Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben

VARGA ÁRPÁD*

1. Bevezetés

Az infokommunikációs technológiákkal (a továbbiakban: IKT) kapcsolatos bűnözés a modern kor olyan problémája lett, amely egyaránt érinti a társadalmat, az üzleti szférát, az ipart és a nemzetbiztonságot. A technológia globalizálódása megnövelte a számítógépes bűnözés veszélyeit az internet által nyújtott anonimitás és a fokozott biztonságérzet következtében.[1] Megjelentek az online térben is értelmezhető devianciák, amelyekre a jog- és a társadalomtudomány területei folyamatosan reagálnak. A kriminológiai kutatások céljukként határozták meg többek között az IKT-hoz köthető bűnözés eddig még ismeretlen területeinek feltárását, az elkövetővé válás folyamatának megismerését, az áldozattá válás okainak kutatását és a bűnmegelőzés lehetőségeinek feltérképezését.

Jelen írásomban az IKT-kkal kapcsolatos bűnözésen belül az informatikához szorosan kötődő – köznyelvi megfogalmazással élve – hekkerbűnözéssel foglalkozom. Tanulmányom célja elsőként a releváns kriminológiai szakirodalomban alkalmazott hekkerfogalmak összegzése, majd segítségükkel saját kriminológiai definícióm megalkotása. Ezt követően az online kriminalitás csoportosítási módjainak összehasonlítására és a kriminológiai kutatásban leginkább alkalmazható, az online devianciák rendszerezésére alkalmas kategorizálás kiválasztására vállalkozom. E tekintetben cél, hogy a későbbi tudományos vizsgálódás elősegítése érdekében a megalkotott bűnelkövető fogalommal konvergáló csoportosítási módot ajánljak. Végül, a kriminológiai gondolkodást vegyítve a büntetőjog-fejlődés konkrétumaival, célom a magyar jogfejlődés áttekintésén és hazai bűneseteken keresztül annak bemutatása, hogy az általam meghatározott bűnelkövető fogalomba és a kiválasztott csoportosítási módba mely büntetőjogi tényállásokkal is leírható elkövetői magatartások tartozhatnak. A vizsgálódás legfőbb célja összességében a bűnözés e területéről egyes fogalmi, csoportosítási módok ajánlásával és a vizsgálandó bűncselekményi kör meghatározásával elősegíteni a Magyarországon ismertté vált informatikai bűnözés kriminológiai elemzését.

* Médiatudományi munkatárs, Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézet. E-mail: varga.arpad@mtmi.hu

[1] Katheryn C. Seigfried-Spellar – Kellyn N. Treadway: Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. 35(10) *Deviant Behavior* (2014) 782–803.

2. Nem minden hekker informatikai bűnelkövető, de minden informatikai bűnelkövető hekker? Esetleg egyik sem?

Az informatikai bűnözés kutatásának egyik kiindulópontja minden esetben az, hogy mely magatartásokat tekintünk ebbe a körbe tartozónak. Alapvetően amikor a komolyabb IKT-kkal kapcsolatos bűncselekményekre gondolunk, a hekkerek jutnak eszünkbe. Ennek oka elsősorban az, hogy az 1950-es évek végén megjelenő 'címke' az 1960-as évek informatikai fejlődésével és a kisebb súlyú informatikai bűncselekmények megjelenésével[2] kvázi átragadt az egyébként fejlesztői motivációjú, az informatika használatát propagáló hobbiinformatikusokról a bűnelkövetőkre.[3] A folyamat során a klasszikus (értsd: nem bűnelkövető) hekkerek igyekeztek e stigmát eltolni maguktól, így ragaszkodtak ahhoz, hogy a bűncselekményekben érdekelt és kártékony tevékenységet végző személyeket a cracker szóval illessék.[4]

A vita során elsőként merült fel annak kérdése, hogy a hekker (hacker) kifejezés használata megfelelően írja-e le az informatikai bűnözés ezen ágát, hiszen a legális keretek között tevékenykedő informatikai szakértőket, hobbihekkereket is a bűnözőkkel egy fogalom alá sorolta.[5] A kifejezés később a szakirodalomban vált széles körben alkalmazottá, a média és a társadalom mégis inkább megmaradt a hekker kifejezés használatánál.[6] A 'címke' így csak másodsorban vált a tudományos életben (például a kriminológiában) használt kifejezéssé, míg elsősorban a médiában, így a popkulturális alkotásokban (mint például a *Háborús játékok,* a *Drágán add az életed* vagy a *Johnny Mnemonic*) és a bűnözési hírekben propagált sztereotip kép határozza meg a fogalom elsődleges jelentéstartalmát egészen napjainkig.[7] Valójában a mérvadónak tekintett médiában megjelent anyagok szinte minden esetben az informatikai bűnözők és kiberbűnözés szinonimájaként használják a „hekker" („hacker") szót és a *„hacking"* kifejezést. Mi több, a hekkerek médiamegjelenése a misztikus és veszélyes informatikai bűnöző sztereotip képét erősíti a társadalomban.[8] Ennek eredményeként a hekkerek gyakran a kiberbűnözés révén a társadalomra leselkedő veszélyek szimbólumaivá válnak.[9]

[2] Thomas J. Holt – Adam M. Bossler – Katheryn C. Seigfried-Spellar: *Cybercrime and Digital Forensics: An Introduction*. London, Routledge, 2017. 738.

[3] Gráinne Kirwan – Andrew Power: *Cybercrime: The Psychology of Online Offenders.* Cambridge, Cambridge University Press, 2013. 280.

[4] Robert G. Morris – Ashley G. Blackburn: Cracking the Code: an Empirical Exploration of Social Learning Theory and Computer Crime. 32(1) *Journal of Crime and Justice* (2009) 1–34.

[5] Marcus Rogers – Natalie D. Smoak – Jia Liu: Self-Reported Deviant Computer Behavior: A Big-5, Moral Choice, and Manipulative Exploitive Behavior Analysis. *Deviant Behavior* (2005) 245–268.

[6] Michael Bachmann: *What Makes Them Click? Applying The Rational Choice Perspective To The Hacking Underground.* MA University of Mannheim, 2008. 229. (Doktori értekezés), https://stars.library.ucf.edu/etd/3790

[7] Hyung-Jin Woo: *The Hacker Mentality: Exploring The Relationship Between Psychological Variables and Hacking Activities*. Doktori értekezés, Athens, GA, UGA, 2003. 128.

[8] Bachmann i. m. (6. lj.); Majid Yar: Computer Hacking: Just Another Case of Juvenile Delinquency? 44(4) *The Howard Journal* (2005) 378–399.

[9] Kris Erickson – Philip N. Howard: A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records. 12(4) *Journal of Computer-Mediated Communication* (2007) 1229–1247.

A hekker fogalmának szakirodalmi ismertetésénél a kriminológusok alapvetően a hekkerek motivációiból, demográfiai jellemzőiből és pszichológiai személyiségképének felépítéséből indulnak ki. Ennek megfelelően lettek a hekkerek például „intellektuális kíváncsisággal megáldott, okos, tanulékony, agresszív, magabiztos, kockázatvállaló, [...] rosszul kommunikáló és vitázó személyek, akik elhivatottak a kibertér problémái iránt".[10] Emellett számos szerző a politikai véleménynyilvánításhoz való erős kötődésüket, a tudásvágyukat, az erőfitogtatást, a szubkulturális kapcsolataik fontosságát vagy éppen a magányos ténykedésüket tekinti a definíciójuk fő elemének.[11]

A hekker kifejezés értelmezése és tartalma nem egyértelmű a szakirodalomban, szemben az olyan kriminológiai fogalmakkal, mint a fehérgalléros bűnelkövető.[12] Annyi azért biztosan kijelenthető, hogy a fogalom kezdetekben olyan személyt jelentett, „aki megszállottja a számítógépes rendszerek megismerésének és megértésének".[13] Robert Taylor és munkatársai a kriminológiai vizsgálódás talaján a *hacking* jellemzően elfogadott fogalmát a számítógépbe való bűnelkövetési szándékú behatolásban és jogellenes használatában határozták meg,[14] ezzel szemben más kutatók a kezdeti közvélekedésre térnek vissza, vagyis szerintük a legmegfelelőbb azt mondani, hogy a „hekker" szó a „pozitív definiálása volt valakinek, aki képes elegáns, kreatív és hatékony megoldásokat találni technikai problémákra".[15]

Eredeti jelentésében a „hacker" név a tisztelet jele volt, amelyet az érdemelhetett ki, aki egy számítástechnikai programban a rövidebb utak, avagy *hack*ek létrehozásához kellő intelligenciával és szakértelemmel rendelkezett, azonban a fogalom az évek során negatív jelentéstartalmat kapott.[16] Bruce Schneier kiberbiztonsági szakértő 2000-ben szintén értéksemleges fogalmat alkotott: „a hekker olyan személy, aki – intellektuális kíváncsiságból vagy puszta élvezetből – a rendszerek korlátait próbálja felderíteni."[17] Ám az elmúlt évtizedekben a hekkerek

[10] Alexander E. Voiskounsky – Julia D. Babaeva – Olga V. Smyslova: Attitudes towards Computer Hacking in Russia. In: Douglas Thomas – Brian D Loader (szerk.): *Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age*. London, Routledge, 2000. 56–84.

[11] Catherine D. Marcum et alii: Hacking in High School: Cybercrime Perpetration by Juveniles. 35(7) *Deviant Behavior* (2014) 581–591.

[12] Edwin H. Sutherland: White-Collar Criminality. 5(1) *American Sociological Review* (1940) 1–12.

[13] Steven Levy: *Hackers: Heroes of the Computer Revolution*. Garden City, Doubleday, 1984.

[14] Robert E. Taylor et alii: *Digital Crime and Digital Terrorism*. Upper Saddle River, NJ, Pearson Prentice Hall, 2010. 368.

[15] Majid Yar: *Cybercrime and Society*. London, SAGE, 2006. 200.

[16] Seigfried-Spellar–Treadway i. m. (1. lj.). Christian S. Fötinger – Wolfgang Ziegler: *Understanding a Hacker's Mind: A Psychological Insight into the Hijacking of Identities.* RSA Security, Krems, Danube University, 2004; Bernadette H. Schell – Thomas J. Holt: A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders. In: Kuanchin Chen – Adam Fadlalla (szerk.): *Online Consumer Protection: Theories of Human Relativism*. Hershey, PA, Information Science Reference, 2009. 190–213.

[17] Bruce Schneier: *Secrets and Lies, Digital Security in a Networked World*. New York, Wiley and Sons, 2000; Parti Katalin: A számítógépes bűnözés és az internet. In: Irk Ferenc (szerk.): *Kriminológiai tanulmányok*. Budapest, Országos Kriminológiai Intézet, 2003. 179–204.

számának növekedésével és tevékenységük pluralizálódásával a megítélésük is folyamatosan változott. A kifejezés ma már komoly aggodalmakat kelt az új számítógépes technológiákban rejlő hatalommal való visszaélés szempontjából.[18]

A hekkerek kezdetben kíváncsiságon, innováción alapuló motivációját, sajátos demográfiai jellemzőit már az informatikai rendszerek társadalmi beágyazottsága és a bűnözés nagymértékű professzionalizálódása jelentősen erodálni kezdte. A fogalom valósághoz való viszonya, amely ma is a hekkerek bűnelkövetői címkézésének alapja, jelentősen eltér az alacsony védettségű rendszerekbe beleső, nagy kíváncsisággal megáldott, de ártalmatlan és jó szándékú informatikai szakértő képétől. Ma egészen más szempontok, motivációk és elkövetői attitűdök jelentik az informatikai bűnözés magját, a bűnözés azon szegmensét, amellyel a kriminológiának igazán foglalkoznia kell: a hekkerfogalmat a behatolás és a tudáskeresés puszta motivációjának elemzése helyett már az informatikai bűnelkövetői gyakorlatok valós társadalmi veszélyességgel rendelkező szegmensének vizsgálatával kell meghatározni.

Nem az informatikai kíváncsisággal megáldott fiatalok tettein keresztül kell a határmezsgyéket meghúznunk – a bűnelkövetés gyakori, általában a közvélemény elől rejtve maradó esetei alapján indokolttá vált egy új bűnelkövető-fogalom megalkotása. Elsődleges cél a hekker fogalmának lezárása, a média által kialakított és befolyásolt, erősen romantizált hekkerkép lebontása, a modern bűnelkövetés helyzetének meghatározása, továbbá az informatikai bűnelkövetők fő tevékenységeinek, motivációinak és demográfiai jellemzőinek feltérképezése, függetlenítve a korábbi hekkerdefinícióktól és a média által kreált hekkerképtől.

A változtatások lénye az, hogy az informatikai deliktumok[19] professzionális elkövetőire tekintsünk egyedi csoportként: e cselekmények elkövetőit jómagam „informatikai bűnelkövetőknek" hívom: az informatikai bűnelkövető olyan személy – utalva korábbi empirikus kutatásom tapasztalataira[20] –, aki számítástechnikai tudásának felhasználásával úgy követ el IKT-kkal kapcsolatos bűncselekményeket, hogy abban információ- és vagyonszerzési vagy károkozási motívum is megjelenik. Bűncselekményének legfontosabb mozzanata a rendszerbe való behatolás, az ezt megkönnyítő vagy egyéb – akár hagyományos bűncselekményhez használatos – program létrehozása, program vagy programegység megváltoztatása, funkcióinak átalakítása. Tevékenysége egyediségét erősíti, hogy cselekményének elkövetéséhez nélkülözhetetlen az átlagosnál fejlettebb informatikai tudás. E meghatározásból következik, hogy – Taylor és munkatársai meghatározásától eltérően, azt tiszteletben tartva – nem az IKT-rendszerekbe behatolókat (értelmezésemben ők a hekkerek) tekintem az egyetlen 'hardcore' informatikai jogsértőknek, így például tartózkodom az elkövetési magatartásoknak az információs rendszer vagy adat megsértése bűncselekményekre redukálásától.

[18] Gisle Hannemyr: *Technology and Pleasure: The Art and Craft of Hacking* (1999), http://hannemyr.com/en/sj98.html

[19] A kategória elemeit – követve a hatályos büntető törvényi meghatározást – l. a következő részben.

[20] Varga Árpád: *Számítástechnikai bűnözés és elkövetők – a bűnelkövetővé válás okainak és jellemzőinek vizsgálata*. OTDK-dolgozat, kézirat, 2014.

Az informatikai rendszerekkel kapcsolatos bűnözés számos területén felbukkannak elkövetők, akik magas szintű technikai ismereteik segítségével követnek el olyan bűncselekményeket, amelyek nem elsősorban a jogosulatlan behatolásban nyilvánulnak meg, illetve őket a köznyelv nem feltétlenül említi egy lapon a hekkerekkel: kódolók, program- és vírusírók stb., akik végső soron inkább informatikai elkövetői minőségükben jelennek meg a bűnözésben. E bűnelkövetők már nem hasonlíthatók össze Richard Tappan Morrisszal, John Draperrel, de már elhagyták a híres hekkereknek – az informatikai bűnözői lét határmezsgyéjén mozgó Kevin Mitnick és Kevin Poulsen által kitaposott – ösvényeit is.[21] Ide már egyértelműen a bűnelkövetők tartoznak, azok, akik egyrészt a felhasználói szintű tudást meghaladó informatikai készségeiket használják behatolásra, vírusírásra, másrészt valamilyen, a fizikai valóságban is értelmezhető (leggyakrabban vagyoni természetű) kárt, jelentős adatvesztést, illetve működési zavarokat is okoznak.

Fogalmam a rugalmassága, illetve a büntetőjogi tényállásokkal leírható természete miatt az informatikai bűnelkövetés kriminológiai racionalizálhatóságát és kutathatóságát növeli, továbbá lehetővé teszi a devianciaszociológiáról való leválasztást is, így elősegíti a büntetőjogi tényállásokban felfedezhető informatikai bűnözés előre meghatározott körének vizsgálatát és okainak keresését, megszüntetve az etikus és a bűnelkövető hekkerek közötti elválasztás nehézségeit. A fogalom mesterséges kritériumként szolgál az informatikai tudásukat visszaélésszerűen használók kriminológiai azonosításához.

E törekvés nem jelenti azt, hogy a különböző hekkertipológiák[22] megalkotása és alkalmazása felesleges lépés volna, csupán azt, hogy azok értelmezésemben elsősorban az informatikai bűnelkövetők motivációs hálójának, célrendszerének, személyiségének, demográfiai jellemzőinek leírására alkalmasak, ezért a későbbiekben az informatikai bűnelkövető jellemzőinek és bűnelkövetővé válásának vizsgálatához a bűnelkövető fogalom alá betagozódva nyújtanak segítséget (kérdéses ugyanis, hogy ha a tipológiák szerint nem minden hekker bűnelkövető, akkor hogyan beszélhetünk kriminológiai hekkertipológiáról).

Az informatikai bűnelkövető fogalmának (hasonlóan a fehérgalléros bűnelkövetőhöz), illetve a *hacking*hez való viszonyának kriminológiai pozicionálása és a releváns bűncselekményi kör meghatározása érdekében a következőkben csoportosítom az informatikai bűnözés formáit. Ennek során az informatikai bűnelkövetők tipikus bűnelkövetési magatartásainak elhelyezésére és a hagyományos vagy – ahogyan látni fogjuk – 'félhagyományos' formájától való leválasztására nyílik lehetőség. Ezt követően áttekintem az informatikai bűnözés hazai fejlődését, amely a jogfejlődés ismertetésével együtt ad biztosabb alapot a fejlett technológiai tudást igénylő informatikai bűnözés határainak meghúzásához.

[21] Bachmann i. m. (6. lj.).

[22] Pl. a black hat – grey hat – white hat, hacktivist – script kiddie – political or religious extremist megkülönböztetés. L. Rutger Leukfeldt – Wouter Stol (szerk.): *Cyber Safety: An Introduction*. Hága, Eleven International Publishing, 2012. Rogers hekkertaxonómiája pedig tartalmazza a *novice* vagy *newbie,* a *cyber punk,* az *internal,* a *petty thief,* az *old guard hacker*, a *virus writer* vagy *coder,* a *professional criminal,* az *information warrior* és a *political activist* kategóriákat. L. Marcus Rogers: A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy. 3 *Digital Investigation* (2006) 97–102.

3. Az infokommunikációs technológiákkal kapcsolatos bűnözés kriminológiai csoportosítása és fogalma

Az informatikai bűnözést vizsgáló kriminológus számára az első kihívást az új technológiák megjelenésének, a társadalom számára alapvetően hasznos szabadalmak elterjedésének és a bűnözés új mintázatainak összekapcsolása jelenti. Nyilvánvaló, hogy az IKT-k fejlődése és a bűncselekmények elkövetési magatartása, a konkrét bűncselekmények megvalósítása között valamiféle kapcsolat van – ennek tartalmára, arra, hogy bizonyos bűncselekményeket a technológiai fejlődés hívott-e életre, vagy csupán megkönnyítette a bűncselekmény elkövetését, számos elképzelés létezik, egyértelmű oksági magyarázattal szolgálni mégis nehéz.

A kriminológiai szakirodalomban ezt a polémiát a Peter Graboskytól[23] származó *„old wine in a new bottle"* dilemmával szokás felvezetni. Grabosky felveti a kérdést, hogy valójában beszélhetünk-e új, a technológiai fejlődés által megteremtett bűncselekményekről, vagy csak 'régi borról van szó új palackban', és a hagyományos bűncselekmények online térre átterjedésével állunk szemben.[24]

Az IKT-eszközök megjelenése és a bűnözés közötti kapcsolatot vizsgáló kriminológus és jogász közösség e kérdéssel már feltűnően régóta, az 1980-as évektől kezdve foglalkozik. Az IKT szerepének kérdése, bűnözésben való elhelyezése elsőként az Egyesült Államokban merült fel,[25] annak következtében, hogy az USA tekinthető az IKT, vagy legalábbis az internet bölcsőjének. Ugyanakkor a hazai jogi szakirodalomban is korán felvetődött már az új technológiai vívmányokhoz való hozzáállás kérdése.[26] Pontos rendszerezés a mai napig nem született, így számos bűnözésinterpretációval találkozunk, amelyek segíthetnek eligazodni a technológia és a bűnözés kapcsolatának definiálása során, örökérvényű választ mégsem nyújtanak.

3.1. Variációk az infokommunikációs technológiákkal kapcsolatos bűnelkövetés csoportosítására

Az új és a régi bűnelkövetés-felfogás közötti különbségeket és érveket hazai terepen Parti Katalin doktori disszertációjában – ugyan az online gyermekpornográfia kutatásához, az IKT-bűnözésre is érvényesen – foglalja össze a hagyományostól kissé eltérő módon.[27] Az IKT-bűnelkövetésről alkotott felfogást három részre osztja. Elkülöníti azokat a nézeteket, amelyek szerint az internet nem más, mint a tömegkommunikáció újabb megjelenési formája *('new bottle'),* ahol a problémák a régiek *('old wine').* E nézőpont szerint nem beszélhetünk új tör-

[23] Peter Grabosky: Virtual criminality: Old wine in new bottles? 10(2) *Social & Legal Studies* (2001) 243–249.

[24] Uo.

[25] Will Gragido – John Pirc: *Cybercrime and Espionage: An Analysis of Subversive Multi-vector Threats*. Burlington, Syngress, 2011. 272; Levy i. m. (13. lj.).

[26] L. Polt Péter: A számítógépes bűnözés. *Belügyi Szemle,* 1983/6., 60–64.

[27] Parti Katalin: *Gyermekpornográfia az interneten*. Miskolc, Bíbor, 2009. 373.

vényszerűségekről, csupán a folyamatok közege változott meg: a világháló közvetítő szerepben beágyazódott a hagyományos bűnözésbe.[28] Külön csoportot alkotnak azok a vélemények, amelyek szerint az internet olyan új közeg, amely „új bűncselekmény-, illetve devianciaformák, mint például a számítástechnikai rendszerekbe való behatolás vagy a spamtevékenység megjelenését tette lehetővé *('new wine, new bottles')*". E felfogásban a már meglévő veszélyek is olyan újabb veszélyforrásokat jelentenek az online térben, amelyekre a büntetőjognak mindenképp reagálnia kell.[29] Parti harmadik csoportja az a felfogás, amely szerint az internet új bűnözési formákat hozott létre, ugyanakkor ezek az internet közege nélkül is kifejlődtek volna. „Ezeknek a bűncselekményeknek az internet mint médium ad speciális formát és teret, de az internettől függetlenül, azon kívül is léteznek." David Wallt idézve Parti Katalin kutató jelzi, hogy ilyen bűncselekmény például – az egyébként a lanzarotei egyezményben[30] is megtalálható – fiktív személyeket ábrázoló obszcén vagy gyermekpornográf tartalmak készítése és megosztása is *('new wine, no bottles')*.[31]

Más csoportosítások afelé irányítanak, hogy elfogadjuk: az IKT-kkal kapcsolatos bűnelkövetés eltér a hagyományos bűncselekményektől. Ezek szerint a kérdés az, hogy mennyiben tekinthető az adott cselekmény egyedinek, így például elkövetési magatartásában is innovatívnak, és mennyiben beszélhetünk a hagyományos bűncselekmények informatikai térbe való áttevődéséről, átszivárgásáról. E csoportosítások abban különböznek az előző bekezdésben idézettől, hogy elfogadják az IKT-val való kapcsolatból eredő egyediséget (vagyis már semmiképp sem érvényes az *'old wine, new bottle'* felfogás). A cselekmény már csupán attól, hogy e közegben történik, nem lehet teljesen a korábbi értelemben vett bűncselekmény; 'félhagyományos': kvázi átmenetet képez a hagyományos kriminalitás és az IKT-val kapcsolatos bűnözés között (például e tekintetében a hagyományos csalás az interneten is része az IKT-bűnözésnek). E felfogás nyilvánvalóan az IKT-khoz immanensen kötődő, azok nélkül kivitelezhetetlen jogsértések körét is tartalmazza.

Marleen Weulen Kranenbarg szerint az IKT szerepét tekintve létezik kibertér által elősegített bűnözés *(cyber-enabled crime),*[32] illetve kibertérfüggő bűnözés *(cyber-dependent crime),*[33] azaz csoportosítása már egyértelműen a deviancia bizonyos szintű egyediségének, informatikai

[28] Uo.

[29] Uo.

[30] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. CETS No. 201. Lanzarote, 25/10/2007. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084822

[31] Parti i. m. (27. lj.).

[32] Máté István Zsolt az Interpol által használt csoportosítás leírásakor a fogalmat kapcsolódó kiberbűncselekménynek fordítja. Ennek ellenére, a kifejezés eredeti jelentését és szövegkörnyezetét tekintve, a tanulmányban olvasható fordítást preferáltam. Érdekesség, hogy az Interpol csoportosításának másik eleme Máté fordításában a „fejlett vagy csúcstechnológiás kiberbűncselekmények" *(advanced cybercrime)*, amely ugyancsak szemléletesen írja le a két bűnözéstípus közötti különbségeket. Máté István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. *Belügyi Szemle*, 2018/7–8., 36–54.

[33] A fogalmat az Europol az éves kiberbűnözési riportjában közel azonos jelentéstartalommal alkalmazza. Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

voltának talajáról indul.[34] Weulen Kranenbarg elősegített bűnözés alatt olyan hagyományos bűncselekményeket ért, amelyek elkövetésében az IKT valamilyen szerepet játszik: lehet csupán egy felület, működhet médiumként vagy közösségi területként. Ilyen cselekmények például az online csalás (amely nem azonos a hazai szabályozásban szereplő információs rendszer felhasználásával elkövetett csalással) vagy az online zaklatás, és idesorolható a rágalmazás, a becsületsértés internetes terjesztése és a gyermekpornográfia online terjesztése is. E 'félhagyományos' formától megkülönbözteti azon új, innovatív elkövetési módokat, a kibertérfüggő cselekményeket,[35] amelyek magát az IKT-t célozzák, és az IKT egyben kulcsszerepet is játszik azok végrehajtásában. Idetartozik Weulen Kranenbarg szerint a kártékony *hacking (malicious hacking),* a weboldalak felülírása *(web defacement),* az IKT-rendszerek feletti irányítás engedély nélküli átvétele, illetve a kártékony szoftver *(malware)* használata is.[36] Ezek a cselekmények egyértelműen a bűnözés olyan új formáit jelentik, amelyek az IKT nélkül ma nem létezhetnének – külön csoportosításuk alapja a technológia ismerete és professzionális használata.[37]

Parti korábban, a számítógépes bűnözés morfológiájának vizsgálatakor írt ehhez hasonlót: „az illegális áruk kereskedelme, a szoftver meg nem engedett másolása, a személyiségi jogokat károsító manőverek esetében az internet csupán egy, a technika fejlődésével megjelenő, újabb elkövetési eszköz, míg például a hackerek, crackerek tevékenysége hálófüggő, kizárólag az internethez kapcsolódó akció."[38] Ez az elkülönítés a hálózatokhoz való kötődés alapján differenciál, mégis hasonlít a Weulen Kranenbarg-féle elkülönítéshez, illetve az én elkövetőfogalmamhoz is, hiszen az IKT itt is mint opcionális felület, platform vagy az elkövetés egyik kizárólagos közege jut szerephez.

Az elkülönítés e módja talán a leghatékonyabb az IKT-kkal kapcsolatos bűnelkövetés kriminológiai aspektusainak vizsgálata során, ugyanakkor fontos megemlíteni, hogy a kibertér által elősegített kriminalitás esetén szinte lehetetlen meghatározni a cselekmények pontos és teljes körét. Ennek oka az, hogy egyéni kutatói mérlegelés kérdése, hogy mely cselekményeket tekintjük idetartozónak, tekintve hogy ma már a legtöbb bűncselekmény elkövethető az IKT felhasználásával, illetve elkövetésében szerepet játszanak az új technológiák, különösen az internet. Emiatt fontos a tényállási áttekintés, amely segít meghúzni a kibertérfüggő bűnözés vizsgálatának határait.

Az európai szakirodalomban emellett találhatunk egyéb, a hagyományos és IKT-közeget összekötő, a bűnözés egyediségét nem firtató tipológiákat is. Ilyen például a Rutger Leukfeldt és Wouter Stol szerkesztette átfogó monográfiában használt, David Wall által kialakított tipizá-

[34] Marleen Weulen Kranenbarg: *Cyber-offenders versus traditional offenders: An Empirical Comparison*. Vrije Universiteit. Doktori értekezés, 2018, http://dare.ubvu.vu.nl/bitstream/handle/1871/55530/complete disser tation.pdf?sequence=6&isAllowed=y

[35] A fogalom széles körű használhatóságát támasztja alá, hogy ezt használja az Europol kiberbűnözéssel foglalkozó központja, a European Cybercrime Centre (EC3) is. A szervezet által meghatározott, e körbe tartozó elkövetési magatartásokat l. az éves jelentésekben, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

[36] Weulen Kranenbarg i. m. (34. lj.).

[37] Weulen Kranenbarg kutatásában az ilyen tudással rendelkezőket az 'IT skill' változója alapján azonosította, amelynek felmérésére speciális kérdésmodult iktatott az általa használt kérdőívbe. Uo., 18., 94–101.

[38] Parti i. m. (17. lj.).

lási módszer.[39] Wall az IKT-kkal kapcsolatos bűnelkövetést, Weulen Kranenbargtól eltérően, nem két, hanem három részre osztotta: a számítógép, illetve számítástechnikai rendszerek integritását sértő bűncselekmények *(computer integrity crimes),* a számítógép segítségével megvalósított bűncselekmények *(computer assisted crimes)* és a számítógépes tartalom-bűncselekmények *(computer content crimes)* kategóriáira.[40]

A rendszerintegritást sértő bűncselekmények az elektronikus kommunikációs hálózatokat érintik, és célpontjukat a rendszer működésének biztosításához nélkülözhetetlen hardverek és szoftverek képezik. Wall szerint idesorolható a *hacking* (amely jelen esetben a jogosulatlan hozzáférést, behatolást és a hálózatok működésébe való beavatkozást jelenti), azon kártékony szoftver terjesztése, amelyek a rendszerek feletti irányítást képesek befolyásolni, és az úgynevezett túlterheléses támadások, amelyek az interneten keresztül képesek működésképtelenné tenni szolgáltatásokat.[41] Ezek a magatartások az IKT-k nélkül nem követhetők el.

Wall megkülönböztetésének második csoportja a számítógéppel támogatott bűnözés. Ennek nevéből is következik, hogy ez esetben a bűnözés hagyományos formáinak átdolgozásával, az IKT adta előnyök kiaknázásával létrejövő határterületen elhelyezkedő cselekményekről van szó. Wall szerint ennek leggyakoribb formája a csalás és a lopás, így ezek nagyrészt valamilyen anyagi előnyszerzést céloznak, de fontos megjegyezni, hogy irányulhatnak pusztán információ, adat megszerzésére, a szellemi termékek jogtalan eltulajdonítására és terjesztésére, vagy szexuális zaklatásra és egyéb abúzusokra is.[42]

A Wall-féle számítógépes tartalom-bűncselekményeknél a szólásszabadság korlátozhatósága kerül középpontba: ezek a cselekmények mintegy meghaladják annak legitim kereteit. Wall e kategóriája mutatja a legnagyobb államonkénti eltérést, hiszen kultúránként, alkotmányos berendezkedés szerint változik, hogy mit tekintünk tilalmazottnak. Ilyenek lehetnek az obszcén vagy erőszakos tartalmak terjesztése, a gyermekpornográfia, vagy például a vallási felekezetekkel, etnikumokkal stb. szembeni sértő megnyilvánulások.

Wall a bűncselekmények e hármas felosztása mellett az elkövetési magatartásokat osztályozta, természetük szerint négy kategóriába: engedély nélküli behatolás *(cyber-trespass),* számítógépes csalás és lopás *(cyber-deception and theft),* számítógépes pornográfia és szeméremsértés *(cyber-porn and obscenity),* valamint kibererőszak *(cyber-violence)*.[43] Az informatikai bűnelkövető általam korábban vázolt definíciója az engedély nélküli behatolás csoportjának felel meg. Wall nyomán Thomas Holt, Adam Bossler és Kathryn Seigfried-Spellar e kategóriába helyezték a hekkerek tipikus elkövetési magatartásait.[44] Ahogyan írják, itt a kapcsolat, a belépés jogosultsága válik kardinális kérdéssé, hiszen egyáltalán nem mindegy, hogy a kávézóba belépő számára van lehetőség az ottani nyílt wifihálózatot használni, vagy a vásárló az üzlet belső wifihálózatát feltörve tevékenykedik az interneten. A hekkerek egyik kedvelt és elsődleges célja a számítógé-

[39] Leukfeldt–Stol i. m. (22. lj.) 348.

[40] David S. Wall (szerk..): *Crime and the Internet: Cybercrimes and Cyberfears*. London, Routledge, 2001. 236.

[41] David S. Wall: *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge–Malden, MA, Polity, 2007. 288.

[42] Uo.

[43] Wall i. m. (40. lj.).

[44] Holt et al. i. m. (2. lj.). 22–26.

pekhez, e-mail-fiókokhoz vagy védett rendszerekhez való hozzáférés, vagyis egy általuk nem birtokolt belépési jogosultság kreálása, eltulajdonítása, a védelem kijátszása stb. Az engedély nélküli behatolás büntetendősége melletti érvként szolgál, hogy a *hacking* és a behatolás egyéb formáihoz általában számítógépes csalás és lopás is kapcsolódik. „Ez a kategória ugyanis tartalmazza az információk vagy egyéb javak illegális eltulajdonításának összes módját, ami általában együtt jár az engedély nélküli behatolással."[45]

A felosztásból az látszik, hogy Bossler és társai is azonosnak tekintik a *hackinget* az engedély nélküli behatolással, ami az informatikai bűnelkövető működési területének definiálása szempontjából hasznos számunkra. Ugyanakkor ki kell emelni, hogy a hagyományos eszközökkel eltulajdonított jelszó felhasználásával való behatolás is egyértelműen idetartozik. Fontos megjegyezni, hogy az informatikai bűnelkövető jellemzője, hogy belépése engedély nélkül és technológiai tudása felhasználásával történik. Ettől eltérő esetben, a pszichológiai manipuláció *(social engineering)*[46] Kevin Mitnick által megalkotott fogalmára gondolva, a hagyományos úton eltulajdonított azonosítókkal való belépést követően informatikai cselekményre – például a rendszer programkódjának módosítására – van szükség ahhoz, hogy a cselekmény elkövetője beilleszthető legyen az informatikai bűnelkövető kategóriájába. Ez azt jelenti, hogy a rendszerbe való behatolás hiába történik meg mindkét esetben, a súlyosság, a komplexitás és az elkövetői tudattartalom a folyamat eltérő kriminológiai értékelését igényli. A két cselekmény tényállásszerűsége (a hatályos Büntető Törvénykönyv szerint is)[47] ugyanaz, az elkövetés kriminológiai vizsgálatához nélkülözhetetlen az elkövetőben felfedezhető informatikai bűnelkövetésre jellemző készségek figyelembevétele. Ennek különösen a visszaesés és a cselekménnyel kapcsolatos neutralizáció csökkentése szempontjából lehet szerepe,[48] hiszen a látszólag bagatell bűncselekmények mögött eltérő célok és motiváció húzódhat meg. Az elkövető bűnözéshez vezető útja jelentősen eltérhet a laikus behatolóétól.

Vélhetően a tudományágban hosszúra nyúlt polémiának is következménye, hogy a 2001-ben Budapesten elfogadott Számítástechnikai bűnözésről szóló egyezmény[49] – amely az IKT-kkal kapcsolatos bűnelkövetés szabályozásának eddigi történetében talán a legismertebb dokumentum – nem kíván egységes definíciót alkotni az IKT és a bűnözés kapcsolatának leírására, és a tipizálására is csak korlátozottan, a jogalkotás elősegítése érdekében törekszik. Ellenben tartalmaz egy részletesebb, a büntetőjog-alkotás számára is adaptálható felsorolást, amely az IKT-kkal

[45] Uo., 22–23.

[46] E módszer a belépési kódokat, jelszavakat tulajdonló alkalmazottak kijátszásán alapuló, informatikai eszközök nélküli behatolást jelenti. A kifejezés nem azonos a „társadalmi mérnökösködés" mint szociológusi szerepfelfogással. Gragido–Pirc i. m. (25. lj.).

[47] 2012. évi C. törvény a Büntető Törvénykönyvről, 423. §.

[48] Gresham M. Sykes – David Matza: Techniques of Neutralization: A Theory of Delinquency. 22(6) *American Sociology Review* (1957) 664–670. A neutralizáció és az informatikai bűnözés kapcsolatának kriminológiai elemzését l. Joshua L. Smallridge – Jennifer R. Roberts: Crime Specific Neutralizations: An Empirical Examination of Four Types of Digital Piracy. 7(2) *International Journal of Cyber Criminology* (2013) 125–140., http://www.cybercrimejournal.com/smallridgerobertsijcc2013vol7issue2.pdf; Yi Ting Chua – Thomas J. Holt: A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. 11(4) *Victims and Offenders* (2016) 534–555.

[49] Az Európai Tanács Budapesten, 2001. november 23-án kelt, számítástechnikai bűnözésről szóló egyezménye. Convention on Cybercrime, CETS. No. 185.

kapcsolatos bűncselekményeket négy részre osztja: számítástechnikai rendszerek és számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekményekre, számítógéppel kapcsolatos bűncselekményekre, számítástechnikai adatok tartalmával kapcsolatos bűncselekményekre és szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekményekre.[50]

Összességében az előzőekben részletezett kriminológiai és egyezményi tipológiákból látható, hogy a legtöbb csoportalkotás között vannak átfedések, azok mégsem alkotnak egységes szemléletet. Ez azt jelenti, hogy egyrészt a büntetőjog-alkotás nem egységes tipológia alapján történik, ami hatással van a jogalkalmazásra, például az elkövetési magatartásukban hasonló jogesetek minősítésénél eltérések mutatkoznak, másrészt a kriminológiai elgondolások is eltérnek e kérdésben. E feloldhatatlan ellentét miatt az anyagi jogi célok és a társadalomtudományi gondolkodás nem képes szinergiában működni, hiszen csak egyes pontokon mutatnak hasonlóságot. Például az informatikai elkövetők kibertérfüggő bűncselekményei a büntetőjogi tényállásokon átívelő formában is megjelenhetnek, így – ha a hazai hekkertényállásra, az információs rendszer vagy adat megsértése bűncselekményre gondolunk – nem feltétlenül csupán egy tényállás alá tartoznak. Például egy készpénz-helyettesítő fizetőeszköz adatainak rögzítéséhez használt program létrehozása a kibertérfüggő bűncselekmény kategóriájába esik. Ehhez hozzátartozik az is, hogy az egyes tényállásokat megvalósító elkövetők és az elkövetési magatartásuk között nagyok az eltérések, és azok alapvetően határozzák meg az egyes büntetőeljárások során figyelembe veendő enyhítő vagy súlyosbító körülményeket.

Itt kell megemlíteni Nagy Zoltán András 2009-es monográfiájában[51] alkalmazott gyakorlatát is: e dilemmák kiküszöbölésére egyszerűen a számítógépes környezetben elkövetett bűncselekmények gyűjtőfogalmát használta. Az 1989-ben megjelent európai tanácsi ajánlásban szereplő *„computer-related crime"* kifejezést vette át,[52] amely a Weulen Kranenbarg kettéválasztott tipológiájába és a Wall hármas elkülönítésébe tartozó cselekményeket egyaránt tartalmazta. Nagy ezzel vizsgálódása alá vonta többek között a számítógépbe való jogosulatlan belépést *(hacking),* az elektronikus adatfeldolgozás és adatátvitel akadályozását, a számítógépes csalást, valamint olyan – Weulen Kranenbarg szavaival élve – kibertér által elősegített cselekményeket is, mint a hagyományos csalás számítógépes megfelelője, a fájlcsere (kalózkodás), a számítógépes zsarolás és a gyermekpornográfia, anélkül hogy vállalkozott volna ezek, illetve elkövetőik részletesebb csoportosítására.

Ennek ismeretében úgy gondolom, hogy nem is feltétlenül kell egységes tipológiát alkotnunk, érdemesebb inkább a különböző elkövetői magatartások kibertérfüggő jellege szerint áttekintenünk, hogy a hazai büntetőjogi fogalmak miként képesek e cselekményeket lefedni, illetve ezek hogyan jelennek meg a hazai jogirodalomban és kriminológiai gondolkodásban. A későbbi kriminológiai vizsgálódás elősegítése érdekében ki kell tehát derítenünk, hogy mely büntetőjogi tényállások, sőt mely konkrét események illeszthetők be a kibertérfüggő kriminalitás, vagyis az informatikai elkövetői magatartások közé.

[50] Uo.

[51] Nagy Zoltán András: *Bűncselekmények számítógépes környezetben*. Budapest, Ad Librum, 2009.

[52] Uo., 21–25.

Weulen Kranenberg csoportosításának használatakor abból indultam ki, hogy a kibertérfüggő kriminalitás indikátora az egyes bűncselekmények elkövetéséhez nélkülözhetetlen informatikai tudás, technológiai képesség, így e kategóriába csupán azokat a cselekményeket sorolom, amelyeknek ez a legelemibb része, ez az elkövetés legfontosabb tényezője, ebből pedig egyenesen következik, hogy a kibertérfüggő kriminalitás egyéb IKT-cselekményekről való leválasztása feltételének a technológiai tudás meglétét vagy nélkülözhetetlen alkalmazását tartom. Az egyes informatikai elkövetői magatartások e csoportosítása különösen fontos lehet a preventív gyakorlatok kialakítása során, hiszen a kibertérfüggő kriminalitás megítélésénél és kezelésénél számba kell vennünk az intellektuális bűnözéssel való kapcsolat meglétét is. A kiemelkedő technológiai ismeretekkel és képességekkel elkövetett cselekmények megítélése és az egyre növekvő IKT-specifikus jogsértések (a köznyelvben helytelenül hekkerbűncselekmények) elkövetőinek megismeréséhez és az elkövetővé válás megakadályozásához szükség van e cselekmények körének pontos meghatározására és értelmezésére.

A jövő folyamatainak megértéséhez fontos látnunk, hogy az IKT-kkal kapcsolatos bűnelkövetés két részre szakadhat: egyrészt tovább terjednek azok a tömeghasználathoz köthető jogsértések, amelyek elsősorban a kibertér által elősegített cselekményeket erősítik, és az egyre növekvő internetpenetrációval általános jelenséggé válnak, másrészt megjelenik a bűnözés még specializáltabb, tudásalapú szegmense. Ez utóbbi a kibertérfüggő kriminalitás részeként egyre nagyobb volumenű biztonsági, anyagi és társadalmi problémát fog jelenteni, illetve jelent már ma is.[53]

4. A kibertérfüggő bűncselekmények elkövetőinek helye a magyar jogban és a kriminológiában

Az IKT-kkal kapcsolatos bűncselekmények megjelenésének pontos idejét hazánkban – és másutt is – szinte lehetetlen megállapítani. Ennek első kutatói dokumentumait Polt Péter,[54] valamint Pusztai László írta, aki egyebek mellett az akkor még internethez nem köthető, de már számítógépes jogsértések megjelenéséről, illetve az NSZK büntetőjogi reformjáról értekezett.[55] Később egyre többen kezdtek foglalkozni a témával, köztük az 1990-es évektől Nagy Zoltán András, és részben az online tér szabályozási kérdésein keresztül Balogh Zsolt György,[56] majd a 2000-es években, ahogyan az internet tömeges használata is egyre nyilvánvalóbb problémákat kezdett felvetni, a jogi, kriminológiai kutatás – Parti Katalinnal az élén – egyre általánosabbá vált.

[53] Erre kiváló példa a közelgő európai parlamenti választás során fokozódó igény a dezinformáció csökkentésére, ami vonatkozik a botnetekre és az egyéb automatizált algoritmusokra is. E cselekmények mögött igen gyakran informatikai bűnelkövetők állnak.

[54] Polt i. m. (26. lj.).

[55] Pusztai László: Komputerbűnözés és büntetőjogi reform az NSZK-ban. *Magyar Jog,* 1987/11., 959.

[56] L. pl. Balogh Zsolt György: *Jogi informatika*. Budapest–Pécs, Dialóg Campus, 1998. 386.

4.1. IKT-bűnözés és csoportosítási kísérletek a számítógépek hőskorában

Az 1980-as években zajló kutatások kezdetben a német és részben, de inkább csak áttételesen az angolszász jogterület – ahogyan akkor hívták – számítógépes bűnözéssel kapcsolatos vívmányait elemezték, és annak átvételéről értekeztek. Ezen írások abban jelentettek újítást, hogy leginkább a szoftverek mint elkövetési tárgyak köré szerveződtek, és az informatikai rendszerekre nem mint fizikai tárgyakra, hanem sokkal inkább mint adathalmazokra kezdtek tekinteni.[57] Érdemes megvizsgálni, hogy milyen jogsértések indították el a gondolkodást és a jogfejlődést e területen.

Tekintve, hogy az 1978. évi Büntető Törvénykönyv egészen 1994-ig nem tartalmazott a ma ismert infokommunikációs technológiákkal kapcsolatos tényállásokat, a terület feltérképezése az egyes jogsértések minősítési problémáinak realizálódása, valamint a masszív technológiai fejlődés hatására kezdődött. E cselekményekről Nagy hozott kiváló példákat: 2009-ben megjelent monográfiájában számos rendszerváltás előtti esetet sorol fel az új típusú bűnözés köréből.[58] A kibertérfüggő cselekmények elhelyezésénél azonban a legfontosabb számunka az, hogy ebben az időben mind Pusztai, mind Nagy négy fő típusát különböztette meg a számítógépes bűnözésnek: a komputermanipulációt, a számítógép-kikémlelést, a számítógépes szabotázst, valamint a gépidőlopást.[59]

Ezek közül az első kettő, ha megnézzük a szerzők definícióit a duális besorolás tekintetében, nem feltétlenül tekinthetők a kibertérfüggő bűncselekmények részének, hiszen azok elsősorban valamely szoftver károkozás céljából való felhasználását vagy az adatok megváltoztatását tartalmazták, így csupán felhasználói szintű ismereteket igényeltek. Emellett a számítógépes szabotázs – „amely az adatfeldolgozási folyamatnak a gép sérelmével nem járó, anyagi haszonszerzési céllal való jogellenes akadályozása volt"[60] – is mindkét módon megvalósulhatott: lehetett valamilyen szoftver létrehozása, amelynek funkciója az adatok hozzáférhetetlenné tétele vagy egy egyszerű törlés véghezvitele volt. A számítógépes bűnözés típusainak e kezdeti szétválasztásából érződik, hogy az internettől és a társadalmi felhasználástól még igen messze állt a fejlődés, ugyanakkor már itt is látható, hogy a laikus használat és az informatikai tudás felhasználásával való elkövetés értékelése nem jelent meg az elválasztásban. Összegezve, ez az NSZK-ból származó elkövetői csoportosítás nem volt képes konvergálni a bűncselekmények elkövetési magatartása szerinti csoportosítással.

[57] Ezt megelőzően a számítógépekkel kapcsolatos bűncselekmények még az eszközök rongálásában, eltulajdonításában, csempészetében stb. merültek ki. Michel E. Kabay: *A Brief History of Computer Crime: An Introduction for Students.* Norwich, M. E. Kabay, 2008.

[58] L. Nagy i. m. (51. lj.).

[59] Nagy kötetében a négy egység neve némileg megváltozott, de jelentésük hasonló maradt. Pusztai László: Számítógép és bűnözés. In: Gödöny József (szerk.): *Kriminológiai és kriminalisztikai tanulmányok XXVI*. Budapest, Közgazdasági és Jogi Könyvkiadó, 1989. 85–145. A felosztás alapvetően A. Girginov nevéhez fűződik, amelyet az európai tipológiaalkotás is átvett. L. Girginov, A.: Elektronikus számítógépek és a büntetőjog. *Magyar Jog,* 1986/12., 1063–1067.

[60] Parti Katalin – Kiss Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin (szerk.): *Pusztai László emlékére*. Budapest, OKRI–ELTE ÁJK, 2014. 297–310.

Részletesebben áttekintve a legkorábbi tipológiákat, azt láthatjuk, hogy a Pusztai által megfogalmazott komputermanipuláció akár tartozhatna is a speciális tudást jelentő cselekmények közé, az ugyanis az „adatfeldolgozási folyamat eredményének jogtalan befolyásolása a program helytelen kialakításával, a program lefutásának megváltoztatásával vagy helytelen, illetve hiányos, optikailag közvetlenül le nem olvasható adatok létrehozásával, illetve alkalmazásával, abból a célból, hogy a beavatkozó saját magának vagy egy harmadik félnek vagyoni előnyt biztosítson".[61] A cselekményre olyan példákat találunk, mint a hamis lyukkártyák előállítása, és ezáltal családi pótlékok jogszerűtlen kiutalása, vagy a tized pfennigek kerekítésével elkövetett csalás.[62] A kibertérfüggő bűncselekmények körül határolásában talán ez a két, az 1980-as évek NSZK-jából származó példa a legkiválóbb kiindulópont, mert a korai szakirodalmat olvasva úgy tűnik, a lyukkártya hamisítása valójában egyfajta okirat-hamisítás volt, és elkövetéséhez nem a hivatalnok kifejezett számítógépes ismerete, technikai tudása vezetett, hanem inkább a családi pótlékok kiutalási folyamatának ismerete és a lyukkártyák létrehozására való lehetőség.[63] Fontos, hogy itt ugyan beszélhetünk fehérgalléros elkövetőről, sőt esetleg még kibertér által elősegített bűncselekményről is (ugyanis a lyukkártyák hamisítása csak megfelelő technológiai eszközzel kivitelezhető), nem látunk az adatfeldolgozásba való olyan beavatkozást, amelyhez különösebb technológiai képesség szükségeltetik, vagyis az informatikai elkövető fogalmába, illetve Weulen Kranenbarg tipológiájába a lyukkártya hamisítása nem fér bele.

Ezzel ellentétben a komputermanipulációba tartozó másik eset, amely az adatfeldolgozási szakaszban végrehajtott változtatásokat jelentett, már egyértelműen a tudásalapú informatikai bűnözést takarta. Pusztai példája szerint a kerekítési trükk néven elhíresült manipulációt egy müncheni bank kamatszámoló szoftverének létrehozásával megbízott programozó követte el úgy, hogy már a program megírásakor utasította a rendszert a maradék összegek egy titkos számlán való összegyűjtésére és átutalására.[64] A bűncselekmény elkövetője egyértelműen a nélkülözhetetlen informatikai tudása segítségével helyezte el a programelemet, így annak ellenére, hogy a mai analógiával élve információs rendszer felhasználásával követte el a csalást, kibertérfüggő cselekményről beszélhetünk, és a tettes egyértelműen informatikai elkövetőnek tekinthető.

Továbbhaladva a tipológia elemein, a Pusztai és Nagy által elemzett komputerkikémlelés példái alapvetően a kibertér által elősegített bűncselekmények kategóriájába tartoztak, elkövetésük pedig leggyakrabban a számítógépeken tárolt adatok jogszerűtlen másolásával valósult meg, ami a mai szoftverkalózkodáshoz hasonlítható, és az online kriminalitás szürkezónájává vált.

Ennél érdekesebb a komputerszabotázs, amely a ma is ismert elkövetési magatartás, az információs rendszer (programok, adatok) károsítását, tönkretételét nevesíti. Pusztai szerint e cselekmények célja is az anyagi haszonszerzés, de az elmúlt 30 év tapasztalatai alapján a megtorlás is idesorolható. Érdekesség, hogy míg Nagy szerint idetartozott az egyszerű programtörlés vagy a hozzáférhetetlenné tétel is, addig Pusztai éppen egy informatikai elkövetői maga-

61 Pusztai i. m. (59. lj.).
62 Nagy i. m. (51. lj.).
63 A példa részletesebb ismertetését l. Pusztai i. m. (59. lj.).
64 Uo.

tartást tárt elénk. Az 1984-ből származó példája szerint egy német főiskola alkalmazottja azzal fenyegetőzött, hogy amennyiben nem helyezik magasabb fizetési fokozatba, az általa kifejlesztett program – az általa beépített elem aktiválásával – egy konkrét időpontban törlődni fog az iskola rendszereiről.[65] Ez a bűncselekmény hasonló formában Magyarországon is előfordult, amiről Nagy tesz említést.[66] Az elkövetési magatartást tekintve ez is az informatikai bűnelkövetéshez tartozott. További érdekesség, hogy ebben az időben a legtöbb ilyen bűncselekményt, internet, illetve otthoni számítógép hiányában valamilyen oktatási intézmény vagy vállalat stb. alkalmazottai követték el munkakörük betöltése alatt – jó példa erre Robert Tappan Morris, az első internetes féreg megalkotója.[67]

Végül, a számos korábbi forrásban megemlített, de ki nem bontott csoport, a gépidőlopás veti fel talán a legtöbb kérdést, hiszen e cselekménytípus ma már nem képezi az IKT-bűnözés részét, illetve alternatív formában épült be a bűnözésbe. E cselekményről akkor beszélhetünk, amikor egy alkalmazott a vállalati számítógépet használja a saját programjainak megírásához és teszteléséhez, írta Ulrich Sieber az 1980-as években.[68] A program elkészítése ez esetben szintén informatikai képességekre utalt, maga a bűncselekmény mégis a számítógép mint eszköz használatát jelentette, és nem az illetéktelen behatolás, a bennmaradás vagy az adatok megváltoztatása, törlése volt az elkövetési magatartás. Példaként gondolhatunk itt a túlterheléses (DoS, DDoS)[69] támadásokra vagy a kiterjedt zombihálózatokra, amelyek létrehozása során már az IKT-rendszerhez való engedély nélküli hozzáféréssel is megvalósul a bűncselekmény, ugyanakkor a számítógép, illetve az internetes sávszélesség párhuzamos használatát, a számítógép működési kapacitásának 'ellopását' is jelenti.

Látható tehát, hogy ekkor még magyar szabályozás nem létezett e cselekmények egyedi kezelésére, és az NSZK-ból átvett, nálunk még inkább csak kriminológiai csoportosítás egyes elemei nagyon eltérő elkövetői magatartásmintákat tartalmaztak. Érdekes, hogy ez a tipizálási probléma már akkor is megvolt, amikor az IKT-hoz kapcsolódó büntetőjogi tényállások megalkotása igen távoli célkitűzésnek számított. Érdemes viszont megemlíteni, hogy a számítógépek kis elterjedtsége és a személyi számítógépek hiánya miatt ebben az időben a 'tömegek' még nem jelenhettek meg az IKT-kkal kapcsolatos bűnözésben, így az informatikai elkövetők is felülreprezentáltak voltak, tekintve hogy pusztán programozói mivoltukból eredően ők fértek hozzá az informatikai eszközökhöz. Ettől eltekintve már Pusztai és Nagy is hozott olyan példákat, ame-

65 Uo. Ulrich Sieber: *Computerkriminalität und Strafrecht*. Köln, Heymann, 1980.

66 Nagy i. m. (51. lj.).

67 Steven J. Vaughan-Nichols: The Day Computer Security Turned Real: The Morris Worm Turns 30. *Networking,* 2018. november 2., https://www.zdnet.com/article/the-day-computer-security-turned-real-the-morris-worm-turns-30/

68 Sieber i. m. (65. lj.).

69 „A szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében, (pl. e-mail-fiókhoz, más banki vagy egyéb fiókokhoz való hozzáférésben, a weboldal elérésében) – innen a szolgáltatásmegtagadással járó elnevezés is – amelynek a leggyakoribb formája, amely a webszerver elérését és rendeltetésszerű használatát gátolja a mesterségesen generált és megnövelt adatforgalommal." Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro,* 2018/1., 66–68.

lyekben a számítógépet csupán használó ügyintéző vagy egyéb, informatikai jártassággal, programozói készségekkel nem rendelkező személy követett el kibertér által elősegített jogsértéseket, azonban ez nem tartozik vizsgálódásom körébe.[70]

4.2. A hazai jogfejlődés és az ezredforduló IKT-bűnözése

A hazai szakirodalom és a magyar jogfejlődés további áttekintése során előbb a számítógépes csalás 1994. évi bevezetéséhez kapcsolódó néhány jogsértést vizsgálok, azután az ezredfordulón átalakult internetezési szokások és a már említett budapesti egyezmény alapján bevezetett 2002-es büntetőjogi változásokról és a bennük azonosítható kibertérfüggő kriminalitásról, valamint az informatikai elkövetők büntethetőségével foglalkozom.

Ahogyan az a számítógépes bűnözés fejlődésénél a legtöbb hazai szakirodalomban olvasható, már az 1980-as évek végén megjelentek különböző európai szintű ajánlások az IKT-eszközökhöz kapcsolódó bűnözés szabályozásának módjára, az egyes bűncselekmények csoportosítására. Ilyen volt például az R (89) 9. számú Európa tanácsi ajánlás is,[71] amely a bűncselekményeknek már egy minimum- és egy fakultatív listáját is meghatározta, illetve előtte az OECD[72] is foglalkozott a kérdéssel egy ajánlás erejéig. Az informatikai bűnözés kodifikációjára gondolva fontos megjegyeznünk, hogy hazánk követi az európai szabályozást és annak minden fejleményét, Magyarország elkötelezett a kibervédelem, a büntetőjogi kodifikáció, az adatvédelem és az online gyermekvédelem iránt is.[73]

4.2.1. Az információs rendszer felhasználásával elkövetett csalás

A nemzetközi ajánlások és a technológia fejlődésének hatására, valamint az első német törekvésekre felfigyelve, mint már említettem, a hazai szakmai plénum is értelmezni kívánta az itthon zajló, informatikához kötődő kriminális folyamatokat (ahogyan azt ma is láthatjuk, nem csak a büntetőjog területén), ami először a számítógépek felhasználásával elkövetett csalás büntetendőségével kapcsolatban nyilvánult meg. Nagy kiváló példával illusztrálta a problémát, és felhívta a figyelmet a 'hagyományos' csalás során a sértett „tévedésbe ejtésének, tévedésben tartásának" hiánya miatt felmerülő alkalmazhatósági hiányosságra. Mint írta, a probléma a kezdetektől az volt, hogy egy számítógép átejtésével, vagyis a benne szereplő adatok, így akár egy bérletidíj-hátralék törlésében megnyilvánuló elkövetői magatartás semmiképp sem tartozhatott az akkori (és a mai) csalás tényállása alá, hiszen nem minden tényállási elem valósult meg, vagyis a cselekmény szétfeszítette az 1978. évi IV. törvény (78-as Btk.) adott szakaszának tényállási kereteit.

[70] A további tipológiák ismertetésétől jelen tanulmányban tartózkodom, tekintve hogy e négyes felosztás kisebb eltérésekkel az európai és az angolszász jogalkotásban is megtalálható volt az 1980-as években.

[71] Az Európa Tanács R (89) 9. számú ajánlása a számítógépekkel kapcsolatos bűncselekményekről.

[72] *Computer related crime: Analysis of legal policy*. Párizs, OECD, 1986.

[73] Erre jó példa az európai szinten is szigorúnak számító 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, a Digitális jólét program és a Magyar kibervédelmi stratégia [1139/2013. (III. 21.) Korm. határozat Magyarország nemzeti kiberbiztonsági stratégiájáról] folyamatos felülvizsgálata is.

Emiatt, hosszú polémia után – amelyben egyébként Pusztai is megfogalmazott egy számítógépes csalás definíciót – 1994-ben megszületett a számítógépes csalás büntetőjogi tényállása.[74] Az 1994. évi IX. törvény elfogadásakor a miniszteri indoklás szintén tartalmazta, hogy nem csupán a piacgazdaság új keretei,[75] hanem „a tulajdont károsító számítógépes manipuláció gyakorisága és az a tény vezetett az új bűncselekmény bevezetésére, hogy a vagyon elleni bűncselekmények nem alkalmazhatók ebben a körben a tényállási elemek hiánya miatt."[76] A helytelen adatok betáplálása, a programmanipuláció és az egyéb adatfeldolgozási módosítások mint új elkövetési magatartások kerültek a tényállásba.

Az alapesetben kibertér által elősegített devianciának tekinthető számítógépes csalás ugyan csak az IT-készségek igénybevételével véghezvitt programmanipulációs, programozási műveletek esetében tartozik vizsgálódásom körébe, néhány mondat erejéig foglalkozni kell vele, hiszen a tényállás megjelenése nagy előrelépésnek számított a számítógépes devianciák kriminalizációja szempontjából. A jogfejlődés e vívmánya érvelésem szempontjából is fontos, hiszen felveti az IKT-bűnözésben való elhelyezhetőség kérdését és az informatikai elkövetői magatartások megjelenését a számítógépes csalások elkövetése során. E tényállás, illetve az ezt követő számítógépes csalás kodifikációk a szakirodalomban általában az IKT-bűnözés hagyományosabb kategóriáihoz állnak közelebb. Ezt támasztja alá, hogy kezdetben a cselekmény még a gazdálkodási kötelezettséget és a gazdálkodás rendjét sértő bűncselekmények között szerepelt,[77] így nem tekintették a vagyon elleni bűncselekmények közé tartozónak, ahol a hagyományos csalás szerepelt, mégsem látszott indokoltnak a külön – informatikai bűnözési – fejezetbe iktatása, különösen, hogy egyéb tényállások felvételére az IKT-bűncselekményi körben nem is volt szükség.

A számítógépes csalás rendszertani elhelyezésének kérdésességére utal, hogy a 2002. április 1-jétől hatályos – a budapesti egyezmény hatására bevezetett – büntetőjogi változások során a cselekmény az akkor bevezetett számítástechnikai rendszerbe való jogosulatlan belépés, valamint annak második bekezdéseként a számítástechnikai rendszer és a számítástechnikai adatok sértetlensége elleni bűncselekményekkel (78-as Btk. 300/C. §) közös tényállásba került. A cselekmény kriminológiai helyének kérdésességét jelzi, hogy továbbra is a gazdasági bűncselekmények között kapott helyet, ami az intellektuális bűnözéssel való kapcsolatát is sejteti. A számítógépes csalás elsősorban az elkövetési tárgy (számítástechnikai rendszer és számítástechnikai adat) azonossága miatt került a 300/C. §-ba, ahol e bűncselekmények esetében a számítógép a bűnelkövetés tárgya, és nem csupán eszköze volt (gondolva itt a számítógépes bűnözés korai kategorizálására), mégis, a közös tényállás alá vonás a magatartás kibertérfüggő cselekményként való azonosítása felé terel minket. Ennek ellenére a számítógépes csalás 1994-es kodifikációjának indokolása a tényállási elemek hiányát említette, pedig e bűncselekményt valójában a hagyományos csaláshoz hasonló céllal követik el.[78]

[74] Nagy i. m. (51. lj.).

[75] Szathmáry Zoltán: *Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban*. Pécs, PTE, 2012. 195.

[76] Szabó Imre: *Internetes bűncselekmények különös tekintettel az internetes csalásra.* OTDK-dolgozat, https://docplayer.hu/1176875-Szabo-imre-internetes-buncselekmenyek-kulonos-tekintettel-az-internetes-csalasra.html

[77] 1978. évi IV. törvény a Büntető Törvénykönyvről.

[78] Szathmáry i. m. (75. lj.).

Így e cselekmény felvet egy fontos kérdést: ez esetben hol húzható meg a kibertér által elősegített és a kibertérfüggő cselekmények közötti határvonal? Annak megállapításához, hogy e cselekmények elkövetői nem feltétlenül, illetve nagyobb arányban nem tartoznak a – szakirodalmi áttekintés segítségével kialakított – informatikai bűnelkövető fogalmába, az elkövetési magatartások mélyebb szintű kriminológiai vizsgálata indokolt: e nélkül nem állíthatjuk biztosan, hogy inkább laikus elkövetési módszereket vagy professzionális számítástechnikai tudást igényel a bűncselekmény végrehajtása.[79]

A gyakorlat szempontjából elgondolkodtató, hogy a csaláshoz gyakran használatosak olyan programok is, amelyek létrehozása és hatékony alkalmazása informatikai tudást feltételez. Azonban ezek megalkotóinak büntethetősége még összetettebb kérdés, mint az informatikai bűnelkövető fogalmának meghatározása. Az álweboldalt létrehozó vagy adathalász e-mailt elkészítő ember vajon bűncselekményt követ el, ha azt nem saját használatra készíti? E kérdés megválaszolásában a büntetőjog 2000-es évek elején lezajlott változásai adnak némi segítséget.

4.2.2. Az információs rendszer vagy adat megsértése és az annak védelmét biztosító technikai intézkedés kijátszása bűncselekmények kodifikációja

Az európai jogfejlődésbe illeszkednek a 2001-ben elfogadott, a Büntető Törvénykönyv átfogó módosításával lezajlott változások, amelyeket elsősorban a budapesti egyezmény elfogadása indított el. Az egyezmény 2. cikke szerint az aláíró országok kötelezettséget vállaltak a számítástechnikai rendszerbe való jogosulatlan behatolás büntetendőségének bevezetésére. Az egyezményben a második rész I. fejezete 1. címének 2. cikke (jogosulatlan belépés), 4. cikke (számítástechnikai adat megsértése), 5. cikke (számítástechnikai rendszer megsértése) és 6. cikke (számítástechnikai eszközökkel visszaélés) hazánkban is megteremtette – ahogyan a 78-as Btk. hívta: – az informatikai bűnelkövetés számítógépes csaláson túli rendezésének lehetőségét.[80] A dokumentum kimondta, hogy „a jogosulatlan behatolás, az egyezmény értelmében, a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan és szándékos belépés" fordulat törvénybe iktatása kötelező az aláíró államok számára.[81] A szerződő országok kiköthették továbbá, hogy a jogosulatlan behatolás a biztonsági intézkedések megsértésével, az adatok megszerzésére irányuló vagy más tisztességtelen céllal, illetve egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan legyen elkövethető.[82]

Az egyezmény elfogadása következtében a 2001. évi CXXI. törvény két új 'informatikai' tényállást tett üldözendővé: a számítástechnikai rendszer és adatok elleni és a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszását. Az átalakított 300/C. § (1) bekezdésébe a jogosulatlan belépés, bent maradás stb., (2) bekezdésébe a károkozás, adatok megváltoztatása stb. került, a tényállást korábban megtestesítő számítógépes csalás pedig a

[79] A hazai büntetőeljárások ügyészségi áttekintésére és az informatikai bűnelkövető fogalma alá tartozó esetek áttekintésére egy 2019-ben engedélyezett kutatással nyílik lehetőség.

[80] Számítástechnikai bűnözésről szóló egyezmény i. m. (49. lj.).

[81] Szathmáry i. m. (75. lj.) 89–91.

[82] Uo., 90.

(3) bekezdésben szerepelt. A számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása deliktum a 300/E. §-ában, három bekezdéssel kapott helyet.[83]

Az informatikai bűnelkövető azonosíthatóságát nézve, a számítógépes csalás tényállása kiegészült a számítástechnikai rendszerbe való jogosulatlan belépéssel, bent maradással, illetve a belépést követő jogszerűtlen magatartásokkal (300/C. §), amelyek már – a Szathmáry Zoltán által *hacking*nek nevezett – jogosulatlan belépést és 'szabotázst' is tartalmazták. E cselekmények kapcsán ismét meg kell említeni, hogy az elkövethető csupán mások jelszavának felhasználásával, illetve a korábban visszavont jogosultággal való belépéssel vagy bent maradással is elkövetheti e bűncselekményt.[84] Ugyanakkor a 300/D. §-ban szereplő elkövetési magatartások, így a program, a jelszó vagy a kód elkészítése talán a leginkább alkalmasak az informatikai bűnelkövetők tipikus tevékenységének leírására, hiszen azok már valamilyen informatikai manipulációt igényelnek. Az informatikai bűnelkövetési magatartások azonosíthatósága tekintetében sajnálatos, hogy e területen a regisztrált bűncselekmények száma az összbűnözéshez mérten elenyésző, amiből egyértelműen az informatikai bűnözést övező nagymértékű látenciára következtethetünk.[85] Fontos viszont, hogy e két tényállás 2002-es hatálybalépése óta képes az információs rendszerekkel kapcsolatos bűnelkövetés szankcionálására Magyarországon.

A módosítást megelőzően az informatikai bűnözés hazánkban nem volt büntethető (pedig például az Egyesült Államokban már az 1984-es Computer Fraud and Abuse Act szankcionálta).[86] Ennek egyik példája az *Elender*-per, amely egyértelműen alátámasztotta a magyar állam büntetőigényének kiterjesztését a 2000-es évek elején. Sajnos az esetről nem készült kriminológiai feljegyzés, annyi azonban tudható, hogy három fiatal (akik közül egy még kiskorú volt) 1999 szilveszterén behatolt az akkor még virágkorát élő, főként internetszolgáltatással foglalkozó Elender Informatikai Rt. szerverébe, majd megváltoztatta a vállalat honlapjának tartalmát. Egy korabeli híradás szerint „a hackerek először 2000. január 8-án törték fel az Elender Rt. biztonsági rendszerét. Behatoltak központi szerverébe; lemásolták és feltették az internetre mintegy kétezer Elender-felhasználó nevét és jelszavát, így az bárki számára elérhetővé vált. Mivel a rendeltetésszerű működtetés nem volt biztosítható, a cégnek egy időre – egyes szolgáltatások esetében napokig – le kellett állni."[87] Még egy behatolásra sor került – ekkor „a betörő- vagy

[83] A behatolással kapcsolatos, röviden már említett, büntetendőségi dilemma szempontjából érdekes, hogy – ahogyan azt az EU Tanácsának 2005/222/IB kerethatározata is írja – a jogosulatlan belépés, vagy ahogyan Szathmáry doktori disszertációjában szerepel, a *'hacking'* (hiszen a rendszerbe való jogosulatlan belépést ő is ezzel azonosnak tekinti) megvalósulásához nem feltétel, hogy az informatikai rendszert valamilyen védelem megsértésével érjék el. Ez azonban a gyakorlatban egyrészt a belépés bizonyíthatósága és – ahogyan Parti Katalin jelzi – előre hozott felelősségi alakzata miatt nem felel meg a büntetőjog dogmatikai feltételrendszernek, másrészt a nem védett rendszerbe való behatolás, a szándékosság büntetőeljárási bizonyítása kérdéses lehet. Ennek tárgyalására azonban jelen írás keretei között nincs lehetőség.

[84] Szathmáry i. m. (75. lj.).

[85] Pergel Józsefné: A számítógépes csalás és egyéb számítógépes bűncselekmények. *Statisztikai Szemle,* 2001/9., 763–775.

[86] L. bővebben H. Marshall Jarrett – Michael W. Bailie: *Prosecuting Computer Crimes. Office of Legal Education Executive Office for United States Attorneys* (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

[87] Vádemelési javaslat az Elender feltörői ellen. *Jogi Fórum,* 2001. február 28., https://www.jogiforum.hu/hirek/552

hacker-csoport ismét megváltoztatta a szolgáltató web-oldalának tartalmát".[88] A három fiatal internetes hekkercsatornákon keresztül szerezte meg az Elender informatikai rendszerének jelszavát, amelyet „felhasználva, rendszergazda jogosultságuk segítségével otthoni számítógépükről beléptek az Elender rendszerébe, és feltöltöttek egy előre megírt honlapot".[89]

A rendszerbe való behatolás miatt az ügy bírósági szakaszba is került, ahol első fokon „folytatólagosan és bűnszövetségben elkövetett közérdekű üzem működésének megzavarásában, és ötrendbeli magántitok jogosulatlan megsértésében találták vétkesnek a fiatalokat. A bíróság 1 év 10 hónap felfüggesztett fogházbüntetésre ítélte az első- és a harmadrendű, fiatalkorú vádlottat, a másodrendű, felnőtt korú vádlott pedig 2 év (felfüggesztett) börtönbüntetést kapott."[90] A budapesti egyezmény ratifikálásában megerősíthette a magyar államot, hogy másodfokon bűncselekmény hiányában felmentették a fiatalokat. A bíróság indokolásában az szerepelt, hogy egy szerver feltörése nem tekinthető közérdekű üzem megzavarásának, a 2002 áprilisától hatályban lévő jogszabály alapján pedig az elítélésre nem volt lehetőség, hiszen a cselekmény a jogszabály-módosítás előtt történt. Így ebben a ma már távoli technológiatörténeti korszakban nagy szükség és főként iparági igény volt a módosításokra: „úgy tűnik, hazánkba visszatér a betyárvilág, de a jelek szerint ezúttal a virtuális teret fenyegetik a múlt századi lovas haramiák kései leszármazottai."[91]

A 2012. évi C. törvénnyel (új Btk.) bevezetett módosítások – a 2000-es évek *Elender*-perhez hasonló történései és az egyezmény miatt bekövetkezett változások tükrében – elsősorban rendszertani változást eredményeztek: a jogalkotó a budapesti egyezményben kiemelt szerepet kapó belépést, szabotázst, csalást és technikai intézkedés kijátszását külön tényállásba rendezte. Az információs rendszer vagy adat megsértése bűncselekmények (a behatolás együtt a 'szabotázzsal' – 423. §) és az információs rendszer védelmét biztosító technikai intézkedés kijátszása továbbra is külön tényállásban (424. §) szerepelnek. Az információs rendszer felhasználásával elkövetett csalás 'félhagyományos' bűncselekményi tényállása az előző alfejezetben említett okok miatt a vagyon elleni bűncselekmények közé került (323. §).

A 2000-es évek utáni szabályozási irányokat vizsgálva az látszik, hogy a büntetőjogi kodifikáció helyett a büntetőeljárási szabályok szigorítása, az új nyomozástechnikai eljárások bevezetése és a különböző ágazati jogszabályok megalkotása irányába fordult a szabályozás. Az internet védelmében a kibervédelmi eseménykezelés, az audiovizuális médiaszolgáltatásokról szóló szabályok kiterjesztése, a pénzintézeti kárenyhítés és a biztonságtechnikai vállalatok által kínált védelmi technológiák nyertek teret.

A büntetőpolitika a büntetőjogi szabályozás *ultima ratio* voltából nem engedve, helyesen, a súlyosabb cselekmények szankcionálására koncentrált. A 2010-es években ennek ellenére a társadalom az 1980-as évekből származó hekkerkép szerint értékeli a kibertérfüggő bűnözést. A közvélemény e 'romantikus' percepcióját támasztja alá, hogy míg például az adathalász cselekmények[92] volumene növekszik, addig továbbra is az olyan események kerülnek a hazai

88 Uo.

89 Uo.

90 K. Endre: Az Elender-hekkelés ítélete és tanulságai. *Prohardver,* 2003. december 15., https://prohardver.hu/hir/az_elender-hekkeles_itelete_es_tanulsagai.html

91 Egri István: Betyár kibervilág. *Hetek,* 2000/6., http://epa.oszk.hu/00800/00804/00099/6757.html

92 Ilyenek pl. az adóvisszatérítésekkel és a Magyar Posta Zrt. nyereményeivel kecsegtető adathalász tevékenységek.

médiafigyelem középpontjába, mint a Telekom-hack néven ismertté vált büntetőügy, holott a nemzetközi bűnözési statisztikák és a biztonsági vállalatok felmérései már egy egészen más informatikai bűnözési jelenséget tárnak elénk.

A Telekom rendszerének 2017-es feltörése azért érdekes, mert – ellentétben az Elender Rt. szerverét feltörőkkel – a bűncselekményt elkövető fiatal, a híradások szerint egész egyszerűen a Telekom által kiadott, IP-cím váltásához használatos, online közzétett elektronikus kézikönyvben talált egy olyan IP-címet, amelyen keresztül lehetővé vált számára a Magyar Telekom belső hálózatába való belépés. A fiatal cselekményével megvalósította az új Btk. 423. §-ába tartozó jogtalan behatolást, de értesítette a vállalatot a hibáról. A hiba részletes leírásával a kezében a cég székhelyén megbeszélésen vett részt, amelyen felvetődött, hogy biztonsági tesztek végzésére szerződéses viszonyba léphetnének egymással. Nem jutottak egyezségre, a fiatal pedig tovább folytatta a cég engedélye nélküli tevékenységét. Ezt követően a törvényi tényállás megvalósítása miatt a Telekom feljelentette, mondván, tevékenysége már nem a jó szándékú rendszervédelmet szolgálta, hanem az ügyféladatokhoz való hozzáférés következtében jelentősen veszélyessé vált a társadalomra. A büntetőeljárás jelenleg is folyik, kimenetele nem jósolható meg.

Kijelenthető, hogy bár ez a cselekmény – vélhetően jogosan – az 'informatikai' tényállás alapján került a rendőrség (ez esetben a Nemzeti Nyomozó Iroda) látókörébe, a súlyosabb és a technológia által fellendülő informatikai bűnözés valós veszélyeit nem a Telekom-hackhez, sőt nem is az *Elender*-perhez hasonló esetek jelentik. Ezek a cselekmények segítenek megrajzolni a kibertérfüggő bűnözés határait, de a társadalmat valóban veszélyeztető és károkozó cselekmények elkerülik a közfigyelmet, sőt az informatikai bűnelkövetést az inkább bagatell kriminalitással azonosítják, holott e cselekmények a modern bűnözés csupán egy kis és ma már viszonylag könnyen kezelhető szeletét képezik.[93]

Kiegészítésként érdemes megemlíteni, hogy a 2002-es nagyobb változást követően hazánk helyzete alapvetően pozitív irányba mozdult az informatikai bűnözés szabályozása tekintetében. Néhány európai uniós dokumentumnak való megfelelés továbbra is megjelent az informatikai bűnüldözésben, így például az Európai Parlament és Tanács 2013/40/EU irányelve, amely a (budapesti egyezményhez hasonló kötelezettségeket tartalmazó) 2005/222/IB kerethatározatot váltotta fel. E folyamat során az információs rendszer vagy adat megsértése bűncselekmény minősített eseteinek kiegészítésével kötelezettséggé vált legalább azon súlyosabb esetek büntetendővé tétele, amelyeknél az irányelvben foglalt bűncselekmények[94] elkövetéséhez eszközöket használnak (ilyen lehet például a számítógépes programok készítése, a belépési kódok, jelszavak felhasználása az információs rendszerhez való hozzáféréshez).[95] Érdekesség, hogy a szabályozás lehetővé teszi a bűnszervezetben történő elkövetés minősített esetté válását, ami – Mezei Kittivel egyetértve – az informatikai bűnözés szerkezetének megváltozása miatt üdvözlendő lenne.

93 Hibát talált a Telekomnak, aztán egy reggel csöngettek a rendőrök. *Index,* 2017. július 26., https://index.hu/belfold/2017/07/26/telekom_t-systems_biztonsagi_res_nni_etikus_hekker_rendorseg_nni_orizetbe_vetel/

94 Pl. kommunikáció tartalmának lehallgatása, ellenőrzése vagy figyelemmel kísérése, és az adattartalmak közvetlenül, az információs rendszerhez való hozzáférés és az információs rendszer használata általi, vagy közvetetten, elektronikus megfigyelő vagy lehallgató eszközök révén történő megszerzése.

95 Mezei Kitti: Az információs rendszerek elleni bűncselekmények uniós szintű szabályozása, különös tekintettel az Európai Unió 2013/40/EU sz. irányelvére. *Jogi Fórum,* 2015, https://www.jogiforum.hu/files/publikaciok/mezei_kitti__informacios_rendszerek_elleni_buncselekmenyek_eu_szabalyozasa%5bjogi_forum%5d.pdf

Összegezve, e rövid történeti áttekintésből az látható, hogy a kibertérfüggő bűnözés feltérképezéséhez e cselekmények is hozzájárulnak, sőt a bűnelkövetés magvát és enyhébb eseteit is segítenek megérteni. Ám, tekintve hogy a büntetőtudományoknak nem feladatuk az informatikai bűnelkövetők személyiségéről, szervezettségük fokáról, motivációjukról való információgyűjtés, e részben a vonatkozó büntetőjogi tényállások történeti és összehasonlító áttekintésével csupán azt mutathattam be, hogy milyen elkövetési magatartások szerepelnek a magyar büntetőjogban, és ezek a Weulen Kranenbarg-i csoportosításban hol kaphatnak helyet. A hazai büntetőjogi tényállások vizsgálata és a példák abban nyújtanak segítséget, hogy meghatározhassuk, melyek azok a főbb büntetőügyek, amelyek elemzése eligazítást nyújthat a kibertérfüggő bűnözés és a bűnelkövetővé válás jellemzőinek vizsgálatában.

5. Összefoglalás

A tanulmány bevezetőjében említett három cél követésével az IKT-kkal kapcsolatos bűnözés fundamentális kérdésire kerestem a választ. Elsőként a legfontosabb hekkerfogalmakat és azok fő tartalmi elemeit vizsgáltam, aminek segítségével arra a következtetésre jutottam, hogy a „hekker" („hacker") és a *„hacking"* kifejezések gyűjtőfogalomként való használata, illetve csupán az információs rendszerbe – informatikai eszközökkel – való belépésre, valamint az oda belépő személyre való alkalmazása a nemzetközi és a hazai szakirodalomra egyaránt jellemző. E két út közül az utóbbi felé orientálódtam, sőt a „hekker" kifejezés számomra értéksemleges jelentéstartalma következtében, fogalommeghatározásomban az „informatikai bűnelkövető" elnevezés használatát preferáltam.

Eszerint az informatikai bűnelkövető olyan személy, aki számítástechnikai tudásának felhasználásával infokommunikációs technológiákkal kapcsolatos bűncselekményeket úgy követ el, hogy abban információszerzési, vagyonszerzési vagy károkozási motívum is megjelenik. Bűncselekményének legfontosabb mozzanata a rendszerbe való behatolás, az ezt megkönnyítő vagy egyéb – akár hagyományos bűncselekményhez használatos – program létrehozása, program vagy programegység megváltoztatása, funkcióinak átalakítása. Tevékenysége egyediségét erősíti, hogy cselekményének elkövetéséhez nélkülözhetetlen az átlagosnál fejlettebb informatikai tudás. Tekintve, hogy az összes online bűnelkövetőre egységes fogalmat alkotni nem lehetséges, és nem is feltétlenül szükséges, a definíció elsősorban a tudásalapú informatikai bűnözők ernyőfogalmaként fogható fel, és csupán az informatikai bűnözés egy kis szegmensére alkalmazható, emellett a bűnelkövetési magatartás jellemzőire koncentrál, így a bűnelkövetői profil szempontjából egyetlen stabil eleme a technológiai tudás megléte. A fogalom alá tartozó alcsoportok konkretizálása (például kódolók, vírusírók, kémek stb.) és további közös elkövetői jellemzők feltárása a fenti elemzésben nem szerepel.

Láthattuk, hogy a kriminológiai szakirodalomban az informatikai bűnözésre számos csoportosítás létezik, ezek az online bűncselekmények diverzitása miatt nem egységesek, és nincs is lehetőség egységes csoportosítás megalkotására e téren. A harmadik részben olvasható csoportosítási módok közötti választás – a kriminológiai vizsgálódás későbbi irányvonalainak meghatározása érdekében – mégis indokolt. Ennek megfelelően Weulen Kranenbarg kettős felosztását

preferálom, szemben a nagyobb részletességű kategorizálási módokkal. Weulen Kranenbarg fogalmának hasznosíthatósága abban rejlik, hogy az online kriminalitást csupán a kibertér által elősegített és kibertérfüggő bűncselekményekre osztja.

A kibertérfüggő bűnözés – amely magát az infokommunikációs technológiát célozza, és az informatika kulcsszerepet játszik a cselekmény végrehajtásában is – képes szemléletesen leírni az online kriminalitás technológiaorientált szegmensének egyedülállóságát. A bűnözési kategória, leválva a 'félhagyományos', inkább laikusok által elkövetett online jogsértésekről, egy terület alá vonja az informatikai bűnelkövetők által megvalósított főbb cselekményeket, amelyek egyik közös jellemzője az elkövetéshez szükséges technológiai tudás.

Végül értekezésem harmadik részében a hazai büntetőjog online kriminalitással foglalkozó szegmensének áttekintésére és az elmúlt közel harminc évben megalkotott tényállások főbb elkövetési magatartásainak a kriminológiai csoportosításban való elhelyezésére vállalkoztam. Ennek részeként példákkal világítottam rá arra az ambivalens helyzetre, hogy bár vannak a Büntető Törvénykönyvben kifejezetten 'informatikai tényállások', ezek elkövetési magatartásai nem minden esetben esnek azonos kriminológiai kategória alá. Nem állítható, hogy például az információs rendszer vagy adat megsértése bűncselekmények a gyakorlatban elsősorban a hekkerek büntethetőségét alapozzák meg, de az az állítás sem feltétlenül igaz kriminológiai szempontból, hogy az információs rendszer felhasználásával elkövetett csalás pusztán kibertér által elősegített bűnözés lenne.

Ennek következtében az látszik, hogy bár az újabb és újabb magyar büntetőjog – megfelelve az európai kívánalmaknak – rögzítette az informatikai bűnözés tényállásait, a valódi kibertérfüggő bűncselekmények átívelnek a büntetőjogi tényállásokon. Emiatt az informatikai bűnözés kriminológiai vizsgálata során, így például egy bírósági vagy ügyészségi aktakutatáskor, az egyes tényállásokon belüli differenciálásra kell törekednünk a kibertérfüggő bűnelkövetői magatartások és az informatikai bűnelkövetők azonosítása érdekében. Mindezen kutatási feladatok elvégzésére azért van szükség, mert a kriminológia és a büntető igazságszolgáltatás által már felismert, kibertér által elősegített bűnözés mellett nem csupán a kisebb súlyú jogosulatlan belépések, hanem a kibertérfüggő bűncselekmények specializált, tudásalapú válfaja is terjed, és mindkettő súlyos társadalmi problémákat okoz.