Kriminológiai elméletek és informatikai bűnözés

VARGA ÁRPÁD*

1. Bevezetés

Az informatikai bűnözés *(cybercrime),* amely gyűjtőfogalomként magában foglalja a kibertér által elősegített *(cyber-enabled crime)* és a kibertérfüggő kriminalitást *(cyber-dependent crime),*[1] a kriminológiai kutatások kedvelt területévé vált az elmúlt több mint három évtizedben. Az informatika kialakulásával és az internet fejlődésével, kiterjedtségének növekedésével a bűnelkövetés hatékony területévé vált e technológia. Az informatikai bűnözés nem csupán az elkövethető cselekmények sokszínűsége, hanem az elkövetővé válás sajátos útjai és a bűnelkövetés szerteágazó jellemzői okán vált a kriminológiai kutatások sajátos gyűjtőpontjává. Az infokommunikációs technológiákkal kapcsolatos bűnelkövetői magatartások fogalmi meghatározása és az elkövetők tipizálása számos eltérő szemléletben manifesztálódott, és hosszú fejlődési utat járt be. Emellett az informatikai bűnözés vizsgálata, a bűnelkövetővé válás okságai összefüggéseinek felfedezése is önálló teoretizálási igényt támasztott a kriminológiával szemben. A folyamat részeként az 1990-es évektől kezdődően jelentősen gyarapodott az empirikus kutatásokkal is tesztelhető elméleti keretek kidolgozását és a meglévő elméletek adaptálását célzó szakirodalom száma.

Jelen írás célja – tovább folytatva a kriminológiai csoportosítások vizsgálatával megkezdett utamat[2] – az informatikai bűnözéssel mint gyűjtőfogalommal kapcsolatba hozható kriminológiai elméletek és kutatások elemzése, az ismertetett elméletek korábbi tapasztalatain keresztül a kibertérfüggő bűncselekmények és az e kategóriába tartozó cselekmények elkövetőinek vizsgálata. Az okságok összefüggések feltárásának elősegítése céljából a tanulmányban kísérletet teszek egyes különálló elméletek összefésülésére is. A terjedelmi korlátok és az informatikai bűnözés kutatásának növekvő kiterjedtsége miatt azon elméletek ismertetésére szorítkozom, amelyek a

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

[1] Marleen W. Kranenbarg: *Cyber-Offenders Versus Traditional Offenders: An Empirical Comparison.* Doktori értekezés, Vrije Universiteit (2018) https://research.vu.nl/ws/portalfiles/portal/56319015/complete+dissertation.pdf.

[2] L. Varga Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. *In Medias Res,* 2019/1. 145–167.

terület kriminológiai kutatása tekintetében meghatározó jelentőségűek, rendelkeznek empirikus kutatási eredményekkel, vagy bizonyos elemei kifejezetten alkalmazhatók az online tér elkövetőinek vizsgálatára.

Elsőként röviden ismertetem a környezeti kriminológia elméletcsoportjába tartozó racionális döntéselméletet és a rutintevékenységi elméletet. Ezt követően az informatikai bűnözés talán legtöbbet idézett és tesztelt elméletcsoportjaként vizsgálom a részben klasszikus kriminológiai, részben pozitivista hagyományokkal rendelkező kontrollelméletek alkalmazhatóságát, így kitérek a bűnözés általános elméletére és Travis Hirschi társadalmi kötődéselméletére is. A második részben célom a pozitivista és az interakcionista jegyeket egyaránt hordozó tanuláselméletek bővebb ismertetése, tekintettel ezen elméletcsoport kiemelt alkalmazottságára a kibertérfüggő bűnözéssel és e cselekmények elkövetőivel foglalkozó kutatásokban. A kulturális és a társas interakciók megközelítésén belül szót ejtek a neutralizációelméletről, az ahhoz szorosan kapcsolódó sodródáselméletről, valamint ezek kapcsolódásáról a tanuláselméletekhez az informatikai bűnözés kontextusában. A befejező részben kitérek a fejlődéskriminológiai paradigma és az életpályamodellek informatikai bűnözésre alkalmazható egyes elméleti és empirikus megállapításaira, valamint e tudás tanuláselméletekkel való összekapcsolhatóságára is. A tanulmány a felsorolt elméletek, elméletcsoportok informatikai bűnözésre történő alkalmazhatóságával foglalkozik. Ezek alapvető téziseit a vizsgált kérdéskör megértéséhez szükséges mértékben ismertetem.

2. Kriminológiai elméletek az informatikai bűnözés tükrében

2.1. A környezeti kriminológia elméletei

2.1.1. Racionális döntéselmélet

A racionális döntéselmélet gyökerei egészen a klasszikus iskoláig nyúlnak vissza, illetve az 1950-es évektől ismét előtérbe kerülő neoklasszikus paradigma szemléletét tekintik hivatkozási alapnak.[3] Emellett mind a racionális döntéselmélet, mind a rutintevékenységi elmélet a környezeti kriminológia részét képezi. Az elméletcsoport a klasszikus iskola azon alapvetésére épít, miszerint a bűnelkövetés az elkövető szabad akaratának, saját elhatározásának kivetülése, így a bűnelkövetés motivációja, a bűnelkövetéshez vezető utak komplex társadalmi és egyénben fellelhető magyarázatai nem képezik vizsgálódása tárgyát.[4] Az 1700-as évek második feléből eredő gondolatok döntéselméleti relevanciája Cesare Beccaria proporcionális büntetést és elrettentést középpontba helyező nézeteivel szemben inkább Jeremy Bentham utilitarista filozófiájából eredeztethető. E felfogás szerint az emberi magatartás annak mérlegelésére épülő döntések soro-

[3] Borbíró Andrea et alii (szerk.): *Kriminológia*. Budapest, Wolters Kluwer, 2019. 45–46.

[4] Thomas J. Holt – Adam M. Bossler: *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. London, Routledge, 2015. 73.

zata, hogy az adott cselekvés milyen mértékben okoz örömöt, vagy jár fájdalommal. Ennek értelmében a bűnelkövetés is egyfajta költség-haszon elemzés, amelynek során az egyén a költségeket felülmúló hasznokért, a boldogságra törekvés érdekében követ el bűncselekményt.[5]

Számos közgazdasági elmélet vitte tovább ennek alapgondolatait. Derek B. Cornish és Ronald V. Clarke 1986-ban megalkotott racionális döntéselméletének közvetlen előzményeként mégis Gary Becker közgazdász 1968-as tételei szolgáltak,[6] amelyek középpontjában a *homo economicus* állt. A (neo)klasszikus paradigma emberképét magáévá tevő döntési elmélet azt feltételezi tehát, hogy a bűnelkövető a cselekvés előtt kikalkulálja az elkövetésből származó költségek és hasznok mértékét, vagyis hogy milyen előnyökre tehet szert, legyen az „pénz, szex vagy izgalom".[7] Cornish és Clark e kalkuláció folyamatát igyekezett azonosítani. Véleményük szerint a kalkuláció során azonosított költségek és hasznok szubjektívek, azok az adott szituációban, élethelyzetben az elkövető kognitív képességeitől és a releváns információk elérhetőségétől függenek. Ezt nevezhetjük egyfajta korlátozott racionalitásnak is, amelyet egyedi és egyéni körülmények, így például alkoholos befolyásoltság, kábítószer-fogyasztás,[8] korábbi tapasztalatok, a bűnelkövetés technikájának meglévő készségei stb. befolyásolnak, sőt ezek a döntések olykor egyáltalán nem is racionálisak.[9] Továbbá a bűnözésben kétféle döntési mechanizmusnak van jelentősége: az általános, bűnelkövetésben való részvételre irányuló, valamint a konkrét elkövetést eredményező, általában rövidebb folyamatot követő döntésnek.[10]

A racionális döntéselmélet szoros kapcsolatban áll az elrettentéselméletekkel is, így a szintén klasszikus tanokból származó, a büntető igazságszolgáltatás hatékonyságának növelését célzó, a bűnözéstől való távoltartást a büntetés elkerülhetetlenségével társító elmélet szintén a racionálisan cselekvő ember képére épít.[11] Emiatt ezt az elméletet az informatikai bűnözés kutatásában gyakran Cornish és Clarke elméletével integráltan alkalmazzák. A racionális döntéselmélet informatikai bűnözésre adaptálásának kulcsa mégis elsősorban az elmélet azon része, amely szerint ez a relatíve racionális döntés, vagy más néven a döntésfelépítés tulajdonságai a különböző bűncselekménytípusok esetében eltérő módon és tartalommal jelennek meg. Ez azt is jelenti, hogy a döntések meghozatalában – Cornish és Clarke 1987-ben írt gondolatai szerint – a végeredményt nagymértékben befolyásolja, hogy milyen mértékben rendelkezik az egyén a cselekmény elkövetéséhez szükséges készségekkel.[12]

[5] Inzelt Éva: A kriminológiai gondolkodás kezdetei. In: Borbíró i. m. (3. lj.) 59–62.

[6] Gary S. Becker: *The Economic Approach to Human Behavior*. Chicago, University of Chicago Press, 1976.

[7] Derek B. Cornish – Ronald V. Clarke (szerk.): *The Reasoning Criminal.* New York, Springer, 1986. 935.

[8] Michael Cherbonneau – Heith Copes: „Drive It Like You Stole It": Auto Theft and the Illusion of Normalcy. 46(2) *British Journal of Criminology* (2006) 193–211.

[9] Ronald L. Akers – Christine S. Sellers: *Criminological Theories: Introduction, Evaluation, and Application*. Los Angeles, Roxbury, (4. kiad.) 2004.

[10] Podoletz Léna: Környezeti kriminológia. In: Borbíró i. m. (3. lj.) 233–253., 241.; Derek B. Cornish – Ronald V. Clarke: The Rational Choice Perspective. In: Richard Wortley – Lorraine Mazerolle (szerk.): *Environmental Criminology and Crime Analysis.* Devon, Willan, 2008. 21–47.

[11] Holt–Bossler i. m. (4. lj.) 75–78.

[12] Derek B. Cornish – Ronald V. Clarke: Understanding Crime Displacement: An Application of Rational Choice Theory. 25(4) *Criminology* (1987) 933–948.; Alice Hutchings: Cybercrime Trajectories: An Intergrated Theory of Initiation, Maintenance and Desistance. In: Thomas J. Holt (szerk..): *Crime Online: Correlates, Causes, and Context*. Durham, Carolina Academic Press, (3. kiad.) 2016. 122–123.

Ezzel együtt az informatikai bűnözés kutatásában fellelhető, színtisztán a racionális döntéselméleten alapuló kutatások száma igen kevés. Azok jelentős része a társas interakciókat mellőző informatikai bűncselekményeket vizsgálja (azon eseteket, amikor az elkövető és a sértett között nincs közvetlen kapcsolat), pontosabban azon technológiafüggő cselekményeket, amelyeknél vagy elhanyagolható mértékű költség merül fel[13] (pl. digitális kalózkodás[14]), vagy az elkövetéssel elérhető hasznok az egyén számára jóval meghaladják a felmerülő költségeket (pl. információs rendszereket érintő bűncselekmények, kártékony szoftverek írása, e-mailes csalások vagy jogosulatlan behatolás). Míg az előbbi esetben a kutatások a felelősségre vonás alacsony valószínűségében és a megengedő büntetőjogi szabályozásban látják az illegális letöltések melletti elhatározás okait, addig az utóbbiban a szakirodalom szerint a rendelkezésre álló segédeszközök, a meglévő készségek és a felelősségre vonás alacsony valószínűsége az, ami a haszonmaximalizálás lehetőségét, így az elkövetés melletti döntést támasztja alá az elkövető számára.

A racionális döntéselmélet vegytiszta formában mindössze egy kutatásban jelent meg, amely kifejezetten a racionális döntéselmélet, pontosabban a költség-haszon elemzés tényezőit is magában foglaló elrettentéselmélet tételeit vizsgálta a digitális kalózkodás viszonylatában. Az egyetemista populáción végzett kutatás a szoftverkalózkodástól elrettentő tényezőket vizsgálta a bűnözésre adott válaszok (pl. felelősségre vonás valószínűsége, szigorú büntetések stb.), a kockázati és profittényezők (pl. korábban szerzett készségek), egyéni tényezők (pl. alacsony önkontroll, szégyen, bűntudat és erkölcsi meggyőződés) és a bűnalkalmak (pl. az adott szituáció értékelése) mérése által.[15]

George Higgins és munkatársainak kutatási eredményei azt mutatták 2005-ben, hogy a bűncselekményért kapható büntetés bizonyossága szignifikánsan negatív kapcsolatban állt a szoftverkalózkodással, vagyis azt sugallja, hogy a biztonság növelésével a szoftverkalózkodás csökken. Az állami és a magánszektornak olyan eszközöket és szerveket kell fejlesztenie tehát, amelyek pontosabban tudják kutatni a jelenséget, és képesek végrehajtani a szükséges biztonsági intézkedéseket a felelősségre vonás elősegítéséhez. Ahogyan a szerzők megjegyzik, ez a megállapítás összhangban áll a klasszikus elrettentéselméleti irodalom jelentős részével. Eszerint a büntetés súlyosságának nem volt preventív hatása az illegális szoftverletöltésre.[16]

E tanulmányról szólva fontos kiemelni, hogy a család elutasítása negatív kapcsolatban állt a szoftverkalózkodással. Ahogyan Higgins és munkatársai jelzik: „az eredmény arra utal, hogy a család felől jövő elutasítás a társadalmi megbélyegzés érzetét keltheti, ami visszatarthat a szoft-

[13] George E. Higgins – Abby L. Wilson – Brian D. Fell: An Application of Deterrence Theory to Software Piracy. 12(3) *Journal of Criminal Justice and Popular Culture* (2005) 166–184.

[14] A digitális kalózkodás a szoftverek, audiovizuális tartalmak, hang- és képfelvételek illegális letöltésének és terjesztésének gyűjtőfogalmaként összegezhető. Ronald Sims, Hsing Cheng és Hildy Teegan 1996-ban önálló fogalomként definiálta a szoftverkalózkodást mint a számítógépes programok illegális másolását. Ehhez képest mások ezt kiterjesztve, a digitális kalózkodás fogalma felé haladva már a szoftverkalózkodást is a szerzői jog által védett tartalmak jogosulatlan másolásával, megosztásával vagy letöltésével azonosították. Ronald R. Sims – Hsing K. Cheng – Hildy Teegen: Toward a Profile of Student Software Pirates. 15 *Journal of Business Ethics* (1996) 839–849.; Marjie T. Britz: *Computer Forensics and Cyber Crime: An Introduction*. Upper Saddle River, Prentice Hall, 2006.

[15] Higgins–Wilson–Fell i. m. (13. lj.) 166–184.

[16] Uo., 177–178.

verkalózkodástól."[17] Ezek a tényezők rezonálhatnak a hosszú távú bűnelkövetéstől való elrettentéssel, de elképzelhető, hogy a tanuláselméleti perspektíva értelmezésében a család negatív megerősítése *(negative reinforcement),* az innen származó retorzió is szerepet játszhat a bűnelkövetésből való kilépésben, a dezisztencia kialakulásában.

A digitális kalózkodás viszonylatában a racionális döntéselmélet más elméletekkel társulva is megjelenik, így például az önkontrollelméletekkel. Higgins 2007-ben az Egyesült Államokban vizsgálta az önkontroll és a racionális döntés kapcsolatát a digitális kalózkodás esetében.[18] A tanulmány Alex Piquero and Stephen Tibbetts közvetítő modelljén alapult,[19] amely a két – egyébként is rokon – elméletet transzformálhatóvá teszi oly módon, hogy az önkontroll mellett a racionális döntéselmélet szituációs jellemzőit is a vizsgálódás tárgykörébe vonja. Érdekes, hogy az önkontrollelméletet eredetileg a racionális döntéselméletre építették,[20] annak perspektívájában értelmezhető elképzelés volt. Az empirikus kutatások viszont később azt mutatták, hogy az alacsony önkontroll szerepét a bűnözésben a racionális választási vagy az elrettentési típusú intézkedések inkább mérsékelték, mint alátámasztották. Ezt követően azonban más kutatások mégis támogatták azt a feltevést, hogy a racionális döntéselmélet részben felerősíti az alacsony önkontroll és a bűnözés közötti kapcsolatot.[21] Azt tehát az informatikai bűnözéshez nem kapcsolódó egyéb kutatások is kimutatták, hogy a két elmélet egymással kölcsönhatásban bizonyos szinten képes magyarázni a bűnözést, így az informatikai bűnözés, ez esetben a kibertér által elősegített bűnözés csoportjába tartozó online kalózkodás okainak vizsgálatára is alkalmas lehet.

Higgins közel 400 egyetemista bevonásával elvégzett kvantitatív felmérésében a résztvevőket többek között különböző szituációk értékelésére kérték: el kellett dönteniük, hogy mely esetekben, mely következményekkel (pénzbüntetés, szabadságvesztés stb.), morális retorziókkal (szégyen, társadalmi elítélés) választanák egy szoftver illegális úton történő megszerzését. Zárt kérdések voltak továbbá a felelősségre vonás esélyének mértékéről, illetve arról, hogy mely esetekben tartózkodnának a cselekmények elkövetésétől, és mi számít értéknek számukra az online térben (digitális médiatartalom, szoftver birtoklása stb.).

A kutatás az alacsony önkontroll, a racionális döntéselmélet elemei és az egyén értékrendje között mutatott ki korrelációt. Higgins szerint önmagában az önkontroll alacsonyabb szintje növeli a digitális kalózkodás valószínűségét, és a digitális tartalom értéke szintén pozitívan hat

[17] Uo.

[18] George E. Higgins: Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value. 1(1) *International Journal of Cyber Criminology* (2007) 33–55.

[19] Alex Piquero – Stephen Tibbetts: Specifying the Direct and Indirect Effects of Low Self-Control and Situational Factors in Offenders' Decision Making: Toward a More Complete Model of Rational Offending. 13(3) *Justice Quarterly* (1996) 481–510.

[20] Christopher Birkbeck – Gary LaFree: The Situational Analysis of Crime and Deviance. 19 *Annual Review of Sociology* (1993) 113–137.; Michael R. Gottfredson – Travis Hirschi: *A General Theory of Crime*. Palo Alto, Stanford University Press, 1990.

[21] L George E. Higgins – Catherine D. Marcum: Can the Theory of Planned Behavior Mediate the Effects of Low Self-Control on Alcohol Use? 39 *College Student Journal* (2005) 90–103.; Daniel S. Nagin – Raymond Paternoster: Enduring Individual Differences and Rational Choice Theories of Crime. 27 *Law & Society Review* (1993) 467–496.; Stephen G. Tibbetts – David L. Myers: Low Self-Control, Rational Choice, and Student Test Cheating. 23(2) *American Journal of Criminal Justice* (1999) 179–200.

erre. A kutatás érdekessége, hogy míg a morális értékek és a szégyen csökkentik az elkövetés melletti döntést, addig a korábbi magatartás (pl. korábbi illegális letöltés, másolás) vagy a külső szankciók nem befolyásolják ugyanezt. A külső szankciók növekedésével, súlyosságának fokozódásával ugyanakkor a válaszadók számára csökkent az adott digitális tartalom értéke, ami indirekt módon redukálja az elkövetés melletti elhatározást.[22] A kutatás egyrészt arra világított rá, hogy az alacsony önkontroll direkt és indirekt kapcsolatban áll a digitális kalózkodással, másrészt az alacsony önkontroll indirekt kapcsolatban áll egyes szituációs faktorokkal (pl. a dolog értékével), harmadrészt a szituációs tényezők ugyancsak indirekt és direkt kapcsolatot mutatnak a digitális kalózkodással.[23]

Összességében tehát az önkontrollelmélet és a racionális döntéselmélet közötti kapcsolat, valamint ezek digitális kalózkodásra való alkalmazhatósága is – a szerző szóhasználatával élve – *lehetséges,* ugyanakkor hangsúlyozza, hogy a kutatás egyetlen egyetemen zajlott, illetve azt keresztmetszeti, és nem longitudinális vizsgálattal végezték, ami a két elmélet komplex tesztelésének gátja.

A racionális döntéselmélet informatikai bűnözésben való alkalmazásának másik körét a kibertérfüggő bűnözés területéhez tartozó technológia-központú bűncselekmények jelentik, amelyek esetében a felelősségre vonás elhanyagolható mértéke és a bűnelkövetéssel elérhető hasznok, valamint a megszerezhető értékek jelentős túlsúlya áll. E terület kutatásai közül a szakirodalom alapvető jelentőségűnek Michael Bachmann 2010-ben, hekkerekkel végzett kutatását tekinti,[24] amely a szerző doktori disszertációjának egyes elemeit is tartalmazza.[25] A kutatás a hekkerekkel végzett felmérések alacsony száma miatt nagy jelentőségű, hiszen e csoport elérése napjainkban is a kriminológiai kutatások állandó problémája. Bachmann elsősorban a szakirodalom által definiált, a bűnelkövető életmódot élő és az etikus hekkerek között elhelyezkedő csoportot, a szürke kalapos hekkereket *(gray hat)* vizsgálta egy hekkerkonferencián.

Kutatásában egyedülálló módon jelenik meg a – hekkerek tevékenysége vizsgálatakor gyakran hangsúlyozott – racionalitás, a megfontolt, mérlegelő magatartás értelmezése. Bachmann célja kettős volt: egyrészt meg kívánta vizsgálni, hogy a hekkerek között e felfogással ellentétben vannak-e kockázatkereső, izgalmat hajszoló személyek, illetve a közösség eltér-e jellemzőiben az átlagpopulációtól, másrészt azt akarta feltérképezni, hogy ebben az összefüggésben a hekkerek mennyire részesítik előnyben a racionális döntéshozatali folyamatokat és a különösen kockázatos tevékenységeket, valamint befolyásolja-e a hekkertevékenységek iránti elkötelezettséget az egyén által elért siker.[26] A kutatás kérdése az volt, hogy a hekkerek bizonyos kockázatos magatartásokban racionális kalkuláció eredményeként vesznek-e részt.

Mint azt Bachmann maga is bevallja, a racionális döntéselmélet esetében problémát jelent a döntési folyamatokban szerepet játszó racionalitás fokának és hatásának operacionalizálása,

[22] Higgins i. m. (18. lj.) 45.

[23] Uo., 48.

[24] Michael Bachmann: The Risk Propensity Computer Hekkers and Rationality. 4(1–2) *International Journal of Cyber Criminology* (2010) 643–656.

[25] Michael Bachmann: *What Makes Them Click? Applying The Rational Choice Perspective To The Hacking Underground*. Doktori értekezés, MA University of Mannheim (2004), https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=4790&context=etd.

[26] Bachmann i. m. (24. lj.) 664.

így annak mérése – ahogyan azt Higgins szoftverkalózkodás-kutatásában is láthattuk – a valósághoz hasonló, fiktív szituációkban hozott döntéseken keresztül történhet. Bachmann a kockázatok vállalására való hajlamot egy ötelemű skála, míg a racionalitást az ún. Rational-Experiential Inventory (REI) skála segítségével kérdezte le.

A kutatás két fő összefüggésre világított rá. Bachmann szerint egyrészt a hekkereknek valóban nagyobb igényük van a megismerésre, és készek nagyobb kockázatokat vállalni, ugyanakkor hajlamosabbak a racionális döntési stílusokat preferálni, és különösen biztosak abban, hogy racionális mérlegelési folyamatok révén képesek optimális döntéseket hozni. Másrészt a racionális döntéshozatali folyamatokat jobban kedvelő hekkerek, úgy tűnik, sikeresebb előkészítési, feltérképezési és támadási rutinokat folytatnak azoknál, akik kevesebb jelentőséget tulajdonítanak a racionális mérlegelésnek.[27]

A kutatás alátámasztja, hogy a hekkerek egy része – saját bevallásuk szerint – racionális döntések eredményeként, megfelelően mérlegelt eszközök kiválasztásával követ el amúgy nagy kockázattal járó büntetendő cselekményeket. Ugyanakkor az is kiderült, hogy egy részük az általánosnál gyakrabban vállal kockázatot, ami megkérdőjelezi a döntés tiszta racionalitását, és felveti azt a kérdést, hogy a saját tudásba vetett bizalom mennyiben nevezhető inkább korlátozott racionalitásnak. Arról nem is beszélve, hogy a kutatás igen kis elemszámmal, 124 hekker megkérdezésével készült egy olyan hekkerkonferencián, ahol a megkérdezettek jelentős része a szürke kalapos, illetve az etikus hekker kategóriákba sorolható, nem pedig a tipikus bűnelkövetői populációba.

A racionális döntési elméletekkel kapcsolatban jelezni szükséges, hogy önmagukban nem nyújtanak kielégítő magyarázatot az informatikai bűnözés okainak megismeréséhez, hiszen ezeknél a bűnelkövetés vizsgálata nélkülözi a bűnelkövetés mikro- és makrotársadalmi tényezőinek értelmezését, és néhány kivételtől eltekintve az egyénre ható külső és belső szocializációs hatásokat, egyéni személyiségjegyeket sem veszi figyelembe. Emellett az elmélet nagyobbrészt a bűnözés általános elméletével és az elrettentéselmélettel együttesen vizsgálható, mint ahogyan azt Higgins kutatásában is láthattuk, illetve Bachmann is a racionális döntések önkontrollténye zőkkel való összekapcsolhatóságára hívja fel a figyelmet.[28] Így megkérdőjelezhető az elmélet alkalmazhatósága az informatikai bűnözés oksági vizsgálatára, illetve önmagában annak magyarázó ereje alacsony, túlságosan leegyszerűsíti az informatikai bűnelkövetést mind a hagyományosabb, felhasználói szintű tudást igénylő cselekmények, mind a technológia-központú, informatikai tudáson alapuló devianciák esetében.

2.1.2. Rutintevékenységi elmélet

A rutintevékenységi elmélet az informatikai bűnözés kutatása terén széles körben ismert, ugyancsak a környezeti kriminológia, mi több, a szituációs bűnmegelőzés egyik alapjául szolgáló megközelítés. A Lawrence Cohen és Marcus Felson által 1979-ben kialakított struktúra a bűn-

[27] Uo., 652.
[28] Uo.

alkalmak felől közelít, vagyis a konkrét – elsősorban ragadozó típusú – szabályszegések bekövetkeztéhez szükséges körülmények fennállását vizsgálja.[29] A bűncselekmény három feltétel teljesülése esetén valósul meg: 1. motivált elkövető; 2. megfelelő célpont; 3. alkalmas őrző (védelem) hiánya. Amennyiben bármelyik komponens hiányzik, a bűncselekmény elmarad. Az elmélet kifejezetten alkalmas azon megközelítés alátámasztására, miszerint a támadó és az áldozat interakciójának mesterséges befolyásolásán keresztül csökkenthető a bűnözés. A szituáció értelmezésén túl figyelembe veszi a társadalmi (pl. a nők foglalkoztatottságának növekedése) és technológiai (pl. a fejlettebb elektronikai eszközök megjelenése) változások hatását is a nemzeti bűnözési rátákra.

Parti Katalin az elmélet technológiai vonatkozásával kapcsolatban John Eck és Ronald Clarke 2003-as tanulmánya nyomán jelzi,[30] hogy a fizikai kapcsolat és az időbeni eltérés ellenére a kibertér megkönnyíti az áldozat és az elkövető konvergenciáját.[31] Ennek következtében helytálló Cohen és Felson azon meglátása, hogy a technológiai eszközök terjedése is hatással van a bűncselekmények elkövetésére.[32] Az elmélet szerint továbbá a bűnözés a legális tevékenységekre épül, így a munka, a tanulás, a szabadidő eltöltésének módja és ideje meghatározó jelentőségű lehet annak alakulásában. Az elmélet elsősorban az áldozattá válás megelőzésének kérdése felől közelít, annak is a mechanikai megközelítését kínálja, ugyanis nem tekint a bűnözés szélesebben értelmezett oksági folyamatai mögé. Az elmélet alkalmazásának elsődleges célja így a gyakorlatban e három tényező együttes fennállásának megszüntetése.

Az elmélet az informatikai bűnelkövetővé válásra, valamint általánosabban az elkövetőre ható tényezők vizsgálatára kevéssé alkalmas, az online térben is csupán a cselekmény közvetlen megelőzésében nyújthat segítségét. Az elkövetőkről ugyanis Cohen és Felson elmélete feltételezi, hogy azok (pl. akiben megvan mind a hajlandóság, mind a képesség az elkövetésre) mindig jelen lehetnek, és különféle vágyak irányíthatják őket, legyen az anyagi, érzelmi vagy szexuális.[33] A vizsgálódás igazi tárgya a mindennapi tevékenységeit folytató megfelelő áldozat és az alkalmas védelmi lehetőségek hiányának feltérképezése. Az elmélet jelentősége – bár az elkövetőkről itt sem foglal állást – abból fakad, hogy az online térben való jelenlét, számos egyéb tevékenységtől eltérően, olyan választott magatartásforma, amelynek folytonossága, gyakorisága, iránya és tartalma gyakran mintaszerű, annak menete megfelelő technológiai készségekkel, de akár csupán jó megfigyelőkészséggel is könnyedén nyomon követhető. Az online tér által nyújtott lehetőségek, az ott végezhető cselekmények száma folyamatosan növekszik, ami a jelenlét megnövekedett időtartamát és a látogatási gyakorlatok, egyéni preferenciák kialakítását

[29] Lawrence E. Cohen – Marcus Felson: Social Change and Crime Rate Trends: A Routine Activity Approach. 44(4) *American Sociological Review* (1979) 588–608.

[30] John E. Eck – Ronald V. Clarke: Classifying Common Police Problems: A Routine Activity Approach. 16(7) *Crime Prevention Studies* (2003) 7–39.

[31] Katalin Parti: Suitable Targets and Capable Guardians Online. An Expansion of The Integrated Cyber-Lifestyle/Routine Activity Theory Explaining Online Victimization. *Victims & Offenders* (megjelenés előtt).

[32] Cohen–Felson i. m. (29. lj.).

[33] Uo., 589.

eredményezi. E folyamathoz hozzájárulhat például a kiskorúak áldozattá válása tekintetében a társadalmi nyomás hatására folytatott online jelenlét (*fear of missing out* – félelem a kimaradástól) is.[34]

Az online tér sajátossága, vagyis az anonimitás és a nyomon követhetőség dichotómiája is fontos ezen elméleti megközelítés szempontjából. Az internet egyszerre szavatolja, legalábbis látszólag, a névtelen jelenlét és az aktivitás lehetőségét, valamint egyszerre könnyíti meg a társadalom és az egyének megfigyelhetőségének folyamatát. Az előbbi valójában a *látszatanonimitásba* vetett hitből ered az átlagfelhasználók szintjén, a megfelelő technológiai ismeretekkel rendelkezők számára viszont valódi anonimitást biztosít.[35] A megfigyelhetőség tényezői ennél egyértelműbbek, így azok az önkéntesen megosztott információkból vagy a megfelelő garanciák nélkül terjesztett személyes adatok viszonylag könnyű elérhetőségéből épülnek fel. A területen végzett kutatások jelentősebb része ezért az áldozattá válás mintázataira világít rá. Gyakran találkozunk itt mind a hagyományosabb kibertér által elősegített, mind a kibertérfüggő cselekmények vizsgálatával. Az előbbihez például az online megfélemlítéssel *(cyberbullying),* a zaklatással *(cyberharassment, cyberstalking)* és a hagyományos csalásokkal foglalkozó kutatások, míg az utóbbihoz az adathalászat *(phishing),* a jogosulatlan behatolás és a kártékony szoftveres *(malware)* támadások vizsgálatai tartoznak.

A kibertérfüggő cselekmények területen végzett kutatások tanulságai szerint az online közösségi felületeken (pl. chatszobák, közösségi média, instant üzenetküldő alkalmazások) való részvétel időtartama hatással van a motivált elkövetőknek való kitettségre,[36] az online képmegosztás pedig növeli a zaklatás esélyét.[37] Ehhez hasonló jelenségre hívja fel a figyelmet Eric Leukfeldt és Majid Yar 2016-os holland mintán végzett kutatása is,[38] amelynek eredményei szerint a direkt üzenetküldő alkalmazások használata, mint pl. az e-mail, az MSN (a Microsoft által már megszüntetett instant üzenetküldő alkalmazás), a Skype vagy a Twitter megnöveli az interperszonális viktimizáció lehetőségét, mert ezek fokozzák az egyén láthatóságát az online térben.[39]

Mint fentebb említettem, az elmélet nem kifejezetten alkalmas az e tanulmányban is érintett bűnelkövetővé válás vizsgálatára, mert a bűnelkövetőt csupán a viktimizáció bekövetkeztét elidéző aktornak tekinti. Sőt, egyes kutatások arra is felhívják a figyelmet, hogy az online közösségekben részt vevő, nagyobb informatikai tudással rendelkezők, sőt az illegális tevékenységet folytatók és a hekkerek maguk is olyan tevékenységi mintákat követnek,[40] amelyek megnövelik

[34] Robin M. Kowalski – Gary W. Giumetti: Bullying in the Digital Age. In: Elena Martellozzo – Emma A. Jane (szerk.): *Cybercrime and its Victims*. London, Routledge, 2017. 167–169.

[35] Parti Katalin – Virág György: A szájbergyerek és a bicikli. A kelet-európai gyerekek nethasználatának specifikumai. In: Virág György (szerk.): *Kriminológiai Tanulmányok 48*. Budapest, OKRI, 2011. 29–48., 42–43.

[36] Holt–Bossler i. m. (4. lj.) 69.

[37] Bradford W. Reyns – Billy Henson – Bonnie S. Fisher: Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. 38(11) *Criminal Justice and Behavior* (2011) 1149–1169.

[38] Eric R. Leukfeldt – Majid Yar: Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. 37(3) *Deviant Behavior* (2016) 263–280.

[39] Thomas J. Holt – Adam M. Bossler – Katheryn C. Seigfried-Spellar: *Cybercrime and Digital Forensics: An Introduction*. London, Routledge, 2017. 465.

[40] Bill Chu – Thomas J. Holt – Gail Joon Ahn: *Examining the Creation, Distribution, and Function of Malware On-Line.* Washington, National Institute of Justice, 2010.

saját viktimizációjuk lehetőségét.[41] Erre példa a gyakori *malware*-támadások elszenvedése, az illegális szoftverletöltéssel együtt járó áldozattá válás,[42] illetve az adathalászatnak való kitettség növekedése.

Az ezen elméleti alapon végzett kutatások elkövetői oldalról csupán annyit mondanak, hogy az online tér bűnözői, különösen a hekkerek és az adathalászatot elkövetők a saját tevékenységüket gyakran a társadalom időbeosztásához igazítják, így például az adathalász tartalmú e-mailek küldése is gyakrabban fordul elő az átlagos munkaórák alatt. Erre David Maimon ún. mézesbödönöket *(honeypot)*[43] vizsgáló izraeli kutatása szolgáltat empirikus tapasztalatot.[44] Cohen és Felson rutintevékenységi elmélete összességében tehát az online tér által nyújtott nagy cselekvési szabadság, az anonimitás látszata, a nagyfokú megfigyelhetőség és a technológiai védelem meglétének vagy hiányának központi szerepe miatt valóban képes hasznos ismeretekkel szolgálni a megelőzés fejlesztéséhez. Az internet fejlődésének sajátja ugyanis, hogy az itt megjelenő büntetőjogi normasértések megelőzése, kezelése gyakran a magánbiztonság piacának, a technológiai vállalatok biztonsági intézkedéseinek terepe. Így e megközelítésből merítve építkeznek nem csupán a bűnmegelőzési gyakorlatok, de a jelenleg zajló közösségi médiaszolgáltatásokkal kapcsolatos szabályozási modellek is, amelyek egyre nagyobb felelősséget rónak a szolgáltatások által kialakítandó moderátori, panaszkezelési és jogsértés-kezelési tevékenységre.

A rutintevékenységi elmélet bár alkalmazható e téren, kevés információval kecsegtet az informatikai bűnelkövetés miértje tekintetében. Az elmélet három tényezőjének vizsgálatakor mindössze a bűncselekmények elkövetésének előszobájából kaphatunk rálátást az online tér bűnelkövetőire, jelenlétük valójában 'csak' az áldozatok aktivitásának fényében, egyfajta reakcióként válik értelmezhetővé.

2.2. Kontroll- és kötődéselméletek

Az informatikai bűnözés, valamint az elkövetővé válás elméleti áttekintésének kihagyhatatlan csoportja a kontrollelméleteké. Ennek sajátossága, hogy célja nem annak magyarázata, miért követ el valaki bűncselekményt, hanem fordítva, azt vizsgálja, hogy miért marad távol a társadalom többsége a bűnözéstől. Akár a külső, akár az egyén viszonylatában értelmezett belső

[41] Holt–Bossler i. m. (4. lj.) 70. A fiatalok *harassment* viktimizációja és a fejlettebb technológiai készségek kapcsolatáról l. Adam M. Bossler – Thomas J. Holt – David C. May: Predicting Online Harassment Victimization Among a Juvenile Population. 44(4) *Youth & Society* (2012) 500–523.

[42] Holt–Bossler i. m. (4. lj.) 71. L. még Scott E. Wolfe – George E Higgins – Catherine D. Marcum: Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses. 26(3) *Social Science Computer Review* (2008) 317–333.; Thomas J. Holt – Heith Copes: Transferring Subcultural Knowledge On-Line: Practices and Beliefs of Persistent Digital Pirates. 31(7) *Deviant Behavior* (2010) 625–654.

[43] A *honeypot* egy olyan nyomozati szoftvercsapda, amely egyebek mellett képes a hekkertevékenységek adatainak rögzítésére és elemzésére. A fogalom főként az adathalászattal kapcsolatban értelmezhető, amely tevékenység vizsgálatakor az elemzést végző személy szándékosan hoz létre és használ támadó e-mail-címeket, számítógépeket, így rögzíthetővé válnak a támadások adatai. Bachmann i. m. (25. lj.) 165.

[44] Holt–Bossler i. m. (4. lj.) 72.; David Maimon et alii: Daily Trends and Origin of Computer-Focused Crimes Against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective. 53 *British Journal of Criminology* (2013) 319–343.

önkontrolltényezőkre gondolunk, ez az elmélet kifejezetten népszerű az informatikai bűnözés tekintetében. Ennek okai között olyan tényezők említhetők, mint az online tér távolító hatása, a „képernyőarc-effektus", az alacsony felderítettség vagy az anonimitásba vetett hit elemeinek fontossága,[45] amelyek a terület kutatói szerint felpuhítják a bűnözéstől távol tartó társadalmi és önkontrollok szerepét. Ezen elméletek informatikai bűnözésre való alkalmazása talán az egyik legtöbbet kutatott terület, és számos empirikus vizsgálat alapjául szolgált. A tanulmány e részében a kontrollelméletek két legismertebbikét, az általános bűnözéselméletet és a társadalmi kötődéselméletet tekintem át.

2.2.1. Általános bűnözéselmélet

Michael Gottfredson és Travis Hirshi elképzelése a kontrollelméletek azon alapfeltevéséből indul ki, hogy az egyén a bűnözést az általános természete egy funkciójaként, az elérni kívánt jutalmak megszerzésének vágya okán választja, legyen az akár gazdasági, akár érzelmi kielégülés.[46] Az elmélet szerint minden motiváció azonos mértékű az emberek között, vagyis senki sem motiváltabb a másiknál a bűnözésre. Ami mégis elválasztja a bűnözőket a jogkövetőktől, az az egyénre nehezedő kontroll mennyisége. E kontroll lehet jogi, társadalmi, iskolai, családi, baráti, vagy intézmények, csoportok felől jövő. Feltevésük szerint a bűnelkövetőkre nehezedő kontroll egyszerűen alacsonyabb szintű, így könnyebben engednek vágyaiknak, akár illegális tevékenységeken keresztül is.[47]

Az elmélet szerint a bűnelkövetéshez nem szükségesek kiforrott képességek vagy készségek, a bűnözés egyszerű szakma, ami könnyen nyújthat kielégülést, az elkövetők pedig osztanak bizonyos viselkedés- és attitűdbeli jellemzőket, mint például az impulzivitást, rövid előrelátási képességet, érzéketlenséget és kockázatkereső magatartást.[48] A bűnözői magatartás így az egyén alacsony önkontrolljának, a viselkedés belső korlátozási képessége hiányának a következménye.[49] Az elképzelés szerint az alacsony önkontroll felelős az iskolai kudarcokért, a rossz kapcsolatokért, a kockázatos magatartásokért, így például a dohányzásért, az alkohol- és a kábítószerfogyasztásért, amelyek mind kapcsolatban állnak a későbbi bűnelkövetéssel is.

Az elmélet, ezen belül is az alacsony önkontroll szerepének vizsgálata a bűnözésben – hasonlóan a tanuláselméleti perspektívához – az egyik legismertebb területnek számít a bűnözéskutatásban, ezért nem meglepő, hogy az informatikai bűnözés vizsgálatában is központi szerepet játszik. Az általános bűnözéselmélet népszerűségét növeli, hogy számos egyéb elméleti megközelítéshez is jól illeszkedik – ez látható a fentebb említett racionális döntéselméletekkel való összekapcsolásából, de megjelenik többek között a tanuláselméletekkel, a fejlődéskriminológiai perspektívával és a neutralizációelmélettel integrált megközelítésekben is.

[45] Parti Katalin: Devianciák a virtuális valóságban, avagy a virtuális közösségek személyiségformáló ereje. *Infokommunikáció és Jog,* 2007/2. 57–64., 60.; Marcus K. Rogers: *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory STUDY*. Doktori értekezés (2003), 57–58.

[46] Gottfredson–Hirschi i. m. (20. lj.).

[47] Uo., 90.; Holt–Bossler–Seigfried-Spellar i. m. (39. lj.) 449.

[48] Holt–Bossler i. m. (4. lj.) 84.

[49] Gottfredson–Hirschi i. m. (20. lj.).

Az önkontroll szerepét vizsgáló tanulmányok a kibertér által elősegített bűncselekmények területén hódítanak igazán, aminek oka az elmélet általános jellege és a bűnözést mint 'egyszerű szakmát' feltételező megközelítése, így az informatikai bűnözés nem kifejezetten bonyolult, laikus felhasználói szinttel is kivitelezhető formáinak vizsgálatára alkalmas igazán. Ezek közül is legjelentősebbek a könnyebben elkövethető, impulzivitáson vagy egyszerű lépéseken alapuló elkövetések, mint például az online zaklatás *(harassment, stalking),* a megfélemlítés *(cyberbullying)* vagy éppen a digitális kalózkodás vizsgálata. E kibertér által elősegített cselekmények felmérései mellett találunk néhány kibertérfüggő kriminalitással foglalkozó kutatást is, ugyanakkor ezek száma jóval alacsonyabb. E téren különösen a *hacking,*[50] a jogosulatlan behatolás, a *malware*-készítés, valamint egyéb automatizált elkövetési formák és módszerek vizsgálata körében mutatkozik hiány. Ennek oka elsősorban a technológia-központú elkövetés nagy specializációigénye, a megfontoltabb döntéshozatal és a komplex tudás szükségessége, ami nem kifejezetten fér bele – hasonlóan a fehérgalléros bűnözéshez – az általános bűnözéselmélet alapvetésébe.

Az átlagfelhasználókat vizsgáló kutatások közül érdemes kiemelni Hyunin Baek és munkatársai 2016-ban több mint 1000 fős mintán végzett kutatását, amely az alacsony önkontrollnak az online zaklatás elkövetésében játszott szerepét kívánta feltárni.[51] A kutatás vállalkozott továbbá a lehetőség moderáló hatásának felmérésére is e kontextusban, ami a szituációs megközelítéshez áll közel. Ez utóbbi alkalmazását indokolja, hogy Gottfredson és Hirschi elmélete szerint azok, akik alacsonyabb önkontrollal rendelkeznek, hajlamosabbak bűncselekményt elkövetni, és mindezt kifejezetten akkor, ha lehetőség kínálkozik az elkövetésre.[52]

A kutatás eredményei közül leginkább figyelemre méltó az a megállapítás, miszerint a nemek tekintetében eltérő az alacsony önkontroll, a lehetőség és az online zaklatás kapcsolata a fiatalkorú elkövetők esetében. Ez azt jelenti, hogy a serdülőkorú, alacsony önkontrollal rendelkező fiúk nagyobb valószínűséggel követnek el online zaklatást, mint a magasabb önkontrollal rendelkező társaik.[53] Emellett e modellben a számítógép-használat feletti kontroll csökkenése az elkövetés nagyobb valószínűségével jár együtt. A serdülőkorú lányok esetében szintén kimutatható volt az alacsony önkontroll és az online zaklatás elkövetése közötti kapcsolat, ugyan-

[50] A *hacking* a szakirodalom jelentős részében mint a jogosulatlan behatolás szinonimája jelenik meg, ugyanakkor a kutatásokban eltérő e cselekmények körének meghatározása. Idetartozhat az egyszerű belépés, amely valamely kifürkészett (meglesett) jelszó felhasználásával történik (l. pl. Skinner és Fream később ismertetett kutatását), vagy a technológiai manipulációval megvalósított behatolás. A fogalom szolgálhat komplexebb informatikai manipulációk megnevezésére is. E tanulmányban a *hacking*et ez utóbbihoz hasonlóan definiálom, így az ismertetett kutatásokban szereplő *hacking*fogalmakkal szemben a következő minimumdefiníciót alkalmazzuk a kutatási eredmények értékelése során: a *hacking* körébe tartozó cselekmény a rendszerbe való behatolás, az ezt megkönnyítő vagy egyéb – akár hagyományos bűncselekményhez használatos – program létrehozása, program vagy programegység megváltoztatása, funkcióinak átalakítása. E tevékenység egyediségét erősíti, hogy a cselekmény 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. L. bővebben: Varga i. m. (2. lj.).

[51] Hyunin Baek – Michael M. Losavio – George E. Higgins: The Impact of Low Self-Control on Online Harassment: Interaction with Opportunity. 11(3) *Journal of Digital Forensics, Security and Law* (2016) 27–42.

[52] Győry Csaba: Kontrollelméletek. In: Borbíró i. m. (3. lj.) 186.

[53] Baek–Losavio–Higgins i. m. (51. lj.) 37.

akkor a lehetőség, így a számítógéphez való hozzáférés nem volt hatással az elkövetésre. Sőt a kutatás eredményei szerint összességében az impulzívabb, alacsony előrelátási képességgel rendelkező, kockázatkereső fiatalok a megfelelő lehetőségek hiányában is nagyobb valószínűséggel követnek el online zaklatást, mint ezekkel az attribútumokkal nem rendelkező társaik. Ugyanakkor a szerzők jelzik, hogy az általános bűnözéselméletet vizsgálók már többször szembesültek a nők bűnözése és a lehetőség közötti disszonancia problémájával, ami némileg kikezdi Gottfredson és Hirschi elméletének általános érvényű feltételezéseit.[54]

Hasonló területen végeztek Vazsonyi és társai kutatást 2012-ben a *cyberbullying* és az alacsony önkontroll kapcsolatának tekintetében az EU Kids Online projekt keretében.[55] Csak kevés kutatás foglalkozik kifejezetten e területtel,[56] mégis érdemes megemlíteni az itt született eredményeket, tekintve, hogy a *cyberbullying* a kibertér által elősegített bűnözés egyik legjellemzőbb formája napjainkban. A felmérés célja volt az alacsony önkontroll hatásának vizsgálata mind az áldozattá válás, mind az elkövetés tekintetében. A kutatás fiatal lányok és fiúk bevonásával készült, és a *cyberbullying* mellett a hagyományos *bullying* elemeinek vizsgálatát is tartalmazta. A 25 európai országban végzett felmérés, amely fejlődéskriminológiai perspektívában kívánta értelmezni az önkontroll szerepét, ugyancsak rávilágított az alacsony önkontroll és az elkövetés közötti kapcsolatra, ugyanakkor e területen csupán mérsékelt egyezést mutatott.[57] Ennél érdekesebb a kutatás azon célja, hogy az alacsony önkontroll és a viktimizáció kapcsolatát vizsgálja. E tekintetben nem meglepő módon az eredmény az alacsony önkontroll csupán kis szerepének igazolása volt.[58] E kutatás is a lányok alacsonyabb elkövetői részvételéről tudósít, amelynek okát a nők magasabb önkontrolljában látja. Ugyanakkor érdemes megjegyezni, hogy mindkét nem esetén elsősorban indirekt kapcsolatot jelez Gottfredson és Hirschi elméletével. Az értekezés szerint e jelenség mögött elképzelhető, hogy a John Suler által 2004-ben megfogalmazott *disinhibition effect* áll,[59] aminek vizsgálata megfontolandó a *cyberbullying* esetében is.[60] Ugyancsak fontos megemlíteni, hogy a vizsgált országok közötti eltérés csupán 10% és 20% között mozgott, mégis felveti a kontrollintézmények eltérő szocializációs szerepének kérdését, ami egy újabb perspektívát nyithat meg a *cyberbullying* kutatása terén.[61]

A digitális kalózkodás népszerű témájával is több kutatás foglalkozott az elmúlt években, ilyen volt többek között Christopher Donner és munkatársai 2014-ben,[62] Higgins, Scott Wolfe

[54] Uo., 39.

[55] Alexander T. Vazsonyi – Hana Machackova – Anna Sevcikova – David Smahel – Alena Cerna: Cyberbullying in Context: Direct and Indirect Effects by Low Self-Control Across 25 European Countries. 9(2) *European Journal of Developmental Psychology* (2012) 210–227.

[56] L. James D. Unnever – Dewey G. Cornell: Bullying, Self-Control, and ADHD. 18(2) *Journal of Interpersonal Violence* (2003) 129–147.; Dana L. Haynie: Delinquent Peers Revisited: Does Network Structure matter? 106(4) *American Journal of Sociology* (2001) 1013–1057.

[57] Vazsonyi et al. (55. lj.) 214–215., 224.

[58] Uo., 224.

[59] John Suler: The Online Disinhibition Effect. 7(3) *Cyberpsychology and Behavior* (2004) 321–326.

[60] Vazsonyi et al. i. m. (55. lj.) 226.

[61] Uo., 226.

[62] Christopher M. Donner et alii: Low Self-Control and Cybercrime: Exploring the Utility of the General Theory of Crime Beyond Digital Piracy. 34(1) *Computers in Human Behavior* (2014) 65–172.

és Catherine Marcum 2008-ban megjelent írása,[63] illetve a tanuláselmélettel integráltan vizsgálta a kérdést Higgins 2007-ben.[64] E kutatások mindegyike alátámasztotta az alacsony önkontroll és a szoftverkalózkodás közötti pozitív korrelációt.

Az általános bűnözéselmélet fentebb említett alacsonyabb informatikai készségigénye okán a kibertérfüggő bűnözés magyarázatával csupán néhány kutatás foglalkozik, mégis fontos szót ejteni a kártékony *hacking* elkövetőiről (amely e tanulmány esetében minden technológiai manipulációval, a technológiai készségek felhasználásával megvalósított informatikai bűncselekményt magában foglal, l. 51. lábjegyzet) kontrollelméleti perspektívából. A hekkerekkel kapcsolatos kutatások egyrészt rávilágítanak arra, hogy a nagy technológiai precizitást igénylő elkövetés, így például a *malware*-készítés nagy energia- és időbefektetést, higgadt gondolkodást igénylő cselekmények, amelyek nem konzisztensek az általános bűnözéselmélet alapkoncepciójával.[65] A kutatások másik része, amelynek többsége Thomas Holt és Max Kilger 2012-es gondolatait emeli ki,[66] azt hangsúlyozza, hogy Gottfredson és Hirschi elmélete csupán a hekkerek azon részére lehet alkalmazható, amelyik nem rendelkezik fejlett technológiai készségekkel (a szakirodalom őket *script kiddie*-knek hívja), így előre elkészített programokat, technikákat, mások által kifejlesztett módszereket és eszközöket használnak, vagyis cselekményük során jobban megjelenik az alacsony önkontroll által vezérelt szükségletkielégítés.[67] Más írások is felhívják a figyelmet arra, hogy a hekkerek populációja erősen diverzifikált, így nem lehetséges egyetlen elmélettel magyarázni az összes elkövetést. Ennek megfelelően egyes kutatások szerint a hekkerek hosszú távú célok nélkül, mások szerint átgondoltan és komplexebb célokkal követik el a szabályszegéseket.[68]

Merőben más irányt képviselnek azok a kutatások, amelyek az önkontrollelméletet Ronald Akers tanuláselméletével kapcsoljak össze. Ilyen például Adam Bossler és George Burruss tanulmánya,[69] Marcum és munkatársai kutatása,[70] valamint átfogóbban az informatikai bűnözésről Holt, Bossler és David May kutatása.[71] E tanulmányok azt hangsúlyozzák, hogy a fenti problémákból eredően a kibertérfüggő elkövetést önmagában az alacsony önkontroll nem képes magyarázni, ezért a tanulási folyamatok vizsgálatának bevonása is szükséges. Bossler és Burruss

63 George E Higgins – Scott E. Wolfe – Catherine D. Marcum: Digital Piracy: An Examination of Three Measurements of Self-Control. 29(5) *Deviant Behavior* (2008) 440–460.

64 George E Higgins: Digital Piracy: An Examination of Low Self-Control and Motivation Using Short-Term Longitudinal Data. 10(4) *Cyberpsychology and Behavior* (2007) 523–529.

65 Holt–Bossler–Seigfried-Spellar i. m. (39. lj.) 452.

66 Thomas J. Holt – Max Kilger: Examining Willingness to Attack Critical Infrastructure Online and Offline. 58 (5) *Crime and Delinquency* (2012) 798–822.

67 L. még Catherine D. Marcum et alii: Hacking in High School: Cybercrime Perpetration by Juveniles, 35(7) *Deviant Behavior* (2014) 581–591.

68 Zhengchuan Xu – Qing Hu – Chenghong Zhang: Why Computer Computer Become Talents Hekkers. 56(4) *Communications of the ACM* (2013) 64–74., 71.

69 Adam M. Bossler – George W. Burruss: The General Theory of Crime and Computer Hacking: Low Self-Control Hekkers? In: Thomas J. Holt – Bernadette H. Schell (szerk.): *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey, Information Science Reference, 2011. 38–67.

70 Marcum i. m. (67. lj.).

71 Thomas J. Holt – Adam M. Bossler – David C. May: Low Self-Control, Deviant Peer Associations, And Juvenile Cyberdeviance. 37(3) *American Journal of Criminal Justice* (2012) 378–395.

ezzel kapcsolatban azt találta, hogy az alacsonyabb önkontrollal rendelkező egyetemi hallgatók nagyobb valószínűséggel kerülnek kapcsolatba az informatikai bűnözés tanulási folyamatát elősegítő csoportokkal, és nyitottabbak az innen származó megerősítésre is.[72] Holt, Bossler és May középiskolai diákokkal végzett kutatása pedig azt mutatta, hogy az alacsony önkontroll minden típusú kiberdevianciát hasonló mértékben jelez előre. A kutatás rávilágított arra is, hogy a kortárs csoportok bűnelkövetésének hatása erősebb az alacsony önkontroll szerepénél,[73] de azt ők is megerősítették, hogy az alacsony önkontroll és a kortárs csoportok nyomása egymást felerősítő tényezőként vannak jelen az informatikai bűnözés esetében.[74] Marcum és munkatársai középiskolai mintán elvégzett *hacking*-kutatásának érdekessége,[75] hogy külön vizsgálta az egyes magatartásokat. Eredményeik azt mutatták, hogy például a mások e-mailjébe való engedély nélküli belépés esetében a kortárs csoportok megerősítése alátámasztható, míg ugyanez az alacsony önkontroll esetében nem állítható. Érdekesség, hogy a Facebook-belépés esetében a fiatalabbak körében mindkét elmélet igazolható volt, ugyanakkor az idősebbek kevésbé vettek részt hasonlóban. A kutatás a weboldalakra történő jogosulatlan belépés esetében is alátámasztotta mindkét elmélet vizsgált elemeinek szignifikanciáját.[76]

A fentebb röviden ismertetett kutatások rámutatnak arra a Holt, Bossler és Katheryn Seigfried-Spellar által hangsúlyozott álláspontra,[77] miszerint az alacsony önkontroll ugyan kapcsolatban áll az informatikai bűncselekmények elkövetésével, az elsősorban csak az alacsonyabb informatikai készségeket igénylő cselekmények, illetve a kibertér által elősegített 'hagyományosabb' devianciák esetében támaszható alá. Holt, Bossler és May kutatásából is látható, hogy a hekkerekkel végzett felmérések is leginkább csupán az alacsonyabb belépési küszöbbel bíró cselekményekre terjednek ki (pl. jelszókifürkészéssel való e-mail-, Facebook-belépés). Azon kutatások pedig, amelyek a magasabb tudást igénylő, technológia-központú elkövetést vizsgálják, az önkontrollal szemben a tanulási elmélet által hangsúlyozott kortárs megerősítést és a tanulási folyamatok nagyobb magyarázó erejét mutatják, illetve jelzik, hogy a hekkerek kutatásához vélhetően több elméleti megközelítés vegyítésére lehet szükség.[78] Bossler és Burruss ugyan alátámasztják az alacsony önkontroll szerepét az elkövetésnél, de a tanulási perspektíva bevezetésekor azt látták, hogy azon hekkereknek, akik a nagyobb specializációt igénylő elkövetési módszereket is meg akarták tanulni, nagyobb önkontrollra volt szükségük, mint az egyszerűbb elkövetési formáknál maradó társaiknak.[79] Ennek következtében elképzelhető, hogy Gottfredson és Hirschi elmélete elsősorban a kisebb súlyú, alkalomszerű és alacsonyabb tudást igénylő cselekmények esetében alkalmas az informatikai bűnözés magyarázatarára.

[72] Bossler–Burruss i. m. (69. lj.).

[73] Holt–Bossler–May i. m. (71. lj.).

[74] Holt–Bossler–Seigfried-Spellar i. m. (39. lj.) 452.

[75] Kutatásukban a *„hacking"* kifejezetten a jogosulatlan belépés cselekményeit jelentette, így a technológia manipulációval megvalósított belépés mellett a jelszókifürkészéssel és egyéb módon végrehatott behatolások is a kutatás részét képezték.

[76] Marcum i. m. (67. lj.) 588–589.

[77] Holt–Bossler–Seigfried-Spellar i. m. (39. lj.) 449–453.

[78] Holt–Bossler i. m. (4. lj.) 85.

[79] Bossler–Burruss i. m. (69. lj.) 57.

2.2.2. Társadalmi kötődéselmélet

Hirschi következőkben ismertetett teóriája a kontrollelméleti perspektívához hasonló konstrukcióra épül, mégis más fókuszba helyezi a bűnelkövetés okát: annak központi eleme az egyén tágabb környezete. Elmélete szerint „a társadalmi kontrollmechanizmust azok a kötelékek jelentik, amelyek az egyént a szűkebb csoportjának más tagjaihoz, vagy a csoport egészéhez kötik."[80] Ezek az elmélet szerint főleg mikroszociológiai kötelékek, így nem kifejezetten a jogi kontrollra utalnak, hanem az informális, az egyén közvetlen társadalmi kötelékeit jelentik. E kötelékek Hirschi szerint természetük alapján négy típusba sorolhatók: a kötődés, az elkötelezettség, a részvétel és a hit csoportjába.[81] Az informatikai bűnözés kutatásában a társadalmi kötődés elméletének tesztelése jelentősen alulmarad a bűnözés általános elméletével szemben, mindazonáltal találhatunk példákat az elmélet önálló alkalmazására és annak összekapcsolására az általános bűnözéselmélettel, illetve Akers társadalmi tanuláselméletével is.

A Hirschi elméletét önállóan alkalmazó informatikai bűnözés kutatások közül érdemes megemlíteni a nemzetközi projekt keretében végzett ISRD-2 felmérést, amelynek hazai eredményeit Parti 2008-ban dolgozta fel.[82] A kutatás a nemzetközi standardoknak megfelelően arra volt kíváncsi, hogy a fiatalok számítógép-használata és a társas kapcsolataik, így a családhoz vagy a kortársakhoz való kötődés, a közös időtöltés és az átlagosnál hosszabb időtartamú számítógép-használat között felfedezhető-e disszonancia, illetve a társas kapcsolatok hiánya, az online térben 'magányosan' töltött idő kapcsolatban áll-e egyes online devianciákkal.[83] „A kutatás hipotéziseit mindenekelőtt Hirschi társadalmi kötődés teóriája határozta meg, fókuszálva a szülőkre, az iskolára, a barátokra, a vágyakra, valamint a szabadidős foglalkozásokra."[84] A kutatási kérdőív egyrészt a kisebbséghez tartozást, az áldozattá válást, a családi, iskolai és lakókörnyezeti kötődést, valamint a szabadidő-eltöltési szokásokat vizsgálta, másrészt a különböző devianciákra, így a számítástechnikai elkövetésre is rákérdezett. Fontos megemlíteni, hogy Parti hangsúlyozza az életútelmélet képviselőinek azon megállapítását, amely szerint az online közösségekben ismert deviáns magatartások és a társak általi megerősítés fontos szerepet játszanak a fiatalok későbbi személyiségének fejlődésében.[85]

A vizsgálat összefoglaló tanulmányából kiderül, hogy azon fiatalok, akiknek van számítógépük, internet-hozzáférésük, televíziójuk, kevesebb időt töltenek a társas kapcsolatok ápolásával, barátokkal, mint akik ilyen hozzáféréssel nem rendelkeznek. Emellett igaz az is, hogy az időt a barátaikkal töltő fiatalok kevesebb időt töltenek számítógép-használattal, illetve televíziónézéssel. Azok viszont, akik szabadidejükben a családjukkal vagy egyedül vannak, több időt töltenek számítógép-használattal, játékokkal, online csevegéssel vagy televíziónézéssel.[86]

[80] Győry i. m. (52. lj.) 182.

[81] Travis Hirschi: *Causes of Delinquency*. New York, Routledge, 2001. 334.

[82] Parti Katalin: Számítástechnikai devianciák és társadalmi kötődés (ISRD-2). *Kriminológiai Tanulmányok 45.* (2008), 149–174.

[83] Uo., 149–153.

[84] Uo., 149.

[85] Uo., 150–151.

[86] Uo., 154–156.

A felmérés legérdekesebb részét a megkérdezettek kriminális viselkedésekkel kapcsolatos válaszai jelentik. A kutatásban két deviáns cselekményre, a prekriminálisnak értékelt illegális fájlletöltésre és a hekkelésre kérdeztek rá.[87] A megkérdezettek több mint 32%-a gondolt már arra, hogy a fájlletöltés morálisan megkérdőjelezhető, míg csupán egy válaszoló fiatal ismerte a kérdés jogi megítélését. A *hacking*gel kapcsolatban a többség egyfajta felmentő attitűdöt fogalmazott meg, ami a cselekmény népszerűségére és a morális megítélés bizonytalanságára utal.[88] A *hacking*et elkövetők körében emellett magasabb volt az egyéb devianciákat is elkövetők aránya, így különösen az alkoholfogyasztás.[89] Azok között, akik nem követtek el ilyen cselekményeket, több volt, aki csupán enyhe deviáns cselekményt követett el. A hekkelők 26,7%-a követett el súlyosabb devianciákat (vagyon vagy személy ellen), míg a nem hekkelőknél ezek száma elenyésző volt.

A tanuláselméleti perspektívát előrevetítve Parti megemlíti, hogy a *hacking* és a fájlletöltés esetében a negatív megítélés hiánya is pozitívan hathat az elkövetésre, valamint e cselekmények esetében ugyan gyakoribb a magányos elkövetés, a szülőkkel való együttes fájlletöltés gyakrabban előfordul, mint a *hacking,* tekintve hogy ez utóbbi esetében nagyobb a társadalmi rosszallás.[90] A társas kapcsolatok tekintetében fontos még megemlíteni, hogy a családon belüli problémák, a válás vagy a szülő halála és a számítógépes aktivitás között direkt kapcsolat állapítható meg. Emellett azok, akik családjában ilyen problémák előfordultak, nagyobb arányban használták egyedül a számítógépet.

Jelen írás szempontjából a legfontosabb konklúzió az, hogy „a baráti társaság megléte és a fokozott számítástechnikai, illetőleg az internetes szabadidő-eltöltés egyidejű érvényesülése nem a társadalmi kontroll hiányát, hanem inkább a közösségi megerősítés érvényesülését igazolja" – írja Parti.[91] E gondolat egybecseng azokkal a kutatási eredményekkel, amelyek a kontrollelméletekkel szemben a társadalmi tanulás, a differenciális megerősítés szerepét tekintik az informatikai bűnözésben és különösen a kibertérfüggő (pl. *hacking*) elkövetésben a kulcsfontosságúnak. Parti jelzi is, hogy e két számítástechnikai devianciával érintett csoportnak kiterjedt baráti köre, társadalmi kapcsolatai vannak, így a kötődések hiánya nem magyarázza az informatikai elkövetést. Parti konklúzióját támasztja alá Reinis Udris összehasonlító elemzése is,[92] amely ugyancsak az ISRD-2[93] adatainak segítségével vizsgálta a családhoz, a barátokhoz, a szomszédsághoz való kötődést és az informatikai devianciák kapcsolatát. A kutatásnak, ellentétben Parti tanulmányával, már nem kifejezetten a társadalmi kötődés, hanem szélesebb perspektívából indulva az önkontrollelmélet és az általános tanuláselmélet is az alapját képezi.

Röviden összefoglalva, Udris a kutatásában alátámasztotta azt az alapvetést, miszerint az otthoni számítógép-birtoklás és az online devianciák elkövetése között szignifikáns kapcsolat

[87] A fogalom részletes attribútumainak és az idetartozó konkrét elkövetési magatartások meghatározására a kutatás nem tér ki.

[88] Parti i. m. (82. lj.) 157.

[89] Uo., 160.

[90] Uo., 162.

[91] Uo., 172.

[92] Reinis Udris: Cyber Deviance among Adolescents and the Role of Family, School, and Neighborhood: A Cross-National Study. 10(2) *International Journal of Cyber Criminology* (2016) 127–146.

[93] International Self-Report Delinquency Study, https://web.northeastern.edu/isrd/isrd2.

van, a családdal való problémás viszony nagyobb arányú fájlletöltéssel jár együtt, az alacsony iskolai kötődés és a letöltés között is van összefüggés (ugyanakkor ennek szignifikanciája alacsony), illetve a szomszédsághoz való kötődés és a letöltés között pozitív szignifikáns kapcsolat mutatható ki. A *hacking* tekintetében a magasabb belépési korral együtt járt a családi kötődés és a közös időtöltés szignifikanciájának hiánya is. Az iskolához való kötődés negatív szignifikáns kapcsolatot mutat a *hacking*gel, míg az iskolai dezorganizáció pozitív és szignifikáns kapcsolatban van a *hacking* elkövetésével.[94]

Udris kutatása rávilágít arra, hogy a családi kapcsolatok, az iskolához való kötődés fontos előre jelzője lehet e két informatikai devianciának, ugyanakkor azok relevanciája eltérő. Nagyobb szerepet a család és az iskola felől jövő direkt kontrolloknak tulajdonít, amelyek az aktív felügyelet mellett hatnak az önkontroll működésére. A szomszédsághoz való kötődés szerepe már alacsonyabb (különös, hogy e kutatás szerint a szomszédsághoz való erősebb kötődés nagyobb fájlletöltéssel társul, a *hacking*gel pedig nem mutat szignifikáns kapcsolatot), míg a szomszédság dezorganizációja és az elkövetés közötti kapcsolat nem mutatható ki. Fontos végül megemlíteni, hogy a tanulmány is jelzi: a vizsgált országok között nincs kiemelkedő eltérés e tényezők tekintetében.[95] A szerző megjegyzi, hogy a néhol inkonzisztens eredmények miatt az ISRD kutatás alapját képező és egyéb – e tanulmányban is ismertetett – elméletek önmagukban nem képesek az informatikai bűnözés magyarázatára, így akár új elméletek kidolgozására is szükség lehet.[96] Udris azt is jelzi, hogy az egyes bűncselekménytípusok eltérő jellemzői és eredményei okán felvetődik, hogy ezek magyarázata csupán önállóan, egymástól leválasztva, akár más-más elméleti struktúrában lehetséges. Ennek oka, hogy a kibertérfüggő és a kibertér által elősegített cselekmények elkövetői között az elkövetés jellemzőiben és az elkövetéshez vezető utakban is eltérés mutatkozhat.

A kötődések és az önkontroll együttes vizsgálatára vállalkoztak Sinchul Back és munkatársai a fiatal hekkerekkel végzett kutatásukban.[97] Meglepő módon ez is az ISRD-2 kutatás adataiból merít, ugyanakkor a fentebb ismertetett írásnál szűkebb kört, mindössze nyolc állam válaszait, köztük Magyarországét vizsgálja. A kutatás hipotézisei egyaránt feltételezik az önkontroll szintje, a részvétel, illetve a családhoz, az iskolához és a szülői felügyelethez való kötődés kapcsolatát a *hacking* magatartásokkal. Érdekesség, hogy hazánkra az ISRD kutatásban részt vevő számos ország közül a statisztikákban szereplő magas informatikai bűnözési mutatók okán esett a választás.[98]

A kutatás alátámasztotta, hogy a nyolc országban mért adatok szerint az alacsony önkontroll és a *hacking* elkövetése között pozitív szignifikáns kapcsolat áll fenn, míg a társadalmi kötődések tekintetében részben sikerült alátámasztani a meghatározott hipotéziseket. Így például

[94] Uo., 135–137.

[95] Uo., 139.

[96] L. Karuppannan Jaishankar: Space Transition Theory of Cyber Crimes. In: Frank Schmalleger – Michael Pittaro (szerk.): *Crimes of the Internet*. Upper Saddle River, Prentice Hall, 2008. 283–301.; Suler i. m. (59. lj.) 321–326.

[97] Sinchul Back – Sadhika Soor – Jennifer LaPrade: Juvenile Hekkers: An Empirical Test of Self-Control Theory and Social Bonding Theory. 1(1) *International Journal of Cybersecurity Intelligence & Cybercrime* (2018) 40–55.

[98] Uo., 45.

Magyarország és további öt ország tekintetében is kimutatták, hogy a szülői felügyelet csökkenti a *hacking* valószínűségét, három államban pedig az iskolai kötődés csökkentette ugyanezt. Végül – hasonlóan Parti elemzéséhez – kiemelték a nemek relevanciáját a *hacking* esetében is, vagyis hogy a fiúk száma jelentősen felülmúlja a lányokét. A kutatás társadalmi kötődésekre vonatkozó további hipotéziseit ugyanakkor nem sikerült alátámasztani. A további tényezők, például a szülőkhöz való kötődés, a közösségi tevékenységekben való részvétel, a születési hely, a város mérete e kutatás szerint nem tekinthetők a *hacking* prediktorainak.[99]

Végül kapcsolódó területen említhető Gustavo Mesch kutatása,[100] amely azt mutatta, hogy az iskolához való kötődés csökkentette a fiatalok online pornográf tartalom fogyasztását. Heng Chan és Dennis Wong kutatása pedig a *cyberbullying*hoz gyakran kapcsolódó *bullying*-elkövetés és -áldozattá válás esetén mutatta ki a gyenge családi kapcsolatok szerepét.[101] Hirschi elméletét alkalmazták továbbá kibertérfüggő bűncselekmények, így például a *hacking* egyéb vizsgálataira is. Sung Bae e téren azt találta, hogy a társadalmi kötődések és az önkontroll megléte csökkentette a *hacking* és egyéb online devianciák valószínűségét a fiatalok körében. Azt is kifejtette, hogy a családhoz való kötődés és a megfelelő szülői felügyelet szignifikáns hatással van a *hacking*ben és egyéb devianciákban való részvétel elmaradására serdülőkorban.[102]

Összességében nagyon eltérő tapasztalatokkal szolgálnak a fenti tanulmányok. Egyrészt fontos megjegyezni, hogy az elérhető kutatások adatai szinte kivétel nélkül a 2005 és 2007 között rögzített ISRD-2 felmérésből származnak, ezen adatok újbóli áttekintését végzik el az informatikai bűnözés viszonylatában. A kutatások pozitívuma, hogy számot adnak nem csupán a technológiai tudást nem igénylő fájlletöltésről, hanem a nagyobb specializációt feltételező *hacking* előfordulásáról és társadalmi kötődéshez való viszonyáról. Az ISRD eredményeinek valósítása szempontjából ugyanakkor fontos azt is megjegyezni, hogy az ISRD a '*hacking*' cselekményének definiálását a kérdőív kitöltőire bízta, így a fiatal korosztály bárhogyan értelmezhette azt. A kutatások továbbá csak részben és mérsékelt szignifikanciával képesek a kötődéselmélet négy tényezőjét alátámasztani, azok közül kifejezetten a családhoz és az iskolához való kötődés, valamint a jogszabályokhoz kapcsolódó morális elköteleződés jelenik meg részlegesen. Az elmélet így – ahogyan Parti és Udris is jelzi – nem igazán képes magyarázni a fiatalok körében megjelenő informatikai devianciákat. A két szerző eltérő elméleti keret alkalmazását veti fel: Parti a tanuláselmélet, Udris pedig a kifejezetten informatikai térre fejlesztett teóriákat, például Suler *disinhibition effect* tézisét. Az pedig nyilvánvaló, hogy az általános bűnözéselmélet a társadalmi kötődéselmélet legfontosabb téziseit bekebelezve, a külső és a belső kontrollok vizsgálatával ugyancsak háttérbe szorítja ezen elmélet alkalmazását.

[99] Uo., 48–55.

[100] Gustavo S. Mesch: Social Bonds and Internet Pornographic Exposure among Adolescents. 32(3) *Journal of Adolescence* (2009) 601–618.

[101] Heng C. O. Chan – Dennis S. W. Wong: The Overlap Between School Bullying Perpetration and Victimization: Assessing the Psychological, Familial, and School Factors of Chinese Adolescents in Hong Kong. 24(11) *Journal of Child and Family Studies* (2015) 3224–3234.

[102] Sung M. Bae: The Influence Ofstrain Factors, Social Control Factors, Self-Control and Computer Use on Adolescent Cyber Delinquency: Korean National Panel Study. 78 *Children and Youth Services Review* (2017) 74–80.; Back–Soor–LaPrade i. m. (97. lj.) 45.

2.3. Interakcionista paradigma

2.3.1. Tanuláselméletek

A tanuláselméleti perspektíva alkalmazását tekintve az önkontroll elméletével egyenrangúnak tekinthető, fejlődése is hasonlóan hosszú utat járt be. Az e körbe tartozó elméletek tesztelésére tucatnyi példát találhatunk világszerte, amelyek túlnyomó többsége az elméleti megközelítés, ezen belül is különösen a differenciális asszociációmegerősítés elmélet alátámasztásáról számolnak be. A tanuláselméleti perspektívát az teszi különösen vonzóvá, hogy a bűnelkövetővé válás folyamatát következetesen, a mikrotársadalmi folyamatok figyelembevételével képes magyarázni.

A tanulás vizsgálatának előtérbe helyezése a biológiai és a pszichológiai tényezőkkel szemben egészen Clifford Shaw és Henry McKay gondolatáig nyúlik vissza a kriminológiában.[103] Az ő társadalmi dezorganizációelméletük nyitott utat azon elméleteknek, amelyek szerint a bűnelkövetés tanult viselkedés. Fő kérdésük az volt, hogy milyen mechanizmusok során sajátítják el a fiatalok a normakövető vagy a bűnöző értékrendet, illetve miért válik ugyanabban a közösségben az egyik fiatal bűnelkövetővé, a másik pedig nem. Továbbá az is foglalkoztatta őket, hogy több értékrend közül mitől függ az, hogy a fiatalok melyikhez igazítják magatartásukat.[104] E gondolatokat fogalmazta meg Edwin Sutherland is 1947-ben, részben a pozitivista alapokon nyugvó szociológiai iskola előretörésének részeként *Principles of Criminology* című kötetében. E nézetek képviselői többek között Charles Cooley és George Herbert Mead nyomán azt a folyamatot akarták meghatározni, amivel az egyének a kriminális viselkedést elsajátítják. Ők a tanulás elméletei mellett köteleződtek el, ennek fényében vizsgálták az utánzás, az attitűdérték, a differenciális asszociáció és bizonyos fokig a kompenzáció és a frusztráció-agresszió szerepét.[105] Ezzel szemben a tisztán szociológiai iskola a társadalmi okokat, a kulturális okokat, az intézményrendszert, a társadalomszerkezetet vizsgálta. Ugyanakkor Sutherland is jelzi, hogy az individuális és a strukturális tényezők elhatárolása túlságosan leegyszerűsítő lenne, így a merev elválasztás a gyakorlatban nem életképes.[106] E tényezők kombinációját Akers később bemutatásra kerülő általános tanuláselmélete hordozza.[107]

Sutherland e nézetekre alapozva határozta meg kilenc tételből álló differenciális asszociációelméletét.[108] Megállapításai szerint a bűnözés tanult viselkedés, amit az egyének az egymás közötti (verbális és szimbolikus) kommunikáció során sajátítanak el. A tanulás kiterjed a készségekre és a mentális beállítódásra, azonban míg a mentális elem minden esetben szükséges, addig a készségek megléte nem elengedhetetlen. Emellett a bűncselekmény elfogadhatóságát biztosító attitűd ugyancsak a folyamat feltétele. Ezen attitűdök kialakulása szempontjából egy

[103] Clifford R. Shaw – Henry D. McKay: *Juvenile Delinquency and Urban Areas*. Chicago, University of Chicago Press, 1969.

[104] Borbíró Andrea – Győry Csaba: Kultúra és társas interakciók. In: Borbíró i. m. (3. lj.) 129–166., 138.

[105] Edwin H. Sutherland: *Principles of Criminology.* Chicago, Lippincott, (3. kiad.) 1939. 55.

[106] Uo., 65.

[107] Ronald L. Akers: *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston, Northeastern University Press, 1998.

[108] Sutherland i. m. (105. lj.) 1–10.

fiatal életében vannak meghatározó személyek és vonatkoztatási csoportok, akik és amelyek a mintákat szolgáltatják,[109] és eltérő felfogást vallanak a büntetőjogi normák követendőségéről. Sutherland a hatodik tételében foglaltakat – vagyis hogy valaki akkor válik elkövetővé, ha a környezetéből jövő támogató képzetek (definíciók) erősebbek, mint a jogkövetést támogatók – tekintette a tanulás kulcselemének.

Az elmélet szerint a tanulási folyamat során kialakuló attitűdök, képzetek, viselkedési formák nem mindig választhatók el a jogkövető magatartást folytatókétól. Ugyanaz a személy adhat normakövető és normaszegő példákat is. A fiatal azokat fogja követni, amelyek erősebben hatnak rá, így kialakítva a normaszegő képzetek túlsúlyát. Ezek általában csak egy vagy néhány típusú normasértésre terjednek ki (pl. adócsalásra igen, de személy elleni erőszakra nem).[110] Végül fontos, hogy milyen szoros a kapcsolat a mintát szolgáltató személlyel, hiszen ez befolyásolja a tanulás intenzitását és tartalmát. Sutherland szerint a kriminális magatartásnál lényeges a személy–szituáció komplexitása, vagyis hogy a résztvevő személy – korábbi élettörténete alapján – hogyan értékel és érzékel bizonyos helyzeteket, és milyen konkrét reakciókat ad az általa definiált szituációra. Az elmélet szempontjából különösen fontos a személy élettapasztalata – írta Sutherland 1939-ben.[111] Az elmélet lényege tehát, hogy ha egy személy a prokriminális, bűnözést támogató definícióknak van kitéve elsődlegesen, és ezek a definíciók gyakoriságukban és intenzitásukban erősödnek, valamint hosszabb ideig fennállnak, akkor az egyén nagyobb valószínűséggel követ el bűncselekményt vagy vesz részt egyéb devianciában.[112]

Sutherland elméletének koherenciája és általános igénye adja annak széles körű ismertségét, de ő maga az elméletet sohasem tesztelte – James Short egyenesen azt állította, hogy az empirikus módon nem is tesztelhető.[113] Donald Cressey 1952-ben,[114] Albert Reiss és Lewis Rhodes 1964-ben,[115] Travis Pratt és munkatársai 2010-ben[116] ugyanakkor empirikus támogató vizsgálatokat folytattak a témában, jelezve az elmélet helytállóságát. Cressey rávilágított arra, hogy a bűnözésben kedvező definíciók tanulása – szemben a kedvezőtlen definíciókkal – tekinthető olyan folyamatnak is, amely során az egyének a prokriminális definíciókat igyekeznek a proszociális vagy konform definíciókkal szemben kiegyensúlyozni. Továbbá logikus, hogy az egyén a bűnözést favorizáló vagy prokriminális definíciókat olyan egyénektől tanulja, akik maguk is érintettek a bűnözésben, míg a bűnözést elutasító definíciókat azoktól sajátítja el, akik nem érintettek ebben, és szerinte ez a feltevés empirikusan is alátámasztott.[117]

[109] Borbíró–Győry i. m. (104. lj.) 138–140.

[110] Uo.

[111] Sutherland i. m. (105. lj.) 9.

[112] Uo.

[113] James F. Short, Jr.: Differential Association as a Hypothesis: Problems of Empirical Testing. 8(1) *Social Problems* (1960) 14–25.

[114] Donald R. Cressey: Application and Verification of the Differential Association Theory. 43(1) *Journal of Criminal Law, Criminology and Police Science* (1952–1953) 43–52.

[115] Albert J. Reiss – A. Lewis Rhodes: An Empirical Test of Differential Association Theory. 1(1) *Journal of Research in Crime and Delinquency* (1964) 5–18.

[116] Travis C. Pratt et alii: The Empirical Status of Social Learning Theory: A Meta-Analysis. 27(6) *Justice Quarterly* (2010) 765–802.

[117] Donald R. Cressey: *Other People's Money*. Glencoe, Free Press, 1953; Donald R. Cressey: Epidemiology and Individual Conduct: A Case from Criminology. 3 *Pacific Sociological Review* (1960) 47–58., 49.

Habár a szakemberek egy része igyekezett megerősíteni Sutherland elméletét, Burgess és Akers kifogásolta, hogy az elmélet nem tesztelhető megfelelően, illetve annak bizonyos részei a kritikák és hiányosságok fényében átgondolást igényelnek.[118] Erre először Clarence Jeffery világított rá,[119] aki a tanulás mellett a társas kapcsolatokban a megerősítés szerepét hangsúlyozta, ugyanakkor Burgess és Akers dolgozott ki koherens revíziót az elmélethez 1966-ban. Akers és társa az Ivan Pavlov és Burrhus Skinner által vizsgált operáns kondicionálást, illetve Albert Bandura komplexebb tanulási elméletét vette alapul, amelyek ma is meghatározzák a tanuláselméleti perspektívát. Pavlov, majd Skinner azt találták, hogy a kutatásuk alanyai olyan döntéseket hoznak és azt a magatartást folytatják, amely jutalmazáson (megerősítésen) alapul.[120] Itt kulcsfontosságú a környezet hatása volt azáltal, hogy a cselekvések mellé pozitív vagy negatív megerősítést társítottak *(reinforcement)*. E folyamat mozgatórugója a jutalmak megszerzése vagy azok elmaradása, esetleg a retorzió volt.[121]

Míg Pavlov és Skinner a kondicionálást tekintette a tanulás alapjának, addig Bandura a megerősítés egyedüli primátusával szemben más tényezőket helyezett előtérbe. Azt mondta, hogy a tanulás megfigyelésen *(observation)* és a szituáció elemzésén *(analysis of situation)* keresztül történik. Elmélete szerint az egyének példaképeken *(role model)* keresztül tanulnak oly módon, hogy a példaképek végrehajtanak egy bizonyos cselekvést, amelyet mások láthatnak, és úgy döntenek, hogy ugyanezt teszik. Burgess és Akers nem csupán e meglátásokat, de azon alapgondolatokat is integrálta, miszerint a folyamat során a látás és a tapasztalás interakcióba lép azért, hogy a magatartást ösztönözve *(instigation of behavior)* utánzást eredményezzen.[122]

E tapasztalatokat (amelyeket a mai tanuláselméletek alaptéziseinek tekinthetünk) gyúrta össze Sutherland differenciális asszociáció téziseivel és tette operacionalizálhatóvá Burgess és Akers, megalkotva a differenciális asszociációmegerősítés elméletét. Mivel Sutherland nem fejtette ki részletesen az általa taglalt pontokat, ők újraformáltak azokat annak érdekében, hogy egy empirikusan is kutatható elmélet jöjjön létre. Ezt az operáns kondicionálás kontextusában tették meg, Sutherland kilenc tételét hétre csökkentve.[123]

A társadalmi tanuláselmélet négy fő tényező, a differenciális asszociáció, a definíciók, a differenciális megerősítés és az utánzás köré csoportosítható elemeket tartalmaz. A differenciális asszociáció tényezője a család, a kortárs csoportok és az iskola, vagyis összességében a deviáns közeg *(deviant others)* és a deviáns magatartás hatását hivatott összefoglalni. Eszerint kezdetben a korai gyermekkorban a család, az iskola, a szabadidő-eltöltés, a kikapcsolódás során

[118] Robert L. Burgess – Ronald L. Akers: A Differential Association-Reinforcement Theory of Criminal Behavior. 14(2) *Social Problems* (1966) 128–147.

[119] Clarence R. Jeffery: An Integrate Theory of Crime and Criminal Behavior. 49(6) *Journal of Criminal Law, Criminology and Police Science* (1959) 533–552.

[120] Jordana N. Navarro – Catherine D. Marcum: Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime. In: Thomas J. Holt – Adam M. Bossler (szerk.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham, Palgrave Macmillan, 2020. 1–18.

[121] Social Learning Theory, http://criminal-justice.iresearchnet.com/criminology/theories/social-learning-theory.

[122] Navarro–Marcum i. m. (120. lj.) 4–5.

[123] Burgess–Akers i. m. (118. lj.).

fontos csoportok szerepe nagy, míg a fiatal felnőtt korban és az élet későbbi szakaszában a házastárs, a munkaközösség és a barátok jelentik a tanulás elsődleges társadalmi kontextusát.[124] Az elmélet e része cseng egybe leginkább Sutherland meglátásaival.

A definíciók azokat a megtanult magatartásokról kialakított attitűdöket jelentik, amelyeket a differenciális asszociáción, az utánzáson és az általános interakciókon keresztül tanul az egyén, vagy amelyeknek ki van téve szociális közegében. Ezek lehetnek általános jellegűek vagy specifikusak. Az elmélet különbséget tesz pozitív (kívánatos, elfogadható, megengedhető), negatív (nem kívánatos, elfogadhatatlan, helytelen) és neutralizáló definíciók (megbocsátható, igazolható, tolerálható) között.[125] E definíciók Grasham Sykes és David Matza később bemutatandó neutralizációelmélete integrálhatósága szempontjából is nagy jelentőségűek.[126]

A differenciális megerősítés vagy büntetés a megtanult cselekvések következményeit jelenti. A társadalmi és egyéb jutalmak vagy büntetések, amelyek a viselkedéssel együtt járnak, hatnak az egyén későbbi magatartására, a tanulási folyamat intenzitására és annak követésére. Burgess és Akers elmélete szerint a későbbi elkövetés annak a függvénye, hogy az egyén milyen típusú megerősítést tapasztal a tetteit követően.[127] A megerősítés lehet pénzügyi haszon, érzelmi kielégülés vagy társadalmi elfogadottság, akárcsak valamilyen büntetés (pl. szabadságvesztés, fegyelmezés, előny megvonása), amelyek befolyásolják, hogy a magatartások hosszabb időn keresztül fennmaradnak, vagy az elkövető felhagy azokkal (dezisztencia következik be).[128]

Végül az utánzás a viselkedés modellezését jelenti mások megfigyelésén keresztül. Az utánzás lehetősége a környező társadalmi csoportoktól, a szülőktől, a kortársaktól, a tanároktól és egyéb forrásoktól (pl. média) származhat. Az utánzásnak a tanulás elején van kifejezetten nagy jelentősége, és kevéssé fontos a viselkedés fenntartásában és elhagyásában. Akers eleinte az elmélet e részét az operáns kondicionálás egyik alfolyamatának tekintette, azonban későbbi revíziójában már elismerte az utánzás egyedülálló jelentőségét a tanulási folyamatban.[129]

Akers egészen 1998-ig számos, az empirikus kutathatóságot megkönnyítő változtatást tett, így elméletét általános tanuláselméletté fejlesztette.[130] Ekkor azt vallotta, hogy a társadalmi tanulás elmélete nemcsak új magatartások megismeréséhez alkalmazható, hanem az új egyéni magatartások és korábban tanult magatartások vizsgálatához is. Más szóval ez olyan keretrendszer, amellyel meg lehet érteni az egyént afelé vezető motivációkat, hogy bűncselekményt kövessen el, vagy éppen ellenálljon a bűnözésnek.[131] Akers elméletének módosítása során kidolgozta a társadalmi struktúra négy dimenzióját a társadalmi struktúra és a társadalmi tanulás (*social*

[124] Social Learning Theory i. m. (121. lj.) 5.

[125] Uo.

[126] Grasham M. Sykes – David Matza: Techniques of Neutralization: A Theory of Delinquency. 22(6) *American Sociological Review* (1957) 664–670.

[127] Burgess–Akers i. m. (118. lj.).

[128] Holt–Bossler i. m. (4. lj.) 81.

[129] Ronald L. Akers: *Deviant Behavior: A Social Learning Approach.* Belmont, Wadsworth, (3. kiad.) 1985.

[130] Akers i. m. (107. lj.).

[131] Navarro–Marcum i. m. (120. lj.) 4–5.

structure and social learning model – SSSL) modelljében, kiegészítve a vizsgált hét tételt. Okfejtésének lényege, hogy a társadalmi struktúra e dimenziói indirekt hatással vannak a bűnözés tanulására, amelyek négy tényezőn keresztül jelennek meg direkt formában.[132]

Az első ilyen dimenzió, a differenciális társadalmi organizáció, olyan társadalmi szintű strukturális elemeket jelent, amelyek hatással vannak a magas vagy épp az alacsony bűnözési ráták kialakulására. Ilyen az életkor-összetétel, a népsűrűség és más kulturális vagy gazdasági indikátorok, amelyekk empirikusan vagy teoretikusan kapcsolódnak a bűnözéshez.[133] A második dimenzió az egyén eltérő helyére utal a társadalmi struktúrában, illetve olyan mikroszintű jellemzőkre, mint a nem, a rassz és az etnikum, a családi állapot, a kor és a társadalmi-gazdasági helyzet, amelyek indirekt módon elhelyezik az embert a társadalmi struktúrában azáltal, hogy meghatározzák a szerepét, a státuszát és a csoportkategóriáit. A harmadik dimenziót jelentik azon elméletileg definiált strukturális változók, amelyek az anómiára, az osztályelnyomásra, a társadalmi dezorganizációra, a csoportkonfliktusra, a patriarchátusra és olyan más fogalmakra utalnak, amelyeket egyéb elméletekben is definiáltak és alkalmaztak a társadalmak, közösségek vagy csoportok kriminogén jellemzőinek azonosítására.[134] Végül az utolsó dimenzió a differenciált társadalmi helyzet, amely az egyén részvételét és kapcsolatát jelenti az elsődleges és a másodlagos viszonyítási csoportjaival. E csoportok lehetnek a család, a kortárs csoportok, a barátok, a munkatársak stb.[135]

E négy dimenzió alapján tehát vannak olyan makro- és mikroszintű tényezők, amelyek meghatározzák az egyén helyét a társadalomban. Eszerint a társadalmi helyzet és egyéb indirekt tényezők hatására az egyén olyan környezetben vagy szituációban van jelen, ahol a deviáns tanulás direkt folyamatai lejátszódhatnak. Akers és Christine Sellers azt írták 2004-ben, hogy e négy dimenzió adja meg a később lejátszódó direkt tanulási folyamatok kontextusát, így a társadalmi tanulás közvetíti a társadalmi strukturális hatásokat.[136] A társadalmi tanulás komplex elméletének tesztelése, annak kiforrottsága ellenére jelenleg még elmarad a differenciális asszociációmegerősítés elméletének vizsgálatától. Annak indirekt és direkt elemei közötti kapcsolat kimutatására még igen kevés példát találunk, mindazonáltal e vizsgálatok az elméleti keret alátámasztása felé tendálnak.

Az elméletek alkalmazása az informatikai bűnözés kutatásában is hasonló megoszlást mutat. A legjelentősebb a differenciális asszociációmegerősítés elmélet négy direkt elemének vizsgálata, míg az SSSL alapján végzett kriminológiai kutatások száma e téren is kevés. Az Akers differenciális asszociációmegerősítés elmélete alapján lefolytatott kutatások mind a kibertér által elősegített, mind a kibertérfüggő bűncselekményeket elkövetők esetén megtalálhatók, azok

132 Akers i. m. (107. lj.).

133 Uo., 332.

134 Social Learning Theory i. m. (121. lj.).

135 Thomas J. Holt – George W. Burruss – Adam M. Bossler: Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. 33(2) *Journal of Crime and Justice* (2010) 31–61.

136 Ronald L. Akers – Christine S. Sellers: *Criminological Theories: Introduction, Evaluation, and Application*. Los Angeles, Roxbury, (4. kiad.) 2004. 91.

egészen az 1990-es évek második feléig nyúlnak vissza, és elsősorban a digitális kalózkodás kutatását érintik, ugyanakkor a jogosulatlan rendszerbehatolással kapcsolatban is találhatunk jelentős kutatási eredményeket a témában.

Az első releváns kutatás William Skinner és Anne Fream 1997-ben egyetemisták körében folytatott vizsgálata volt.[137] Ezt megelőzően egyedül Richard Hollinger végzett a témában hasonló felmérést,[138] azonban ő csupán a szoftverkalózkodásra és a jogosulatlan belépés elkövetésére kérdezett rá, valamint két tényező, a barátok bevonódottsága és a lebukás fenyegető hatása mint negatív megerősítő tényező szerepelt a kérdőívében.[139] Ezzel szemben Skinner és Fream az életprevalenciát, a múlt évben és a múlt hónapban elkövetett szoftverkalózkodást, a jelszavak próbálgatását belépési céllal, a jogosulatlan belépést kizárólag a keresgélés céljával, a jogosulatlan belépést az adatok megváltoztatásának céljával és a számítógépes adatok törlésére alkalmas vírusok vagy programok írását vizsgálták.[140] Skinner és Fream a kutatást Akers 1985-ös differenciális asszociációmegerősítés elméletére alapozták, tekintve hogy ennek alkalmazhatóságát számos korábbi felmérés is alátámasztotta. Cressey-re[141] hivatkozva jelzik, hogy az egyén nem csupán azt tanulja meg, hogyan kövesse el a bűncselekményt, mindegy, hogy mennyire egyszerű vagy komplex, hanem megtanul specifikus motívumokat, szándékokat, motivációkat, racionalizációkat és attitűdöket, amelyet Skinnerék az informatikai bűnözés tekintetében különösen fontosnak tartottak.[142] Az informatikai bűnözés nemcsak azt igényli, hogy az egyén megtanulja, hogyan kezeljen egy technológiai eszközt, hanem specifikus folyamatokat, programozást, a számítógép illegális használatának technikáit is elsajátítja a tanulási folyamat részeként. Ezzel kapcsolatban más szerzők, így például Jordana Navarro és Marcum is hasonló véleményen vannak.[143] Szerintük is a szofisztikáltabb informatikai bűnözésben muszáj másokkal együtt dolgozni, hiszen az elkövetők egyedül nem tudják megszerezni a szükséges tudást. Ugyanakkor az ún. *low-tech cybercrime* esetén (pl. *cyberbullying, cyberstalking*) is szükség van tudásra ahhoz, hogy elkerülhető legyen a lebukás, illetve lehetőség nyíljon a hatékony technikák megtanulására.

Skinner és Fream kutatása három ma is releváns hipotézisre épült. Az egyik vizsgált és az elmúlt két évtizedben több ízben is alátámasztott feltevésük szerint a kortárs csoportoknak, a közvetlen kapcsolatoknak van a legnagyobb szerepe az informatikai devianciák elsajátításában, illetve a barátok lehetnek a forrásai a technikai rész tanulásának is. A tanulás során az egymással kapcsolatban állók rendelkezésre bocsáthatnak szoftvereket (pl. kalózkodáshoz, rendszerbehatoláshoz), amelyek az elkövetési módszerek elsajátítását segíthetik elő. Ezen interakciók lehetnek személyes vagy online formájúak is, ahol elektronikus a kapcsolat a tanulási folyamatot biztosító felek között.[144]

[137] William F. Skinner – Anne M. Fream: A Social Learning Theory Analysis of Computer Crime among College Students. 34(4) *Journal of Research in Crime and Delinquency* (1997) 495–518.

[138] Richard C. Hollinger: Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. 4 *Security Journal* (1993) 2–12.

[139] Skinner–Fream i. m. (137. lj.) 497.

[140] Uo., 496.

[141] Edwin H. Sutherland – Donald R. Cressey: *Criminology*. Philadelphia, Lippincott, (9. kiad.) 1974.

[142] Holt–Bossler i. m. (4. lj.) 75.

[143] Navarro–Marcum i. m. (120. lj.).

[144] Skinner–Fream i. m. (137. lj.) 498–501.

A második hipotézisük szerint a jogi szabályozás hatással van a negatív definícióalkotásra. Az emberek nagy része tisztában van azzal, hogy bizonyos cselekmények tiltottak, a szigorúbb jogszabályok pedig csökkenthetik a jogellenes magatartások gyakoriságát. Ugyanakkor az idősebb diákok az online jelenlévő fiatalok morális és etikai értékrendjét befolyásolhatják a barátok és a 'mindenki ezt csinálja' álcája alatt. Ez a jogszabályi tilalmakkal ellentétes hatást fejthet ki. Feltevésük szerint ezért a diákok elkezdik neutralizálni a cselekmények illegális, negatív megítélését, azt kvázi erkölcsileg elfogadhatónak tételezik. E neutralizációkat a fiatalok a barátoktól, a filmekből, a nyomtatott médiából tanulják. Megjegyzendő, hogy Skinner és Fream a kutatásukat 1997-ben publikálták, amikor a nyomtatott sajtó nagyobb mértékben volt jelen, és hitelesebb információt szolgáltatott az online sajtónál. Az informatikai bűnözés médiamegjelenése és megítélésének változása jelentős tényező a társadalmi tanulás során, mert a médiában megjelenő kép a neutralizációt és a definícióalkotást befolyásolja, emellett a média által tükrözött alacsony lebukási arányok is a differenciális megerősítésre vannak hatással.[145]

A harmadik hipotézisük szerint a pozitív megerősítés legfontosabb szereplői az ún. példaképek, akik magatartása, viselkedése hatványozottan szerepet játszik a prokriminális definíciók kialakításában és a jogi tilalmazottsággal szemben ható neutralizáció folyamatában. Kutatásukban a következő eredményekre jutottak: a barátok és a tanárok tanulásban betöltött szerepe (vagyis az általuk képviselt minta) szignifikáns kapcsolatban van különösen a kalózkodással, de a barátokkal való kapcsolat is a kalózkodás esetében volt a legerősebb. A joghoz való viszonyulás szintén erős kapcsolatot mutatott, ezen belül leginkább az illegális belépés (böngészési céllal) cselekménye esetén volt a jog ismeretének visszatartó hatása. A letartóztatás bizonyossága ugyanakkor nem visszatartó erő a kalózkodás esetében, vagyis a jogszabályok megítélése és a felelősségre vonás nem tekinthető e téren negatív megerősítő tényezőnek.[146] Ez utóbbi meglátásokat többek között Holt és munkatársai is megerősítették 2010-ben.[147] A kalózkodásnál a büntetés súlyossága sem mutatott összefüggést, viszont e tényező hatása az illegális behatolásnál már jelen volt. Ez azt jelenti, hogy a büntetések szigorodásával az elkövetési hajlandóság is csökken a fiatalok körében. Ugyanakkor azon feltevés, miszerint a büntetés súlyossága felelős a jogsértő magatartások számának csökkenéséért, nem volt bizonyítható.[148]

Fontos kiemelni továbbá, hogy azon diákok, akik szerint a vállalatoknak jobb biztonsági eszközöket kellene alkalmazniuk, jobban hajlottak a jelszavak tippelgetésére és a fiókadatok, belépési kódok illegális keresésére, mint azok, akik nem ezen a véleményen voltak. Emellett akik szerint az online elérhető termékek és szolgáltatások túl drágák, vagy a megkérdezett nem jelentene fel egy barátot, aki kalózkodik, az hajlamosabb elkövetni e cselekményeket. Más neutralizációs tényezők viszont nem voltak megállapíthatók.[149]

145 Uo.
146 Uo.
147 Holt–Burruss–Bossler i. m. (135. lj.).
148 Skinner–Fream i. m. (137. lj.) 506–512.
149 Uo., 512–514.

Míg Skinner és Fream kutatása a kalózkodással és a jelszókifürkészéssel történő illegális rendszerbehatolást érintették, vagyis nem volt számukra feltétel a technológiai manipuláció elvégzése, addig más szerzők a társadalmi tanuláselmélet egyéb kibertérfüggő elkövetésre, a jogosulatlan belépéstől szélesebb körben értelmezett *hacking*re való alkalmazására is rávilágítottak. A szakirodalom szerint az ún. hekkercsoportokba tartozás, a deviáns társakkal való együttműködés és a deviáns definíciók internalizálása fontos rizikófaktor a *hacking* során. Pozitív megerősítés pedig a többiektől való tanulás, a sérülékeny pontok *(exploitok)* megismerése, a társadalmi státusz elérése, a tevékenységük hasonló személyekkel együtt történő racionalizálása során következik be.[150] Csupán korlátozott mennyiségű kutatás áll rendelkezésre a tanuláselmélet egészére nézve ezen a téren, ugyanakkor alátámasztható, hogy az utánzás hagyományos és nem hagyományos módjai is jelen vannak a folyamat során. Az előbbi a családon, a barátokon és a tanárokon, az utóbbi az ún. hirdetőfelületeken *(bulletin board)* keresztül fejti ki hatását, vagyis ad tanulható mintákat.[151]

Patrick Kinkade és munkatársai szerint az önazonosság is azt mutatja, hogy működik a társas tanulás, amelynek során a csoportba való beilleszkedésnek nagy szerepe van. Ilyen például, hogy a csoporton belül a sérülékenységek kiaknázásával szereznek megbecsülést, státuszt, amelynek feltétele, hogy e tettek az egyén képességein, tudásán alapuljanak.[152] Azok pedig, akik mások eszközeit, szoftvereit használják elkövetésre *(script kiddie),* a tőlük magabiztosabb elit hekkerek alatt helyezkednek el a hierarchiában. Az előbbiek nem is igazán részei a szubkultúrának, míg az utóbbiak számíthatnak a közösség védelmére. Emiatt fontossá válik, hogy komolyabb *'hekkekben'* is részt vegyenek a fiatal, kisebb tudással rendelkezők, mert így lehet helyük a csoportban. Azokat, akik akadoznak az elkövetés során, vagyis nem tudnak sikereket elérni, kiközösítik, míg a sikeresek feljebb jutnak a közösségi ranglétrán, és egyre több elkövetési módszert tanulnak meg.[153]

Robert Morris és Ashley Blackburn szintén a tanulás fontosságát emeli ki a *hacking* kapcsán.[154] Kutatásuk szerint a hekkertevékenységet a tudás megosztásának, az információhoz való hozzáférés ideájának és az elfogadható magatartások meghatározásának egyedi módjai jellemzik, és összességében is hangsúlyos a társas tanulás szerepe az ilyen típusú informatikai bűnözésnél. Emellett a hekkerek a digitális környezetet kevésbé tekintik védettnek a fizikai valósághoz képest, amelynek eredményeként kritikus lehet annak szerepe, hogy az egyén milyen mértékűnek érzi a lehetséges jutalmakat és büntetéseket. Vagyis a differenciális megerősítés jóval nagyobb szerephez juthat, mint a fizikailag érzékelhető valóságban, ahol a tanulás során

[150] Thomas J. Holt – Adam M. Bossler: An Assessment of the Current State of Cybercrime Scholarship. 35(1) *Deviant Behavior* (2014) 20–40.

[151] Holt–Bossler i. m. (4. lj.) 82–83.

[152] Patrick T. Kinkade – Michael Bachmann – Brittany Smith-Bachmann: Hekker Woodstock: Observations on an Offline Cyber Culture at the Chaos Communication Camp 2011. In: Thomas J. Holt (szerk.): *Crime Online: Correlates, Causes, and Context*. Durham, Carolina Academic Press, 2016. 29–55.

[153] Uo.; Navarro–Marcum i. m. (120. lj.) 8–9.

[154] Morris és Blackburn *hacking*definíciója a Skinner és Fream által meghatározott egyszerű belépésnél, valamint a *script kiddie* elkövetésnél bonyolultabb, nagyobb technológiai tudást igénylő tevékenységek körét tekinti idetartozónak. E felfogás hasonlatos az e tanulmány szerzője által az 50. lábjegyzetben kifejtett definícióhoz.

szóba jöhető egyéb faktorok közel egyenrangúan érvényesülnek.[155] Meglátásuk szerint az utánzás és a társak közötti együttműködés is fontos, amely részben annak köszönhető, hogy ezek az egyének szándékosan olyan társakat keresnek, akik hasonló magatartást tanúsítanak.[156]

A társas tanulás alkalmazhatósága tekintetében kulcsfontosságú Morris és munkatársa azon meglátása, miszerint a hagyományos deviáns cselekedetekkel szemben az informatikai bűnözéssel kapcsolatos lehetőségeknek és ideáloknak nincs morális története, így az, hogy valaki hogyan építi fel a bűnelkövetésre irányuló attitűdöket és definíciókat, a tanuláselmélet segítségével egyedi módon írható le. Ez azt jelenti, hogy a modern informatikai bűnelkövetők esetén valószínűtlen, hogy a szüleiktől tanulják meg az online térben létező és értelmezhető magatartások morális megítélését, hiszen az elkövethető cselekmények jelentős része csupán néhány évtizede létezik, és csak néhány éve vált széles körben elterjedtté.[157]

Marcum és társai 2014-es kutatásukban emellett szignifikáns összefüggést találtak a deviáns kortárs kapcsolatok és a *hacking* elkövetése között a fiataloknál. Akiknek online devianciát elkövető kortársa volt, az hajlamosabb volt az e-mail-fiókokba és a közösségi médiaprofilokba való behatolásra, sőt weboldalak feltörésére is.[158] Ez hasonlít arra, amit Skinner és Fream a szoftverletöltés kapcsán állítottak, de az általuk felvetett kapcsolatok szerepét, amelyeket ők csupán a szoftverkalózkodás esetében voltak képesek bizonyítani, a későbbi kutatások a nagyobb tudást igénylő, technológiaközpontú elkövetés esetén is alátámasztották.

A legtöbb tanuláselméletet tesztelő és informatikai bűnözéssel foglalkozó felmérés hiányossága, hogy csupán a differenciális asszociáció és a definíciók vizsgálatára szorítkozik, míg az utánzás és a differenciális megerősítés hasonlóan fontos elemeit kihagyja.[159] Továbbá az SSSL alkalmazhatóságának vizsgálata, így a társadalmi strukturális elemek és az informatikai bűnözés közötti kapcsolat elemzése ez idáig szinte teljesen elmaradt. Eddig egyetlen kutatás, Holt, Burruss és Adam Bossler tanulmánya foglalkozik a kérdéssel. Holt és társai a kutatásában mind a négy, Akers által azonosított faktort, valamint az SSSL által felvázolt, ugyancsak négy társadalmi strukturális faktort egyszerre vizsgálták.[160] Eredményeik közül fontos kiemelni, hogy a társas tanulás részben hatással van a kiberdevianciákhoz szükséges számítástechnikai készségek szintjére. Ez a kapcsolat szerintük logikus is a tanuláselmélet függvényében, hiszen aki jelentős mértékben érdeklődik a technológia és a számítógépes készségek iránt, az hajlamosabb olyan társakat keresni, akik ezt a korai érdeklődést osztják.[161] Továbbá szerintük azok az egyének,

155 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.

156 Uo., 33.

157 Navarro–Marcum i. m. (120. lj.) 8.

158 Marcum i. m. (67. lj.) 581–591.; Navarro–Marcum i. m. (120. lj.) 9.

159 L. pl. George E. Higgins – David A. Makin: Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy. 2(2) *Journal of Economic Crime Management* (2004) 1–22.; George E. Higgins – Abby L. Wilson: Low Self-Control, Moral Beliefs, and Social Learning Theory in University Students' Intentions to Pirate Software. 19(2) *Security Journal* (2006) 75–92.

160 Holt–Burruss–Bossler i. m. (135. lj.).

161 Uo., 50.; l. még Steven Furnell: *Cybercrime: Vandalizing the Information Society*. London, Addison-Wesley, 2002; Thomas J. Holt: Subcultural Evolution? Examining the Influence of On- And Off-Line Experiences on Deviant Subcultures. 28(2) *Deviant Behavior* (2007) 171–198.

akiknek már fejlett számítástechnikai készségeik vannak, olyan definíciókat szolgáltathatnak, amelyek támogatják a kiberdevianciákban való részvételt, ami utánzáshoz, így közvetlenül a deviáns cselekedetekben, különösen rendszerek elleni támadásokban, zaklatásban vagy megkérdőjelezhető jogi megítélésű (ún. *borderline*) tettekben való részvételhez vezet.[162]

A deviáns kortársakkal kapcsolatos differenciális asszociáció és a jogszabályok megsértését favorizáló definíciók is szignifikáns kapcsolatot mutattak az elkövetéssel, vagyis e két tényező szerepe az informatikai bűnözés tanulásában kiemelten fontosnak bizonyult. Holt, Burruss és Bossler kutatása ugyanakkor azon szakirodalmi megállapításokat is támogatja, amelyek szerint a differenciális megerősítés közvetlen kapcsolatban áll a legtöbb deviáns online magatartással: az egyének nagyobb valószínűséggel követnek el kiberdevianciákat, amikor jutalmat vagy támogatást kapnak érte például az iskolában vagy a munkahelyen. E megállapítás egyezik Skinner és Fream kutatásának fentebb ismertetett konklúziójával.[163]

Ami Holt, Burruss és Bossler kutatásában meglepő, az az utánzás szerepének bizonyítása. A korábban végzett kutatások az informatikai bűnözés és egyéb bűncselekmények terén marginális szerepet tulajdonítottak az utánzásnak, míg Holt és munkatársai annak a differenciális megerősítést meghaladó szignifikanciáját jelezték.[164] Ez Holték szerint az informatikai bűnözés egyedi jellemzője, aminek az az oka, hogy e területen a legnagyobb a szerepe az egymástól való tanulásnak, amihez hozzájárul a társas kapcsolatokból eredő pozitív támogatás, a definíciók rögzülése is, és ezt követően történik meg az informatikai bűncselekmények elkövetési módjainak elsajátítása, részben utánzás útján. E tekintetben jellemző, hogy az elkövetési módszerek bonyolultsága miatt nagyobb is az utánzás szerepe, ami egyben a rövid távú, epizódszerű elkövetést erősíti a bűnözői karrier kialakulásával szemben.

A tanulmány hiányossága, hogy keresztmetszeti adatokon alapul, valamint a differenciális megerősítés esetén elsősorban az informális megerősítés változóit vizsgálta, így a különböző jogi, pénzügyi és munkahelyi szankciók nem képezték az elemzés részét. E változók hatására ugyanis lehetséges, hogy az utánzás mellett a differenciális megerősítés szerepe is megnövekedik. A kutatás továbbá, a korábbiakhoz hasonlóan, szintén elsősorban az SSSL négy direkt faktorának vizsgálatára szorítkozott, az indirekt faktorok hatását csak közvetett módon vonta be az elkövetővé válás kutatásába.

A tanuláselméleti perspektívát nem csupán önmagában tesztelték már az informatikai bűnözés viszonylatában, találhatunk példát az önkontroll és a társas tanulás változóinak együttes vizsgálatára is. A korábban már ismertetett példák mellett Brooke Nodeland és Morris 2018-as tanulmánya a differenciális asszociáció és a definíciók szerepét vizsgálja az informatikai bűncselekmények elkövetésében, majd e tényezőkhöz kapcsolja az önkontrollt is, aminek meglátásuk szerint nincs direkt kapcsolata az online elkövetéssel, a differenciális asszociációval és a definíciókkal való kapcsolata mégis bizonyítható.[165] A tanulmány érdeme, hogy teszteli az elméletet nemcsak az online, hanem az offline társaktól való tanulás hatásainak viszonylatában is.

[162] Uo., 51.
[163] Uo., 52.
[164] Uo.
[165] Brooke Nodeland – Robert Morris: A Test of Social Learning Theory and Self-Control on Cyber Offending. 41(1) *Deviant Behavior* (2018) 41–56.

Nodeland és Morris a társas tanulásról a korábban ismertetett kutatókhoz hasonlóan vélekednek. Szerintük a tanulási folyamatokhoz adott környezet nagyon kedvező az online térben, mivel könnyen elérhető az anonimitás, az elkövetők gyorsan és viszonylag alacsony kockázattal juthatnak jutalmakhoz, ami a magatartások differenciális megerősítéseként szolgálhat. Továbbá az elkövetőknek szinte korlátlan hozzáférésük van az instrukciókhoz és a társak által elkövetett támadások demonstrációihoz, valamint a különböző szintű tapasztalattal rendelkező internetfelhasználókhoz.[166] A virtuális környezet emellett támogatja az utánzást, amelynek során végrehajthatnak cselekményeket, és szemtanúi lehetnek a virtuális ismerősök tevékenységének – elenyésző vagy teljesen hiányzó felügyelet mellett. Holt, Bossler és May 2012-es kutatása is hangsúlyozza,[167] valamint Holt, Kristie Blevins és Joseph Kuhns 2008-as,[168] illetve Gordon Meyer 1989-es kutatása[169] is alátámasztja az online közösségek szerepét a társas hálózatok kiépítésében és az információszerzésben.

Tanulmányuk továbbá azon korábbi kutatások által felvetett gondolatokon alapul,[170] hogy a tanulás általános szerepe mellett az egyéni különbözőségek, így például az önkontroll is növelheti a kriminális magatartásokba való bevonódást, amely az informatikai bűncselekmények esetében is igaz lehet. Pratt és Francis Cullen metaanalízise is azt mutatta,[171] hogy a társadalmi tanuláselmélet és az önkontrollelmélet inkább kiegészítik egymást, mintsem egymás konkurenciái, amely gondolatot már Akers is megfogalmazta. Ő az önkontrollt úgy látja, mint egy viselkedés irányításának képességét annak függvényében, hogy mások mennyire erősítik meg az egyén konformitását a kezdeti szocializációs időszakot követően.[172] Nodeland és Morris kutatásukban a társadalmi tanulás szerepét igazolták. Eszerint a deviáns társak szerepe szignifikáns az informatikai bűnelkövetésben és önmagában az informatikai tudás, az eszközök használatának fejlett ismerete nem indikál elkövetést. E cselekményekben nagy szerepe van a társas kapcsolatok megerősítő és támogató hatásának.[173]

Nodeland és Morris az önkontroll szerepét – a korábbi, részben fentebb is ismertetett vizsgálódásokkal ellentétben – nem tudták igazolni. Ennek ellenére kimutatták, hogy az önkontroll szignifikáns interaktív (pl. moderáló) hatással bír a társadalmi tanuláselmélet bűnözést támogató definíciós és a differenciális megerősítő/büntető elemeire. Ez azt jelenti, hogy a magasabb önkontroll csökkentheti a bűnözést támogató definíciók hatását. Még ha egy fiatal a bűnözést favorizáló definíciókkal rendelkezik is, és általában véve nagyobb eséllyel követ el infor-

166 Uo., 42–43.

167 Holt–Bossler–May i. m. (71. lj.).

168 Thomas J. Holt – Kristie R. Blevins – Joseph B. Kuhns: Examining the Displacement Practices of Johns with On-Line Data. 36(6) *Journal of Criminal Justice* (2008) 522–528.

169 Gordon R. Meyer: *The Social Organization of the Computer Underground*. Szakdolgozat, Northern Illinois University (1989), http://aom.jku.at/archiv/cmc/text/meyer_89.pdf.

170 L. T. David Evans et alii: The Social Consequences of Self-Control: Testing the General Theory of Crime. 35(3) *Criminology* (1997) 475–504.; Chris Gibson – John Wright: Low Self-Control and Coworker Delinquency: A Research Note. 29(6) *Journal of Criminal Justice* (2001) 483–492.

171 Travis C. Pratt – Francis T. Cullen: The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis. 38(3) *Criminology* (2000) 931–964.

172 Ronald L. Akers: Self-Control as a General Theory of Crime. 7(2) *Journal of Quantitative Criminology* (1991) 201–211.

173 Nodeland–Morris i. m. (165. lj.) 51.

matikai bűncselekményt e definíciók segítségével a tanulási folyamat során, akkor is lehetséges, hogy az önkontroll magasabb individuális szintje kioltja a bűnözést támogató definíciók hatását.[174] Nodeland és Morris tehát azt állítja, hogy az önkontrollelmélet önmagában nem bír magyarázó erővel, az csupán a társadalmi tanuláselmélettel való interakciója útján befolyásolja az informatikai bűnelkövetést, pontosabban a társadalmi tanulás elemeinek hatását. A legfontosabb az online és az offline kapcsolatok szerepe a differenciális asszociáció során. A technológiai tudásnál fontosabbnak tartják azt, hogy a fiatal kivel tölti az idejét, így az informatikai ismeretek birtoklása önmagában nem növeli az elkövetővé válás esélyét.

A Sutherland, Akers, Burgess, sőt Bandura által megalapozott, megalkotott vagy épp újragondolt tanuláselméleti perspektíva annak általános igényű magyarázó ereje folytán a kibertérfüggő bűnözésre leginkább alkalmazható elmélet. Ezt támasztják alá a fentebb ismertetett kutatások, amelyek mind a kibertér által elősegített, mind a kibertérfüggő, szofisztikáltabb bűnelkövetés esetén a tanuláselméleti elemek alkalmazhatóságát bizonyítják. A tanuláselméleti perspektíva fejlődése során kidolgozott teóriák közül egyértelműen Akers differenciális asszociációmegerősítés elmélete bír a legnagyobb támogatottsággal az informatikai bűnözés terén. Ezen belül is a definíciók és a differenciális asszociáció elemének primátusa érvényesül, ugyanakkor egyre többen emelik ki az utánzás szerepét is, amelynek relevanciája a hagyományos bűnelkövetésben alacsonyabb volt a korábbi kutatások szerint. A fentebb ismertetett elemzések azt jelzik, hogy az online társak által közvetített értékek, tanulást elősegítő folyamatok és a bűnözést követő megerősítés megnöveli az elkövetővé válás esélyét. Emellett vannak olyan szerzők is, akik a felelősségre vonás csekély valószínűségében, a büntetések elmaradásában vélik felfedezni a visszatérő bűnözés vagy éppen a karrierbűnözés kialakulásának egyik okát. E gondolatok, valamint az empirikus kutatások mind afelé mutatnak, hogy az informatikai bűnelkövetés tanult viselkedés, amelynek értelmezésére Akers differenciális asszociációmegerősítés elmélete a leginkább alkalmas.

Az Akers elméletének gerincét képező mind a négy tényező vizsgálata elengedhetetlen az online devianciák tanulási folyamatainak elemzése során. Ugyanakkor annak egyes elemeinek, például a bűnözést támogató, a neutralizáló definíciók szerepének vizsgálata, vagy a bűnözési karrier egyéb kriminológiai elméleti keretekkel kiegészítve történő értelmezése lehet igazán alkalmas komplex magyarázatokra. Míg a definíciók elemzéséhez segítséget nyújt Sykes és Matza neutralizációelmélete, addig az informatikai bűnözés mint életpályát átívelő folyamat vizsgálatához hasznos tudást adnak a fejlődéskriminológia egyes, később bemutatott gondolatai.

2.3.2. Neutralizációelmélet

A neutralizációelmélet megjelenése a Stanley Cohen, illetve Richard Cloward és Lloyd Ohlin által megfogalmazott szubkultúra-elméletekre való reflexióként jelent meg 1957-ben.[175] Sykes és Matza a szubkultúra-kutatások azon állításával ment szembe, amely szerint annak tagjai

[174] Uo., 52.

[175] Richard A. Cloward – Lloyd E. Ohlin: *Delinquency and Opportunity: A Theory of Delinquent Gangs*. New York, Free Press, 1960.

olyan egységes értékrenddel rendelkeznek, amely a bűnözést közvetlenül támogatja.[176] Ez azt jelenti, hogy a bűnelkövető fiatalok tisztában vannak a többségi társadalom által vallott erkölcsi meggyőződéssel, sőt annak megsértése esetén szégyent és bűntudatot is éreznek, ugyanakkor valamilyen oknál fogva mégis elkövetik az adott cselekményt. Sykes és Matza e jelenséget a bűnelkövetést megelőző és a kriminalitás során jelenlévő mentális folyamat következményének látja. Vagyis nem kifejezetten a bűnözést támogató nézetek egyeduralmáról van szó, mint inkább a konform erkölcsi és jogi normákat tagadó önigazolásról, önfelmentésről, mentesülésről. Sykes és Matza szerint ehhez öt típusú neutralizációs technika áll rendelkezésre, amelyek közül akár egy vagy egyszerre több is alkalmas lehet a bűnözésért vállalt morális felelősség semlegesítésére. E technikák a felelősség tagadása, az okozott sérelem tagadása, az áldozat tagadása, az elítélés és az elítélők elutasítása, valamint a magasabb értékekre hivatkozás.[177] E technikák segítségével a fiatalok számára elfogadhatóvá válik cselekedetük, függetlenül attól, hogy mit diktálnak a társadalmi normák.[178] Az egyen áthárítja a cselekménnyel járó felelősséget, vagy egészében tagadja azt, így lehetővé válik a cselekmény által okozott sérelmek létének tagadása, vagy a meglévő társadalmi normák helytállóságának megkérdőjelezése. Mindemellett Sykes és Matza a fiatalok közötti interakciók fontosságát is kiemeli a neutralizációs folyamatban.[179]

Az elmélet nem csupán önmagában nagy jelentőségű, annak kapcsolata Sutherland differenciális asszociációelméletével is szoros. Sykes és Matza ugyanis bizonyos szempontból a Sutherland, majd később Akers által megfogalmazott, a bűnözést támogató képzeteket (definíciókat) töltötték meg tartalommal. E kapcsolódási pont abban rejlik, hogy a tanulási folyamat során átadott prokriminális definíciók e neutralizációs technikák tartalmi elemeit foglalják magukban, így magyarázatot adnak arra, hogy milyen módon férhetnek meg egymás mellett a konform morális sémák és a bűnözést támogató alternatív képzetek. Mi több, Sykes és Matza az elmélet kiterjesztésével, a fiatalok sodródásának megfogalmazásával arra is magyarázatot adtak, hogy miért csupán a bizonyos típusú és epizodikusan megjelenő bűnelkövetés a jellemző. Eszerint a többségi társadalom normáinak megfelelően élő fiatal számára csupán epizodikusan kerülnek többségbe a bűnözést támogató vagy a morális elítélendőséget neutralizálni képes magyarázatok.[180]

Az elmélet részeként szolgáló neutralizáció az évek során nem csupán a sodródás jelenségével, hanem egyéb neutralizációs technikák megfogalmazásával is bővült. Ezek közül a legjelentősebbek az ún. főkönyvi metafora *(metaphor of the ledger),*[181] a William Minor által meg-

[176] Borbíró–Győry i. m. (104. lj.) 150.

[177] Sykes–Matza i. m. (126. lj.) 664–670.

[178] Robert G. Morris – George E. Higgins: Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration among College Undergraduates. 34(2) *Criminal Justice Review* (2009) 173–195.

[179] Borbíró–Győry i. m. (104. lj.) 150.

[180] Russell Brewer – Sarah Fox – Caitlan Miller: Applying the Techniques of Neutralization to the Study of Cybercrime. In: Thomas J. Holt – Adam M. Bossler (szerk.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London, Palgrave Macmillan, 2020. 547–565., 552.

[181] Ez azt jelenti, hogy az egyén úgy véli, hogy mivel életében már véghez vitt jó cselekedeteket, megengedhető, hogy bizonyos rossz cselekedeteket is elkövessen. Carl B. Klockars: *The Professional Fence*. New York, Free Press, 1974.

fogalmazott védelem szükségessége *(defence of necessity),*[182] a negatív szándék tagadása *(denial of negative intent),* a viszonylagos elfogadhatóság *(claim of acceptability),*[183] a jogosultság *(claim of entitlement),*[184] a normális követelés indoka *(claim of normalcy)* vagy az összehasonlítással való igazolás *(neutralization by comparison)*.[185] Legszélesebb körben ugyanakkor továbbra is a Sykes és Matza által megfogalmazott öt technikával találkozhatunk a kriminológiai szakirodalomban.

A neutralizációelmélet az informatikai bűncselekmények kutatása terén fontos szerepet tölt be, de annak alkalmazására gyakran nem önmagában, hanem egyéb elméletek, így különösen Akers differenciális asszociációmegerősítés elméletének kiegészítéseként, annak definíciós eleméhez kapcsolódva kerül sor. Az elmélet e területen történő alkalmazását nem csupán a morális önigazolás virtuális térre való látványos illeszkedése, hanem a sodródás érvényesülésének egyértelmű jelei is megerősítik. E folyamatot a szakirodalom a *digital drift,* vagyis a „digitális sodródás" jelzővel illeti, ami nem más, mint az az „egyedülálló szerep, amelyet a technológia a társadalmi normák és értékek lazításában is játszhat, ezáltal lehetővé teszi az egyének számára, hogy elkötelezzék magukat a bűnözés irányába és el is szakadjanak attól".[186] Továbbá fontos, hogy ez a neutralizáció és sodródás az online térben értelmezhető egyedülálló folyamatként játszódik le, amely gyakran nincs hatással a hagyományos tér, a 'való világ' normáinak semlegesítésére.

A neutralizációelmélet így jól illeszkedik az előző részben felvázolt, Akers által kibontott differenciális asszociáció tételébe is. Sőt, annak informatikai bűnözésre való alkalmazhatósága is széles körben támogatott. E neutralizációs tényezők, valamint maga a sodródási folyamat a tanulási elmélet részeként képes magyarázatot adni arra a jelenségre, hogy egyes fiatalok miért követnek el informatikai bűncselekményt, vagy ezzel párhuzamosan miért tartózkodnak a hagyományos bűnelkövetés formáitól. Az e nézetet valló kriminológusok szerint ugyanis az informatikai bűnözéshez társuló és az online társaktól tanult (neutralizáló) definíciók csupán az online tér kriminalitásával kapcsolatosan fogalmazódnak meg, így például hagyományos, fizikai sérelemokozással társuló cselekmények esetében egybevágnak a többségi társadalom normáival.

Az informatikai bűnözés, pontosabban a digitális kalózkodás területén alkalmazta az elméletet Sameer Hinduja 2007-ben.[187] Ő az öt neutralizációs technika mellett az újabb technikákat is vizsgálta. Azt találta, hogy az eredeti elméletből származó tényezők közül kettő, az okozott sérelem tagadása és a magasabb értékekre hivatkozás, valamint az újabb elemek közül a negatív szándék tagadása és a viszonylagos elfogadhatóság (pl. mindenki csinálja) pozitívan hat

[182] W. William Minor: Techniques of Neutralization: A Reconceptualization and Empirical Examination. 18(2) *Journal of Research in Crime and Delinquency* (1981) 295–318., 298.

[183] Stuart Henry (szerk.): *Degrees of Deviance: Student Accounts of Their Deviant Behaviour*. Salem, Sheffield, 1990.

[184] James W. Coleman: *The Criminal Elite: The Sociology of White Collar Crime*. New York, St. Martin's, 1985.

[185] Paul Cromwell – Quint Thurman: The Devil Made Me Do It: Use of Neutralizations by Shoplifters. 24(6) *Deviant Behavior* (2003) 535–550.

[186] Brewer–Fox–Miller i. m. (180. lj.) 2–3.; Andrew Goldsmith – Russell Brewer: Digital Drift and the Criminal Interaction Order. 19(1) *Theoretical Criminology* (2015) 112–130.

[187] Sameer Hinduja: Neutralization Theory and Online Software Piracy. 9(1) *Ethics and Information Technology* (2007) 187–204.

az online szoftverkalózkodásra. Vizsgálta a főkönyvi metafora szerepét is a kalózkodásban, azonban e technika esetében nem talált szignifikáns összefüggést a szoftverkalózkodás előre jelezhetősége tekintetében.[188]

Jason Ingram és Hinduja a témában 2008-as, több mint 2000 egyetemistával végzett kutatása azt mutatta, hogy a neutralizáció egy része segítségével (négy technika az elítélés és az elítélők elutasítása esetén kívül) előre jelezhető az online zenekalózkodás. Ennél is fontosabb a szerzők megállapításai szerint, hogy a neutralizáció szerepe az online zenei kalózkodásban attól függően változhat, hogy az egyén milyen mértékben vesz részt a tevékenységben.[189] Holt és Heith Copes a témában végzett 2010-es, mélyinterjúkon alapuló kutatása arról számol be,[190] hogy a Sutherland által megalkotott differenciális asszociáció téziseihez szorosan illeszkedve számos példát találhatunk a digitális kalózkodásra. E kulturálisan szürkezónában lévő cselekménnyel kapcsolatban írnak a 'kalóz szubkultúra' kialakulásáról, amelynek lényegi elemét képezi az illegális letöltéseket támogató definíciók kialakítása, ezek továbbadása, valamint a morális önigazolást nyújtó definíciókon keresztüli neutralizáció. Az interjúk szerint egyfelől a tartalom tesztelése végett történik a letöltés, majd annak megítélését követi a vásárlás vagy az attól való tartózkodás, másfelől a szoftverek magas ára szolgál a jogsértő letöltés indokául, továbbá például az elítélés és az elítélők elutasítása leggyakrabban a szerzői jogot védő entitásokkal, vagy egyenesen a jogszabályokkal szembeni ellenérzésekben jelenik meg. Kutatásuk mind az öt neutralizációs technika meglétét igazolta az online letöltés esetében.[191]

A digitális kalózkodás mellett találhatunk a kibertérfüggő bűncselekményekkel, közelebbről a jogosulatlan behatolással, szoftvermanipulációval vagy a vírusírással kapcsolatos kutatásokat. Morris 2010-ben azt találta, hogy a technikák többsége képes előre jelezni, hogy a felhasználó részt vesz-e jelszavak próbálgatásában, illegális rendszerbehatolásban vagy fájlmanipulációban. Az áldozat tagadása például akkor mutat szignifikáns kapcsolatot az elkövetéssel, amikor e három cselekmény egy komplex elkövetésben egyszerre jelenik meg *(hacking attack)*. A neutralizációs technikák együttesen voltak jelen továbbá a jelszópróbálgatás során és az illegális belépésnél, ugyanakkor a fájlmanipulációnál nem. Külön-külön vizsgálva pedig az okozott sérelem tagadása volt szignifikáns mindhárom elkövetési formában.[192]

A kibertérfüggő bűncselekmények és a neutralizáció kapcsolatát vizsgáló kutatásában Holt és Yi Ting Chua az informatikai bűnözés egy letisztult csoportosítását fogalmazza meg, és kiemelik a szofisztikáltabb informatikai bűnelkövetés, így például a *malware*-készítés, a rendszerbehatolás stb. készségeivel rendelkezők egyedi motivációit, tanulási folyamatait és neutralizációs technikáit.[193] A neutralizációnak nagy szerepet tulajdonítanak, de nem tartják feltétlenül

188 Uo., 194–198.

189 Jason R. Ingram – Sameer Hinduja: Neutralizing Music Piracy: An Empirical Examination. 29(4) *Deviant Behavior* (2008) 334–366.

190 Holt–Copes i. m. (42. lj.) 625–654.

191 Uo., 648.

192 Robert G. Morris: Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. In: Thomas J. Holt – Bernadette H. Schell (szerk.): *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey, Information Science Reference, 2011. 1–17.

193 Yi Ting Chua – Thomas J. Holt: A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. 11(4) *Victims & Offenders* (2016) 534–555.

alkalmazhatónak a társadalmi tanuláselméletet e bűnelkövetői körre, tekintve hogy annak tagjai nagyobbrészt egyedül követik el a cselekményeket. Ennek következtében az informatikai bűnözés szituációs természetét felismerő keretrendszerek fontosságát emelik ki, és azon kognitív folyamatokat, amelyek által az elkövetők igazolhatják vagy felmenthetik jogsértő magatartásukat.[194] Az eredmények szerint három neutralizációs technika mutatott szignifikáns kapcsolatot az 'egyszerű' *hacking*gel és a *malware*-ekkel kapcsolatos magatartásokkal: a felelősség tagadása, az okozott sérelem tagadása és a magasabb értékekre hivatkozás.[195] Susan Harrington 1996-ban szintén erős kapcsolatot talált a felelősség tagadása és a kibertérfüggő bűncselekmények elkövetése között, munkahelyi környezetben.[196] Mindezek ellenére a legtöbb, kibertérfüggő bűnözéssel kapcsolatos kutatás nem támasztja alá a felelősség tagadásának szignifikanciáját.[197]

Russel Brewer, Sarah Fox és Caitlan Miller összefoglaló írása alátámasztja a neutralizáció egyéb technikáinak relevanciáját a kibertérfüggő cselekmények esetében.[198] A neutralizációs technikák alkalmazása az online kalózkodás esetében igazolódik be, ugyanakkor a *hacking*gel kapcsolatban is megjelenik. Ez utóbbira jó példa Sigi Goode és Sam Cruise 2006-os,[199] Alice Hutchings 2013-as,[200] valamint Chua és Holt már említett 2016-os vizsgálata,[201] amelyek főként az okozott sérelem és az áldozat tagadását, valamint a magasabb értékekre hivatkozást tekintik lényegesnek a kibertérfüggő bűnözés esetében. Brewer és munkatársai összefoglaló tanulmánya ugyanakkor jelzi, hogy e kutatások eredményeivel óvatosnak kell lennünk, hiszen azok operacionalizálása és különösen a technikák pontos tartalma az egyes bűncselekménytípusoknál és szerzőnként is eltér.[202]

Végül a neutralizációval összefüggésben fontos bővebben szót ejteni a társadalmi tanuláselmélettel való kapcsolat fontosságáról, illetve annak empirikus megjelenéséről. Morris röviden már említett, 2011-ben végzett kutatásában a neutralizációs vizsgálatba bevonta a társakkal való differenciális asszociáció szerepének elemzését is.[203] De nem csupán a neutralizációból merített, hanem az elemzésbe beépítette a deviáns társakhoz való differenciális asszociációt is. Eredményei szerint mind a neutralizáció technikái, mind a hekkerekkel való asszociáció szignifikáns előre jelzője a kártékony *hacking* tevékenységnek. Sőt szerinte a hekkertársakkal való együttműködés, a közös tanulás nagyobb szerepet játszik, mint az előzetes és az utólagos semlegesítés, ugyanakkor mindkettőnek érdemi hatása van a cselekmény bekövetkeztére.[204]

194 Uo.

195 Uo., 545–550.

196 Susan J. Harrington: The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. 20(3) *MIS Quarterly* (1996) 257–278.

197 Brewer–Fox–Miller i. m. (180. lj.) 553.

198 Uo.

199 Sigi Goode – Sam Cruise: What Motivates Software Crackers? 65(2) *Journal of Business Ethics* (2006) 173–201.

200 Alice Hutchings: Hacking and Fraud: Qualitative Analysis of Online Offending and Victimization. In: Karuppannan Jaishankar – Natti Ronel (szerk.): *Global Criminology: Crime and Victimization in a Globalized Era*. Boca Raton, CRC, 2013. 93–114.

201 Chua–Holt i. m. (193. lj.)

202 Brewer–Fox–Miller i. m. (180. lj.) 561–563.

203 Morris i. m. (192. lj.).

204 Uo., 14–16.

Morris korábban ismertetett neutralizációs eredményeivel szemben a kortársakkal való differenciális asszociáció minden vizsgált informatikai jogsértés esetén megfigyelhető volt. Ennek következtében szerinte a neutralizációs technikák részleges alkalmazhatósága miatt a társas tanuláselmélettel való kiegészítés szükséges a *hacking* magatartások okainak szélesebb körű megismeréséhez.[205] Mindazonáltal nem szabad megfeledkezni Morris azon álláspontjától, miszerint a digitális tér egyedi szocializációs hatását, a kortársakkal való differenciális asszociáció és a neutralizáció sajátos dinamikáját nem sikerült egyértelműen alátámasztani.

Brewer és társai azon a véleményen vannak a társadalmi tanuláselmélet és a neutralizáció összekapcsolhatóságáról, hogy az előbbi 'definíciói' fogalmilag hasonlók az utóbbi technikáihoz, mert mindkettő az egyén deviáns magatartásának észlelésével és a bűncselekmény elősegítésében játszott szerepével foglalkozik. A semlegesítés technikái azonban eltérnek a társadalmi tanulás elméletétől abban, hogy arra összpontosítanak, hogy az egyén hogyan használja fel ezeket a definíciókat az ilyen viselkedésekben való részvétel semlegesítésére vagy igazolására. Ezzel szemben a társadalmi tanuláselmélet inkább ezen felfogások átadásával foglalkozik a bűnözés legitimálása és ösztönzése céljából.[206]

Összességében a fenti kutatási tapasztalatokból az látható, hogy a társadalmi tanuláselmélet egyik direkt tényezőjeként az Akers által azonosított definíciók tartalmukban átfedést mutatnak a neutralizáció elemeivel, így Sykes és Matza elmélete elősegítheti a társadalmi tanulás e részének operacionalizálását. Sőt, Mark Lanier és Stuart Henry 1998-ban a neutralizációs elméletet egyenesen a tanuláselméletek csoportjába sorolta.[207] Sykes és Matza neutralizációelmélete az informatikai bűnözéssel kapcsolatos definícióalkotás és az online tér egyedi morális dinamikája következtében jelentős népszerűségnek örvend. Az elmélet számos elemét a kriminológiai kutatások alátámasztották, de az elsősorban a bűnözéssel kapcsolatos morális folyamatok értelmezésére, és kevéssé az informatikai bűnelkövetővé válás egészének leírására alkalmas. Az elmélet magyarázatot adhat tehát az epizódszerű, bűnelkövetésbe sodródó egyén belső folyamatairól, ám nem képes a szélesebb szocializációs és makrotársadalmi hatások magyarázatára. Továbbá az informatikai bűnözés enyhébb formáival (pl. online kalózkodás) és a fiatalkori, főként kíváncsiságvezérelt *hacking*gel szemben a karrier típusú, szofisztikáltabb és hosszú időn át visszatérő bűnelkövetés okaira sem képes magyarázatot adni. Az elmélet inkább a társadalmi tanuláselmélet definíciós elemeit konkretizáló, rendszerező és támogató szerepében igazán hasznos az informatikai bűnözés súlyosabb, kibertérfüggő formáit elkövető személyekben lejátszódó (a cselekményt megelőző és azt követő) folyamatok vizsgálatára.

[205] Uo.

[206] Brewer–Fox–Miller i. m. (180. lj.).

[207] Mark Lanier – Stuart Henry: *Essential Criminology*. Boulder, Westview, 1998.

2.4. A fejlődéskriminológiai perspektíva és az életpályamodellek alkalmazhatósága az informatikai bűnözésben

A fejlődéskriminológiai kutatások az informatikai bűnözés terén elsősorban a fentebb ismertetett kontrollelméleti perspektívával együtt jelennek meg, de találhatunk egy-egy társadalmi tanuláselmélettel kapcsolatos példát is, amely elsősorban az informatikai bűnelkövetésbe való belépés, a karrierút és a dezisztencia jellemzőinek és folyamatának értelmezéséhez járul hozzá. A fejlődéskriminológia olyan modell, amely nem az oksági elméletekből indul ki, nem azok operacionalizálása a célja, hanem a megvizsgált bűnelkövetésre ható párhuzamos oksági láncolatok és összefüggések feltárása longitudinális empirikus vizsgálatok segítségével.[208] Például Alfred Blumstein, Jacqueline Cohen, Jeffrey Roth és Christy Visher például a bűnözés dinamikus folyamatát longitudinális adatfelvétellel vizsgálták az individuális elkövetőknél.[209] E paradigma keretén belül a hangsúly a bűnözés longitudinális, fejlődési és életútszerű jellemzőin, valamint a bűnelkövetői aktivitás sajátos pontjain van, amelyeket külső (társadalmi) és belső (egyénben rejlő) tényezők befolyásolnak.[210] E tényezőket a szakirodalom ún. kockázati és védőfaktoroknak nevezi, amelyek a bűnözés kezdete, a karrier tartama, tartalma, a bűnözésből való kilépés és a bűnelkövetővé válással szembeni védettség kialakulása szempontjából bírnak nagy jelentőséggel.[211]

E faktorok közül Balogh Karolina a következők jelentőségét emeli ki: individuális faktorok (pl. az intelligencia mértéke, a személyiségvonások és a temperamentum), családi háttér (pl. a szülő nevelési módszerei, szülői fegyelem vagy családtag általi bűnelkövetés), szocioökonómiai státusz (pl. alacsony jövedelem, rossz lakáskörülmények és bizonytalan foglalkoztatás), kortárs kapcsolatok (pl. deviáns kortásakkal való társulás), iskola (pl. iskolai teljesítmény és sikeresség szintje, iskolai légkör), közösségi faktorok (pl. társadalmi dezorganizáció, közösségek státusza). E faktorok *(trajectories)* tartalmuk szerint megjelenhetnek védő- és rizikótényezőkként is, így például a nem deviáns kortársakkal való baráti kapcsolat vagy a pozitív iskolai légkör védőfaktorként játszhat szerepet, illetve ezek megjelenése elősegítheti a bűnözésből való kilépést vagy a védettség kialakulását a bűnözéssel szemben.[212]

A fejlődési paradigma a korábbi oksági elméletektől eltérően a bűnelkövetői létet dinamikus jelenségként értelmezi, amely a bűnözés és az abból való kilépés előrejelzésére, előre jelezhetőségének kialakítására helyezi a hangsúlyt a dinamikus faktorok tartalmának hosszú távú

[208] Balogh Karolina: A fejlődéskriminológia mint a fiatalkori bűnmegelőzés elméleti kerete. In: Fazekas Marianna (szerk.): *Jogi tanulmányok: Előadások az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskoláinak Konferenciáján*. 2018 június 7. Budapest, ELTE ÁJK Állam- és Jogtudományi Doktori Iskola, 2018. 367–378., 367–368.

[209] Alfred Blumstein et alii (szerk.): *Criminal Careers and „Career Criminals", 1. Report of the Panel on Criminal Careers*. Washington, National Academy of Sciences, 1986.

[210] Wesley G. Jennings: Life-Course/Developmental Theories. In: Wesley G. Jennings (szerk.): *The Encyclopedia of Crime and Punishment*. Chichester, John Wiley & Sons, 2016.

[211] Balogh i. m. (208. lj.) 368.; Tara Renae McGee – David P. Farrington: Developmental and Life-Course Theories of Crime. In: Alex R. Piquero: *The Handbook of Criminological Theory*. Oxford, Wiley Blackwell, 2016. 337.

[212] Balogh i. m. (208. lj.) 370–375.

vizsgálatán keresztül. Mi több, más elméletekhez képest jóval korábbra helyezi a rizikó- és a védőfaktorok vizsgálatát, így már a korai gyermekkortól kezdve értelmezi a bűnelkövetővé válást. Ennek következtében a paradigma értelmében az életvitelszerűen folytatott elkövetés oka a korai fejlődési *(neurodevelopmental)* és kognitív hiányosságokban, valamint a káros környezeti életkörülményekben is rejtőzhet.[213]

Sampson és Laub megjegyzi, hogy a fejlődéskriminológiai paradigma több, mint puszta longitudinális vizsgálatok összessége. A fejlődés a szisztematikus változásra összpontosít, és főleg arra, hogy a viselkedés milyen dinamikus folyamatokat indít el, amelyek megváltoztatják a jövőbeni kimeneteket.[214] Ezzel a paradigmát a bűnözés általános elméletével és a társadalmi tanuláselmélettel is szembeállítják. Érvük szerint a statikus nézőpont – amilyen az önkontroll vizsgálata – azt állítja, hogy a bűnözés az élet elején, korán kialakul, és az idő múlásával stabil marad, amelyet a népesség bűnözési hajlandóságának homogenitása is bizonyít. Továbbá, ellentétben a társas tanulással, segítségével az a folyamat, a mérföldkövek és életesemények is vizsgálhatók, amelyek az adott deviáns magatartás felé fordítják az egyént, és megjósolható a kilépés és a karrier hossza is.[215]

E longitudinális szemlélet hasznosságát továbbá a bűnelkövetői karrier fázisainak meghatározhatósága adja, amely a bűnelkövetés tartama és tartalma szerint teszi lehetővé a bűnelkövetők csoportosítását. A fejlődéskriminológia szerint vannak, akik esetében a bűnelkövetés korai kezdetű és a serdülőkorra korlátozódik, és van, amikor csak felnőtt korban jut el az elkövető a dezisztencia szakaszába. Az tehát nagyon eltérő, hogy ki mikor lép ki a bűnelkövetésből, feltéve, hogy kilép egyáltalán. Az idetartozó elméletek szerint az, hogy kinek milyen intervallumú lesz a karrierje, megjósolható, vagyis előre kalkulálható.

Fontos megemlíteni Terrie Moffitt fejlődési taxonómiáját,[216] amely a későbbi bűnözői pályák vizsgálatának is alapjául szolgált.[217] Moffitt elméletében két kategóriába sorolta az elkövetőket: az egyik az élethosszig tartó bűnözői karrierrel rendelkezőké, a másik a serdülőkorra korlátozódó bűnözői pályával rendelkezőké. E két csoport jellemzőit Moffitt gondolatai nyomán Szabó Judit fogalmazza meg a legszemléletesebben:

> „[A]z előbbi csoportot a kötődés zavarai, neuropszichológiai deficitek és tanulási kudarcok jellemzik. Gyermekkorban kezdenek el bűnözni, és később sem hagynak fel vele, mivel személyiségjegyeik (különösen az impulzivitás és a hiperaktivitás) és kedvezőtlen körülményeik (rossz családi háttér, iskolai kudarcok) együttes hatása, tehát az egyéni és a környezeti tényezők változásnak gátat szabó interakciói egész életüket végigkísérik.[218] Ezzel szemben a serdülőkorra korlátozódó bűnelkövetői

[213] Jennings i. m. (210. lj.).

[214] Robert J. Sampson – John Laub: A Life-Course Theory of Cumulative Disadvantage and the Stability of Delinquency. In: Terence Thornberry (szerk.): *Developmental Theories of Crime and Delinquency: Advances in Theoretical Criminology*, *7*. New Brunswick, Transaction, 1997.

[215] Uo.

[216] Terrie E. Moffitt: Adolescence-Limited and Life-Coures-Persistent Antisocial Behavior: A Developmental Taxonomy. 100(4) *Psychological Review* (1993) 674–701.

[217] Szabó Judit: A bűnözői karrierből való kilépés kutatásának aktuális kérdései. *Magyar Rendészet,* 2011/1. 32–48.

[218] Uo., 40.; Nick Flynn: *Criminal Behaviour in Context. Space, Place and Desistance from Crime*. New York, Willian, 2010.

pálya nem gyermekkorban, hanem kamaszkorban kezdődik, és mivel általában helyzetfüggő, még a serdülőkorban véget is ér. A serdülőkorra korlátozódó bűnelkövetők esetében tehát a dezisztencia szinte törvényszerűen bekövetkezik."[219]

Moffitt szerint az élethosszig tartó bűnözés okai a fentebb már említett korai fejlődési zavarok, az antiszociális és a deviáns viselkedés, illetve az életkor-specifikus bűncselekmények elkövetése. Úgy véli, ebben az esetben nem várható, hogy ez a körforgás tinédzserkorban abbamarad.[220]

A bűnelkövetők második csoportjánál két okot említ: az egyik a társadalmi utánzás *(social mimicry),* a másik az érettségi szakadék *(maturity gap).* Az előbbi értelmében a jogkövető fiatalok elkezdik megfigyelni azokat, akik magatartásuk (pl. csavargás, marihuánafogyasztás vagy bolti lopás) eredményeképpen valamilyen társadalmi státuszt, jutalmat vagy népszerűséget szereznek, majd követik e magatartásokat. A második esetben a fiatalok azért követnek el devianciát, hogy azzal érettebbnek tűnjenek. Ilyen tipikus magatartás az alkoholfogyasztás vagy a korai szex. Általában ez utóbbi esetekben rövid az elkövetői időtartam, és többnyire nem erőszakos bűncselekményekről van szó. Az elkövetői lét serdülőkorban kezdődik, és körülbelül akkor is fejeződik be.[221]

Rolf Loeber 1996-ban részletgazdagabb csoportokat alakított ki. Elképzelése abban különbözik Moffitt taxonómiájától, hogy itt a karrier egy logikus, lépcsőzetes folyamat, amit úgynevezett mérföldkövek *(stepping stones)* tűzdelnek, vagyis ahhoz, hogy valaki magasabb fokokra lépjen, előbb az alsóbbakat kell végigjárnia. Loeber három, egymás között átjárható utat különböztetett meg. Az első *(overt pathway)* az enyhébb agresszív cselekedetekkel, például verekedéssel kezdődik, majd megjelennek az egyre komolyabb erőszakos bűncselekmények, míg a második *(covert pathway)* főként kisebb súlyú tulajdon elleni elkövetéssel indul, ami folyamatosan súlyosbodik, végül a harmadik *(authority–conflict pathway)* inkább kisebb cselekményeket, makacs tetteket, például az elmenekülést, a felelősség előli elfutást jelenti. Loeber szerint ezek között folyamatos átmenet, váltakozás van, és a krónikus elkövetés azon fiatalok körében jelenik meg, akik több út jellemző cselekedeteit is elkövetik, de különösen az első kettőt.[222]

Sampson és Laub tanulmányukban írnak a korábbi kriminológiai elméletekkel való kiegészítés lehetőségéről is. Okfejtésük szerint a fejlődéskriminológia dinamikus szemlélete a formális és az informális kontroll szerepét hangsúlyozó elméletekkel egyeztethető össze elsődlegesen – Hirschi társadalmi kötődéselméletét, valamint Thornberry 1987-es interakciós elméletét említik. A fejlődési szemléletet ugyanakkor csupán a címkézéselméletben tartják felfedezhetőnek a korábbi kriminológiai elméletek áttekintését követően.[223]

[219] Szabó i. m. (217. lj.) 40.

[220] Moffitt i. m. (216. lj.).

[221] Jennings i. m. (210. lj.) 2–3.

[222] Rolf Loeber: Developmental Continuity, Change, and Pathways in Male Juvenile Problem Behaviors and Delinquency. In: J. David Hawkins (szerk.): *Delinquencyand Crime: Current Theories*. New York, Cambridge University Press, 1996. 1–27.

[223] Sampson–Laub i. m. (214. lj.).

Az informatikai és különösen a kibertérfüggő informatikai bűnözés vizsgálatára gondolva a fejlődéskriminológiai megközelítés és az életpályamodellek alkalmazása nem jellemző. E területen nem találunk releváns kutatásokat, sem gyűjtéseket, amelyek az e területen végzett longitudinális kutatásokat ösztönöznék. Ennek oka az lehet, hogy az informatikai bűnözés a növekvő számú vizsgálatok ellenére is a kriminológiai kutatások marginális területe, valamint a rejtett bűnelkövetés és a látencia következtében problematikus a bűnelkövetők hosszú távon végzett felmérése, így különösen a karriergörbe és a dezisztencia vizsgálata. Szinte alig vannak olyan írások, amelyek a fentebb leírt, Moffitt és Loeber által felvázolt, vagy ahhoz hasonló elkövetői életpályákat az informatikai bűnözésben is vizsgálnák.

Egyetlen olyan kutatás elérhető, amelynek alapját az informatikai bűnözésnek a fejlődéskriminológiára jellemző dinamikus megközelítése adja, illetve amelyben a különböző életpályák is megjelennek. Hutchings tanulmányában önálló modellt alakított ki, amelyben megkülönbözteti az általános informatikai bűnözői karrierutat és a technológiai központú elkövetők karrierútját.[224] Megközelítésében az általánosabb utat választókra az általános feszültségelmélet tétele, míg a technológiai úton indulókra a differenciális asszociáció és a neutralizáció hat. Az előbbi esetben inkább az egyedüli elkövetés a jellemző (pl. internetes csalás), míg utóbbinál a társas elkövetési formák dominálnak, hiszen a csoportok nyomása, megerősítése és az utánzás itt működik.[225] A Hutchings doktori disszertációjának alapját képező megközelítés olyan integrált elmélet, amelyben minkét esetet tekintve a karrier fennmaradását a lebukás alacsony szintje és az elérhető hasznok segítik elő, amelyek a racionális döntéselméletek sajátjai, így a kilépés is a magas költségek és az alacsony hasznok miatt következik be. Elmélete szerint a fiatalok gyakran a felnőtté válással egyidejűleg lépnek ki a bűnelkövetésből, mert az összeütközésbe kerül karrierjükkel vagy a magánéletükkel.[226]

Az informatikai bűnözők életútja így Hutchings szerint az elkövetett bűncselekmények és az elkövető tudása szerint különböző hatások által befolyásolt, és azok menete, illetve a dezisztencia bekövetkezése hasonló jellemzőkre vezethető vissza. Ennek következtében az informatikai bűncselekmények vizsgálatára alkalmas társas tanuláselmélet és az életpályamodellek összefűzése nem elképzelhetetlen, sőt a tudásalapú, technológiaorientált elkövetői karrier esetében kifejezetten hasznos adatokkal szolgálhat. Azonban Hutchings számára sem állt fenn a lehetőség, hogy az elméletet longitudinális vizsgálattal tesztelje. Ennek ellenére a longitudinális vizsgálatok segíthetnek megismerni a serdülőkorra korlátozódó és az élethosszig tartó kibertérfüggő bűnelkövetői pálya jellemzőit és eltéréseit a Moffitt által is felvázolt karrierutak mintájára. Ennek vizsgálata hazánkban Szabó dezisztenciával foglalkozó írása szerint is problémás, de mint Szabó jelzi: keresztmetszeti kutatások és utánkövetéses vizsgálatok is alkalmasak lehetnek a karrier elemzésére. Sőt az informatikai bűnelkövetőkkel készített életútinterjúk is többletinformációt adhatnak akár a serdülőkorra korlátozódó, akár az élethosszig tartó bűnelkövetés okairól, a társas tanulás szerepéről és a kilépés körülményeiről, legyenek azok a negatív megerősítés vagy a társadalmi kötelékek megerősödésének eredményei.

[224] Hutchings i. m. (12. lj.).
[225] Uo., 131–134.
[226] Uo., 134–135.

3. Összegzés

Jelen tanulmány célja az informatikai bűnözéshez kapcsolódó, leggyakrabban alkalmazott kriminológiai elméletek alapvetéseinek, illetve azok kibertérre való alkalmazási gyakorlatának értékelő bemutatása volt a teljesség igénye nélkül. A tanulmány, egyfajta fokozatosságot követve, a vizsgált elméleteknek az informatikai bűnözés kutatására való alkalmasságát is tükrözi, így a területhez kevéssé illeszkedő és változatos eredményeket adó paradigmák felől halad a konzisztensebb, relevánsabb kutatási perspektívák felé.

Bemutatja a környezeti kriminológia két legismertebb elméletét, a racionális döntéselméletet és a rutintevékenységi elméletet. E teóriák alkalmazásának példáin keresztül láthatóvá teszi, hogy ugyan lehetséges, sőt az online tér kutatásának bizonyos aspektusai esetén szükséges is a szituációs elemek és a költség-haszon elemzés során kialakított bűnözési preferenciák vizsgálata, e két elmélet a bűnelkövetővé válás szempontjából pusztán a szűken mért okok feltárására adhat lehetőséget. Különösen igaz ez a rutintevékenységi elméletre, amely mindinkább az áldozattá válás közvetlen folyamatainak megértését, valamint a bűnmegelőzés lehetőségeinek kiaknázását segítheti elő. A racionális döntéselmélet számos területre, így például az online kalózkodás vagy a szürke kalapos hekkerek által elkövetett cselekmények során alkalmazott kalkulációra is rálátást adhat, mégis inkább – a bűnelkövetés előszobájából nézve – az egyes konkrét cselekményeket megelőző racionalizálási folyamatokat tudja megmutatni. E két elmélet nem képes kifürkészni az informatikai és különösen a kibertérfüggő bűnözés szélesebb társadalmi és egyéni okait.

A kontrollelméletek közül a társadalmi kötődéselmélet és az általános bűnözéselmélet tekint vissza a leghosszabb múltra az informatikai bűnözés kutatásában. A kontrollelméletek kiválóan alkalmasak az online térben megjelenő 'tömeges' devianciák és bűnelkövetési formák okságának vizsgálatára, így magyarázatot adhatnak az illegális szoftverletöltésre, a pornográfia fogyasztására, vagy akár a *cyberbullying* elkövetésére is. E két elmélet segíthet továbbá megérteni az alacsony önkontrollban és a társadalmi kontroll, valamint a társadalmi kötődések hiányában rejlő okokat, amelyek láthatóan alkalmasak az online tér számos interakciójának értelmezésére. Ennek ellenére a tanulmány fókuszát képező kibertérfüggő informatikai bűnelkövetés esetében kevéssé alkalmazhatók – ezt támasztja alá a vázolt kutatásokban is hangsúlyozott magas tudásigény, amely sok esetben a magasabb önkontrollt, valamint az online közösségekhez való szorosabb kötődést jelzi.

Az interakcionista paradigma részeként tárgyalt differenciális asszociációelmélet, majd a Burgess és Akers által megfogalmazott differenciális asszociációmegerősítés elmélet bemutatása segítségével empirikusan igazolhatóvá vált a tanulás fontossága az informatikai bűnözésben. E tekintetben az elmélet kiemelten fontos, hiszen egyedülállóan képes magyarázni a kibertérfüggő kriminalitás okait, és vizsgálhatóvá teszi azt a tanulási folyamatot, amely a kisebb súlyú online devianciáktól a súlyosabb, akár szervezettebb informatikai elkövetésekig vezet. Az e körben ismertetett kutatások alátámasztják a tanulási folyamatok során lényeges tényezők, így az utánzás és a pozitív megerősítés elsődleges szerepét. Mi több, az elmélet a később bemutatott fejlődéskriminológiai paradigma egyes elemeivel kiegészítve a bűnelkövetői karrier tartalmának és tartamának megismeréséhez is hozzájárulhat.

A neutralizációelmélet nem kifejezetten önmagában, inkább a tanuláselméleti elképzeléseket kiegészítve, így a differenciális asszociációmegerősítés elmélet definíciós tényezőjét tar-

talommal megtöltve segítheti a tudásalapú informatikai bűnözés vizsgálatát. Sykes és Matza elmélete így képes árnyalni a tanuláselmélet társas interakciókra támaszkodó nézeteit, megjeleníteni az egyénben zajló semlegesítő érveket, képzeteket, sőt a sodródás megfogalmazásán keresztül a serdülőkori bűnözés epizodikus megjelenését is jobban képes leírni, mint önmagában a tanulási perspektíva. A neutralizációs technikák tehát segíthetnek árnyalni a többségi társadalmi normák és a bűnözést támogató képzetek elhatároltságát.

Végül az írás bemutatja a fejlődéskriminológia, illetve az életpályamodellek azon nézeteit, amelyek szerint a bűnelkövetővé válás vizsgálatát a dinamikus megközelítés segítheti elő. A paradigmát jelenleg csupán elvétve alkalmazzák a kibertér kutatásában, de annak longitudinális megközelítése, így az életútinterjúk készítése, a bűnözői karrier fordulópontjainak, rizikófaktorainak vizsgálata és az informatikai bűnözői életutak csoportosítása új perspektívákat nyithat a kibertérfüggő bűnözés kutatása terén. E tekintetben fontos a tanuláselméletek és a fejlődéskriminológia egymáshoz való közelítése, amely különösen a dezisztencia okainak vizsgálata során egymást támogató nézetekben teljesedhet ki. Az életpályamodellek közül kifejezetten Moffitt megközelítése segíthet értelmezni az informatikai bűnelkövetővé válás hosszú távú folyamatát és a karrier sajátos jellemzőit.