ahogyan a bűncselekmények esetében megfigyelhető a változás az informatika fejlődésével, úgy a terrorizmussal kapcsolatban is elmondható, hogy -bár a támadásoknak sokszor ugyanazok a célpontjai maradtak (ilyenek például a létfontosságú rendszerelemek[309])- de a módszerek tekintetében már a kritikus információs infrastruktúra[310] ellen (is) irányulhatnak.

A Büntető Törvénykönyv alapján három tényállást vizsgáltuk meg:

A Btk. 323.§-a a közérdekű üzem működésének megzavarása, valamint a Btk.314-316§§., terrorcselekmény és az információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk.424.§).

10.6.1 Közérdekű üzem működésének megzavarása

Tényállás: *323. § (1) Aki közérdekű üzem működését jelentős mértékben megzavarja, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.*

[308] Jonathan Barker, *A terrorizmus* (Budapest: HVG Könyvek, 2003), 26.
[309] Létfontosságú rendszerelem (kritikus infrastruktúra): a 2012. évi CLXVI. törvény 1.§ f) pontja alapján a törvény 1-3. sz. mellékletében meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához- így különösen az egészségügyhöz, a lakosság személy-és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához- és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna
[310] Kritikus információs infrastruktúra az európai programról szóló Zöld könyv szerint: „Kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúrának minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak st.)

A közérdekű üzem fogalmát a Btk. záró rendelkezése tartalmazza. Ez alapján közérdekű üzem: a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek, hadianyagot, haditechnikai eszközt termelőüzem, energiát vagy üzemi felhasználásra szánt alapanyagot termelőüzem.

A közmű olyan termelő-vagy szolgáltató üzemek, amelyek a lakosság, továbbá az ipar, a mezőgazdaság, a szolgáltató tevékenység kiterjedt körét vízzel, elektromos, gáz-, gőz-, vagy hőenergiával látja el.[311] Továbbá a közösségi közlekedési üzem, amely a tömeges közlekedés lebonyolítására alkalmas, a használók széles köre által igénybe vehető közlekedési eszközök üzeme. A tényállást kell alkalmazni az elektronikus hírközlő hálózatokra is, továbbá az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemekre is.

A tényállás, nyitott törvényi tényállás, mert a jogalkotó nem határozza meg benne az elkövetési magatartást, így elkövethető szándékosan, tevéssel vagy éppen mulasztással is.

A deliktum a fent felsorolt közműhálózatba okozott bármilyen zavarral már bekövetkezett a az eredmény. A bűncselekmény elkövetője tettesként bárki lehet.

10.6.2 Terrorcselekmény

Tényállás*: 314. § (1) Aki abból a célból, hogy*

a) állami szervet, más államot vagy nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűrjön

b) a lakosságot megfélemlítse

c) más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetve nemzetközi szervezet működését megzavarja,

a (4) bekezdésben meghatározott személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekményt követ el,

[311] Kereszty Béla és mtsai., *A magyar büntetőjog –Különös része* (Budapest: Korona Kiadó, 2004), 457.

(2) Az (1) bekezdés szerint büntetendő, aki az a) pontban meghatározott célból

a) jelentős anyagi javakat kerít hatalmába, és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé, vagy

b) terrorista csoportot szervez.

(4) E § alkalmazásában személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekmény vízi közlekedés veszélyeztetése [233. § (1)-(2) bekezdés],

…….

c) a radioaktív anyaggal visszaélés [250. § (1)-(2) bekezdés],

d) a jármű hatalomba kerítése [320. § (1)-(2) bekezdés], a közveszély okozása [322. § (1)-(3) bekezdés], a közérdekű üzem működésének megzavarása [323. § (1)-(3) bekezdés], a robbanóanyaggal vagy robbantószerrel visszaélés [324. § (1)-(2) bekezdés], a lőfegyverrel vagy lőszerrel visszaélés [325. § (1)-(3) bekezdés],

e) a nemzetközi szerződés által tiltott fegyverrel visszaélés [326. § (1)-(5) bekezdés], a haditechnikai termékkel vagy szolgáltatással visszaélés [329. § (1)-(3) bekezdés], a kettős felhasználású termékkel visszaélés [330. § (1)-(2) bekezdés],

f) a rablás és a rongálás,

g) az információs rendszer vagy adat megsértése

315. § (1) Aki a 314. § (1) vagy (2) bekezdésében meghatározott bűntett elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja...[312]

Ahogyan Horváth Attila megemlíti, célszerű megkülönböztetni a terrortámadások és terrorfenyegetettségnek kitett terek jellemzői alapján:

- a rurális tereken végrehajtott terrortámadások
- a városi tereken végrehajtott terrortámadások

[312] 2012. évi C. törvény a Büntető Törvénykönyvről.

- a kibertérben elkövetett terrortámadások.[313]

A terrorcselekmény jogi tárgya az állami szervek, más államok, a nemzetközi szervezetek zavartalan, kényszertől mentes működéséhez, a lakosság megfélemlítéstől mentes életviteléhez fűződő társadalmi érdek.[314]

Az elkövetési magatartás a tényállás alapján a tűrésre kötelezés, megfélemlítés, alkotmányos rend megváltoztatása, nemzetközi szervezet működésének megzavarása, anyagi javak hatalomba kerítése és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé.[315]

A szakirodalom ennél a bűncselekménynél meghatároz egy cél- illetve eszközcselekményt is. Az eszközcselekménye a jelentős anyagi javak hatalomba kerítése, amely nem feltétlenül jelenti a jogellenes birtokbavételt és a rendelkezési jog gyakorlását. A kibertérből érkező fenyegetések[316]- értve ezalatt például a zsarolóvírus kritikus információs infrastruktúrához történő eljuttatását, ami kimeríti a terrorcselekmény fogalmát[317].

A Btk. már az előkészületet is bünteti, így már akkor önmagában csak azzal elköveti valaki a cselekményt, hogy akár egy adott kritikus infrastruktúra információs rendszerének sérülékenységét ismerve, arra célzottan elkészíti a programvírust, de ugyanúgy az is elköveti a jogellenes cselekményt, aki – bár nem tudva a sérülékenységekről- az általa megírt rosszindulatú programot megír, ami egy adott, létfontosságú rendszerelem működését veszélyezteti vagy, abban zavart okoz.

Nyomozati probléma:

Magyarországon a terrorcselekmény és a közérdekű üzem működésének megállapítása miatt folytatott eljárás elenyésző. A legnagyobb problémát jelenti, hogy önmagában ennek a

[313] Horváth Attila: Terrorfenyegetettség: célpontok, nagyvárosok közlekedés (N*emzetvédelmi Egyetemi Közlemények* 10., sz. 3. (2006)): 1–19.
[314] Béla Blaskó és mtsai., *Büntetőjog különös rész II.* (Budapest: Rejtjel Kiadó, 2015), 16.
[315] Btk. 314.§ (1) és (2).
[316] Ibtv 1.§ 16. pontja meghatározza, hogy mit is jelent a fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemi védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.
[317] A Nemzeti Közszolgálati Egyetem Rendészettudományi Kar hallgatói 2017-ben a BM RTT által kiírt pályázaton benyújtottak egy olyan tudományos munkát, amely a Budapesti Vízművek ellen elképzelt kibertámadást vezették le, és amely rámutat a kibertér illetve a létfontosságú rendszerelemek információs infrastruktúrájának sérülékenységére: http://www.bm-tt.hu/assets/letolt/folyoi/2018_1.pdf 103-149.oldal letöltve: 2018. július 21.

deliktumnak a nyomozása sokkal inkább másodlagos, mint a jogellenes cselekmény bekövetkezésének felismerése és a helyzet kezelése.

Az egyik legnagyobb kihívást jelenti, hogy azokkal a közérdekű üzemek és azon szervezetek, akik ellen terrorcselekmény követhető el, sokszor a magánszektor áll, amellyel a nyomozati szerveknek az együttműködése még csak kívánalom, de törvényben nincs meghatározva.

10.7 Konklúzió

A disszertációban nem kívántunk valamennyi számítógépes bűncselekménnyel kapcsolatos tényállást megemlíteni, csak azokat emeltük ki, amelyek a bizonyítás szempontjából figyelmet érdemelnek. A kutatás során is bebizonyosodott, hogy a jogalkalmazók számára nem a törvényi tényállások értelmezése jelenti a legfőbb problémát, hanem az azokat elkövetőkkel szemben a nyomozás és a felderítés jelent nehézséget, valamint a kényszerintézkedések végrehajtása vagy azok helyes megválasztása.

A célja ennek a fejezetnek sokkal inkább az arra való rámutatás, hogy bár eleget tett hazánk is a Számítástechnikai Bűnözésről szóló Egyezménynek, de annak 2001-ben aláírt szövegén túl nem sok esetben követte az újabb és újabb kihívásokat és továbbra sincs felkészülve a számítógépes bűncselekmények dinamikus fejlődésének, így kockáztatva azt, hogy esetleg az elkövetők cselekménye épp a törvényi tényállás hiánya vagy hiányossága miatt nem lesz büntethető.

A technikai fejlődés felgyorsította, részben elő is idézte azt a folyamatot, amelynek során egyre világosabbá vált: a hagyományos büntetőjog nem alkalmas az újfajta veszélyek megfelelő kezelésére[318].

[318] Korinek László: Tendenciák korunk bűnözésében és bűnüldözésében, 2014 (forrás: https://jura.ajk.pte.hu/JURA_2014_1.pdf, letöltve: 2019. február 04.) 134.

11 A KUTATÁSSAL ELÉRT EREDMÉNY BEMUTATÁSA

A felállított hipotézisek és a levont következtetések, javaslatok[319]:

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 jelenlegi szabályozás szerint:

***„3. §** (1) A nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt - sorozat-bűncselekmények esetén a bűncselekmények többségét - elkövették.*

(2) Ha az elkövető a bűncselekményt több nyomozó hatóság illetékességi területén követte el vagy több nyomozó hatóság illetékességi területén követett el bűncselekményeket, vagy az elkövetés helye nem állapítható meg, a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelyik az ügyben korábban intézkedett, intézkedés hiányában pedig az, amelynek a bűncselekmény saját észlelése vagy bejelentés, feljelentés alapján legkorábban a tudomására jutott.

(3) Ha az elkövető a bűncselekményt Magyarország határain kívül követte el, a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek - miniszteri rendeletben meghatározott - illetékességi területén az elkövetőt fogva tartják, ennek hiányában pedig, amelynek - miniszteri

[319] előfordulhat, hogy a 11. fejezetben leírt megállapítások már korábban is megfogalmazásra kerültek vagy teljes egészében vagy kisebb-nagyobb eltérésekkel ismétlem azokat

rendeletben meghatározott - illetékességi területén az elkövető utolsó ismert belföldi lakó- vagy tartózkodási helye van."[320]

1. Javaslat: a BM rendelet fent leírt szabálya azonban nem alkalmazható vagy legalábbis nem minden esetben alkalmazható. Így megfontolandó lenne annak rögzítése, hogy a kibertérben elkövetett bűncselekmények esetében eltérő szabályok bevezetése lenne indokolt, így:

- 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 *bűncselekmény elkövetés idejének* különös jelentősége van, hiszen főszabályként az ekkor hatályban lévő törvényt kell alkalmazni. A bűncselekmény elkövetési idejének meghatározása az egymozzanatú bűncselekményeknél nem okoz problémát, mert ez esetekben a törvényi tényállás elemei egyszerre valósulnak meg (például egy lövéssel megölt ember, aki a sérülésbe azonnal belehal). Kérdéses azonban az elkövetési idő olyan bűncselekmények törvényi tényállásánál, ahol a tényállási elemek nem egy időben valósulnak meg. A jogtudomány több elméletet dolgozott ki e problémák megoldására.

[320] 5/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről

- A *magatartás- (vagy tevékenység-) elmélet* szerint az elkövetési idő, amikor az elkövetési magatartás utolsó mozzanatát is kifejtik, azaz az adott tényálláshoz tartozó valamennyi magatartást megvalósították. Például lassú, több hónapon át tartó méregadagolással elkövetett emberölés esetén az utolsó adag méreg beadása lesz az elkövetési időpont.
- A *cselekményegység-elmélet* szerint a bűncselekmény elkövetésének ideje az, amikor az elkövető az adott tényálláshoz tartozó bármely magatartási elemet megvalósította. Az előző példánál maradva: ennek az elméletnek az alapján elkövetési időnek számít az első adag, de az utolsó adag beadása is.
- Az *okfolyamat-elmélet* szerint a bűncselekmény elkövetési ideje az, amikor az okfolyamat már önállóan, a tettes magatartásától függetlenül fejlődik. Az eddigi példát használva elkövetés időpontjának számít annak az adagnak a beadása, amellyel már a halálos eredményhez elegendő méreganyag gyűlik fel a sértett szervezetében.
- Az *eredményelmélet* alapján a bűncselekmény elkövetési ideje a törvényi tényállás megvalósulásához szükséges eredmény bekövetkezése, azaz a megmérgezett sértett halálának bekövetkezésének időpontja[321].

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 tudtuk.

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.

Ebben nyújt segítséget, hogy a számítógépes bűncselekmények és a kiberbűncselekmények fogalma között mégis különbséget tettünk, még akkor is, ha ezt a két fogalmat ma már egymás szinonimájaként használják a külföldi jogalkotók és kutatók.

[321] Dr. Háger Tamás: A büntetőtörvény időbeli hatályára vonatkozó rendelkezések, mint alapvető alkotmányos, garanciális szabályok (forrás: https://ujbtk.hu/dr-hager-tamas-a-buntetotorveny-idobeli-hatalyara-vonatkozo-rendelkezesek-mint-alapveto-alkotmanyos-garancialis-szabalyok/, letöltve: 2018. december 23.)

A számtógépes bűncselekmény és a számítógépes bűncselekmény között az alábbiak szerint teszünk 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

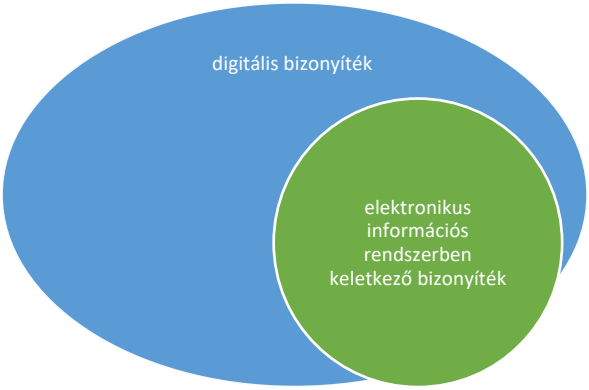
bizonyítási eljárásokat a hagyományos bűncselekményektől, úgy lenne értelme a „jó gyakorlat” kialakításának.

Javaslat: a digitális bizonyíték és 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.



2. 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.

Javaslat: Olyan keretjogszabály megalkotása, 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 vizsgáltuk 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...*[322]*"*

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 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.

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

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.

A szakértő kirendelésének szükségessége kérdésénél érdemes megemlíteni dr. Simon Béla rendőr őrnagy úrral és Kiss Tibor rendőr őrnagy úrral folytatott közös kérdőívünket[323], amely a rendőrség hivatásos állományának számítógépes bűncselekmények. Nyomozásának képzéséhez járul hozzá, és amelynek célja, hogy felmérjük a kérdőív készítésekor a Nemzeti Közszolgálati Egyetem Rendészettudományi Karának hallgatói és a Rendőrség hivatásos állományához tartozó állomány tekintetében a számítógépes bűnözéssel, a tudatossággal kapcsolatos ismereteit.

[323] A két említett kollégám hozzájárult, hogy a kérdőívet a disszertációban felhasználjam

12 A KUTATÁSSAL ELÉRNI KÍVÁNT CÉL

A kutatás során megvizsgáltuk a számítógépes bűncselekmények elleni fellépés hazai és nemzetközi szabályozását, a magyarországi és az uniós nyomozó hatóságokat, azok feladatait, továbbá egy-egy sarkalatos kérdést, mint a szakértő kirendelésének szükségessége a nyomozás során.

A következőben röviden ismertettük valamennyi fejezetet és azokat a problémákat, amelyek a számítógépes bűncselekmények nyomozása során az elkövetők kézre kerítésében nehézséget okoznak.

Az első fejezetben meghatároztuk a kutatás célját és aktualitását, az alkalmazott módszereket és eszközöket. Áttekintettük a legfontosabb jogszabályi hátterét mind a hazai, európai és nemzetközi jogi aktusokat. Nem a sokat emlegetett Számítástechnikai Bűnözésről szóló Egyezmény a jogi aktusok alapja, hanem az azt megelőző ENSZ Közlemények, ajánlások, bár vitathatatlanul a számítástechnikai rendszerrel kapcsolatos büntető anyagi jogi és büntetőeljárásjogi szabályozások 2001 után bekövetkezett változásai az Egyezménynek is köszönhetők.

A második fejezetben a számítógépes bűncselekmények azon jellemzőit emeltük ki, amelyek figyelembevételével a jogalkotást és a nyomozást folyamatosan nehezítik. Így felsoroltuk a számítógépes bűncselekmények ismérveit, megkíséreltük annak fogalmát meghatározni. Röviden áttekintettük a számítógépes bűncselekmények kriminalisztikai és kriminológiai jellemzőit.

A harmadik fejezetben bemutattuk azokat a szervezeteket, amelyek a számítógépes bűncselekmények elleni fellépés szervezeteit. Minden országban mintegy elvárásként fogalmazódott meg, hogy hozzanak létre olyan szervezeteket, amelyek tudása, technikai háttere megfelelően magas szinten van ahhoz, hogy a számítógépes bűnözőkkel szemben hatékony fellépést legyenek képesek produkálni. Bár az értekezés a számítógépes bűncselekményekkel foglalkozik, ennek ellenére nem lehet elmenni az olyan szervezetek mellett, akik a kibervédelemmel és kiberbiztonsággal foglalkoznak. Ezek a szervezetek Magyarországon a nemzetbiztonsági szinten, valamint 2018-tól a honvédelem területén találhatóak, valamint a katasztrófavédelem szervezete, amely a 2017-ben nagy médiafigyelmet kiváltó WannaCry és Petya zsarolóvírus támadásnál töltött be kiemelkedő szerepet, továbbá a kritikus infrastruktúra

rendszerelemeinek kijelölését végzi. A rendőrség és a NAV szervezetein kívül a Terrorelhárítási Központot emeltük ki, mint olyan szervezetet, amelynek a kibertérből érkező terrortámadások- így a kritikus információs infrastruktúrákat érő támadások és azok megelőzése és elhárítása tekintetében is végzik feladataikat.

A nemzetközi szervezetek felsorolása nem teljes és nem is törekedtünk rá, hiszen az értekezés terjedelme nem ad rá lehetőséget, valamint leginkább a hazai nyomozást végző szervezetek feladataival foglalkoztunk. Emellett ismertettük az Európai Unió és az azon kívüli, nemzetközi számítógépes bűncselekményekkel, a kibervédelemmel és kiberbiztonsággal foglalkozó szervezetek munkáját is.

Mind a hazai, mind a nemzetközi szervezetek „rövid" áttekintésekor megállapíthattuk, hogy azok a téves nézeteket, amelyek nem tartják a számítógépes bűncselekményeket veszélyesnek és igazi fenyegetésnek, az erre irányuló kutatások pedig feleslegesek, több oldalról is meg lehet cáfolni. Mind a Symantec 2018-as jelentése, mind a Cyber-Telecom Crime 2019-es jelentése a kibertámadások és számítógépes bűncselekmények 2018-as évre vonatkozó adatai szerint a malware és ransomware jellegű támadások, az interneten keresztül megvalósuló csalások számában nem tapasztalható csökkenés, ezen felül újabb és újabb támadások és deliktumok valósulnak meg.

A negyedik fejezetben a számítógépes bűncselekmények alanyai- így a hazai speciális nyomozó hatóságok, az elkövetők. A büntetőeljárások során vizsgálják a hatóságok az elkövetés helyét, mind pedig az idejét, amivel kapcsolatban a felmerülő problémákat- így a hatáskör, illetékesség dilemmáját tekintettük át és fogalmaztunk meg javaslatokat.

Az értekezés megírásának kezdetekor és befejezésekor épp a számunkra egyik legfontosabb jogszabály és az azzal összefüggő törvények, rendeletek 2018. július 1-től megváltoztak. Az, hogy ez a változás számomra megnehezítette-e a kutatás befejezését vagy pedig könnyítette, nem tudok válaszolni. Tény, hogy akkora változás következett be az eljárási törvényben, amelyek miatt sok fejezetet, alfejezetet szükséges volt átírni. Tapasztalat az új eljárás hatékonyságában az eddig eltelt idő rövidsége miatt még nincs, nem is lehet. Sok esetben csak az új törvény szövegében bekövetkezett változásra és a 2017. évi XC. törvény Miniszteri Indokolására tudtunk hagyatkozni.

Szem előtt tartottuk mindenekelőtt, hogy *a büntetőjogi felelősség vizsgálata azokon a bizonyítékokon alapul, melyet a nyomozó hatóság az eljárási szabályok megtartásával*

összegyűjt. Tudjuk, hogy a bizonyítási eljárás egy formalizált eljárás, melynek szereplői minden lépésükkel a jog, az állam és a társadalom érdekeit szem előtt tartva funkcionálnak. Tehát, mindezekből következően a bizonyítási eszközök megszerzésére és bizonyítékok értékelésére vonatkozó szabályanyag kiemelt jelentőségű, lényegében az igazságszolgáltatási funkció alkotmányos sine qua nonja.[324]

Először szükséges volt a digitális bizonyíték vagy elektronikus bizonyíték fogalmával foglalkozni. Ugyanakkor az, hogy erre egy teljes felsorolást lehetne adni, a lehetetlenséggel érne fel. A digitális környezetünk olyan mértékű változásokon megy keresztül, ami miatt elegendő egy keretet megadni. A változékony fogalom miatt azonban érezhető, hogy úgy Magyarországon, mint egyes uniós tagállamokban, a nyomozó hatóság és ügyészség szoros kapcsolatára, a bizonyítékok feletti közös értékelésére van szükség. Ezt a hiányosságot az Európai Unió is érzékelte, hiszen 2016 óta folyamatosan törekszik arra, hogy egységesítse az elektronikus bizonyítékok összegyűjtésével és értékelésével kapcsolatos szabályokat, egy közös értékelést sikerüljön úgy kialakítani, hogy a nemzetközi szinten se okozzon gondot azok beszerzése. Ugyanakkor az Unió is elismerte, hogy legnagyobb problémát a harmadik országok felé történő elismerés és az adatkérések gyors teljesítésének kikényszerítése jelenti.

Álláspontunk szerint ezen felül problémát jelent az is, hogy a hazai eljárási törvény az elektronikus bizonyítékok tekintetében érezhető, hogy kézzel fogható tárgyként kezeli és nem veszi sokszor figyelembe a technikai jellemzőit.

A 2017. évi XC. törvény, a büntetőeljárási törvényben nem tesznek különbséget a kényszerintézkedés során a fizikai térben található evidenciák és a virtuális térből beszerezhető bizonyítékok között. Ezek tisztázása is szükséges lenne, hiszen mind a két „helyszín" más és más cselekményt tenne szükségessé a kényszerintézkedések végrehajtása tekintetében.

Az elektronikus bizonyítékokkal kapcsolatos külföldi szabályozással kapcsolatban indokoltnak tartottam külön fejezetben foglalkozni, hiszen nemcsak egyszerűen az e-evidenciák fogalmával foglalkoztam, hanem egyes országok (így Hollandia, Írország, Spanyolország vonatkozásában) a rendőrség és az ügyészség feladataival és ez előbbi tagozódásával, szervezeteivel.

A szakértő szerepével (7. fejezet) mindenképpen szerettünk volna foglalkozni, azt vizsgálni. Nem akartunk abban állást foglalni, hogy van-e értelme, szükséges-e a szakértő, mint külső

[324] Kovács Gábor: Az Európai Forenzikus Tudományos Térség (EFSA-2020) megalkotásának koncepciója(forrás: https://dfk-online.sze.hu/images/JÁP/2017/1/kovács.pdf, letöltve: 2019. február 15.) 84-85.

személy igénybevétele az eljárásokban, kényszerintézkedések során, hanem arra kerestük a választ, hogy hogyan lehetne arra megoldást keresni, hogy a hatóság tényleg csak a legszükségesebb esetben rendelje ki, és ténylegesen csak a különleges szaktudást igénylő kérdésben. A kutatás során többször is arra a megállapításra jutottunk, hogy szakértő kirendelésére nem mindig a szükség miatt került sor, hanem az ügyben eljáró hatóság kényelme vagy a saját hibából eredő bizonyítékvesztés elkerülése miatt.

Külön fejezetben (8. fejezet) foglalkoztunk a kényszerintézkedésekkel, valamint a szemlével, mint nyomozati cselekménnyel. A (ház)kutatás, mint kényszerintézkedés helyét átvette a kutatás, ami szabályozásában előrelépés érezhető az 1998. évi XIX. törvénnyel szemben. A hatályos büntető eljárásjogi törvénnyel összhangban a Kormány a 100/2018. (VI.8) Korm. rendelettel a nyomozás és az előkészítő eljárás részletes szabályairól, összhangban az Alaptörvény 15. cikkével a kutatással kapcsolatban megállapított részletszabályokban ugyanakkor kiemeli, hogy az információs rendszer átvizsgálása során biztosítani kell az adatok megismerését, de a védelmi eszköz vagy informatikai megoldásának megkerülése vagy kijátszása nélkül. Ezt a kritériumot sokkal inkább elméleti, mint gyakorlati szakemberek találták ki, hiszen a legális forrásból letölthető jelszófeltörő vagy titkosítást feloldó szoftverek használata akár a helyszínen, akár a nyomozó hatóság irodájában egyes esetben megkönnyítené a bizonyítékok megszerzését, megrövidíthetné az eljárások idejét.

A lefoglalással szabályozással kapcsolatban ugyanazt lehet érezni, mint a kutatásnál. A virtuális bizonyítékok használhatósága tekintetében, a bíróság előtt történő felhasználás végett a jogalkotó el sem tudja képzelni, hogy ne kézzel fogható módon legyen a bizonyíték (elektronikus adat kimentése adathordozóra, annak írásvédetté tétele stb.), amely lehetőséget ad a nyomozó hatóság számára a legkisebb hiba következtében ne lehessen értékelni a bizonyítékot vagy hitelességéhez ne férjen kétség.

A kényszerintézkedések között, mintegy kitekintésként, foglalkoztunk a bitcoinnal, mint virtuális fizetőeszközzel, a hatóság kihívásaival.

A többi kényszerintézkedés tárgyalását követően az ENISA által kiadott gyakorlati útmutatót ismertettem, mint egy 2011-ben megalkotott ajánlást, azért, hogy az előtte részletezett új eljárási szabályok tekintetében szembe tűnjön az, hogy további változásra van szüksége a 2017. évi XC. törvénynek ahhoz, hogy hatékonyabb legyen a hatóság fellépése.

A leplezett eszközök ismertetése, -mint *speciális lehetőség a számítógépes bűncselekményeknél* -nélkülözhetetlen a számítógépes bűncselekmények felderítéséhez. Megemlítettem még az előkészítő eljárást, mint egy új szabályozást a Be.-be, amely az egyszerű gyanú megállapítására vagy elvetésére alkalmas bizonyítást, eljárást tesz lehetővé a nyomozó hatóságnak. Ez az egyik olyan új szabályozásunk, ami lehetővé teheti, hogy a hatóságok saját, monitorozó tevékenységük körébe bizonyítékokat gyűjtsön egy-egy kibertámadás előkészülete, internetes zaklatás, csalás tekintetében.

A legutolsó fejezetben az egyes számítógépes bűncselekmény típusok- kivéve a gyermekpornográfia tényállását- problémás kérdéseit feszegetem, valamint azokat a sarkalatos kérdéseket, amelyek újításra szorulnának. A felsorolás nem terjedt ki az összes kibertérben elkövethető deliktumra, csak egyes kiemelt tényállásokat vizsgáltuk meg.

A számítógépes bűnözők az egyik legnagyobb kárt okozó elkövetők, akik sokszor nemcsak a névteleség mögé bújva maradnak ismeretlenek a hatóságok előtt, hanem a jogszabályok rugalmatlansága miatt nem vonhatók felelősségre. Egyik ilyen emlékezet ügy volt az Elender-ügy, amelyben egyik volt kollégám nyomozott. Ő volt a mentorom, amikor 2009-ben a Budapesti Rendőr-főkapitányság Gazdaságvédelmi Főosztály Felderítő Alosztályon a számítógépes bűncselekményekkel elkezdtem foglalkozni és a tapasztalatait megosztva velem kezdett érdekelni ez a típusú bűncselekmény. Az Elender-ügyben elkövetett cselekmény, illetve az elkövetők a jogszabályok hiányosságai miatt, akkor nem voltak felelősségre vonhatók. Ennek kiküszöbölése lehetett volna akkor, ha az akkori Btk. bűncselekményként értékeli a honlap feltörését és a felhasználók jelszavainak megszerzését, de abban az időben még nem tartalmazta a büntetőtörvénykönyvünk ezt a tényállást.

Valamennyi fejezet esetében elmaradt az Európai Unió több dokumentumában is emlegetett magánszektor és államiszektor együttműködése a számítógépes bűnözés, a kibervédelem és a kiberbiztonság területén, aminek vizsgálata álláspontunk szerint új irányt vehetne a kibertérből származó bűncselekmények megakadályozása területén, de ennek a lehetősége jelenleg még mindig sötét folt a hazai büntetőeljárásban.

A disszertációban Dr. habil. Boda József, a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar volt dékánjának gondolatait idézve- aki dékánként sürgette az ezzel kapcsolatos képzés kiépítését- „már a 24. órába léptünk a számítógépes bűncselekményekkel kapcsolatos képzés tekintetében”. Nemcsak egy-egy nyomozó professzionális szintű tudását

kellene erősíteni, hanem valamennyi leendő rendőrtiszt és már hivatásos állományú rendőr, természetesen tiszthelyettesek ismeretét, szakértelmét fejleszteni, oktatni folyamatos képzéssel, ismerettel. Úgy a bűnügyes állomány tekintetében, mint a közterületen, közlekedésrendészet területén, mint a határvédelmi feladatokat ellátó állomány esetében is szükséges lenne.

.

13 ÖSSZEGZÉS

„*Egyre inkább függünk az internethez kapcsolt számítógép-rendszerektől; ezeken kommunikálunk, bankolunk, fizetjük az adóinkat, foglaljuk le utazásainkat, és rajtuk keresztül vásárolunk. Eközben fel sem merül bennünk, hogy ezek a rendszerek esetleg nem lesznek elérhetőek, és talán nem is mindig biztonságosak, nem mindig óvják meg személyes adatainkat. Az internet és az internetre épülő technológiák erőssége az, hogy általuk rengeteg dologhoz kapcsolódunk. Ám ez az erősség gyakran fogyatékosság is: mindig és mindenhonnan ki vannak téve támadásoknak. Ráadásul az internetes rendszereket olcsón meg lehet támadni. Az internet segít abban is, hogy névtelenek maradjunk.”*[325]

A fenti idézet és Mark Russinovich Nulladik nap című könyve tökéletesen bemutatja azokat a kihívásokat, amelyekkel az internet felhasználók minden egyes nap látatlanul találkoznak és amellyel a számítógépes bűnözés elleni harccal foglalkozó szervezetek minden nap szembesülnek.

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

[325] Mark E. Russinovich, *Zero day*, First edition (New York: Thomas Dunne Books, 2011).

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 [...][326]

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 cybercriminals

[326] Russinovich.

14 IRODALOMJEGYZÉK

14.1 Felhasznált jogszabályok jegyzéke:

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/.

14.2 Felhasznált magyar nyelvű irodalom jegyzéke:

1. Anti Csaba-Dr. Barta Endre-Dr. Bócz Endre-Dr. Lakatos János-Dr. Romasz Árpád: Krimináltaktika 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.

14.3 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)

14.4 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.

14.5 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))

15 MELLÉKLETEK

Az Evasys kérdőív, amelynek kérdéseit dr. Simon Bélával rendőr őrnagy úrral és Kiss Tibor rendőr őrnagy úrral készítettünk el:

Kibervédelmi attitűdfelmérés ()
Válaszadók száma = 152

Felmérés eredmények

1. Demográfia: Az alábbiakban az Ön képzettségére és beosztására vonatkozó kérdést teszünk fel.

1.4) **Neme?** n=150

Nő	36%
Férfi	64%

1.6) **Mi az Ön befejezett iskolai végzettsége? (Kérem, a legmagasabbat jelölje!)** n=152

szakközépiskola/technikum	9.9%
gimnázium	5.3%
érettségire épülő szakképzés	11.2%
felsőfokú szakképzés	4.6%
főiskola (BA/BSC)	55.9%
egyetem, felsőfokú mesterképzés (MA/MSc/LLM), osztatlan képzés	13.2%
doktori iskola (PhD)	0%

1.7) **Ön irányítói/vezetői beosztásban dolgozik? (kérem válasszon!)** n=151

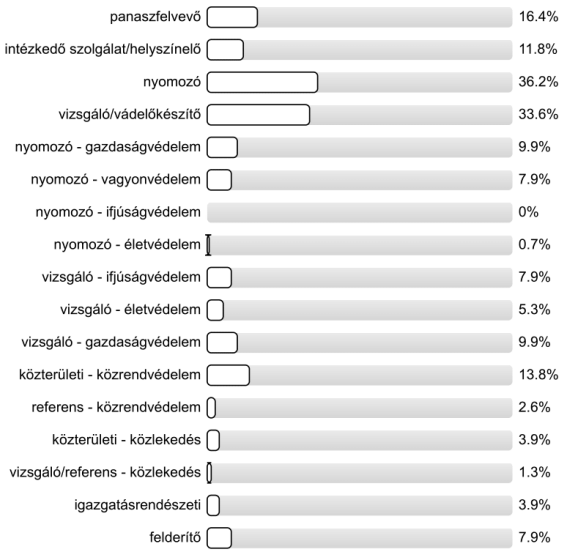
nem	86.1%
csoportvezető	6.6%
csoportvezető helyettes	0.7%
alosztályvezető	2.6%
alosztályvezető helyettese	2.6%
osztályvezető	0.7%
osztályvezető helyettese	0.7%
kapitányságvezető	0%
kapitányságvezető helyettese	0%

1.9) **Melyik szolgálati ágban dolgozik a rendőrségen?(Kérem, írja ki betűkkel (pl.: bűnügy)** n=152

közlekedés	2.6%
közrend	17.1%
bűnügy	75.7%
igazgatásrendészet	2.6%
hivatal	0.7%
közalkalmazott/köztisztviselő	0.7%
körzeti megbízott	0.7%

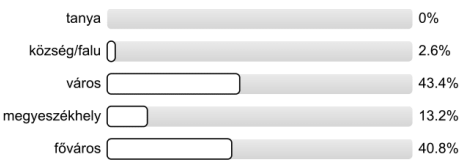
1.10) **Milyen szolgálati feladatot lát el szolgálata alatt? (Többet is jelölhet!)**

n=152



1.12) **Jelenlegi munkahelyének mi a településtípusa?**

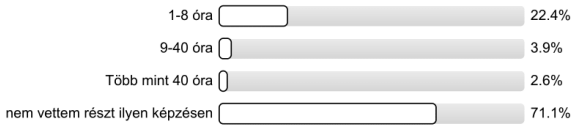
n=152



2. Képzettség: Ebben a kérdéscsoportban a kiberbűnözéssel kapcsolatos ismereteire és rendőri képzettségére vonatkozó kérdéseket sorolunk fel.

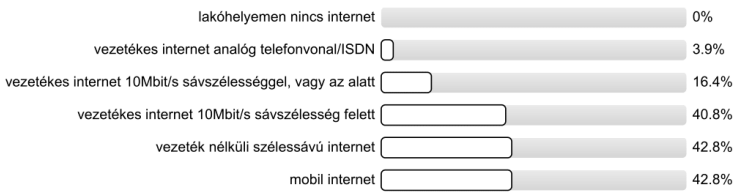
2.1) **Vett már részt kiber-bűncselekmények nyomozásával, kezelésével kapcsolatos képzésben?**

n=152



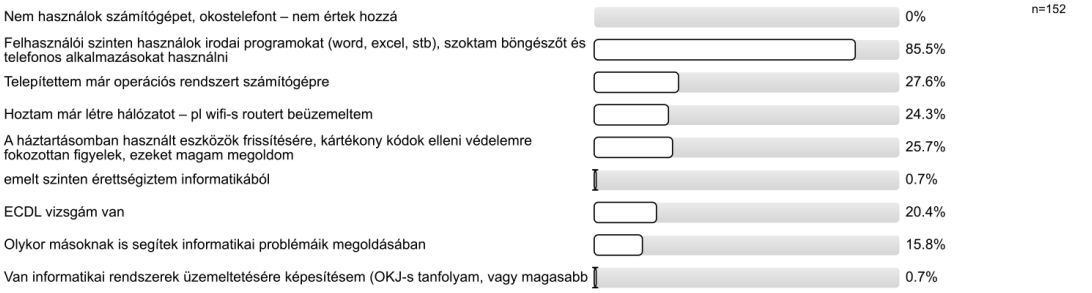
2.2) **A háztartásában milyen internet hozzáférés áll rendelkezésre?(több válasz is lehetséges)**

n=152



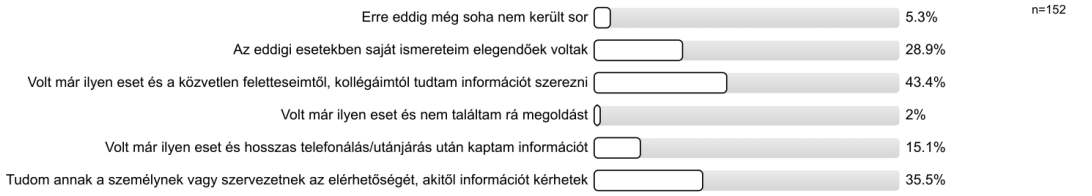
2.3) **Milyen szinten ért az informatikához? (több válasz is lehetséges)**

n=152



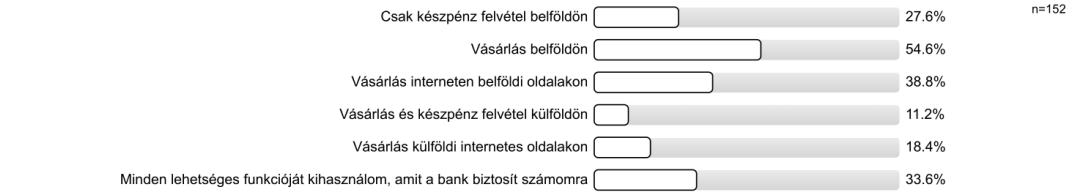
2.4) **Ha szolgálati feladati ellátása során informatikával kapcsolatos kérdés merül fel, akkor tud segítséget kérni? (több válasz is lehetséges)**

n=152



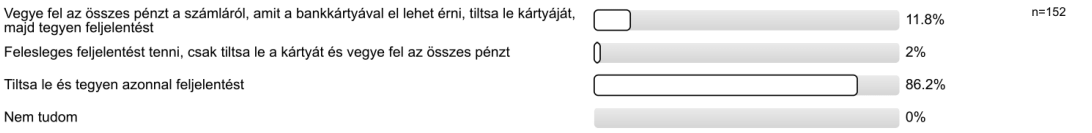
2.5) **Bankkártyáját mire használja?(több válasz is lehetséges)**

n=152



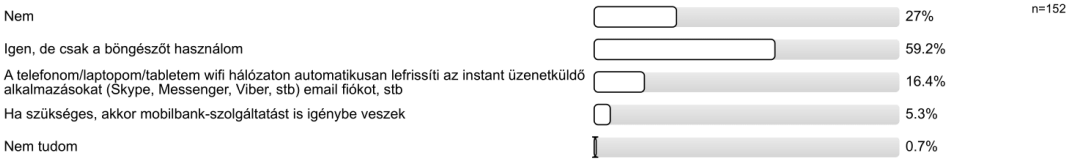
2.6) **Ha Önhöz állampolgári jelzés érkezik, hogy az érintett személy értesítést kapott SMS-ben, hogy a bankkártyájával illetéktelenek éppen vásároltak, akkor Ön mit javasol számára?(több válasz is lehetséges)**

n=152



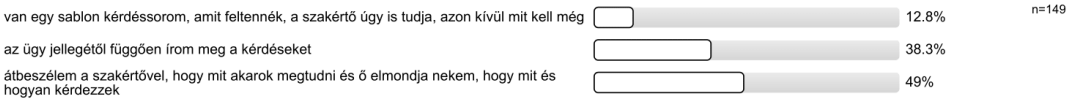
2.8) **Szokott-e nyilvános wi-fi hálózatokhoz kapcsolódni? (étteremben, vonaton, áruházban, közterületen, ha igen, akkor milyen műveleteket hajt végre?)(több válasz is lehetséges)**

n=152



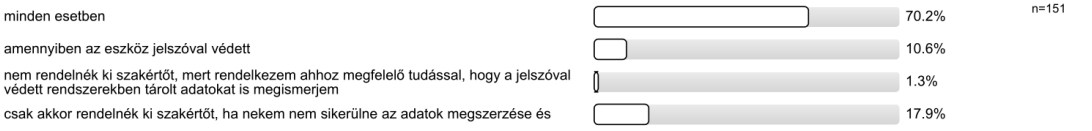
2.9) **Amennyiben szakértő kirendelésére van szükség a kibernyomozás területén, Ön tudja-e, hogy a kirendelő határozatban milyen alapvető kérdéseket kell feltenni?**

n=149



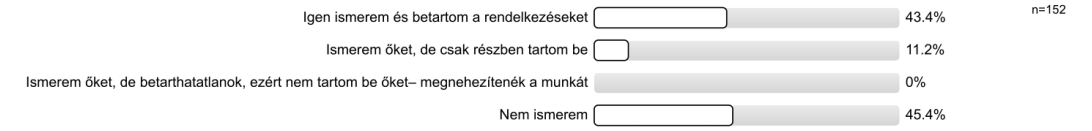
2.10) **Amennyiben a nyomozás során bármilyen informatikai eszköz kerül lefoglalásra (okos telefon, táblagép, laptop, PC.) milyen esetben rendelne ki az eszköz által tárolt adatok tartalmának megismerésére szakértőt?**

n=151



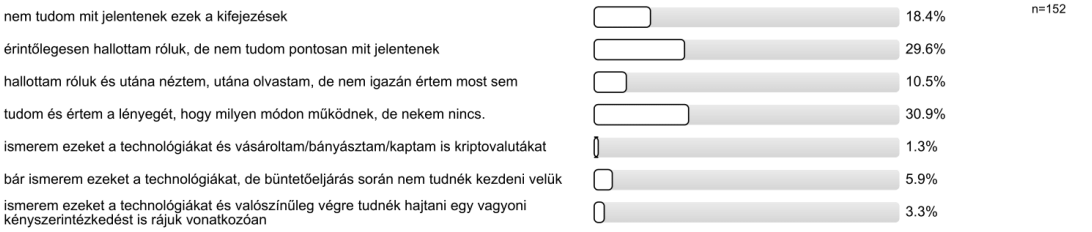
2.11) **A 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatáról és a 45/2013. (XI. 15.) ORFK utasítás az intranethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer rendőrségi igénybevételének szabályairól szóló jogszabályokat ismeri és betartja?**

n=152



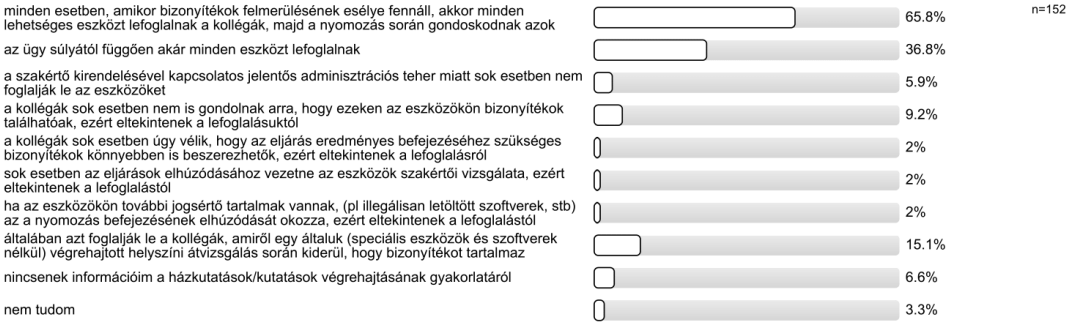
2.14) **Van ismerete a kriptovalutákról (Bitcoin, Ethereum, stb), blokklánc technológiáról? (kérem válasszon!)**

n=152



2.15) **Egy olyan bűncselekménnyel kapcsolatos nyomozás során, amikor házkutatás/kutatás végrehajtásakor különféle infokommunikációs eszközökön (számítógép, laptop, tablet, pendrive, mobil merevlemez, memória kártya, okostelefon, hálózati meghajtó, stb) vélhetően vannak a bűncselekménnyel kapcsolatos bizonyítékok, akkor a jelenlegi gyakorlat szerint a kollégák milyen módon hajtják végre az eljárási cselekményt? (több válasz is jelölhető) (ha be lehet állítani, akkor max 4 választ jelöljön be)**

n=152



2.16) **Ha a tulajdonában álló informatikai eszközöket (személyi számítógép/laptop/okostelefon) ransomware (zsarolóvírus) támadás éri, akkor mit tesz? (több válasz is lehet)**

n=152

Tudom mi az a ransomware, de azt nem tudom, hogy mit tennék	15.1%
Ha értékes adatokat veszítenék el emiatt, akkor lehet, hogy fizetnék azok visszaszerzéséért	3.3%
Semmiképpen nem fizetnék, ismerőseimtől próbálnék tanácsot kérni	19.7%
Felkészültem egy ilyen támadásra és az értékes adataim, képeim, egyéb adataim archiválásáról gondoskodtam	32.9%
Semmiképp sem fizetnék, mert nem akarok bűnelkövetőket támogatni	46.1%

2.17) **Gyakorlata során vett részt olyan rendőri intézkedésben, eljárási cselekményben, amikor nem tudta, hogy mi a digitális adathordozó eszközök, infokommunikációs eszközök lefoglalásának, kezelésének helyes módja? (Kérem jelöljön egy választ!)**

n=150

igen, és jelenleg is bizonytalan lennék egy ilyen intézkedés során	11.3%
Igen, de már utánanéztem az ismereteknek	18.7%
nem	70%

2.18) **Szeretne-e részt venni kiberbűnözés elleni fellépéshez kapcsolódó képzésben? (több választ is jelölhet!)**

n=152

igen, ezt fontosnak tartanám	39.5%
igen, mert szeretem bővíteni az ismereteimet	47.4%
igen, mert szeretek képzéseken részt venni	6.6%
nem, mert nem használnám a megszerzett ismereteket	7.2%
nem, mert sok időt venne el	3.3%
nem, mert én ezekkel a kérdésekkel nem akarok foglalkozni	10.5%
nem, mert azt én úgysem érteném meg	3.9%

2.20) **Milyen időtartamban és helyszínen venne részt ilyen képzésben? (kérem, válasszon egyet!)**

n=150

nem vennék részt	22%
igen, 1-3 napos képzésen a szolgálati helyemen	29.3%
igen, több alkalommal néhány órás képzésen a szolgálati helyemen	11.3%
igen, 1-3 napos képzésen is szolgálati helyemtől távol is	18.7%
igen, akár több hetes kurzuson is a szolgálati helyemtől távol	14%
igen, - véleményem szerint e-learning képzéssel ez javarészt elsajátítható volna	4.7%

2.21) **Milyen témákban szeretné ismereteit bővíteni? (több válasz is lehetséges)**

n=152

nem szeretném ismereteimet bővíteni	9.2%
már az informatikai alapoktól szükséges volna oktatás	20.4%
információbiztonsági tudatosságot javító oktatás	33.6%
speciális informatikai ismeretek eszközökről, hálózatokról	32.2%
digitális nyomok rögzítése, biztosítása, kezelése – kriminál technikai szempont	50.7%
kiberbűncselekményekkel kapcsolatos oksági mechanizmusok – kriminológiai szempont	31.6%
kiberbűncselekmények nyomozásának taktikai, metodikai ajánlásai	48.7%
a kibertérhez kapcsolódó cselekmények büntetőjogi megítélése	25.7%
kriptovaluták és a velük kapcsolatos bűnüldözési ismeretek	39.5%
kiberbűncselekményekkel kapcsolatos bűnmegelőzési ajánlások, lehetőségek	28.9%
készpénz helyettesítő fizetési eszközökkel való online és offline visszaélések	47.4%
kibertérhez kapcsolódó vagyon elleni, csalás jellegű bűncselekmények (aukciós csalások, hirdetési csalások, stb) nyomozásával kapcsolatos ajánlások	38.8%
gyermekpornográfiával kapcsolatos nyomozások gyakorlati tapasztalatai	40.8%

Hozzászólások jelentése

1. Demográfia: Az alábbiakban az Ön képzettségére és beosztására vonatkozó kérdést teszünk fel.

1.1) **Kérdező neve.**

- Balogh Regina
- Benczés Kornél
- Berke Bernadett (3 előfordulás)
- Biber Zita (3 előfordulás)
- Boros Anita (4 előfordulás)
- Bérczes Kornél (2 előfordulás)
- Czibere Tamás
- Deak Bence
- Deák Bence (2 előfordulás)
- Dolhai Katalin (4 előfordulás)
- Dr. Kiss Noémi
- Duschák Sarolta
- Dékáni Sára
- Dékány Sára (2 előfordulás)
- Elischer Márk (3 előfordulás)
- Farkas József
- Fecskovics Norbert (2 előfordulás)
- Forgó Gergely (2 előfordulás)
- Fülöp Eszter (2 előfordulás)
- Gorjanácz Brenda
- Gróf Klaudia
- Gróf Klaudia Emese (2 előfordulás)
- Gyöngy- Papp Henrietta
- Gyöngy-Papp Henrietta (3 előfordulás)
- Hajas Alaxendra
- Hajas Alexandra (2 előfordulás)
- Hágel Bence (6 előfordulás)
- Ihász Vivien (3 előfordulás)
- Jobbágy Edit (3 előfordulás)
- Jobbágy Edit
- Jónás Dávid (2 előfordulás)
- Jónás Dávid
- Kiss Krisztián (3 előfordulás)
- Kiss Sándor (4 előfordulás)
- Kovács Balázs (3 előfordulás)

- Kovács Dominika (5 előfordulás)
- Kovács Kristóf (2 előfordulás)
- Kovács László (2 előfordulás)
- Kovács László
- Kudlák Judit (3 előfordulás)
- Kóczán László (3 előfordulás)
- Ladányi Laura
- Ladányi Laura Zsuzsanna
- Lechner Krisztián (3 előfordulás)
- Lőrincz Edit Klára
- Moldicz Máté
- Moldicz máté
- Moldova Máté
- Molnár Péter (3 előfordulás)
- Márton Mercédesz (3 előfordulás)
- Nagy Ivett (4 előfordulás)
- Németh Bálint (3 előfordulás)
- Németh Dàvid
- Németh Dávid (2 előfordulás)
- Peti Bálint Kristóf (2 előfordulás)
- Petz Dávid (3 előfordulás)
- Preininger Lilla (2 előfordulás)
- Preininger Lilla
- Rigó Zsuzsanna (2 előfordulás)
- Rigó Zsuzsanna Rita
- Ruzsa Nóra (3 előfordulás)
- Scheriner András
- Schreiner András
- Schreiner András
- Sebők Regina
- Szalai Bálint (3 előfordulás)
- Szokoli Bence (4 előfordulás)
- Szondi Zoltán
- Tuska Natália (3 előfordulás)
- Tóth Szófia (2 előfordulás)
- Tóth Szófia
- Urbán Ivett
- Vizi Viktoria (3 előfordulás)

[1.2)] **Kérdező szakaszszáma.**

- 1. szakasz (2 előfordulás)
- 2.
- 2.
- 2. szakasz (2 előfordulás)
- 3.
- 3/1 (3 előfordulás)
- 3/2
- 3/3
- 3/6
- 3/6.
- 4. (4 előfordulás)
- 4. Szakasz
- 4. szakasz
- III / 2
- III./1. (2 előfordulás)
- III./2.
- III./4. (3 előfordulás)
- III./6. (2 előfordulás)
- III/1 (11 előfordulás)
- III/1
- III/1. (28 előfordulás)
- III/2 (12 előfordulás)
- III/2. (7 előfordulás)
- III/3 (9 előfordulás)
- III/3. (14 előfordulás)
- III/4 (7 előfordulás)
- III/4. (5 előfordulás)
- III/4.
- III/6 (5 előfordulás)
- III/6. (9 előfordulás)
- III/6.
- lll/2.
- 1 (3 előfordulás)
- 2
- 3 (2 előfordulás)
- 4 (2 előfordulás)
- 6 (2 előfordulás)

[1.3)] **Kérdező NEPTUN kódja.**

- A1J6IV (2 előfordulás)
- A6APHT
- A9KK5V (3 előfordulás)
- AC1ZZS
- AHKTB4
- B04EJB (3 előfordulás)
- BCLGYT
- BGK6BQ (3 előfordulás)
- Bclgyt
- C2LGQG (4 előfordulás)
- CRHZUM
- CTRFZY (2 előfordulás)
- CXDQ9Z (3 előfordulás)
- CY7XME (3 előfordulás)
- Cxdq9z
- D7D446 (4 előfordulás)
- DS4JD5 (2 előfordulás)
- EKO4PN (2 előfordulás)
- EKO4pn
- ETRQ2L (4 előfordulás)
- FGY0RR
- FJLS9g
- FSBAZL (3 előfordulás)
- G3NPQ9 (3 előfordulás)
- GBSW1Q (3 előfordulás)
- Gmdjsa
- H073Z1
- H4I2YX (3 előfordulás)
- HO73Z1
- Ho73z1
- I6QUELE
- IY4PGP (3 előfordulás)
- LOYXSK (3 előfordulás)
- MLV6AY (3 előfordulás)
- MLV9AY
- MM3YVQ (3 előfordulás)
- MU2FAG (3 előfordulás)
- MYEXMD (3 előfordulás)

- Mwrqap
- N1GTLT
- N4XYF4 (3 előfordulás)
- NF2BUP (3 előfordulás)
- NTG3CR (2 előfordulás)
- OAFMR5
- PBNY5X (3 előfordulás)
- Q42ZX6 (3 előfordulás)
- Q42zx6
- SX3BY0
- U16QQE (3 előfordulás)
- UUYSC3 (3 előfordulás)
- UY69KF (3 előfordulás)
- WFRYKJ (3 előfordulás)
- X09I7N (6 előfordulás)
- X9061C (2 előfordulás)
- X9061c
- YOC224 (2 előfordulás)
- ZEZW1N (3 előfordulás)
- a6apht (2 előfordulás)
- gmdjsa (4 előfordulás)
- i6qele (2 előfordulás)
- kge18d
- kk4lok (3 előfordulás)
- mwrqap (2 előfordulás)
- oafmr5
- rsriyt (3 előfordulás)
- sx3by0 (2 előfordulás)
- wrkmuz (4 előfordulás)

1.5) **Mióta dolgozik a rendőrségen?(Kérem, írja évek számában a választ, pl.: 22!)**

- -
- 1 (28 előfordulás)
- 2
- 2 (22 előfordulás)
- 3
- 3 (12 előfordulás)
- 4 (8 előfordulás)
- 4
- 5 (7 előfordulás)
- 6 (8 előfordulás)
- 7 (9 előfordulás)
- 8 (4 előfordulás)
- 9
- 9h
- 10 (13 előfordulás)
- 12 (3 előfordulás)
- 13 (5 előfordulás)
- 14
- 15 (3 előfordulás)
- 17 (3 előfordulás)
- 18 (5 előfordulás)
- 20 (4 előfordulás)
- 21 (3 előfordulás)
- 22 (2 előfordulás)
- 25
- 26
- 32
- 40

1.8) **Egyéb beosztásban (csak ha az előző kérdés válaszai közt nem szerepel):**

- Előadó (3 előfordulás)
- Főnyomozó (5 előfordulás)
- Jaror
- Járőr (3 előfordulás)
- Járőr
- Járőrvezető
- Kmb
- Körzeti megbízott
- Nyomozo tiszt
- Nyomozó (4 előfordulás)
- Nyomozótiszt
- Panaszfelvevő
- Segédelőadó
- Szolgalairanyito
- Szolglatiranyito pk
- Szolgálatirányító-pk
- Szolgálatparancsnok
- VIZSGÁLÓ
- Vizsgalo tiszt
- Vizsgaló
- Vizsgáló (7 előfordulás)
- Vizsgálótiszt (2 előfordulás)
- bűnügyi nyomozó
- bűnügyi vizsgáló
- elóadó
- előadó (3 előfordulás)
- fogalmazó
- járőr (2 előfordulás)
- kiemelt főnyomozó
- nyomozó (7 előfordulás)
- szolgálatparancsnok
- vizsgáló (5 előfordulás)
- vizsgáló tiszt
- vizsgálótiszt (5 előfordulás)
- Áld.védelmi referens

1.11) **Melyik évben született Ön? (Kérem írja ki számokkal!)**

- 19 (5 előfordulás)
- 25
- 26
- 56
- 65
- 69 (2 előfordulás)
- 70
- 71
- 73
- 74 (2 előfordulás)
- 75 (3 előfordulás)
- 76 (3 előfordulás)
- 78 (3 előfordulás)
- 80 (6 előfordulás)
- 81 (4 előfordulás)
- 82
- 83 (3 előfordulás)
- 84 (4 előfordulás)
- 85 (3 előfordulás)
- 86 (4 előfordulás)
- 87 (5 előfordulás)
- 88 (2 előfordulás)
- 89 (5 előfordulás)
- 90 (13 előfordulás)
- 91 (10 előfordulás)
- 92 (11 előfordulás)
- 93 (12 előfordulás)
- 94 (20 előfordulás)
- 95 (17 előfordulás)
- 96 (5 előfordulás)

2. Képzettség: Ebben a kérdéscsoportban a kiberbűnözéssel kapcsolatos ismereteire és rendőri képzettségére vonatkozó kérdéseket sorolunk fel.

2.7) **Ha állampolgári bejelentés érkezik Önhöz gyermekpornográfiával kapcsolatos tartalomról egy internetes oldalra vonatkozóan, akkor tudja, hogy milyen elsődleges intézkedések megtétele szükséges? (Kérem, néhány sorban fejtse ki véleményét!)**

- Weblab elérhetőséginek vmint a tartalom rögzítése pl. képernyő fotóval, feljelentés megtétele
- - (2 előfordulás)
- - Rögzítem a bejelentését
  - Illetékes osztály részére azonnali tájékoztatás+vezetőség
- ----
- -feljelentés megtétele, oldal adatainak beszerzése, hatáskörrel rendelkező szerv értesítése majd segítségükkel a lehető legtöbb információ bizt. mentése (képek, stb.),
- A bejelentés jegyzőkönyven történő rögzítése. Az ip cím beazonosítása, a honlap letilása.
- A büntetőeljárási törvény alapján van egy olyan kényszerintézkedés, hogy elektronikus hírközlő hálózat útján közzétett adat ideiglenes hozzáférhetetlenné tétele.
- Adatgyűjtés, rendőri jelentés, feljelentés
- Alapkérdések, melyik internetes oldalon látható ...
- Alosztályvezetőt megkérdezem.
- Annak a felületnek az azonosítása, ahol a tartalom találhato. Tarhelyszolgaltato megkeresese majd a tartalom feltoltojenek az azonositasa es a tartalom eltavolitasa.
- Az adatok pontos felvételét követően jelezni kell az illetékes hatóságnak
- Az internetes oldal ellenőrzése.
  A bejelentőnek elmondani, hogy lehet letiltani az oldal elérését.
  Elindítani egy büntetőeljárást.
- Az oldal aktuális elérhetőségének,forrásának feljegyzése,ki hogyan találta meg,honnan fedezte fel a honlapot, feljelentés megtétele
- Az oldal letiltása, IP cím használójának azonosítása
- Az oldalt le kell tiltatni, a felvételeket le kell foglalni, az üzemeltető adatait, az IP címet, amiről a feltöltés történt be kell szerezni.
- Az ügy a KR-NNI hatáskörébe tartozik, sürgősen telefonálnék oda.
- Azonnal jelentés kötelezettség a parancsnok irányába, majd a forró nyomos tevékenység során a szükséges nyomozati cselekmények végrehajtása. (adatgyűjtés, tanúkihallgatások, megkeresések küldése, iü. szakértő bevonása)
- Elektronikus adat hozzáférhetetlenné tételéről intézkedni szükséges, továbbá fel kell venni a kapcsolatot a bűncselekménnyel érintett tartalom számára szervert biztosító vállalattal, irányába megkeresést szükséges küldeni a feltöltő regisztrációs adatainak beszerzése érdekében.
- Eljárás megindítása, illetékes szerv értesítése. Tőlem telhető részletes felvilágosítás a cselekmény veszélyességével kapcsoltban, mint az ifjúságvédelem.
- Elsodleges, azonnalos intezkedesek megtetele, ugymint feljelentes felvetele, bejelentes felvetele, bunugyes vezeto ertesitese, esetleges buntetoeljaras meginditasa. Inkriminalt internetes tartalomrol minel tobb info gyujtese stb.
- Első körben intézkedni kell az elektronikus hírközlő hálózat útján közzétett adat ideiglenes hozzáférhetetlenné tételéről, vagy a az elektronikus adat ideiglenes eltávolításával vagy pedig a hozzáférés ideiglenes megakadályozásával. Ezt a kényszerintézkedést a bíróság rendelheti el.
- Ez a bűnügyi szakterület része, nem az én feladatkörömbe tartozik, nem volt még ilyennel dolgom.
- Fel kell kutatni az oldal szerkesztőjét.
- Felhívom az illetékest.
- Feljelentès megtètele a legközelebbi kapitányságon, valamint a szükséges információk átadása.
- Feljelentès megtètele szüksêges az ügyben, tovàbbà az adott internetes olfalon talàlhatò tartalom azonnali lementèse a tovàbbi bizonyitàsi eljàràs cèljàbòl
- Feljelentés , majd nyomozás
- Feljelentés felvétele után elöljáró tájékoztatása, aki intézkedik a továbbiakról.

- Feljelentés felvétele, forrónyomos parancsnok felé jelzés, az oldal használójának felderitése, lakcimén házkutatás tartása, számitógép lefoglalása, iü.informatikai szakértő kirendelése.
  Feljelentö részletes kihallgatása. További tanuk felkutatása. Adatgyüjtés.
- Feljelentés felvétele,oldal megrekintése,valóban megfelel e a valóságnak a feljelentés. Ha igen, akkor az adott internetes oldal ip címének beszerzése megkereséssel.ip cím alapján az oldal létrehozójának felderítése.
- Feljelentés felvétele? Hatáskörrel rendelkező sherv sk tájékoztatása
- Feljelentés megtétele az illetékes hatóságnál
- Feljelentés megtétetele, a tartalom mielőbbi eltávolítása miatt.
- Feljelentés tétele
- Feljelentési jegyzőkönyv felvétele, tanúként történő kihallgatása azonnal. Forrónyomparancsnok / készenlétes parancsnok értesítése. A bejelentésben lévő tartalom ellenőrzése. A szóban forgó weboldal üzemeltetője felé megkeresés küldése, melyben kérném, az elhelyezett tartalommal kapcsolatos minden információ részemre való átadását.
- Feljelentést kell tenni.
- Gyermek védelméről gondoskodni.
- Gyámja kapcsolat felvétel, iskolai kapcsolatfelvétel, környezet tanulmány készítés.
- Ha ismeretlen elkövető, akkor az oldalról információkat gyűjteni, milyen üzemeltető, milyen szerver, jelzést küldeni a felső vezető felé. Minél többet tudjunk meg a forrásról, lefoglalnibgépeket, adattárakat.
- Honlap üzemeltetőjének megkeresése a felhasználó adatainak, IP cím és feltöltött tartalom beszerzése, illetve a tartalom blokkolása érdekében. Amennyiben az elkövető kiléte ismert, nála házkutatás és lefoglalás (számítógép, laptop, telefon, tablet, kamera)
- Ideiglenes hozzáférhetetlené tételt kezdeményezek
- Ifjúságvédelmet értesítem, nem értek ezekhez.
- Igen, jelentési kötelezettség az állományilletékes parancsnok, illetve a központi nyomozó szerv irányába.
- Igen, soron kívüli intézkedés megtétele. Jelentés, feljelentés.
- Igen, vezetőnek jelezni és majd ő eldönti, hogy mi az amit elsődleges cselekményként végre lehet hajtani.
- Igen, értesítem a gyámügyet, mivel még nem voltam ilyen helyzetben tanácsot kérek a felettesemtől.
- Igen.
- Illetékes hatóság értesítése, forrónyomos szolgálat értesítése indokolt esetben.
- Információ hozzáférhetetlenné tétele
- Információ továbbítása a felettes parancsnok irányába. Állampolgár adatainak és elérhetőségének rögzítése. A kapcsolatos oldal címe vagy elérhetőségének rögzítése. Jelentés készítése.
- Jelenleg nem tudom milyen elsődleges intézkedések szükségesek. Felvenném a kapcsolatot az NNI erre szakosodott osztályával a kapcsolatot mi a teendő.
- Jelentem a közvetlen parancsnoknak, ő adja a további utasításokat.
- Jelenteni a megfelelo szerv fele
- Jelenteni kell az oldal üzemeltetőjének, valamint szükség esetén el kell rendelni a nyomozást.
- Jelentés a vezetőm részére
- Jelentés elöljárónak, feljelentés felvétele, jelzés megtétele hatóságok részére.
- Kihallgatás, internetes oldal letiltása, ip cime lekérdezés, szakértő kirendelése.
- Közrendvédelmi szakterület lévén az elsődleges adatfelvételeket, meghallgatásokat követően intézkedem, hogy az illetékesek felé továbbítva legyenek az információk, adatok.
- Meg nem volt erre precedens így nem tudom.
- Meggyőződni a hiteles információkról.
- Meghallgatom a bejelentést, készítek RZS-ben róla egy iratot, hogy maradjon nyoma, majd elöljárómnak szólva, közösen megbeszéljük mi a teendő.
- Megkell keresni azt a szolgaltatot aki feltette

- Megkeresen a megfelelő szervet, gyivót.
- Megkeresesek, ip cim beszerzese, hazkutatas, gyanusitas
- Megállapítani az ip címet. Feltételezett elkövetőnél házkutatás és számítógépek lefoglalása.
- Mentse le a linket, majd print screen-elje a weblapot, a feltöltő profilt mentse le valamilyen formában, tegyen feljelentést.
- Minden adat kimentése a későbbi bizonyításhoz, majd az oldal értesítése, felszólítása a tartalom eltávolítására, illetve hozzá megkeresés küldése a feltöltő felhasználó adatainak beszerzéséhez
- Mivel az ilyen nem hozzám tartozik,így szólok az elöljárómnak, hogy keresse fel az illetékest és így megfelelő helyre tudom irányítani a bejelentőt.
- Még nem volt ilyen ügyem, de úgy tudom, hogy ideiglenes hozzáférhetetlenséget kell elrendelni.
- NNI Kiber Bűnözés Elleni Főosztállyal próbálnám felvenni a kapcsolatot. Feljelentési jegyzőkönyvet készítenék.
- Nem (2 előfordulás)
- Nem dolgoztam még ilyen bűncselekmény vonatkozásában, így értesíteném a parancsnokomat.
- Nem foglalkozom ilyesmivel. De gondolom az internetes tárhelyet adót fel kell hívni, hogy tiltsa az oldalt.
- Nem fordult még elő. De elsődlegesen vezető értesítése, majd mivel szakirányon, tapasztalaton kívül eső a kérdés, illetékesektől segítség kérése.
- Nem szoktam ilyen ügyekben dolgozni, de a kollégámtól megkérdezném , akinél ilyen ügyek vannak.
- Nem tudom (4 előfordulás)
- Nem tudom a szükséges intézkedéseket, azonban minden esetben meghallgatnám a bejelentőt, a kérdéses weboldalt feljegyezném és közvetlen felettesemnek jelenteném az esetet, illetve kérnék útmutatást a további szükséges intézkedések megtételére vonatkozóan.
- Nem tudom az elsődleges intézkedéseket, valószínűleg utánajárnék, hogy ezen a szakterületen kik az illetékesek, azokat keresném fel és látnám el a tudomásomra jutott információkkal ezzel kapcsolatban.
- Nem tudom az ezzel kapcsolatos intézkedéseket.
- Nem tudom mi az intezkedes menete
- Nem tudom, hozzám ilyen bejelentés még nem érkezett.
- Nem tudom, nem fordult meg ilyen elo velem.
- Nem tudom, segítséget kérek osztályvezetőmtől.
- Nem tudom. (3 előfordulás)
- Nem volt ebben tapasztalatom.
- Nem volt még rá precedens, így ezen a téren sajnos hiányosak az ismereteim. Hozzáférhetetlenné kell tenni az oldalt mindenképp, ha valóban fellelhető az oldal.
- Nem.
- Nem. Ilyen jelegű bűncselekményekkel kapcsolatos intézkedésekre ezidáig nem került sor. Amennyiben állampolgári bejelentés érkezik ilyen jellegű bűncselekményekről vezető beosztású személyhez fordulok.
- Nem. Jelzem a feletteseimnek
- Nincs
- Oldal beazanosítása
- Oldal elérhetősége,hozzá kapcsolódó információk rögzítése
- Oldal hozzáférhetetlenné tétele
- Oldal lementése, meggyőződni a bejelentés valódiságáról, IP cím megállapítás
- Oldal valódiságának az ellenőrzése.
- Oldal üzemeltetőjének a megkeresése a feltöltési adatokra vonatkozóan, ezek alapján megkeresés a további szolgáltatóknak (IP cím-internet szolgáltató, e-mail cím stb.). Előterjesztés ele ktronikus adat ideiglenes hozzaférhetetlenné tételének az indítványozására.(A szolgáltatók általában ilyen esetekben határozat nélkül is eltávolítják a tartalmat)

- Parancsnoknak jelentem, hivatalból indul az eljárás
- Pontosan nem tudom, határrendészeti szakterületen nem jellemző
- Pontosan nem tudom, szólnék az illetékes nyomozónak, vezetőnek
- Robotzsarut használom ,megteszem amit szükséges, jelentem. Majd a közvetlen alosztályvezetőm,amint tudok rendelkezik ilyen ismeretekkel, így a továbbiakban segít.
- Részletes feljelentés, az oldal elérhetőségének és egyéb adatainak mentése, valamint az eljárás lefolytatására illetékes hatóság soron kívüli értesítése.
- Sajnos nem tudom ilyenkor mit kell tenni.
- Segítsèget kèrek ès jelzem a felettesemnek
- Szólni az illetékes hatosagnak,lefoglalás,ellenőrzés.NNI Kiberbunozes
- Tegyen feljelentest
- Tudom mit kell tennem.
- Véleményem szerint az elsődleges feladat az illetékes hatóságok megkeresése az IP cím beazonosítása végett.
- az oldal készítőjének személyazonosságának megállapítása, IP cím bekérés, tartózkodási helyének megállapítása, az oldal hozzáférhetetlenné tétele más felhasználók számára
- azonnali bejelentés, esetleg oldal elérhetőségének megjegyzése, az biztosan kell majd a további eljáráshoz, illetve jelenteni az oldalt, ahol felbukkant
- elektronikus hirközlő hálozat útján közzétett adat ideiglenes hozzáférhetetlenné tétele
- fekjelentés rögzítése, internetes oldal üzemeltetőjének soron kívüli megkeresése, a pornográf tartalmak azonnali mentése, ismert gyanúsítható személy esetén soron kívüli házkutatás megtartása, informatikai eszközök lefoglalása, szakértő kirendelése
- feljelentés
- gyermekkorú törvényes képviselőjének felkutatása, feljelentés felvétele, az internet szolgáltató megkeresése IPC adatok bekérése
- ideiglenes hozzáférhetetlenné tételt kezdeményezek (2 előfordulás)
- igen
- nem
- nem tudom
- segítséget nyújtok neki, hol teheti meg a bejelentését, feljelentését.
- Értesíteni kell a TIK-et, ők megteszik az elsődleges intézkedést, hogy az oldal üzemeltetőjével szemben majd eljárást kezdeményezhessenek

2.12) **Ha egy állampolgári bejelentés érkezik Önhöz, hogy egy vállalkozás internetes oldala elérhetetlen DDoS támadás miatt, akkor vannak ismeretei a lehetséges teendőkről? (Kérem fejtse ki néhány sorban!)**

- A városi kapitányság informatikusával venném fel a kapcsolatot
- - (2 előfordulás)
- Az oldal tárhelyszolgáltatójának megkeresése a log adatok beszerzése érdekében. Oldal lekérési IP-k alapján megkeresés a szolgáltatóknak, hogy mely előfizetőjük részére osztották ki a kérdéses időpontokban az IP-ket.
- Azon kívül, hogy jelentem az elöljárómnak, nincs.
- Azonsítani a tamado gepek IP cimet. A sertett pedig helyezze at az oldalat mas IP cimere.
- BRFK csúcstechnológiai bűnözés elleni osztály osztályvezetőjét felkeresném telefonon és értesíteném az üggyel kapcsolatban
- DDos támadás, egy túlterheléses számítógépes támadás, melynek következtében a felhasználók számára elérhetetlen lesz az oldal. Mindenképpen informatikus segítségét kell kérni, de fogalmam sincs a további teendőkről, még sosem dolgoztam ilyen ügyben.
- Erről sajnos nincsenek ismereteim.
- Ez már magasabb fokú tudást igényel, nincsen elég ismeretem a DDoS támadásokról.
- Felveszem a feljelentést részletesen és utána a vezetöi utasitást követem.
- Fogalmam nincs!
- Ilyen nem történt még velem.
- Ismetem a problémát de nem tudom mi a teendő olyan esetben.
- Jogi felvilágositás
- Kollégáktól és vezetőktől kérnék segítséget ehhez. Esetleg szakértőtől.
- Közvetlenül nem dolgozom ilyenben,így hasonlóképpen járok el,mint előzőleg.Osztályvezetőmet tájékoztatom, aki felhívja az illetékest a megyén.
- NIncsenek ismereteim a teendőkről.
- Nem (3 előfordulás)
- Nem igazán. (2 előfordulás)
- Nem ismerem a DDoS támadást, a vezetőm segítségét kérném.
- Nem ismerem a DDoS-t
- Nem ismerem ezt.
- Nem rendelkezem a szükséges ismeretekkel.
- Nem rendelkezem ismeretekkel ezzel kapcsolatosan.
- Nem tudom mi a teendo.
- Nem tudom mi az.
- Nem tudom mi ez
- Nem tudom, feletteseimhez fordulnék tanácsért.
- Nem tudom, sajnos.
- Nem tudom. (2 előfordulás)
- Nem, hasonló módon járnék el mint a gyermekpornográf felvételekkel kapcsolatos kérdés esetén.
- Nem, nincs.
- Nem. (2 előfordulás)
- Nincs (5 előfordulás)
- Nincs ilyenről információm
- Nincs ismeretem a teendőkről.

- Nincs, kérdezek a kompetens személytől.
- Nincs. (7 előfordulás)
- Nincsen (2 előfordulás)
- Nincsen róla megfelelő szakmai ismeretem, olyanhoz fordulnék akinek van.
- Nincsen.
- Nincsenek (10 előfordulás)
- Nincsenek
- Nincsenek erről ismereteim, de véleményem szerint a 2.7-es pontban leírt intézkedések szükségesek.
- Nincsenek ilyen ismereteim (2 előfordulás)
- Nincsenek ilyen ismereteim, valószínűleg megkérdeznék egy gv-s kollégát.
- Nincsenek ismereteim (3 előfordulás)
- Nincsenek ismereteim errol.
- Nincsenek ismereteim. (2 előfordulás)
- Nincsenek konkrét ismereteim. Elsődlegesen felvenném a kapcsolatot a megyei informatikai osztállyal a teendőkkel kapcsolatban.
- Nincsenek mélyreható ismereteim, de tudom kihez kell fordulni ilyen esetben.
- Nincsenek sajnos.
- Nincsenek. (10 előfordulás)
- Nincsenek. (3 előfordulás)
- Nincsenek. Elöljáró értesítése, aki intézkedik a továbbiakról.
- Nincsennek megyei informatikai osztály véleményét kérem ki.
- Passz
- Rendszergazda azonnali értesítése, vírus megsemmisítése, elkövető felderítése
- Sajnos etekintetben nincsenek ismereteim.
- Sajnos nem ezen a szakterületen dolgozom.
- Sajnos nem tudom ez mit jelent.
- Sajnos nincsenek
- Sajnos nincsenek.
- Szakértő segítségét venném igénybe.
- Szólok egy kollégámnak, aki ilyen területen dolgozik.
- Várjon amíg a rendszergazdák megszübtetik a problémát.
- informatikai ismereteim nincsenek ezzel kapcsolatosan, azonban javasolnám a feljelentés megtételét a Ddos támadás kezdeményezőjének esetleges felderítése érdekében
- kapcsolja ki
- nem
- nem igazán
- nem tudom
- nincs (3 előfordulás)
- nincs információm
- nincs.
- nincsen ismeretem-e területen

- nincsenek (5 előfordulás)
- nincsenek ilyen ismereteim.
- tanultam róla, el vannak mentve a jegyzeteim, azokból el tudok indulni, de eddig nem volt szükség ezen tudás alkalmazására.
- Általános teendő, az ügy jellegétől függően.
- Össze kell gyűjteni mindent adatot a vállalkozásról.
  Ezeket az adatokat kell elemezni, és valódiságukat ellenőrizni.
  Meg kell nézni cégnyilvántartásban, és egyéb nyilvántartásokban a vállalkozást.
  Amennyiben van elérhetőség, ki kell deríteni a probléma okát.
  Ha felmerül a bűncselekmény gyanúja (pl.: csalás), meg kell indítani a büntetőeljárást.

2.13) **Egy házkutatás során kell intézkednie bekapcsolt személyi számítógép adattartalmának rögzítésére. Ismeri a helyes eljárásrendet? (Kérem, fejtse ki néhány sorban!)**

- -
- - USB-n keresztüli adatmentés /vagy hordozható winchester
  - jelszavak feloldása
- A NAV munkatársaival közösen dolgozunk ilyen esetben akik hiteles másolatot kèszítenek a helyszínen az adattartalomról
- A büntetőeljárás alapján intézkedek a lefoglalásról.Az abban leírtakat tekintem irányadónak.
- A gépet azonnal le kell kötni a hálózatról. Majd kikapcsolt állapotban lefoglalni. A gép tartalmát szakértő ellenőrzi.
- A helyes eljárási rend folyamatosan változik és függ az adott ügyben releváns bűncselekmények súlyától.
- A személy mihamarabbi eltávolítása az eszköztől. A számítógép kiapcsolása. A ki-és bemenő perifériák zárása úgy, hogy azokhoz ne lehessen hozzáferni, illetve a zárócimkék hitelesítése.
- A szàmìtògêpen lèvő szüksêges adatot adathordozòra lementem, illetőleg amennyiben szüksèges, a hàzkutatàst informatikus jelenlètèben az ő segìtsègèvel foganatosìtom
- A teljes számítógépet lefoglalnám a perifériákkal együtt.
- Amennyiben lehetséges, a szakértő vagy szaktanácsadó igénybevétele az adatok lementése vagy a megfelelő kikapcsolt állapotba helyezés érdekében. Amennyiben nincs rá lehetőség, a számítógép kikapocsolása egészben történő lefoglalása és szakértőhöz küldése.
- Az eszköt leállítása tilalmazott, szakértő másolatot készít a rendszer egészéről, majd az eszköz lefoglalásra kerül.
- Az áramforrás megszüntetése, és nem a számítógép szabályos kikapcsolása, majd lehetőség esetén az egész számítógép rögzítése.
- Biztonságos leállítás, tartozékaival együtt lefoglalás, kapitányságra behozni.
- Biztosítani hogy a gépet ne kapcsolják ki valamint bit azonos mentést un. Hash kulcsot alkalmaznék.
- Doksik mentése másként, majd áramtalanítani, hogy automatikusan induló programok ne töröljék az adattartalmat.
- Elektronikus adat hozzaferhetetlenne tetele! 1998 evi XIX torveny vonatkozo resze.
- Először bezárom a futó programokat, szabályosan kikapcsolom, kihúzom az áramforrásból, lefoglalom a tartozékait (akkumulátor, töltő) leragasztva foglalom le.
- Először vizsgálni kell, hogy futnak e a számítógépen az eljárás szempontjából releváns programok, szoftverek. Fénykép, videó felvétel, jegyzőkönyv. Bontható IT eszközök egyedi azonosító jeleit is rögzíteni kell. Bitazonos adatmentés.
- Forrónyom pk!
- Fénykép készítése a bekapcsolt számítógépről, annak képernyőjéről,a csatlakoztatott eszközökről, majd a számítógép kikapcsolása az áramforrás megszakításával.
- Gépet nem szabad kikapcsolni, kihúzni, áramtalanítani. Szakértőt kell hívni aki ért hozzá.
- Ha lehet tudni, hogy azonnal adatmentésre lesz szükség, akkor már célszerű informatikussal, vagy szakértővel menni. Ha nem, akkor a laptopot kikapcsolás nélkül, hibernált állapotban kell elhozni és lehetőleg soron kívül kell eljuttatni szakértőhöz. Az asztali gépet ki kell kapcsolni.
- Ha lehetséges a helyszínre hívok egy szakértőt ,de ha nem lehetséges akkor szaktanácsadó igénybevételével ideiglenesen biztosítom az eszköz hozzáférhetőségét és amint lehet szakértő segítségével megoldom.
- Ha nagyon fontos, felhívom az informatikai osztályt, hogy mentsék ki az adatokat.
- Helyszin biztosítása, szakértő helyszínre hivása, lefoglalás, házkutatás.
- Helyszínre hívom az iü.informatikai.szakértőt , az a biztos.
- Igen
- Igen, odahivom a szakertot es majd o megcsinalja.
- Igen.
- Igen. Nem kapcsoljuk ki,megprobaljuk kinyerni az adatokat.
- Ki kell kapcsolni a számítógépet és le úgy kell lefoglalni.
- Kikapcsolom és lefoglalom, majd a szakértő fogja átvizsgálni

- Kikapcsoltatom a tulajdonossal, majd hatósági szalaggal leragasztom az összes bemeneti nyílást.
- Kikapcsolás után lefoglalnánk a készüléket, és csak később rögzítenénk az adatait, kivéve, ha halaszthatatlan a bizonyíték beszerzése.
- Közrendesként nem én fogom csinálni.
- Lefoglaljuk mint a többi eszközt és majd a későbbiekben a szakértő rendezi.
- Lefoglalnam a szamitogepet. Kernem segitseget, mert meg nem volt ilyen esetem.
- Lefoglalom
- Lefoglalom a gepet.
- Lefoglalás majd, szakértő menti le.
- Lefoglalás, majd szakértő kirendelése és ő lementi.
- Lefoglalás, szakértő kirendelés, szakértő megküldi a lementett adatokat
- Lefoglalás, szakértő, megvizsgálom én is.
- Lefoglalási jegyzőkönyvben rögzíteni, hogy mit mentek le, melyet további a hatóság által vitt adathordozóra mentenék.
- Lefoglaló határozat, birtokos jelenléte,
- Lementem pendrive-ra
- Megfelelő határozatok beszerzése.
  Figyelmeztetések, nyilatkozatok megtétele.
  Adathordozóra történő áthelyezés a számítógép tulajdonos jelenlétében.
- Megkérdezem a házkutatást elszenvedő személyt, hogy hozzájárul-e ahhoz, hogy az üggyel kapcsolatban és az üggyel releváns információk a számítógépről lementésre kerüjenek.
- Minden esetben informatikai szakértő jelenlétében házkutatok és rögzítem az adattartalmat.
- Minden esetben videófelvételt készítenék a nyomozási cselekményről a kényszerintézkedéssel érintett jelenlétében
- Mindenképpen informatikus szakemberrel megyünk ki házkutatni. Ki kell jelentkeznie a felhasználónak, a helyszínen nem rögzíthető az adattartalom, csak szakértő teheti ezt meg.
- Mivel ilyen szituációban nem voltam, konkrétan nem tudnám mi a helyes sorrend, de az általános szabályokat átvitten alkalmaznám.
- Nem (13 előfordulás)
- Nem házkutatás során rögzíteném az adatokat, hanem kikapcsolnám a számítógépet, majd lefoglalnám.
- Nem ismerem (2 előfordulás)
- Nem ismerem
- Nem ismerem a helyes eljárási rendet, hasonló jellegű intézkedésre ezidáig nem volt példa. Megfelelő adattároló eszközre menteném le a szükséges tartalmakat, illetve szakértő segítségét venném igénybe, ha az különleges szakértelmet igényel.
- Nem ismerem az eljárást
- Nem ismerem de biztos hogy informatikus kollégát rendelnék elsőnek a helyszínre.
- Nem ismerem. (6 előfordulás)
- Nem ismerem. (2 előfordulás)
- Nem kapcsolnám ki, szakértő segítségét venném igénybe.
- Nem kikapcsolom, hanem áramtalanítom. Érkezés után azonnal felügyelet vonom a számítógép közelében tartózkodókat, nehogy adatot semmisítsenek meg vagy egyéb kárt okozzanak. A lefoglalt számítógép pedig mehet a szakértőnek.
- Nem minden esetben, de ha a szóban forgó bűncselekmény elkövetésének gyanúja merül fel, akkor igen.
- Nem volt még rá példa, így nem lennék biztos a dolgomban.
- Nem, a parancsnokomhoz fordulnék segítségért.
- Nem. (6 előfordulás)
- Olyat bízok meg vele aki ért hozzá.

- Pendrive-ra lementem, szakértőt rendelek ki.
- Részben ismerem.
- Semmiképp nem kapcsolom ki a számítógépet. Helyszínen megpróbálok minden adadtot kinyerni akadály esetén szakértőt rendelek ki.
- Szakember kapcsolja ki a gépet, hash kulcs lefolgalásnál.
- Szakerto segítséget kérjük telefonon vagy személyesen.
- Szaktanácsadó kirendelése
- Szaktanácsadóval lementjük az adatokat, az esetleges adatvesztés megakadályozása céljából.
- Szakértőt hívok. Mindenféle képpen azt hivok.
- Szakértőt rendelek ki, hogy ha van rá idő.
- Szakértőt rendelnék
- Szakértővel kimentetem.
- Szerintem igen. Szakértőt rendelnék ki először is. Ha be van kapcsolva a számítógép, akkor megkísérlem a helyszínen az adatrögzítést, majd ezt követően lefoglalom a gépet,
- Számítógép szabályos leállítása, majd a bűnjel csomagolása.
- a gép kikapcsolást követően lefoglalásra került, a továbbiakban szakértő igénybevételére kerül sor.
- a számítógép közelében tartózkodók kontroll alá vonása,hogy ne nyúlhassanak a géphez vagy a tartozékaihoz. A számítógép áramtalanítása, nem pedig kikapcsolása. Érdemes informatikus szakértő segítségét igénybe venni. Hash-kulcs alkalmazása.
- a számítógépet azonnal kikapcsolni, majd szakértelemmel rendelkező személyt felkérni az adatok mentése céljából.
- a számítógépet kikapcsolom, majd lefoglalom és szakértő bevonásával végzem el az adatok rögzítését.
- igen
- le kell foglalni a számítógépet és adathordozókat.
- nem (4 előfordulás)
- nem ismerem.
- szaktanácsadót veszek igénybe
- szakértő, szaktanácsadó igénybevétele
- szgép szabályos leállítása és ármatalanítása után biztonságos csomagolás és elszállítás szakértői vizsgálatra
- szükség esetén szólok a rendszergazdának, vagy szakértőnek.
- tudomásom szerint a lefoglalt számítógépről mentés a rendőri intézkedés során nem célszerű, annak szakszerű csomagolásáról és szakértőhöz történő megküldéséről kell intézkedni, ugyanis a számítógép tartalmának lemetése és annak átvizsgálása stakértői feldata. az eljárás sikerességét is meghiúsíthatja, ha az intézkedő rendőr nem megfelelően hajtja végre a számítógép tartalmának lementését és az a későbbiek során bizonyítékként már nem lesz felhasználható.
- Úgy kapcsolpm kikalózait h kihúzom a tápegységet a falból. Laptopnál kiveszem az aksit. Hash kulcsot használok.

2.19) **Ha szeretne részt venni kiberbűnözés elleni fellépéshez kapcsolódó képzésben akkor Ön milyen okból tenné? (Kérem, fejtse ki röviden!)**

- - (2 előfordulás)
- ..
- 400%-os bérezés.
- 400%-os bérilletmény miatt minden képzésen részt veszek, amire lehetőségem adódik, illetve érdekel is a téma.
- A hasonló jellegű bűncselekmények egyre gyakoribb elterjedése miatt
- A magánéletben is és munkámban is fontosak lesznek ezek az ismeretek, és a technikai fejlődés előrehaladtával még nagyobb jelentősége lehet az ilyen ismereteknek később.
- A technika felgyorsult fejlődésével a rendőrségnek is lépést kellene tartani, ehhez szükséges az állomány képzése is, és nem csak azé a szűk köré akik konkrétan ezzel foglalkoznak, ezen kívül érdekel is a dolog.
- Abból,hogy későbbi munkámra tekintettel, olyan ismeretekre tehetnék szert,ami akár segítséget nyújthat.
- Ahogy azt az előbb is jelöltem fontosnak tartom.
- Alaphelyzetben is érdeklődök az informatikai dolgok iránt, és használom is azokat napiszinten, ezért is vagyok nagyjából képbe a cryptocurrency és hasonló dolgokkal, és ezt a tudásom jó lenne ha tudnám, hogyan tudom felhasználni a rendőrségen belül, tekintettel arra, hogy attól függetlenül, hogy tudom mik ezeknek a dolgoknak a lényege, hogyan lehet ezzekkel bcs.-ket elkövetni pl. darkneten, hogy miért lekövetethetlenek ezek a currency folyamatok, még nem tudom, hogy a rendőrségen belül erre milyen eljárási szabályzók vannak, vagy hogyan dolgoznak ilyen és hasonló ügyeken. A 2.20-as kérdésre az utolsó válaszhoz hozzáfűzni valóm, hogy szerintem a rendőrségen belül mindenki tisztában van azzal, hogy az e-learninges képzesek a valóéletben hogyan is mennek a kapitányságokon.:)
- Amennyiben ilyen bűncselekménnyel találkozom, tudjam mi a teendő.
- Az ismereteim bővítése céljából
- Az ismeretem fejlesztése érdekében, a munkában történő hasznosítás végett.
- Azon okból hogy minél tájékozottabb legyek.
- Azért mert az informatika rohamosan fejlődik.ezért a bűnözők ezen a területen is egyre több bűncselekményt követnek el. Én pedig szeretem ismereteim bővíteni.
- Azért tenném, mert véleményem szerint nem rendelkezem a megfelelő ismeretekkel a témában.
- Azért, hogy egy összefoglaló képet kapjak az ilyen típusú bűnözésről.
- Azért, hogy ilyen jellegű ügyeimben tájékozottabb legyek.
- Azért, hogy megismerjem az ehhez kapcsolodó bűncselekményeket
- Bár közrend vonalon dolgozom, véleményem szerint fontos, hogy széleskörű ismereteim legyenek, ezért nagyon szívesen részt vennék ilyen képzésen.
- Bővítsem az ismeretemet.
- Effajta jellegű bűncselekmények visszaszorítása miatt
- Egyre gyakoribbak az elektronikus úton történő bűncselekmények, ezért szeretném ha lenne rálátásom.
- Egyre inkább elterjedtebb a munkánkban és a magánéletünkben is a számítógép használata, az azzal kapcsolatok bűncselekmények száma is növekszik. Fontos, hogy szakmai szempontból képzettek legyünk és ennek a tudásnak adott esetben a magánéletben is hasznát vehetjük.
- Egyre jellemzőbbek ezek a típusú ügyek.
- Egyre nagyobb teret nyer a kiberbűnözés, ezért hasznos lenne az ismeretek bővítése.
- Egyre több ilyen jellegű bcs van, így szüksègesnek tartom
- Egyre több ilyen jellegű bcs. fordul elő nálunk, legtöbbször csak a feljelentés jön meg, azzal igazolják, hogy megtettek mindent ígx a pénzüket az érintettek visszakapják, mi nem tudunk csinálni vele sok mindent.
- Ez a jövő, és tisztában kell lennünk vele.
- Fejlődésem érdekében
- Fontos a mai világban tisztában lenni vele

- Gazdaságvédelmi Alosztályon dolgozom, és úgy gondolom ez lesz a "jövő" bűncselekménye. Sajnos az ismereteim nem a legbővebbek, ezért szeretném azokat bővíteni.
- Gyermek pornográfia és az internetes zsarolás felszámolására.
- Hogy az ismereteimet bővítsem.
- Hogy bővítsem ismereteimet.
- Hogy jobban atlassam a temat es lefoglalaskor ismerjem az eljarasi rendet.
- Hogy napra készebb legyek ebben is.
- Hogy tudjak védekezni és intézkedni ilyen esetekben.
- Hogy tudjam hasznosítani a munkám során
- Igen keveset tudok ezekről a témákról és szükséges lenne a munkám elvégzéséhez.
- Ismeretbővírés és mert még hasznos lehet.
- Ismereteim bővítése és a kiberbűnözés csökkentése miatt
- Ismereteim bővítése, munkám eredményesebbé tétele.
- Ismereteim gyarapításának céljából.
- Ismereteimet bővíteném, érdekel a téma, hiszen ez napjainkban jelentős problémákat okoz.
- Ismeretek bővítése
- Ismeretek bővítése.
- Ismeretek elmélyítése.
- Kint az utcán vagy bármely intézkedés során lehet még jól jöhet.
- Legalább saját védelmem érdekében
- Mert a mai világban már egyre inkább számítógépes bűncselekményeket követnek el.
- Mert a számítástechnikai világ rohamosan fejlődik, mely által véleményem szerint a kiberbűnözéses bűncselekmények elkövetésének száma is.
- Mert bővíteni akarom az ismereteimet.
- Mert egy izgalmas téma és mindannyiunkat érinti/heti.
- Mert fontosnak tartom ezen ismeretek bővítését a mai modern eszközök, technika mellett.
- Mert fontosnak tartom. (2 előfordulás)
- Mert járőrként rengeteg állampolgári megkeresést kapok,és szeretnék napra kész lenni a válaszokat illetően.
- Mert kivancsi vagyok az ilyen jellegu cselekmenyekre.
- Mert szeretném boviteni az ismereteimet, erdeklodo tipus vagyom es az informatikat is szeretem.
- Minél szélesebb ismeretekkel szeretnék rendelkezni.
- Mivel engem a kiberbűnözés érdekel a legjobban, munkám során is az internetes csalásokkal kapcsolatos ügyeket is külön kérem magam részére a nyomozás lefolytatására.
- Mostanában egyre több eszközt kell lefoglalnunk, vagy ha nem is kell, de kapcsolatba kerülünk ilyen eszközökkel. A kibertérben elkövetett bűncselekményeket újdonságuk miatt nagyon nehezen nyomozhatónak találom. Mivel nem tudja szinte senki, hogy mi a pontos eljárási menet, ezért úgy gondolom, jobb lenne, ha néhány szakembert kiképeznének, akik segítik a többieket is akár, így felkészítve szép lassan mindenkit az ilyen bűncselekményekre.
- Munkám során hasznát venném, ismereteim bövitésére. Jobban képben lennék a feljelentéskor történö kérdések feltevésében. Ha vizsgálnám is az ügyet jobban átlátnám a lényeget.
- Munkánk során is egyre gyakrabban találkozhatunk majd ilyen jellegű esetekkel, melyeknél gyakran meg van kötve a kezünk a hiányos ismeretek miatt. Azt gondolom, hogy a magánéletben is nagyon fontos és hasznos lenne ilyen képzés, ugyanis nincs csak a rendőrséghez kötve.
- Nem
- Nem munkaköri, hanem inkább magánéleti szempontból

- Nem sok mindent tudok az informatikai eszközökről, a bitcoinról és érdekel a kiberbűnözés.
- Nem szeretnék
- Nem szeretnék.
- Nincsen megfelelő szintű képzés jelenleg ami elérhető lenne, ezért tartanám szükségesnek.
- Saját tudásomat és szakmai hozzállásomat szeretném fejleszteni.
- Speciális ismereteket szerezhetek, amelyek hasznosak lehetnek.
- Szakmai ismeretek bővítése
- Szeretnék alap szinten értrni hozzá. Úgyrögzöteni adatokat, hogy azok a büntetőeljárás során biztosan felhasználhatóak legyenek.
- Szeretném bővíteni ismereteimet.
- Számomra ez viszonylag ismeretlen téma, így ezzel kapcsolatban ismereteim bővítésre szorulnak.
- Szükségesnek tartom megismerni egy ilyen típusú bűncselekmény nyomozását és az ahhoz kapcsolódó speciális intézkedéseket.
- További ismeretek szerzése a teljes témában, legújabb módszerek megismerése.
- Továbbképzés céljából
- Tudjam mit kell kezdeni az üggyel.
- Tudás bővítése
- Tudásom bővítése érdekében valamint a jövő bűnözése miatt fontosnak tartom megismerni az ilyen fajta bűnelkövetőket is.
- Tudásomat bővítsem és még jobban tisztában legyek az ilyen bűncselekmények nyomozásával.
- Tájékozott legyek a bűncselekményekkel és az eljárással kapcsolatban.
- Ugyan nem tartozik a szakterületemhez, azonban a mi okoseszközök elterjedese miatt szükséges lehet mindenki számára, hogy egy ilyen képzésen részt vegyen és szeretem az ismereteimet bővíteni, a nyomozás során felhasználjató eszközöket, technikákat megismerni, hátha tudom azt használni saját szakterületem során.
- Változik a világ, változnak a bűncselekmények, nekünk is fejlődni kell, valamint nem nagyon kaptunk oktatást erről.
- Véleményem szerint a mai világban egyre többször fordulnak elő ilyen jellegű bűncselekmények, amelyekre csak a megfelelő ismeretek elsajátításával lehet felkészülni.
- alapvető fogalmak, tények megismerése, már lefolytatott nyomozások tapasztalatainak megosztása (hibák feltárása, ezekből következtetés levonása) jövőbeli minimum teendők megállapítása, meghatározása, ill folyamatos képzés, ismeretek megosztása.
- azért hogy bővítsem az ismereimet
- bűnügyi szakmai ismeretek bővítése, tapasztalatszerzés, helyes elmélet és gyakorlat kialakítása
- elszaporodott az ilyen jellegű bűncselekmények elkövetése, és sok elkövetési mód, eszköz ismeretlen
- fejlesszem az ismereteimet
- hogy a tudásomat fejlesszem
- ismeretbővítés és továbbképzés céljából
- saját tudásom bővítése érdekében
- szakmai ismereteim bővítése és saját érdekeim végett egyaránt
- Érdekesnek tartom ezt a témát.
- Így is 1 héttre legalább 1 nap képzés jut, az ügyek meg nem haladnak.

2.22) **Milyen plusz témákat javasolna? (Kérem fejtse ki néhány sorban)**

- \- (10 előfordulás)
- --
- .
- ..
- A fent említettek úgy gondolom egy nagyon széleskörű lehetőséget fogtak át. Esettanulmányok vizsgálatát tartanám még érdekesnek vagy hasznosnak. Konkrét esetekből és azok hibáiból is nagyon sokat lehet tanulni.
- A fentieken kívül nincs más javaslatom.
- Adathalászat az inzernetről. (Gyors és hatékony adatszerzés, személy ellenőrzés az interneten segítségével)
- Az elozo kerdes kimeritette az altalam ismert temakat.
- Az előzőeken kívül más javaslatom nincs.
- Elég átfogónak tartom a felsorolást.
- Felderitessel kapcsolatos témában.
- Jelenleg nem tudok más témákat.
- Jelenleg nincs javaslatom.
- Közösségi oldalak veszélyei, azokon elkövetett személyiséglopások, zsarolás, pedofília.
- Külföldi internetes közösségi portálok irányába küldendő megkeresések, adatszolgáltatások lehetőségének bővítése.
- Minden érdekel.
- Minnél gyakorlatibb legyen, nem informatikus akarok lenni.
  A jelenlegi nyomozási/intézkedési gyakorlatot kéne alapul venni, amit nap mint nap használnak egy kapitányságon,nem csak az elméleti ismereteket. Nem kell órákat beszélni egy adott dolog hátteréről, hogy hogyan épül fel az adott rendszer stb..,hanem, praktikákról, amivel az adott problémát meg lehet oldani ott a helszínen a legegyszerűbben. Nem attól fogom tudni megoldani, hogy tudom, hogy mennyi a váltószám a kilobyte és a megabyte között.
- Mivel nem ertek hozza, nincs etdemi javaslatom.
- Nem
- Nem javaslok
- Nem javasolnék
- Nem javasolnék más témát, a megadott témákat elegendőnek találom.
- Nem javasolnék mást.
- Nem jut eszembe más
- Nem tudok ebben a témában javaslatot tenni.
- Nem tudok plusz témát.
- Nem tudom
- Nem tudom, ez elegendő.
- Nincs ilyen.
- Nincs javaslatom. (2 előfordulás)
- Nincs más ötletem.
- Nincs több téma, a fenti kiválasztott témák teljesen megfelelőek
- Nincs több ötletem
- Nincsen
- Pl: A rendőri szakma tanulásának gyakorlatiasabbá tétele. Több intézkedéstaktikai és jármű vezetéstechnikai képzés.
- Programozás "hackerkedés"

- Semmit.
- Szervezett bűnözés elleni küzdelem hatékony fellépésének lehetőségei.
- Szervezett kiberbűnözés
- Számomra ezek a témák kimerítők voltak.
- nem javasolnék, elég sok témát felölel
- nincs ilyen
- nincs javaslatom
- nincsen jeveslatom

Az interjúkészítés során feltett kérdések:

A kutatómunkával kapcsolatban az alábbi kérdéseket szeretném tisztázni, úgy, hogy abból- vagyis az elhangzott interjú és a dokumentumkutatás során- a saját hipotéziseimet alá tudjam támasztani vagy azokat megcáfoljam, szükséges a következőkre a válasz:

- *A nyomozások során az ügyészség részéről tapasztalt általános hibák- így jogértelmezési problémák, jogszabályismeret hiányossága, az ügymenetek elhúzódásának okai (szakértő kirendelése, szakértelem hiánya, együttműködés hiánya stb.) jogalkalmazói*
- *A házkutatások, lefoglalások és bizonyítékok összegyűjtése során észlelt tapasztalatok a rendőrségi eljárásokban (OSINT tevékenység)*
- *Észlelhető-e különbség a speciálisan számítógépes bűnözéssel foglalkozó szervezetek és azon szervezetek munkája között, akiknek „elvétve" akad ilyen jellegű ügyük? (ha igen milyen eltérések vannak?)*
- *A Btk. –ban található számítógépes bűncselekmények tényállásainak nyomozási problémái*
- *A büntetőeljárásban/nyomozásokban az ügyész szerepe*
- *Az ügyészség nemzetközi szerepvállalásai a számítógépes bűnözés elleni harcban*
- *A bíróság előtti evidenciák összegyűjtése és azok szakértése*
- *Szükség van-e szakértőre, ha igen, mikor? A forenzikus vizsgálat rendőrségi elvégzése*
- *A titkos információgyűjtéssel kapcsolatos tapasztalatok*

A dokumentumkutatás során –leginkább az ügyészségi állásfoglalások, iránymutatások-, bírósági végzések, határozatok érdekelnének, ugyanakkor a disszertációm témája miatt 4 vagy 5 olyan számítógépes bűncselekmény elkövetése miatti eljárásban/aktában szeretnék betekinteni, amelyben az eljárás vádemeléssel zárult- esetleg már ítélet is született, valamint szintén ugyanannyi olyan ügybe szeretnék betekinteni, amelyet az ügyészség megszüntetett, vagy felfüggesztett (akár azért, mert az elkövető kiléte nem volt megállapítható).

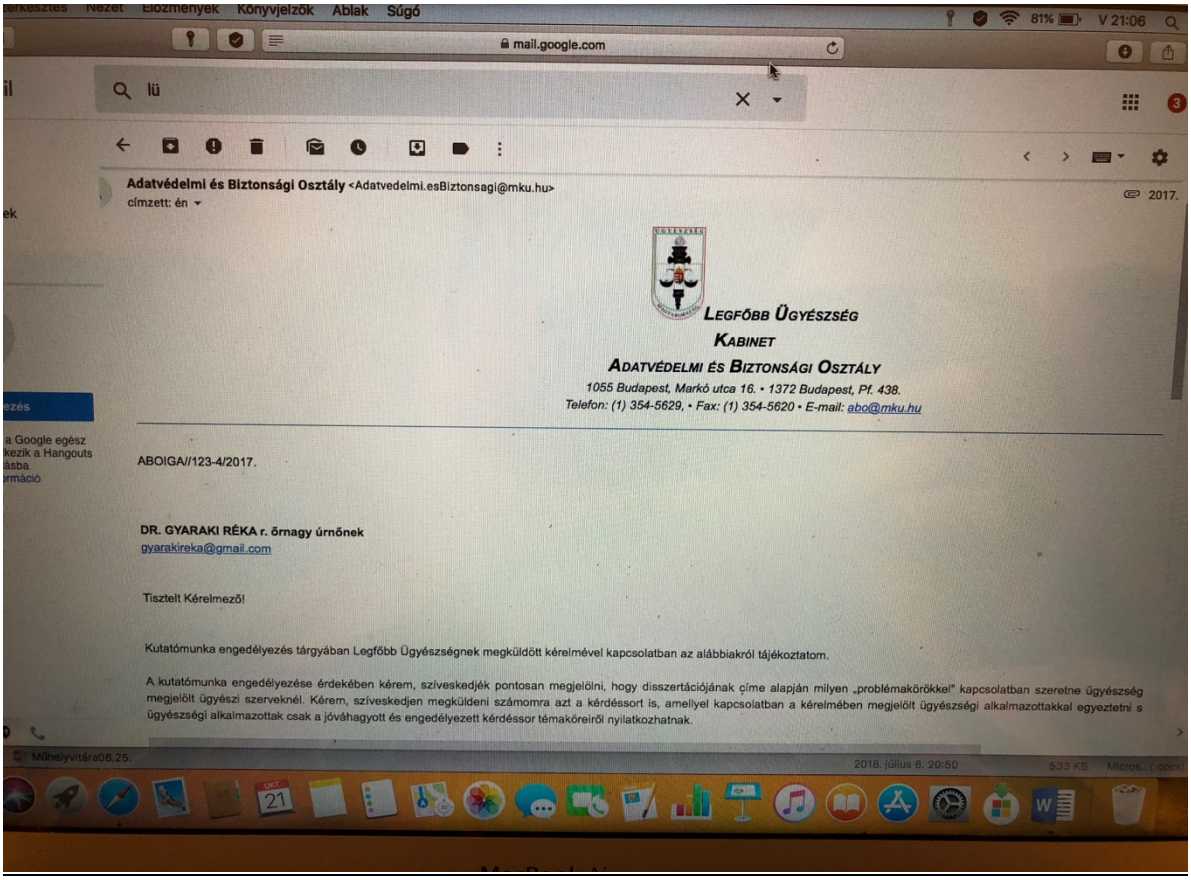
Nyilatkozom arról, hogy a kutatás során az ügyészségi iratanyagok adattartalmára tekintettel a Be. rendelkezésein túlmenően az Adatkezelési Szabályzat kiadásáról szóló 8/2012. (II. 16.) LÜ utasítás, illetve az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény személyes adatok megismerhetőségével kapcsolatos rendelkezéseit is betartom. Az ügyészségi iratanyagokból kizárólag anonimizált formában használhatom fel az adatokat , amely felhasználást az ügyészség belső adatvédelmi felelőse ellenőrizni fog és amely ellenőrzés után fogom a Pécsi Tudományegyetem Állam-és Jogtudományi Kar Doktori Iskolájába leadni.

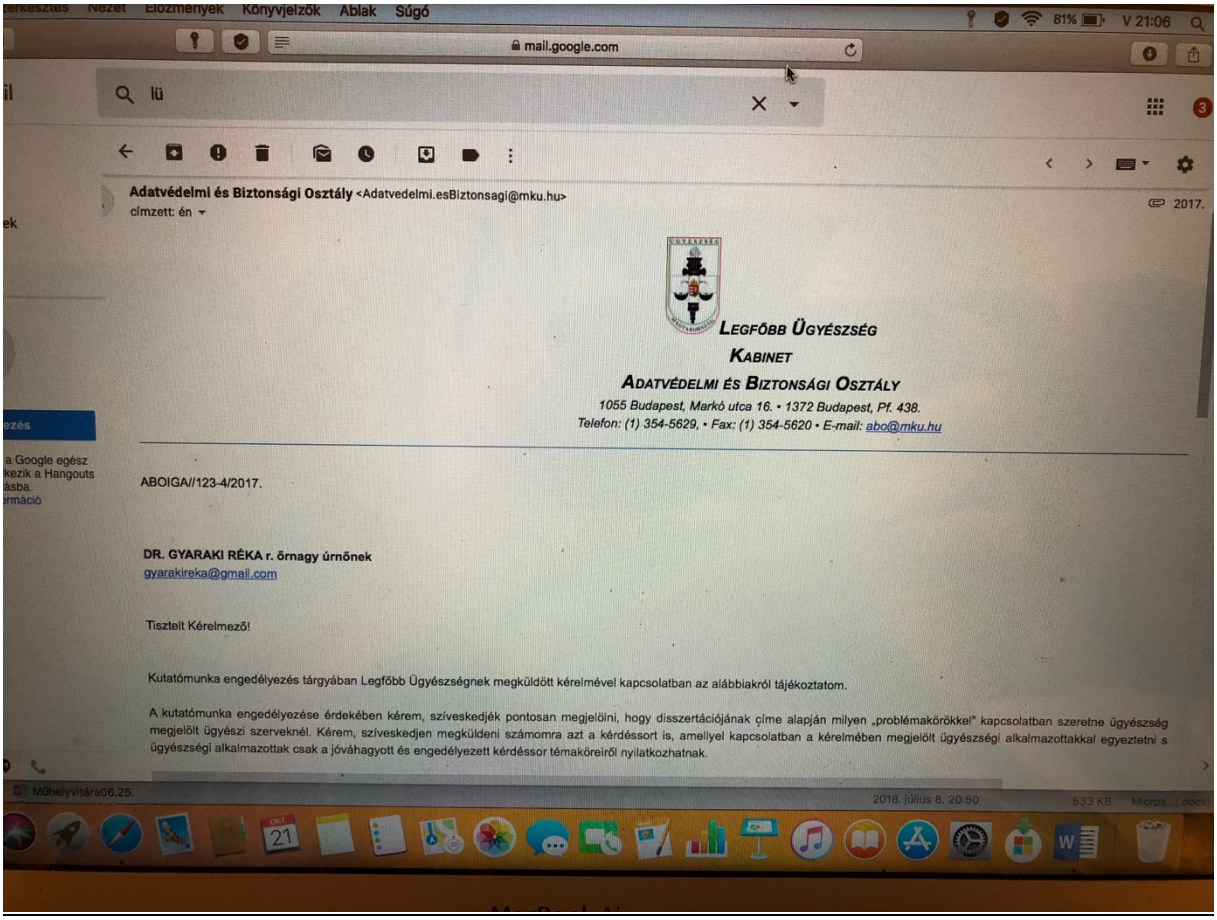
A fentiekre tekintettel a kutatásomat az adatvédelmi rendelkezésekre figyelemmel fogom végezni, illetőleg, hogy a tájékoztatóban – a fentieket- tudomásul vettem.

Budapest, 2017. augusztus 18.

dr. Gyaraki Réka r. őrnagy

egyetemi tanársegéd


Adatvédelmi és Biztonsági Osztály <Adatvedelmi.esBiztonsagi@mku.hu>
címzett: én
2017.
LEGFŐBB ÜGYÉSZSÉG
KABINET
ADATVÉDELMI ÉS BIZTONSÁGI OSZTÁLY
1055 Budapest, Markó utca 16. • 1372 Budapest, Pf. 438.
Telefon: (1) 354-5629, • Fax: (1) 354-5620 • E-mail: abo@mku.hu
ABOIGA//123-4/2017.
DR. GYARAKI RÉKA r. őrnagy úrnőnek
gyarakireka@gmail.com
Tisztelt Kérelmező!
Kutatómunka engedélyezés tárgyában Legfőbb Ügyészségnek megküldött kérelmével kapcsolatban az alábbiakról tájékoztatom.
A kutatómunka engedélyezése érdekében kérem, szíveskedjék pontosan megjelölni, hogy disszertációjának címe alapján milyen „problémakörökkel" kapcsolatban szeretne ügyészség megjelölt ügyészi szerveknél. Kérem, szíveskedjen megküldeni számomra azt a kérdéssort is, amellyel kapcsolatban a kérelmében megjelölt ügyészségi alkalmazottakkal egyeztetni s ügyészségi alkalmazottak csak a jóváhagyott és engedélyezett kérdéssor témaköreiről nyilatkozhatnak.


Adatvédelmi és Biztonsági Osztály <Adatvedelmi.esBiztonsagi@mku.hu>
címzett: én
2017.
LEGFŐBB ÜGYÉSZSÉG
KABINET
ADATVÉDELMI ÉS BIZTONSÁGI OSZTÁLY
1055 Budapest, Markó utca 16. • 1372 Budapest, Pf. 438.
Telefon: (1) 354-5629, • Fax: (1) 354-5620 • E-mail: abo@mku.hu
ABOIGA//123-4/2017.
DR. GYARAKI RÉKA r. őrnagy úrnőnek
gyarakireka@gmail.com
Tisztelt Kérelmező!
Kutatómunka engedélyezés tárgyában Legfőbb Ügyészségnek megküldött kérelmével kapcsolatban az alábbiakról tájékoztatom.
A kutatómunka engedélyezése érdekében kérem, szíveskedjék pontosan megjelölni, hogy disszertációjának címe alapján milyen „problémakörökkel" kapcsolatban szeretne ügyészség megjelölt ügyészi szerveknél. Kérem, szíveskedjen megküldeni számomra azt a kérdéssort is, amellyel kapcsolatban a kérelmében megjelölt ügyészségi alkalmazottakkal egyeztetni s ügyészségi alkalmazottak csak a jóváhagyott és engedélyezett kérdéssor témaköreiről nyilatkozhatnak.

A 7. fejezethez tartozó melléklet:

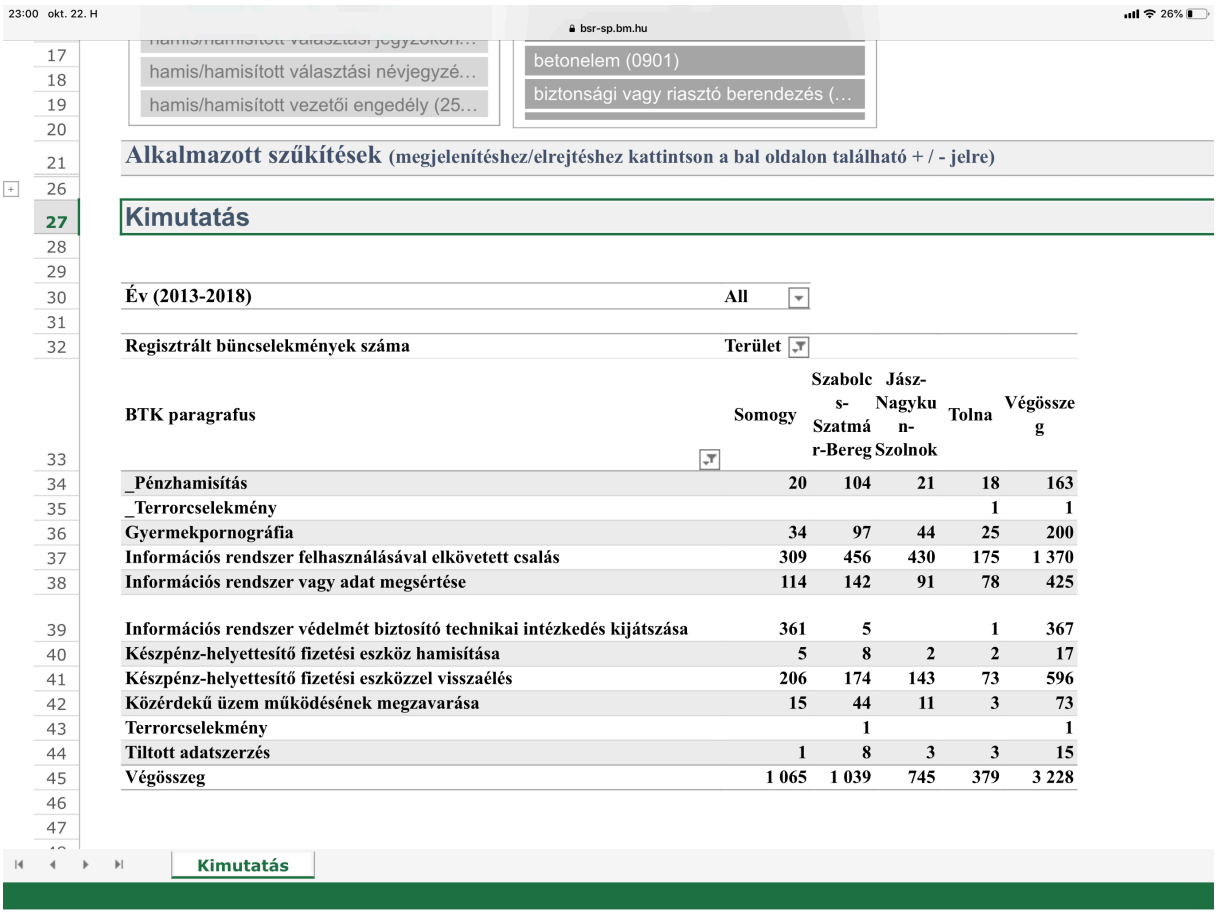
Igazságügyi szakértői szakterületek és az azokhoz kapcsolódó képesítési feltételek az informatikai területeken a 6. számú melléklet a 9/2006. (II. 27.) IM rendelet szerint:

Szakterület megnevezése	**Képesítési feltétel**
1.informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus vagy f) okleveles fizikus
2. informatikai biztonság	g) villamosmérnök vagy h) okleveles villamosmérnök vagy i) okleveles rendszerinformatikus vagy j) mérnök-informatikus vagy k) okleveles mérnök-informatikus vagy l) okleveles programtervező matematikus vagy m) okleveles fizikus vagy n) okleveles matematikus vagy o) okleveles alkalmazott matematikus vagy p) programozó matematikus
3. informatikai rendszerek tervezése, szervezése	q) villamosmérnök vagy r) okleveles villamosmérnök vagy

	s) okleveles rendszerinformatikus vagy t) mérnök-informatikus vagy u) okleveles mérnök-informatikus vagy v) programozó matematikus vagy w) okleveles programtervező matematikus vagy x) okleveles informatika szakos tanár vagy y) számítástechnika szakos tanár vagy z) informatikai szakirányon végzett okleveles gazdaság-informatikus vagy aa) okleveles fizikus vagy bb) okleveles matematikus vagy cc) okleveles alkalmazott matematikus
4. stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység	dd) villamosmérnök vagy ee) okleveles villamosmérnök vagy ff) okleveles rendszerinformatikus vagy gg) mérnök-informatikus vagy hh) okleveles mérnök-informatikus
5. számítástechnikai adatbázis, adatstruktúrák	a) villamosmérnök vagy b) okleveles villamosmérnök vagy c) okleveles rendszerinformatikus vagy d) mérnök-informatikus vagy e) okleveles mérnök-informatikus vagy

	f) okleveles programtervező matematikus vagy g) okleveles alkalmazott matematikus vagy h) okleveles matematikus vagy i) programozó matematikus vagy j) okleveles informatika szakos tanár vagy k) számítástechnika szakos tanár
6. szoftverek	a) programozó matematikus vagy b) okleveles programtervező matematikus vagy c) okleveles informatika szakos tanár vagy d) számítástechnika szakos tanár vagy e) informatikai szakirányon végzett okleveles gazdaság-informatikus vagy f) okleveles alkalmazott matematikus vagy g) okleveles gazdaságmatematikai elemző szakos közgazdász vagy h) okleveles mérnök-informatikus vagy i) mérnök-informatikus vagy j) okleveles matematikus vagy k) villamosmérnök vagy l) okleveles villamosmérnök

A 10. fejezettel összefüggő melléklet: az egyes számítógépes bűncselekmények számának alakulása megyénként és a fővárosban[327]:



23:00 okt. 22. H — bsr-sp.bm.hu — 26%

hamis/hamisított választási névjegyzé…
hamis/hamisított vezetői engedély (25…
betonelem (0901)
biztonsági vagy riasztó berendezés (…

Alkalmazott szűkítések (megjelenítéshez/elrejtéshez kattintson a bal oldalon található + / - jelre)

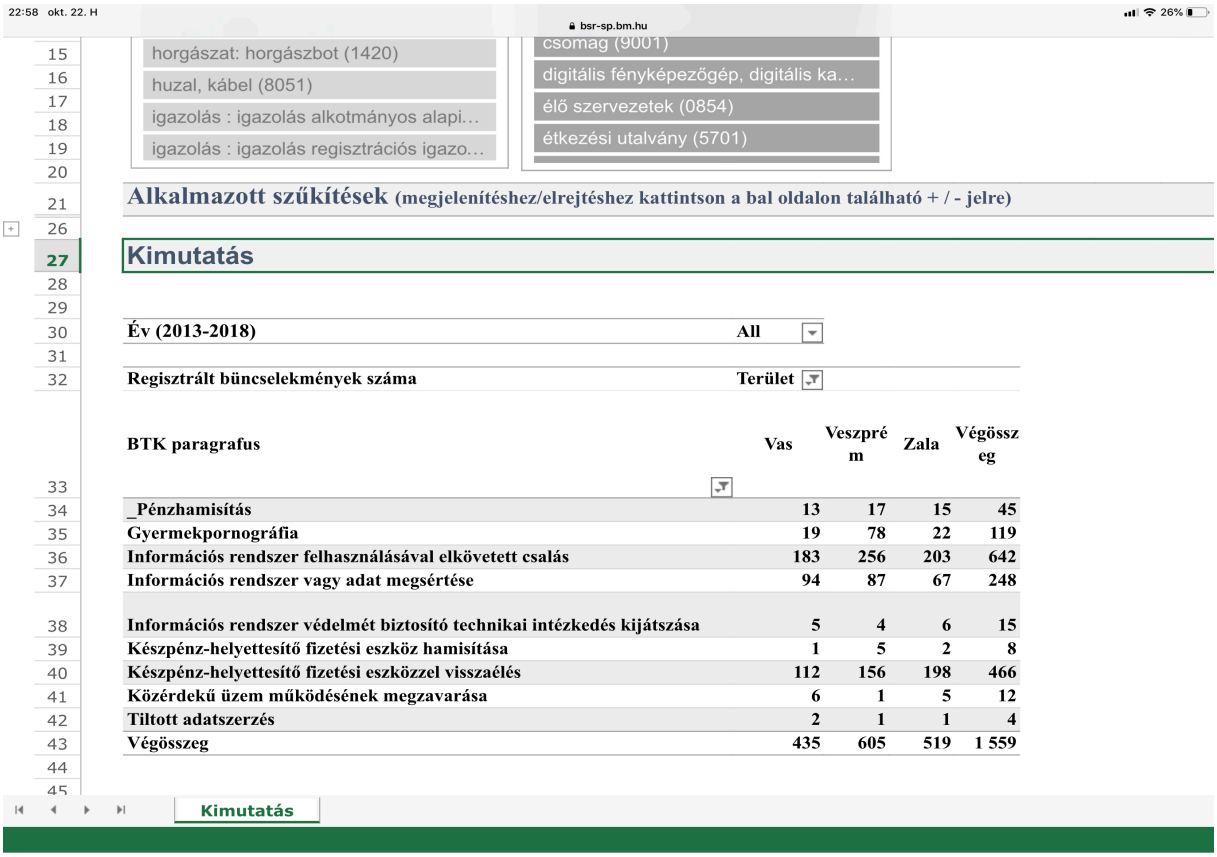
Kimutatás

Év (2013-2018) — **All**

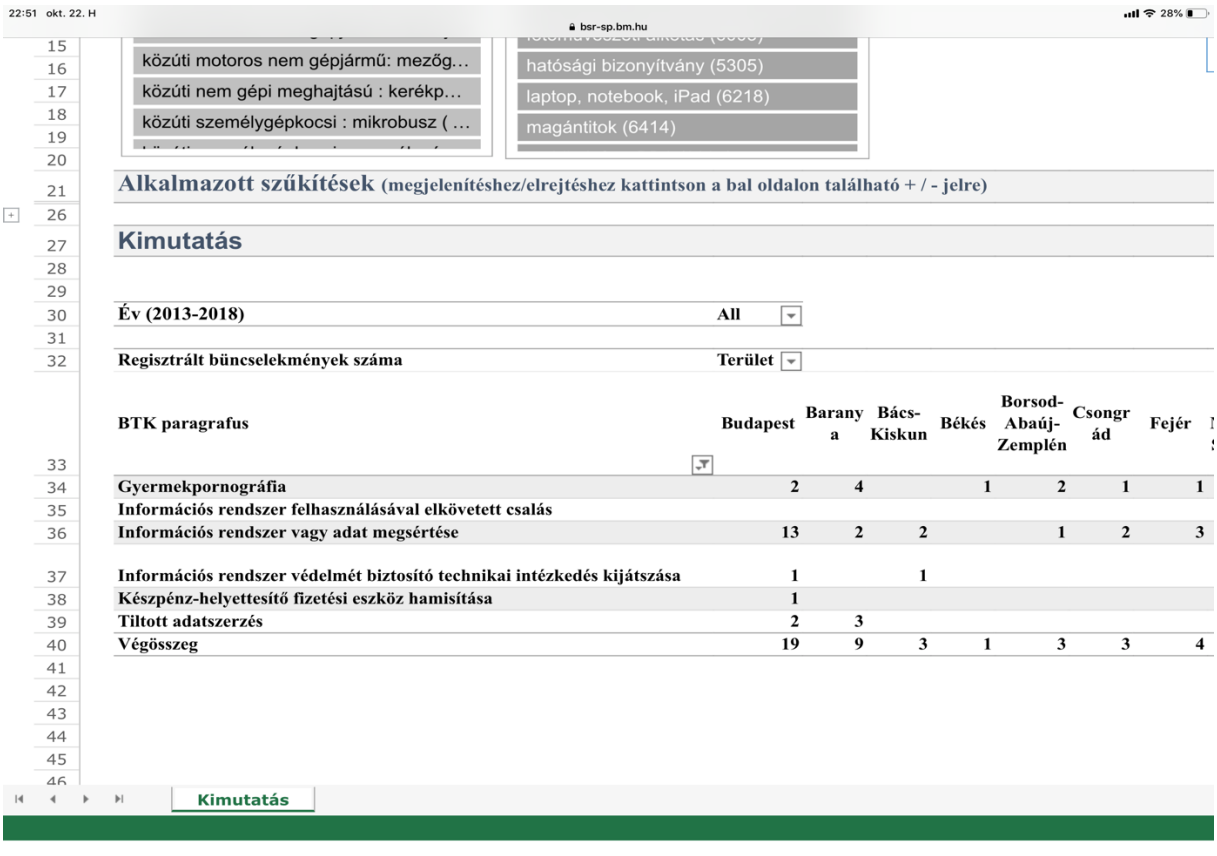
Regisztrált büncselekmények száma	Terület				
BTK paragrafus	**Somogy**	**Szabolcs-Szatmár-Bereg**	**Jász-Nagykun-Szolnok**	**Tolna**	**Végösszeg**
_Pénzhamisítás	20	104	21	18	163
_Terrorcselekmény				1	1
Gyermekpornográfia	34	97	44	25	200
Információs rendszer felhasználásával elkövetett csalás	309	456	430	175	1 370
Információs rendszer vagy adat megsértése	114	142	91	78	425
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	361	5		1	367
Készpénz-helyettesítő fizetési eszköz hamisítása	5	8	2	2	17
Készpénz-helyettesítő fizetési eszközzel visszaélés	206	174	143	73	596
Közérdekű üzem működésének megzavarása	15	44	11	3	73
Terrorcselekmény		1			1
Tiltott adatszerzés	1	8	3	3	15
Végösszeg	1 065	1 039	745	379	3 228

Kimutatás

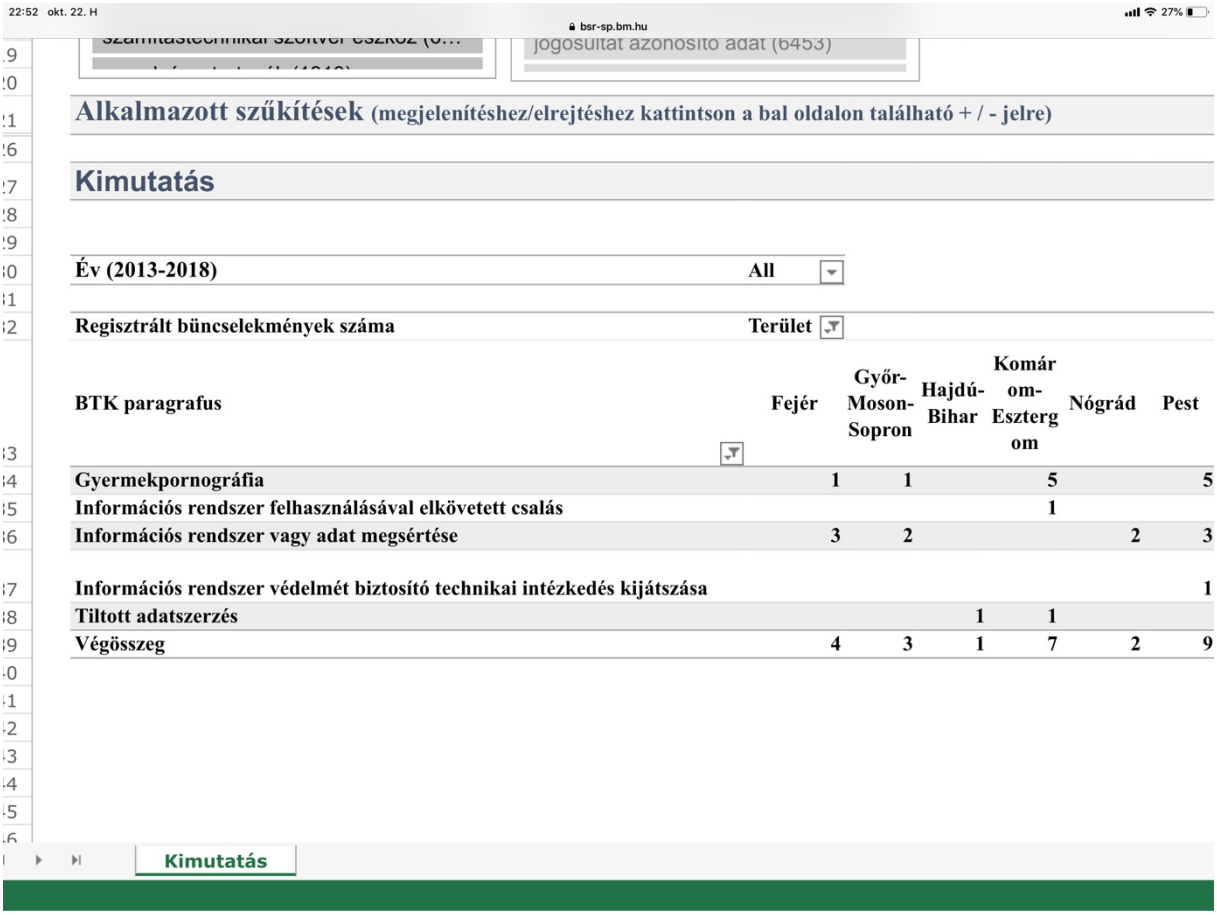
[327] https://bsr-sp.bm.hu/SitePages/ExcelMegtekinto.aspx?ExcelName=/BSRVIR/Regisztrált_büncselekmények száma az elkövetés helye szerint_ver20180713094758.xlsx&Token=UktIZ0dXUTFhMmpWdHRnWWFHVkRxWG8yQ1oyTmdvbC9zQTBTTEhTNk1WbUxlVGttL0UwVFdNaUxid3BlSUt5djE1MFJyQjJpT3d4NjFCck9qYTR4bkFUTlJNTjFDS0p6UUxDMmIwUHE0Z2MxNllDeWh2VnR1M3NiZm1Mb2cwL0o=



BTK paragrafus	Vas	Veszprém	Zala	Végösszeg
_Pénzhamisítás	13	17	15	45
Gyermekpornográfia	19	78	22	119
Információs rendszer felhasználásával elkövetett csalás	183	256	203	642
Információs rendszer vagy adat megsértése	94	87	67	248
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	5	4	6	15
Készpénz-helyettesítő fizetési eszköz hamisítása	1	5	2	8
Készpénz-helyettesítő fizetési eszközzel visszaélés	112	156	198	466
Közérdekű üzem működésének megzavarása	6	1	5	12
Tiltott adatszerzés	2	1	1	4
Végösszeg	435	605	519	1 559



BTK paragrafus	Budapest	Baranya	Bács-Kiskun	Békés	Borsod-Abaúj-Zemplén	Csongrád	Fejér
Gyermekpornográfia	2	4		1	2	1	1
Információs rendszer felhasználásával elkövetett csalás							
Információs rendszer vagy adat megsértése	13	2	2		1	2	3
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	1		1				
Készpénz-helyettesítő fizetési eszköz hamisítása	1						
Tiltott adatszerzés	2	3					
Végösszeg	19	9	3	1	3	3	4


22:52 okt. 22. H
bsr-sp.bm.hu
27%
jogosultat azonosító adat (6453)
Alkalmazott szűkítések (megjelenítéshez/elrejtéshez kattintson a bal oldalon található + / - jelre)
Kimutatás
Év (2013-2018)
All
Regisztrált büncselekmények száma
Terület
BTK paragrafus
Fejér
Győr-Moson-Sopron
Hajdú-Bihar
Komárom-Esztergom
Nógrád
Pest
Gyermekpornográfia 1 1 5 5
Információs rendszer felhasználásával elkövetett csalás 1
Információs rendszer vagy adat megsértése 3 2 2 3
Információs rendszer védelmét biztosító technikai intézkedés kijátszása 1
Tiltott adatszerzés 1 1
Végösszeg 4 3 1 7 2 9
Kimutatás