EÖTVÖS LORÁND TUDOMÁNYEGYETEM

ÁLLAM- ÉS JOGTUDOMÁNYI DOKTORI ISKOLA

KRIMINOLÓGIA DOKTORI PROGRAM

AZ INFORMATIKAI BŰNÖZÉS ÉS A BŰNELKÖVETŐVÉ VÁLÁS OKAI – A MAGYARORSZÁGI KIBERTÉR-FÜGGŐ BŰNÖZÉS KRIMINOLÓGIAI VIZSGÁLATA

DOKTORI ÉRTEKEZÉS TÉZISEI

VARGA Árpád

TÉMAVEZETŐK:

Dr. PARTI Katalin, egyetemi docens

Prof. Dr. LÉVAY Miklós, egyetemi tanár

DOKTORI ISKOLA VEZETŐJE:

Dr. NAGY Marianna, egyetemi tanár

Budapest

2023

Tartalomjegyzék

1. A doktori disszertáció célkitűzései

Az informatikai bűnözés kutatása a kriminológia egy új területe, amelyet az információs technológia körülbelül 1960-as évektől tartó töretlen fejlődése hívott életre. Az első igazán jelentős informatikai bűncselekmények már az 1980-es években nagy publicitást kaptak és az 1990-es évek végére társadalmi szinten is látható jelenséggé váltak, különösen az Egyesült Államokban[1], de már az Európa Tanács[2] és az OECD[3] is megkezdte az 1980-es évek végétől a terület feltérképezését. A 2000-es évek elejére megszülettek az első olyan dokumentumok, amelyek lehetővé tették és megalapozták az informatikai bűnözés elleni fellépést és büntetőjogalkotást Európában, így Magyarországon is.

A magyar kriminológia az időközben hazánkban is láthatóvá váló informatikai bűnözéssel azonban még ma is csak szórványosan foglalkozik. Többségében olyan munkák születtek a 2000-es évek elejétől – az informatikai bűnözés összetétele szempontjából helyesen –, amelyek az alacsonyabb belépési küszöbbel operáló és a társadalom szélesebb rétegét érintő bűnözést és áldozattá válást vizsgálják a kriminológiai elméletek figyelembevételével. Olyan kutatásokból azonban kifejezetten kevés van, amelyek a nagy tudásigényű és az információs rendszerek átfogó ismeretétől függő informatikai bűnözést vizsgálják. E területet hívja Marleen W. Kranenbarg[4] kibertér-függő bűnözésnek, Parti Katalin és Kiss Tibor számítástechnikai bűnözésnek[5], míg David S. Wall számítástechnikai rendszerek integritását sértő bűncselekményeknek[6].

A terület vizsgálatával nemzetközi szinten ugyan egyre többen foglalkoznak, hazánkban mégis hiány van azon kutatásokból, amelyek kifejezetten az ún. kártékony hackinget, vagy más néven a fekete zóna *„hacker”*-ei által elkövetett bűncselekményeket vizsgálnák.

A disszertáció és az ennek alapjául szolgáló kutatások célja tehát kettős volt: egyrészt a magyarországi kibertér-függő bűnözés általános jellemzőit és helyzetét összegezni képes feltáró kutatás elkészítése; másrészt azon mintázatok és hatások felderítése, amelyek az

[1] Majid YAR: *Cybercrime and Society*. SAGE Publications Ltd., 2006. 28.
[2] Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime https://rm.coe.int/09000016804f1094
[3] *Computer related crime: Analysis of legal policy*. Párizs, Organisation for Economic Co-operation and Development, 1986.
[4] Marleen W. KRANENBARG: *Cyber-offenders versus traditional offenders: An empirical comparison*. Netherlands, Vrije Universiteit, 2018. (Doctoral dissertation) https://research.vu.nl/en/publications/cyber-offenders-versus-traditional-offenders-an-empirical-compari
[5] KISS Tibor − PARTI Katalin: Informatikai bűnözés. In: BORBÍRÓ Andrea − GÖNCZÖL Katalin – KEREZSI Klára − LÉVAY Miklós (szerk.): *Kriminológia*. Budapest, Wolters Kluwer, 2016. 491–517.
[6] David S. WALL (szerk.): *Crime and the Internet: Cybercrimes and Cyberfears*. London, Routledge, 2001.

informatikai bűnelkövetővé válásban, illetve az abból való esetleges kilépésben szerepet játszanak.

A kutatás első feladatának megvalósításához szükséges volt egy feltáró jellegű kvantitatív aktakutatás elkészítése, amelynek célja a legjelentősebb hazai kibertér-függő bűncselekmények megismerése és az informatikai bűnelkövetők jelenlétének és tipikus elkövetési módszereinek felrajzolása. Az aktakutatás során a Budapesten található nyolc kerületi ügyészség 2013 és 2018 között indított 274 eljárásának áttekintésével lehetőségem nyílt a kibertér-függő elkövetés jelenlétének, főbb jellemzőinek és dinamikájának feltérképezésére.

A disszertáció a következő kutatási kérdések megválaszolására irányult:

1. Milyen az informatikai bűnözés karakterisztikája ma Magyarországon?
2. A budapesti kerületi ügyészségek aktáiban azonosíthatók-e a kibertér-függő bűnözés jellemzői?
3. Megjelennek-e gyanúsítottak vagy elkövetők a vizsgált informatikai bűncselkemények esetében?
4. Milyen információkkal rendelkezünk az informatikai bűncselekmények elkövetőire vonatkozóan és milyen informatikai készségekkel rendelkeznek?
5. Milyen problémák merülnek fel az informatikai bűncselekmények nyomozása során?

A kérdések megválaszolása nem büntetőjogi vizsgálatot igényelt, így az akták elemzése kifejezetten a kibertér-függő bűnözés kriminológiai sajátosságaira irányult és a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 375., 392., 394., 423. és 424.§-ainak vizsgálatát tartalmazta.

A disszertáció másik célja a kriminológiai elméletek mentén az informatikai bűnelkövetővé válás, a bűnelkövetői karrier jellemzőinek és az abból való esetleges kilépés okainak megismerése volt. Ehhez a megfelelő kriminológiai elméletek kiválasztása és részelemeinek összefűzése szükségeltetett.

Az elméleti keret tesztelése az elérhető, informatikai jogsértésben már érintett hackerek alacsony száma miatt egy hólabda módszeren alapuló félig strukturált mélyinterjús kutatás elkészítését tette szükségessé. E kvalitatív módszer lehetőséget biztosított a jogsértést elkövető hackerek életútjának részleges vizsgálatára, az informatika területéhez való viszonyulásuk feltárására, motivációik és attitűdjeik megismerésére. Az interjú-módszerű kutatás 2021 októbere és 2022 decembere között zajlott és mindösszesen 11, önbevallása alapján legalább valamilyen kisebb súlyú informatikai jogsértésben, kihágásban részt vevő hackerrel készült.

Ezt kiegészíti továbbá két, a 2014-es OTDK dolgozatomban[7] bűnelkövető hackerekkel készült interjúm újra elemzése is. Az interjúalanyok alacsony számának okát magyarázza többek között a hackerek nagyfokú bizalmatlansága és a területen uralkodó magas látencia.[8]

Az interjúkat az alábbi kutatási kérdések mentén készítettem:

1. Milyen informatikai bűncselekményekre találunk példát a hazai hackerközösségben?
2. A szakirodalomban fellelhető hacker fogalmak és csoportosítások milyen formában élnek Magyarországon és mennyiben fogadják el ezt a megkérdezettek?
3. Milyen törésvonalak vannak a jogszabályi környezet és a hackerek tevékenysége között?
4. Fellelhető-e összefüggés a családi minták, a kortársak attitűdjei, az online közösségek normái, a hacker tevékenység jutalmazási rendszere, valamint az informatikai bűnözéshez való viszony között? (Differenciális asszociáció-megerősítés[9])
5. A megkérdezettek által elkövetett, vagy vélhetően elkövetett jogsértések esetén felmerültek-e neutralizációs tényezők, így különösen a felelősség tagadása, a kár okozásának tagadása, vagy a magasabb értékekre hivatkozás? (Neutralizációelmélet[10])
6. A hazai hackerközösségben az informatikai jogsértések a fiatalkorra korlátozódó „szárnypróbálgatások" megnyilvánulásai vagy megfigyelhető a bűnelkövetői karrier kialakulása? Amennyiben igen, úgy vannak-e érzékelhető kilépési pontok a karrier során? (Életút elmélet)

2. A disszertációban bemutatott kutatások módszertana

2.1. Az informatikai bűnözés feltáró aktakutatásának módszertana

A disszertáció célul tűzte ki a hazai informatikai bűnözés legfontosabb jellemzőinek, csoportosítási lehetőségeinek és tudásigényének feltárását. A hazai informatikai bűnözés reális képének kialakítása érdekében szükségessé vált a regisztrált bűncselekmények áttekintése, ezen

[7] VARGA Árpád: *Számítástechnikai bűnözés és elkövetők – A bűnelkövetővé válás okainak és jellemzőinek vizsgálata*. OTDK dolgozat. 2014. (kézirat).
[8] Alice HUTCHINGS – Thomas J. HOLT: Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice & Criminology*, 7:1, 2018. 75-94.
[9] Robert L. BURGESS – Ronald L. AKERS: A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems*, 14:2, 1966. 128–147.
[10] Grasham M. SYKES – David MATZA: Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22:6, 1957. 664–670.

keresztül a szakirodalom segítségével kialakított bűnözéskép felülvizsgálata és kis részben a büntetőeljárások során tapasztalható anomáliák felkutatása.

A kutatás a 2013-2018. években indult ügyek egy részének elemzését tartalmazza. Az adatfelvétel területileg Budapestre korlátozódott, amely döntést az ügyek kriminálstatisztikai adatokban látható Budapestre koncentrálódása, másrészt az a feltételezés indokolta, hogy az informatikai bűnözésben érintett vállalatok, cégek, pénzintézetek és számos weboldal tárhelyszolgáltatója budapesti központtal rendelkezik, így azon célpontok, amelyeknél nagyobb a kibertér-függő elkövetés megjelenésének valószínűsége itt találhatók kiemelt számban. Ennek következtében a feltáró kutatás elvégzése szempontjából a reprezentativitás helyett az ilyen ügyek kiemelkedő számának elérése volt a cél. A budapesti ügyek kiválasztását indokolta továbbá az a tény is, hogy a 2016-tól kezdődően a kutatásban szereplő két legfontosabb tényállás, a Btk. 423. és a 424.§ alapján indított ügyek vitele a IX. kerületi ügyészség feladatává vált.

Az ügyészség által rendelkezésre bocsátott akták közül a Fővárosi Főügyészséggel kialakított megállapodás értelmében az összes 2013 és 2018 között a Btk. 423., 424., 392. és 394.§-ai alapján Budapesten vizsgált ügy áttekintésére lehetőségem nyílt. Míg a nagy ügyszám következtében a Btk. 375.§-ához kapcsolódó eljárások közül 10-10 akta rendelkezésre bocsátásáról szólt a megállapodás, amelyek kiválasztását az ügyészség munkatársai véletlenszerűen végezték. Az adatfelvétel során az első kutatási helyen bebizonyosodott, hogy a Btk. 423., 424., 392. és 394.§-ai alapján indított eljárások száma kifejezetten kevés. Ennek okán a kutatásra engedélyezett idő több akta áttekintését tette lehetővé más területen, így a Btk. 375.§-a alapján indított eljárások nagyobb számban kerültek a mintába.

A kutatás a Legfőbb Ügyészség támogatásával, a társadalomtudományokra vonatkozó Nemzetközi Statisztikai Intézet Szakmai Etikai Kódexében[11] szereplő alapelveket szem előtt tartva, a rendelkezésre bocsátott aktákban megjelenő személyes és szenzitív adatok védelmére vonatkozó jogszabályok betartásával készült.

Az adatfelvétel két időintervallumban zajlott: míg Budapest III., V. és XIII., VIII., IV és XV. Kerületi Ügyészségek aktáinak 2019. április 1. és május 31. között, addig Budapest VI-VII. IX., XI. és XXII., XIV. és XVI. Kerületi Ügyészségek aktáinak áttekintésére 2019. július 1. és

[11] Nemzetközi Statisztikai Intézet: *Szakmai Etikai Kódex.* 1985. https://www.ksh.hu/docs/files/404385.PDF

augusztus 31. között került sor. A nyolc kerületben összesen 274 büntetőeljárás elemzését végeztem el.

A kutatás során elsődleges szempont a cselekmények elkövetési magatartásainak és elkövetői jellemzőinek feltérképezése volt, így az csupán kis részben tartalmazza a büntetőeljárásra vonatkozó adatokat, míg a statisztikai adatelemzés nem képezte a kutatás szerves részét.

2.2. Az interjú-módszerű kvalitatív kutatás módszertana

A disszertáció részét képezte a hazai hacker közösség tudományos megismerése is. Ennek magyarázata, hogy önmagában az aktakutatás nem alkalmas a hazai informatikai elkövetők jellemzőinek feltárására, ezért alternatív megismerési módok alkalmazása is nélkülözhetetlen. A hacker közösség sajátos hozzáállása, világnézete és életútja félig strukturált, életút elemekkel tűzdelt mélyinterjúk elkészítését igényelte. A kutatás elsődleges célja a jogsértő magatartásokhoz vezető utak felrajzolása, a hackerré válók tanulási folyamatainak megismerése és a kiválasztott kriminológiai elméletek hazai alkalmazhatóságának tesztelése volt.

A kutatás bemeneti feltétele valamilyen olyan cselekmény elkövetése volt, amely az interjúalany feltételezése vagy a Btk. alapján bűncselekménynek minősülhet. E kritérium azt a célt szolgálta, hogy a kutatás alanyai csak olyan személyek legyenek, akik életük valamely szakaszában feltételezhetően elkövetettek büntetendő informatikai cselekményt.

A kutatás e kritériummal a szürke és fekete zónában tevékenykedő hackerek gondolatait, életútját, fontosabb tevékenységeit és dilemmáit kívánta feltérképezni. A felmérés elsősorban a hacking motivációinak, az életútbeli fordulópontoknak és a mintakövetés korlátozott vizsgálatára, valamint a tanulás és a neutralizáció egyes mozgatórugóinak feltárására alkalmas. A kutatásban a fókusz – az interjúalanyok preferenciái okán – jelentős részben a sérülékenységvizsgálat körüli erkölcsi dilemmákra helyeződött, a vagyon elleni informatikai bűnözés csupán helyenként jelent meg, gyakorlati tapasztalatok e téren az interjúalanyok kisebb részénél fordultak elő.

Az interjúalanyok elérésének lehetőségét szűkítette az a kritérium is, amely szerint a kutatásban csupán olyanok vehetnek részt, akik – saját meglátásuk szerint – a hétköznapi felhasználói szintet meghaladó tudással rendelkeznek. A kiválasztás során e tudás szubjektív önmeghatározására került hangsúly, így a részvevők maguk beszéltek tudásuk mértékéről és annak „átlagfelhasználói” szinttől való eltéréséről.

A kutatás legnehezebb részét az interjúalanyok elérése, azaz a rekrutáció jelentette. A területen gyakran alkalmazott hólabda módszerrel, vagyis azzal a feltételezéssel indult a keresés, hogy a kezdeti fázisban elért interjúalanyok saját ismeretségi körükből további ajánlásokkal segítik majd a kapcsolatfelvételt. A nemzetközi tapasztalatok alapján legalább 20 mélyinterjú elkészítését irányoztam elő. A hacker konferencián való részvétel, illetve az online fórumokon és chatszobákban való aktivitás azonban nem váltotta be a hozzá fűzött reményeket. Az adatfelvétel 2021. októbere és 2022. decembere között zajlott, amelynek során 11, informatikában jártas és legalább valamilyen kisebb jogsértést elkövető személlyel sikerült interjút készíteni. A megkeresések során világossá vált, hogy a résztvevők vonakodnak közreműködni a felhívás továbbadásában, vagy – a továbbadott információk alapján – az általuk megkeresett személyek a hatósági eljárás feltételezett veszélye miatt nem kívánnak részt venni a folyamatban. Ez az adatfelvételi időszakban tapasztalt hozzáállás megegyezik a Hutchings és Holt által végzett megfigyeléssel.[12]

A kutatás hasznosíthatóságának növelése érdekében két, a 2014-es Országos Tudományos Diákköri Konferenciára szánt és hasonló kutatási kérdések mentén lefolytatott interjú ismételt elemzésére is sor került, merítve a Jordan és Taylor[13] által egyszer már alkalmazott gyakorlatból. Ebben a korábbi kutatásban összesen 15 interjúalany megkérdezésére nyílt lehetőségem.

Az interjúalanyok kiválasztása során a fent ismertetett tudásbéli és jogsértések elkövetésére vonatkozó kritériumok mellett egyéb megkötés nem állt fenn, így demográfiai összetételüket tekintve az alanyok lehető legszélesebb körének kiválasztására adódott lehetőség. A kutatásban kilenc férfi és két nő szerepelt, életkorukat tekintve pedig a legfiatalabb megkérdezett 17 éves, míg a legidősebb 49 éves volt. A legalacsonyabb iskolai végzettséggel életkorából adódóan a 17 éves gimnazista interjúalany rendelkezett, legmagasabb iskolai végzettsége – így egyetemi mesterdiplomája – több megkérdezettnek is volt.

3. A disszertáció eredményei

3.1. Az informatikai bűnözés feltáró vizsgálatának eredményei

[12] HUTCHINGS–HOLT i.m.
[13] Tim JORDAN – Paul TAYLOR: A sociology of hackers. *The Editorial Board of The Sociological Review*, Oxford, 1998. 762–763.

Az aktakutatásban olyan hazai informatikai bűnözés képe rajzolódott ki, amelyben – legalábbis Budapesten – még máig az alacsony informatikai tudást igénylő cselekményeké a főszerep. Ez egyrészt azt jelenti, hogy a vizsgált öt tényállás alapján folytatott eljárások közül magasan az információs rendszer felhasználásával elkövetett csalás emelkedik ki, amelyek között elenyésző az „átlagos felhasználói tudást meghaladó" informatikai jogsértések száma. Az esetek túlnyomó többségében a lopott bankkártyákkal kapcsolatos készpénzfelvételek és eltulajdonított bankkártyákkal történő online vagy offline fizetések dominálnak. A budapesti akták emellett arra engednek következtetni, hogy az információs rendszer vagy adat megsértése tényállások alapján induló ügyek száma manapság meglehetősen kevés az összbűnözéshez mérten, és ezek módszere sem tekinthető a kriminológiai szakirodalom fogalomalkotása szerint a hétköznapi informatikai tudást meghaladó készségeket igénylő jogsértéseknek. A Btk 423.§-a alapján vizsgált és felderített ügyek körülbelül kétharmada valamilyen egyszerű jelszókifürkészéssel vagy korábban önkéntesen megadott jelszó felhasználásával kapcsolatos visszaélés. Az esetek további részében olyan külföldi kapcsolatokkal rendelkező nyomozásokkal találkozhatunk, amelyeknél az elkövető személyének ismerete hiányában szinte semmilyen információ nem áll rendelkezésre a hazai kibertér-függő informatikai bűnözés valós helyzetéről.

A jelszókifürkészéssel kapcsolatos ügyek, a sérülékenységek kihasználásának és a DDoS támadások hazai megjelenésének áttekintése a megfogalmazott öt kutatási kérdés tekintetében a következő eredményekre jutott:

- Magyarországon a budapesti ügyek körében láthatóan az e-mail címbe történő belépés és adatmódosítás, valamint ezen keresztül a közösségi média profilba történő belépés dominál.
- Az ilyen esetek körülbelül kétharmada laikusok által alkalmazott módszerekkel, így különösen a jelszavak korábbi megismerésével (pl. párkapcsolat idején) zajlik.
- A sértettek gyakran maguk adják meg belépési adataikat az elkövetőnek.
- A belépés oka általában valamilyen párkapcsolati vagy családi probléma, míg kisebb részben az e-mail címek felhasználásának célja valamilyen más, anyagi haszonszerzésre irányuló bűncselekmény elkövetésének előkészítése.
- A közösségi média profilba való belépést az e-mail fiókba történő behatolás előzi meg.
- Az ismertté vált jogosulatlan behatolással kapcsolatos cselekmények döntő többségükben nem igényeltek semmilyen informatikai tudást.

- A vizsgált 85 esetből mindössze 16 esetben (18,8%) merül fel egyértelműen az átlagos felhasználói szintet meghaladó informatikai tudást igénylő elkövetés, amelyből 11 eset a sérülékenységek kihasználásához, vagy túlterheléses támadásokhoz kötődik. Ezek körül mindössze három esetben történt meg az elkövető felelősségre vonása.
- Budapesten is találhatunk elszórtan példákat a szofisztikált kibertér-függő bűnözésre, ugyanakkor ezek elterjedtsége a vizsgált időszakban még nem volt jelentős, illetve felmerül a területen uralkodó alacsony feljelentési hajlandóság problémája.
- Azon esetekben, ahol az elkövető rendelkezik informatikai tudással, így valamilyen szoftvert használ, zombigépet vesz igénybe, vagy IP cím maszkolással megváltoztatja a belépés helyét a nyomozás elenyésző számban jár sikerrel.
- A nyomozóhatóság az e-mail szolgáltatók megkeresésén és az internetszolgáltatói adatkérésen keresztül próbálkozhat a cselekmény felderítésével, ugyanakkor az időmúlás, vagy a külföldi belépési hely valószínűtlenné teszi az eljárás sikerességét.

A kutatás annak ellenére, hogy kifejezetten az informatikai készségek megjelenésével foglalkozott a kibertér-függő elkövetés terén, azon cselekmények feltárására is irányult, amelyeknél az információs rendszerekkel való kapcsolat erős, illetve a jogalkotás leképezi e kapcsolatot. Ez az átfedés a kutatás alapkoncepciója szerint az információs rendszer felhasználásával elkövetett csalás esetén a legnagyobb. A kranenbargi értelemben vett csoportosításra gondolva e tényállás az, amely ugyan a kibertér-függő cselekmények körébe esik, tekintve, hogy az információs rendszerbe történő adatbevitel, adatmódosítás, törlés, vagy egyéb manipuláció segítségével történik meg az információs rendszer „tévedésbe ejtésén”, vagy „tévedésben tartásán” keresztül a kár okozása, mégsem egyértelmű az informatikai készségek szükségessége.

Az információs rendszer felhasználásával elkövetett csalás kutatásban vizsgált aktáinak tanulságai az öt kutatási kérdés fényében a következők:

- A vizsgált 174 ügy alapján a nyomozóhatóság által felderített információs rendszer felhasználásával elkövetett csalás esetei néhány kivételtől eltekintve nem kibertér-függő bűncselekmények.
- Az eredményesen és eredménytelenül záródó eseteket között is elenyésző azon elkövetési módszerek száma, amelyek az átlagos informatikai tudást meghaladó készségekről tanúskodnak.

- A felderítési sikeresség azon esetek tekintetében nagy, ahol az elkövetéshez nem társul semmilyen informatikai tudás, és fizikai módon eltulajdonított bankkártyák vagy bankkártya adatok felhasználásához kapcsolódik.
- A kibertér által elősegített bűncselekmények esetében magas azon esetek száma, ahol a sértett maga adja meg a pin kódot, vagy az elkövető a kártya mellett elhelyezve találja azt.
- Az esetek egy részében az elkövetők pin kód hiányában is megpróbálkoznak a kártyák használatával. E gyakorlat az online fizetések és a paypass segítségével történő vásárlásoknál fordul elő.
- A kibertér-függő bűnözés jeleit azon esetek hordozzák, ahol a bankkártyaadatokhoz online fizetés, külföldi vásárlás vagy kártékony szoftver segítségével jutottak.
- Az ilyen ügyek esetén ugyanakkor nem állnak rendelkezésre kimerítő adatok a bűncselekmények technológiai körülményeinek elemzéséhez.
- Az adathalászat szakirodalmi példáiból kiindulva azon esetekben merül fel az informatikai bűnöző aktivitás, ahol az adatok továbbítása és felhasználása külföldön történik.
- A külföldön elkövetett kibercsalások esetében a nyomozóhatóság tevékenysége egy esetben sem járt sikerrel.
- A budapesti kerületi ügyészségek által 2013 és 2018 között vizsgált esetek során egyetlen alkalommal merült fel olyan eset, ahol az elkövető rendelkezhetett az átlagos felhasználói tudást meghaladó készségekkel és személyét azonosították. Ebben az esetben az elkövető *script kiddie*-nek tekinthető.

Fontos megjegyezni, hogy a kranenbargi csoportosítás kriminológiai szempontból továbbra is megállja a helyét, ugyanakkor az nem esik egybe a büntetőjogi szabályozással, hiszen míg az információs rendszer vagy adat megsértése esetén ugyan a behatolás és egyéb jogsértések kibertér-függő cselekményeknek tekinthetők, az azokat elkövetők nagy többsége nem esik az informatikai bűnelkövető fogalma alá. Az információs rendszer felhasználásával elkövetett csalás tekintetében is arról van szó, hogy ezek nagy általánosságban a kibertér által elősegített cselekmények, ugyanakkor találunk olyan elkövetési módokat, ahol informatikai bűnelkövetők tevékenységére utaló jelek fedezhetők fel. Ennek következtében érdemes a cselekményeket kriminológiai szempontból az elkövetéshez szükséges tudás alapján megítélni és a kibertér-függő vagy kibertér által elősegített elkövetést e mentén megkülönböztetni.

Az alacsony esetszám okán a Btk. 424., 392., és 394. szakaszai kapcsán az öt kutatási kérdés tekintetében megalapozott konklúziók megfogalmazására nem volt lehetőség.

3.2. Az interjú-módszerű kvalitatív kutatás eredményei

Az interjú-módszerű kutatás elemzése során kirajzolódott, hogy az esetek túlnyomó többségében a hackerek körében a fiatalkorra korlátozódó és elsősorban a sérülékenységek feltárása köré csoportosuló jogsértések a jellemzők, de találhatunk szórványosan komolyabb, nagyobb társadalomra veszélyességgel fenyegető cselekményeket is. A többségnél e cselekmények a jogismeret növekedésével, az egyetemi tanulmányokkal és a hacker közösségek képlékeny etikai dilemmáinak letisztulásával kikoptak a fiatalok életéből. Ehhez képest kisebb részt képviseltek azok, akik ugyan tartózkodtak a súlyosabb cselekményektől, de olykor a pozitív megerősítés, és például az izgalom, önbíráskodás, vagy a segítségnyújtás szándéka mentén epizodikusan elkövettek kisebb-nagyobb kihágásokat, amelyek nem jutottak a hatóságok tudomására. Végül az életutak harmadik típusába tartoznak azok, akiknél a bűnelkövetést támogató definíciók és az informatika világának alternatív értelmezése, vegyülve a magánélet nehézségeiből eredő szükségletekkel a bűnelkövetés erősebb és hosszabban tartó megjelenését segítették elő. Ez esetben az látható, hogy a karrier hossza függ az egyén környezetétől és lehetőségeitől. A legális boldogulás, az informatikai tudás útjainak megtalálása, a hagyományos informatikai életpálya mellett szóló érvek és a stabil családi légkör pozitívumai ugyanis itt is a jogkövetés felé billenthetik a mérleg nyelvét.

Az életutak tekintetében az is látható, hogy míg Moffit elmélete[14] általánosan a fiatalkorra korlátozódó és az élethosszig tartó elkövetést különböztette meg, addig a kibertér-függő elkövetés esetében megjelenik egy harmadik életút, amely a jogsértéseket epizodikusan elkövetőket tömöríti. Esetükben két alcsoportról is beszélhetünk, amelyek a régi vágású hackerek és a kártékony hackingben inkább érdekelt „átcsúszó" hackerek alcsoportjai.

Kiemelve a két, felnőttkori elkövetéssel is járó csoportot, így az epizodikus jogsértőket és a karrier elkövetőket, az látható, hogy az epizodikus elkövetésnél, ha adott a jogsértést támogató pozitív megerősítés és a neutralizáció is felerősödik (különösen a magasabb értékekre hivatkozás és a felelősség tagadása), akkor megnő az elkövetésre való vállalkozás esélye. Ennek ellenére az informatikai szféra nagy jövedelmekkel és jó érvényesüléssel kecsegtető útjai a

[14] Terrie E. MOFFITT: Adolescence-Limited and Life-Coures-Persistent Antisocial Behavior: A Developmental Taxonomy. *Psychological Review*, 100:4, 1993. 685–694.

legális tevékenységek melletti stabil állásfoglalást teszik kifizetődőbbé, így nem beszélhetünk összefüggő elkövetői karrierről.

A karrierbűnözés esetén viszont az látható, hogy megjelenik a vagyon elleni informatikai bűnözés felé nyitás akkor, ha a társadalom felől, így például a családi életből, a szakmai közegből vagy az online kapcsolatokból nem származnak olyan pozitív élmények, amelyek a legális utakat tennék vonzóvá. Ilyenkor az érvényesülés eszközeként alternatívát jelent a bűnelkövetés. Így például két interjúalanynál az alternatív definíciók, az adatokkal való visszaélés normativitása és a legális karrierből való kiszorulás hatott erősen a bűnelkövetéssel kapcsolatos asszociáció-megerősítésre. Ezzel szemben a fiatal felnőttként elkövetői karriert folytató hackert a legális boldogulás útjainak megnyílása, a sikerekből következő pozitív élmények és a stabil családi élet lehetősége, így például a párkapcsolatból érkező támogatás a konvencionális fejlesztői pálya felé irányította, még akkor is, ha a bűnelkövetéssel kapcsolatos felelősségre vonás elmaradása és az anyagi hasznok segítették életének ezen szakaszában.

A tanuláselmélet tekintetében az látható, hogy a differenciális-asszociáció, a bűnözést támogató definíciók és a pozitív megerősítés is fontos szerepet játszik az informatikai jogsértések elkövetésében. Ezek ugyanakkor nem kifejezetten stabilak és az egyén nem is mindig közvetlenül érzékeli hatásukat. Így az esetek jó részében az informatikai szakterület egészének kusza erkölcsi és etikai szabályai közül olykor egyik, olykor másik narratíva kerül felszínre. Ez leginkább a differenciális asszociációnál és definícióknál jelenik meg azért, mert a rendelkezésre álló számos online információ és a mögötte lévő ideák miatt a hacker társadalom gyakran a jogilag aggályos cselekmények és a társadalmi jó közötti határvonalat nem tudja pontosan meghatározni. Ezért különösen fiatalkorban a tudásvágy, a szakmai érvényesülés és a kíváncsiság olyan cselekmények elfogadottságát is növeli, amelyek alapvetően büntetendők. Emellett a pozitív megerősítés is hol egyik, hogy másik típusú magatartás jutalmazását szolgálja, amelyet a cselekmények mögé helyezett, neutralizációt lehetővé tévő narratíva is támogat. Gyakran a támogató visszajelzéseket és a sikerélményeket követően így olyan cselekmények is vonzóvá válhatnak számukra, amelyek a későbbiekben erkölcsi dilemmákat, így például bűntudatot eredményeznek.

A disszertációban ismertetett elemzés és az életút kontextusában vizsgált két elmélet alkalmazhatósága tehát alátámasztható, de az kizárólag a kibertér-függő jogsértést elkövetők esetében érvényes. Az interjúalanyok életútjának jó azonosíthatósága és az általuk hosszan kifejtett, gyakran a saját informatikai közegükről alkotott véleményüket is felvonultató

beszélgetések, a szakirodalomban található és a disszertációban ismertetett kutatásokkal összehangban álló eredményt mutattak.

4. A disszertáció hasznosíthatóságának lehetőségei

A jelen disszertációban megfogalmazott eredmények összességében az informatikai bűnözés hazai összetételének elemzését és az informatikai elkövetővé válás okainak és folyamatának bemutatását szolgálták. Ennek ellenére a disszertáció mind az aktakutatás, mind pedig a mélyinterjús vizsgálat tapasztalataira építve fogalmazott meg olyan megállapításokat, amelyek az informatikai bűnözés további megismerésének alapjául szolgálnak. A disszertáció elősegítheti továbbá a bűnelkövetővé válás folyamatának értelmezését és ezen keresztül rávilágít azon belépési pontok helyére, amelyek a jogkövető magatartás elősegítésének lehetőségét hordozzák magukban.

A kutatás ugyan nem összpontosít a megelőzési lehetőségekre, abból a bizonyos megoldási irányok mégis kirajzolódnak. Mindenekelőtt látszik az oktatási rendszer, így különösen az informatikai oktatás átalakításának, kiegészítésének szükségessége. Ennek oka nem csupán az elkövetővé válás, így a neutralizáció és az alternatív értékekkel szembeni pozitív megerősítés kialakításának, hanem az áldozattá válás területén is fennálló tudatossági hiány leküzdésének igénye is. Az informatikai oktatás feladata így az informatika területén kialakuló jogtudatosság, a technológia mögött álló etikai, erkölcsi és jogi normák átadása lenne. E feladat a digitális kompetenciafejlesztés és bűnmegelőzés együttes erejével hathat az információs technológia „élővé" tételére. E terület fejlesztése elsősorban a kíváncsiság alapú, az érzelmi indíttatású és az anyagi haszonszerzésre irányuló elkövetés esetén gyakorolhat prevenciós hatást.

Ehhez kapcsolódóan – az interjúalanyok által elhangzottakat is figyelembe véve – javaslom az informatikai oktatás kiegészítését olyan szakkörrendszerrel és versenyekkel, amely nem csupán a programozói és kiberbiztonsági ismeretek, de az etikus hacking szabályrendszerének világos és jól körülhatárolt átadására is törekszik. Ezzel a legális érvényesülés és tanulás mellett a jogi normák által meghatározott definíciók átadására is lehetőség kínálkozhat. A hivatalos, akár kizárólag a fiataloknak szervezett versenyek jó kiugrási lehetőséget biztosíthatnak az érdeklődő, de helyüket nem találó fiatal hackerek számára.

A tanulás legalitásának kérdése felől közelítve a sokat emlegetett bug bounty programok hazai terjesztése, népszerűségük növelése és támogatása lehet jó megoldás. A fiatal hackerek e lehetőségekkel való megismertetése elősegítheti a hivatásos etikus hackerré válás során az engedély nélkül végzett sérülékenységvizsgálat kiiktatását. Ez különösen azért is fontos, mert az anyagi motivációt is képes kiiktatni a hackerek oldaláról, tekintve, hogy a kihívások magas haszonnal kecsegtetnek és a későbbi szakmai előmenetelt is elősegítik.

A joggyakorlat szempontjából az 5. fejezetben bővebben ismertetett, ENISA által támogatott Koordinált Sérülékenység Feltárási rendszer hazai átültetése és annak általános gyakorlattá tétele segíthet kialakítani egy, büntetőjogi oldalról is körülbástyázott hibafeltárási rendszert, az önkéntes, biztonságnövelést célzó tesztelés eszközével. Ez különösen a nagyvállalatok információs rendszereinek vizsgálata során a kártékony célok teljes hiánya mellett nyújthat védelmet a felelősségre vonás alól.

A nyomozóhatóságok oldaláról a probléma felszínre hozatalához hozzájárulhat a digitális kompetenciák oktatás keretein belül történő fejlesztése. Ennek pedig részét kell képeznie az áldozattá válás esetén a feljelentések szükségességének és a tudatos védekezési módoknak a hangsúlyozása.

Ez a gyakorlat ugyanakkor, a megfelelően hatékony felderítés nélkül valós eredmények elérésére alkalmatlan. Különösen a külföldi elkövetési helyű cselekmények esetén nemzetközi együttműködések kialakítására van szükség, annak érdekében, hogy az IP cím átirányításon keresztül, vagy egyéb módon elfedett cselekmények esetén is nyomozást folytathassanak a hatóságok. Enélkül ugyanis a kibertér-függő cselekmények továbbra is a hazai informatikai bűnözés rejtett formáját fogják képviselni.

Végül az IP cím lekérését akadályozó tényezők kiiktatása ugyancsak elengedhetetlen az állampolgári bizalom, így a feljelentési hajlandóság növelése érdekében. Ez különösen az aktakutatásban említett jogosulatlan behatolásokkal – kiemelten az egyszerű jelszókifürkészéses esetekkel – kapcsolatban jelenthet nagy előrelépést.

Összességében tehát a disszertáció rávilágít, hogy a tudatosítást képviselő oktatási szektor, a legális informatikai karrierek láthatóvá tétele és támogatása, valamint a konzekvens és megfelelő eszközökkel rendelkező nyomozóhatósági munka teremthet jó táptalajt a pozitív megerősítés és a jogszerűség mellett kialakuló definíciók rögzüléséhez a hackertársadalom egészében.

5. Publikációs jegyzék

VARGA Árpád: A számítógépes sütik és az adatgyűjtés problémája. In: Koltay András – Török Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején.* 4. kötet. Budapest, Wolters Kluwer, 2017. 233-263.

VARGA Árpád: Review of the Monograph on 'Information – Society – Security': Zsolt Haig: Információ – Társadalom – Biztonság. In: Marcel, Szabó – Petra, Lea Láncos – Réka, Varga (szerk.): *Hungarian Yearbook Of International Law And European Law 2016*. The Hague, Hollandia, Eleven International Publishing, 2017. 741–743.

VARGA Árpád: Médiaértés a médiajog és a kriminológia határán: a digitális technológia kihívásai. In: Fazekas Marianna (szerk.): *Jogi tanulmányok,* Budapest, 2018. 439–450.

VARGA Árpád: Koltay András - Török Bernát (szerk.): Sajtószabadság és médiajog a 21. század elején 3. Recenzió. Magyar Jog, 65:3, 2018. 188–192.

VARGA Árpád: A kiskorúak online aktivitásának kriminológiai értelmezése, különös tekintettel az állam és a szülők szerepére. *Belügyi Szemle, 66*:12, 2018. 98–119.

VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. *In Medias Res,* 8:1, 2019. 145–167.

VARGA Árpád: Informatikai bűnözés egy ügyészségi aktakutatás tükrében. In: Kiss Tibor (szerk.): *Kriminológiai Közlemények 80. 2020.* 125–135.

VARGA Árpád: Az adathalászat általános jellemzői, trendjei és észlelési kérdései napjainkban. *Infokommunikáció és Jog*, 74, 2020. 14–20.

VARGA Árpád: Kiss Tibor – Parti Katalin – Prazsák Gergő: Cyberdeviancia. Könyvismertető. *In Medias Res,* 9:1, 2020. 184–187.

VARGA Árpád: Kriminológiai elméletek és informatikai bűnözés. *In Medias Res*, 1, 2021. 155–196.