2018
10.

BELÜGYI SZEMLE

A BELÜGYMINISZTÉRIUM SZAKMAI, TUDOMÁNYOS FOLYÓIRATA

66.
évfolyam

TARTALOM 2018/10.

SZERZŐK 2018/10.

PROF. DR. FANTOLY ZSANETT egyetemi docensi munkakörben foglalkoztatott egyetemi tanár,
Szegedi Tudományegyetem Állam- és Jogtudományi Kar Bűnügyi Tudományok Intézete

DR. FOGARASI MIHÁLY egyetemi docens,
Nemzeti Közszolgálati Egyetem
Rendészeti Magatartástudományi Intézet
kriminálpszichológiai tanszék

GERZSENYI EGON ERNŐ rendőr főhadnagy,
Szabolcs-Szatmár-Bereg Megyei Rendőr-főkapitányság Kisvárdai Rendőrkapitányság

KOLLÁR CSABA oktató,
Nemzeti Közszolgálati Egyetem
Katonai Műszaki Doktori Iskola

DR. LICHTENSTEIN ANDRÁS PhD-hallgató,
Szegedi Tudományegyetem
Állam- és Jogtudományi Doktori Iskola
Bűnügyi Tudományok Intézete

DR. NAGY ZOLTÁN ANDRÁS tanszékvezető,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar kiberbűnözés elleni tanszék
Pécsi Tudományegyetem
Állam- és Jogtudományi Kar büntetőjogi tanszék

DR. NYITRAI ENDRE PHD tanársegéd,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar
krimináltaktikai és -metodikai tanszék

DR. PARTI KATALIN tudományos főmunkatárs,
Országos Kriminológiai Intézet
óraadó,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Doktori Iskola

DR. SIMON BÉLA rendőr őrnagy, tanársegéd
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar
kiberbűnözés elleni tanszék

DR. VIGH ANDRÁS egyetemi docens,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar Kriminalisztikai Intézet
krimináltechnikai tanszék

VARGA CSILLA LAURA rendőr hadnagy,
Berettyóújfalui Rendőrkapitányság

SUMMARY

Fantoly, Zsanett – Lichtenstein, András
Computer-based risk assessment and criminal procedure [5–22]
The authors provide an overview of the computer-based risk assessment tools used in US criminal procedure and prospects for of using such algorithms in the Hungarian criminal justice system.

Parti, Katalin
Obligation to co-operate for electronic communications service providers in criminal proceedings in practice [23–35]
In the light of recent legislative amendments, this author provides an overview of data processing obligations of electronic communications service providers for law enforcement purposes in Hungary.

Nagy, Zoltán András
The future began yesterday [36–55]
The author provides an overview of technological challenges for law enforcement.

Kollár, Csaba
Online fraud in Hungary [56–70]
The author provides an overview of online fraud in Hungary.

Simon Béla
Cryptocurrency and law enforcement responses [71–87]
The author provides an overview of potential criminal activity related to cryptocurrencies along applicable law enforcement responses.

Vigh András
Drones in law enforcement [88–107]
Cautious to point to potential dangers, the author provides an overview of the wild scale of use of drones in policing and law enforcement.

Nyitrai, Endre
E-investigation and interoperability [108–121]
With interoperability and penetration among databases in focus, the author provides an overview of electronic investigation and its role in criminalistics

DOI: 10.38146/BSZ.2018.10.1

FANTOLY ZSANETT – LICHTENSTEIN ANDRÁS

Számítógépes kockázatelemzés és büntetőeljárás[1]

Napjaink digitális társadalmában az élet számos területén alkalmaznak a döntéshozatalt segítő kockázatelemző algoritmusokat, nem kivétel ez alól a büntető igazságszolgáltatás sem. Az ilyen kockázatértékelési szoftverek lényege és alapja, hogy egy kialakított profil alapján valószínűségszámítás segítségével előrejelzések alkothatók a prediktív igazságszolgáltatás számára. Az alkalmazhatósági terület alapján a kriminálprognózisok több típusát lehet megkülönböztetni: a rendőrség bűnmegelőzési munkáját segítőt, a büntetés-végrehajtásban érvényesítettet, illetve a szoros értelemben vett büntető igazságszolgáltatásit, azaz az ítélkezésre fókuszáló változatot.

A rendőrség által a bűnmegelőzés során alkalmazott algoritmusok olyan – eddig nem ismert – összefüggéseket tárnak fel, amelyek alapján előre jelezhető, hogy mely helyek válnak nagyobb eséllyel bűncselekmény elkövetésének helyszínévé, illetve mely, meghatározott profilú személyek esetében valószínűbb a bűncselekmény elkövetése. A hagyományos térképes előrejelzéseken túllépve, különböző számítógépes adatbázisok összekapcsolásával olyan nehezen feltárható kapcsolatokat is lehet találni személyek, helyek és elkövetési eszközök között, amikre eddig nem volt példa.

A büntetés-végrehajtási intézményben is megjelenik a kockázatelemzés mint a prediktív előrejelzés eszköze. Az algoritmusok segítségével előre definiált kockázati tényezők alapján sorolják alacsony, közepes, illetve magas kockázatú csoportba az elítélteket, és ehhez kapcsolják például a feltételes szabadságra bocsáthatóság lehetőségét.

A büntető igazságszolgáltatás, azaz az ítélkezés esetén pedig arról van szó, hogy az eljárás során a vádlott profiljának figyelembevételével matematikai módszerek alapján próbálják megjósolni nem csupán azt, hogy a terhelt várhatóan megjelenik-e a tárgyaláson, hanem azt is, hogy a terhelt előélete és az elkövetett bűncselekmény típusa alapján milyen nemű, mértékű és tarta-

1 A kutatást az EFOP-3.6.2-16-2017-00007 azonosítószámú, *Az intelligens, fenntartható és inkluzív társadalom fejlesztésének aspektusai: társadalmi, technológiai, innovációs hálózatok a foglalkoztatásban és a digitális gazdaságban* című projekt támogatta. A projekt az Európai Unió támogatásával, az Európai Szociális Alap és Magyarország költségvetése társfinanszírozásában valósul meg.

mú szankció lenne az ideális számára, amely mind a generális, mind a speciális prevenciót megfelelően szolgálja.

Az ítélkezés során a bíró feladata a megfelelő, adekvát szankció megválasztása. Nem csupán a bűncselekmény tárgyi súlyát, hanem – részben a szankció egyéniesítésének követelményéből fakadóan, annak kiválasztása során – az elkövető személyében rejlő társadalomra veszélyességet is vizsgálja, szem előtt tartva az ismételt bűnelkövetés kockázatát. Ebben a tevékenységben az amerikai bírákat – csakúgy, mint magyar kollégáikat – segítik a vádlott korábbi elítélésére vonatkozó adatok. Míg azonban az Amerikai Egyesült Államokban már évtizedek óta használják a büntetéskiszabást megelőző szakvéleménynek *(pre-sentence investigation report; PSI)* nevezett (pártfogó felügyelői) jelentéseket, amely információbázis az elmúlt években több tagállamban is új elemmel bővült: az információs rendszeren alapuló kockázatelemzés adataival, hazánkban ez még várat magára. Ha a társadalom az élet olyan fontos területén, mint a büntető igazságszolgáltatás, támaszkodni kíván az algoritmusokon alapuló kockázatelemzésekre, különösen indokolt e módszerek kritikus vizsgálata, amelyre jelen tanulmány keretében vállalkozunk.

Az Amerikai Egyesült Államokban az ilyen módszerek alkalmazásának szükségességéhez és létjogosultságához a tágabb értelemben vett büntető igazságszolgáltatás egyik legnagyobb problémája, a büntetés-végrehajtási intézetek túlzsúfoltsága vezetett. Az elrettentés céljából szigorúan alkalmazott büntetőjogi jogkövetkemények miatt az országban rendkívül magas a fogvatartottak száma (2016-ban összesen 2,1 millióan voltak büntetés-végrehajtási intézetben[2]). Ez természetesen túlságosan költségigényes, így nem meglepő, hogy az utóbbi években a takarékossági szempontok az amerikai büntető igazságszolgáltatási rendszer egyik központi kérdésévé váltak. Ennek keretében felismerték, hogy a szabadságelvonással járó büntetéseket és intézkedéseket – amelyek jelentős anyagi terhet rónak az államháztartásra, azok alternatívájaként felfüggesztett szabadságvesztéssel vagy próbára bocsátással helyettesítsék. Ezzel a folyamattal párhuzamosan, ismét a jogászi érdeklődés középpontjába került a krimálprognózisok alkalmazásának lehetősége, és egyre erősebb igény mutatkozott a bűnismétlés kockázatának a korábbiaknál pontosabb előrejelzésére és az ilyen előrejelzések figyelembevételére az ítélethozatalkor. Ennek megvalósítása érdekében mára már minden tagállamban

2 Bureau of Justice Statistics, Key Statistics, Total Correctional Population. https://www.bjs.gov/content/keystatistics/excel/Total_correctional_population_counts_by_status.xlsx

használnak különböző, számítógépes kockázatelemzésen alapuló értékelési eszközöket az igazságszolgáltatás számos területén. Így például Florida állam hatóságai elsősorban a Northpointe által az 1990-es évek végén fejlesztett COMPAS *(Correctional Offender Management Profiling for Alternative Sanctions ~ Büntetés-végrehajtási elítéltiprofil-alkotás az alternatív szankciók érdekében)* Assessment Toolt, amelyet Wisconsin államban szintén alkalmaznak a büntetőeljárás minden szakaszában és minden szintjén.[3]

A számítógépes kockázatelemzés problémái és eszközei

A büntető igazságszolgáltatás gyakorlása – ideértve a büntetések kiszabását és az intézkedések alkalmazását is –, ahogyan azt a bevezetésben említettük, hagyományosan kizárólag bírói feladat. A kezdeti, pusztán a bírák szubjektív belső meggyőződésén alapuló ítélkezés gyakran vezetett nem csupán a bűnösség kérdésében, hanem az alkalmazott jogkövetkezmények vonatkozásában is téves ítéletekhez. Éppen ezért a büntetéskiszabás objektív kritériumainak kidolgozását már a felvilágosodástól kezdve szorgalmazták és szorgalmazzák.[4] Mindezen törekvések ellenére a bűnügyi előrejelzést és kockázatelemzést szolgálni hivatott módszerek mindegyike azonos problémával küszködik, nevezetesen azzal, hogy százszázalékosan megbízható eredmények nem garantálhatók. Ugyanis egy adott – jelen esetben előrejelezni kívánt – emberi magatartás kiváltó okai közé nem pusztán a vizsgálati alany személyiségjegyei tartoznak, hanem cselekedeteit számos egyéb szituációs tényező befolyásolhatja, amelyek változatosságuk és változékonyságuk miatt csak pontatlanul becsülhetők fel.

Erre a problémára az amerikai, úgynevezett *Baxstrom-eset* és annak utóélete világított rá világszerte 1966-ban.[5] Ennek során kilencszáz-ezer erőszakos cselekményt elkövető, kóros elmeállapotú személyt bocsátottak szabadon New York-i büntetés-végrehajtási intézetekből különböző alapjogi, eljárásjogi, illetve végrehajtási okokból. Négy éven belül a korábban veszélyesnek minősített személyek mindössze 14,2 százaléka követett el újabb ha-

3 Wisconsin Department of Correction. https://doc.wi.gov/Pages/AboutDOC/COMPAS.aspx

4 Ennek legjelentősebb korabeli képviselője Cesare Beccaria. Cesare Beccaria: A bűnökről és a büntetésekről (Dei delitti e delle pene) 1764. Magyarországon a büntetéskiszabás során értékelhető tényezőkről szóló 56. BK vélemény léte bizonyítja, hogy ez a folyamat a mai napig tart, és érezteti hatását.

5 Baxstrom v. Herold, 383 U.S. 107 (1966) US Supreme Court. https://supreme.justia.com/cases/federal/us/383/107/case.html

sonló cselekményt, amelyeknek csupán két és fél százaléka volt súlyos és erőszakos.[6] Az eset tanulsága tehát, hogy bár a kockázatelemzés alapján az összes személynél valószínűsíthető volt a „bűnismétlés”, sőt a „különös visszaesői minőség”[7], a valóság és a gyakorlat ezt – még ha véletlenszerűen is, de – egyértelműen megcáfolta.[8] Ez az eset már ötven évvel ezelőtt ráirányította a figyelmet a kockázatelemzés gyengeségeire, az akkori szintjén megbízhatatlanságára.

A *Baxtrom-esetet* követően a bűnügyi előrejelzés ellenőrzött és kipróbált módszertani alapokra helyezésére irányuló törekvések során számos kockázatelemző eszközt fejlesztettek ki.[9] Manapság olyan mennyiségű effajta eszköz áll rendelkezésre, hogy a szakirodalom indokoltnak tartja ezek generációnkénti megkülönböztetését.[10]

A bűnügyi statisztikai adatgyűjtés kezdete a XVII. századi Franciaországhoz köthető, de a XIX. századra Magyarországon is általánossá vált a rabtabellák, azaz a törvényhatóságok és uradalmak tömlöceiben fogva tartottak adatai nyilvántartásának alkalmazása.[11]

Lombroso bűnügyi embertani elméletét követően az első olyan nyilvántartásokat, amelyek a bűncselekmények elkövetésére hajlamosító – nem fizikai – tényezőket összegezték, és amelyektől a potenciális bűnelkövetők azonosítását remélték, a XX. század elején állították össze, ezek voltak a statisztikai kockázatelemzések alapjai.[12] A bűnismétlés és a visszaesés szempontjából jelentős adatokat már szabadon bocsátott elítéltek aktáiból gyűjtötték össze.

---

6 Henry J. Steadman: Implications from the Baxstrom experience. Bulletin of the American Academy of Psychiatry & the Law, vol. 1, no. 3, 1973, pp. 189–196.; Joachim Obergfell-Fuchs: Gefährliche Straftäter aus kriminologischer und psychologischer Sicht. In: Sicherungsverwahrung und Führungsaufsicht. Wie gehen wir mit gefährlichen Straftätern um? Evangelische Akademie, Bad Boll, 2011

7 Habár kóros elmeállapotuk miatt az eset alanyaira a magyar büntetőjog rendszerében nem pontos a bűnismétlés, illetve a visszaeső kifejezések használata, e helyütt az előrejelzett erőszakos cselekmények ismételt elkövetésének leírására használjuk őket.

8 A magyar büntetőjog fogalmi rendszeréből kifolyólag nyilvánvalóan nem beszélhetünk bűnismétlésről, illetve különös visszaesői minőségről a kóros elmeállapotú személyek vonatkozásában, azonban a kockázatelemzés gyengeségeit jól érzékelteti az ismertetett eset.

9 Laura S. Guy: Performance indicators of the structured professional judgment approach for assessing risk for violence to others. A meta-analytic survey. Dissertation. Simon Fraser University, 2008

10 Anne-Luise Döbele: Standardisierte Prognose-instrumente zur Vorhersage des Rückfallrisikos von Straftätern Eine kritische Betrachtung des Einsatzes in der Strafrechtspflege aus juristischer Sicht. Hamburg, 2014, S. 20–26.

11 Brandl Gergely – Gönczi Gergely – Hajdú Dóra – Marsovszki Ádám – Szakály Zsuzsa – Tamás Csaba: Egy méltatlanul elhanyagolt jogtörténeti forrás elemzése. Mire jó a rabtabella? Jogelméleti Szemle, 2014/3.

12 Norbert Nedopil: Prognosen in der Forensischen Psychiatrie: ein Handbuch für die Praxis. Pabst, 2005

A második generációs eszközökkel ezeket az ismérveket az elkövető személyének és az elkövetett cselekménynek a sajátosságaival egészítették ki, azonban egyes személyiségjegyeket továbbra is figyelmen kívül hagytak. Ezt a hiányosságot voltak hivatottak pótolni a kockázatelemzés harmadik generációs módszerei, amelyek az adatbázisokat olyan dinamikus jellegű faktorokkal bővítették, mint az egyén személyes beállítottsága, társadalmi kapcsolatai stb.[13]

A bűnügyi előrejelzés és a számítógépes kockázatelemzés legújabb, jelenlegi korszakát azok a negyedik generációs eszközök jelentik, amelyek a legkülönbözőbb területeken, széles körben alkalmazhatók. Egyfelől alkalmazásuk folytán egyre több szempontból befolyásolhatják az ítélkezési gyakorlatot, másfelől pedig már nem csupán figyelembe veszik az elkövető viselkedését és magatartását, hanem például egyenesen cselekvési, kezelési tervet ajánlanak a bíróság és a büntetés-végrehajtás számára, vagy azzal hirdetik magukat, hogy azt is meg tudják jósolni, hogy a terhelt megjelenik-e a bíróság előtt, vagy sem.[14]

Az egyik legismertebb ilyen, negyedik generációs „automatizált döntéshozatalt támogató” kockázatelemző eszköz a COMPAS. Fejlesztője, a Northpointe azt állítja, hogy a 137 ismérvet figyelembe vevő algoritmusának segítségével olyan pontosan előre jelezhető a vádlott bűnismétlésének valószínűsége[15], hogy az Egyesült Államok néhány tagállamában már a büntetőeljárásban is alkalmazzák, például a büntetések kiszabása és intézkedések alkalmazása körében.

Mint ahogyan a negyedik generációs kockázatelemző eszközök szinte mindegyike, a COMPAS is zárt forráskódú, a feketedoboz-[16] elméleten alapuló rendszer, azaz a transzparencia hiánya, az algoritmus működésének és így az adatok értékelésének viszonylagos átláthatatlansága a COMPAS esetében is probléma. Ennek lehetséges informatikai megoldását a szoftverfejlesztőktől kölcsönzött úgynevezett feketedoboz-vizsgálatok jelenthetik[17], amelyek

13 Anne-Luise Döbele: i. m.

14 Northpointe: Practitioner’s guide to COMPAS core. 2012. http://www. northpointeinc.com/downloads/compas/Practitioners-Guide-COMPASCore-_031915.pdf

15 Tim Brennan – Bill Dieterich – Markus Breitenbach – Brian Mattson: A Response to “Assessment of Evidence on the Quality of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)”. Northpointe Institute for Public Management, Inc. 2009. http://www.northpointeinc.com/files/whitepapers/Response_to_Skeem_Louden_Final_071509.pdf

16 A feketedoboz a rendszerelméletben jellemzően olyan eszközt jelöl, amelynek belső működése nem ismert, ezért elsősorban a bemenete és a kimenete alapján vizsgálható.

17 Boris Beizer: Black-box testing: Techniques for functional testing of software and systems. Wiley, New York, 1995

segítségével a bevitt adatok és a várt, illetve ténylegesen kapott eredmények összevetésével az algoritmus működési mechanizmusa annak pontos és előzetes ismerete nélkül is visszafejthető.

2016-ban a ProPublica nevű nonprofit szervezet készített egy tanulmányt, amelyben jelentős egyenlőtlenségeket mutattak ki a COMPAS eredményeiben fehér, illetve afroamerikai alanyok vonatkozásában. A Northpointe erre adott reakciója bizonyos szempontból megerősíteni látszott a tanulmányban publikált eredményeket, bevezették ugyanis az úgynevezett *Fairness-kritérium* alkalmazását, amely a hasonló eszközök finomhangolását hivatott szolgálni.[18]

A *wisconsini legfelsőbb bíróság* egyszersmind kimondta, hogy – a bírák részére nyújtott figyelmeztetések ismertetése miatt – nem sérül a terhelt tisztességes eljáráshoz való joga azáltal, hogy a visszaesés valószínűségét egy speciális algoritmuson alapuló információs rendszer kalkulálja ki, akkor sem, ha az algoritmus, illetve maga a valószínűségszámítás alapját képező matematikai rendszer pontos működése sem az ítélkező bíró, sem pedig az eljárásban részt vevő felek által nem ismert[19].

A Loomis-ügy és tanulságai

A Loomis-ügy tényállása szerint 2013-ban büntetőeljárás indult *Eric Loomis*szal szemben gépkocsiból történő fegyveres lövöldözés és egyéb, kisebb tárgyi súlyú bűncselekmények miatt. Loomis a büntetőeljárásban tagadta a bűnösségét, mindössze annyit ismert el, hogy a bűncselekmény eszközéül használt gépkocsit vezette az elkövetés idejéhez viszonyítottan jóval később, de még aznap éjjel. Végül vádalkut kötött, amelynek keretében két kisebb súlyú bűncselekmény (közúti veszélyeztetés és jármű önkényes elvétele) elkövetését beismerte *(pleaded guilty)*. A büntetéskiszabási eljárás során a wisconsini pártfogó felügyelő olyan *PSI- (pre-sentence investigation)* adatbázist bocsátott az eljáró bíróság rendelkezésére, amely főként a COMPAS kockázatelemző módszerén alapult. A COMPAS rendszer lényege szerint az elkövető ismételt bűnelkövetésének kockázatát a terhelttel készített személyes beszélgetésből kapott információk és a terhelt korábbi elítélésére vonatkozó adatok alapján becsülik meg. Az algoritmus, amely a rendszer lényege,

18 Megjegyzendő továbbá, hogy a tanulmány publikálása után a Northpointe Equivantra változtatta a nevét.

19 State v. Loomis, 881 N.W.2d 749 (Wis. 2016); State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing. Harvard Law Review, Mar 10, 2017, p. 1530. http://harvardlawreview.org/wp-content/uploads/2017/03/1530-1537_online.pdf

titkos, így csak a vizsgálat eredményét tartalmazó jelentés kerül az eljáró bírósághoz. A Loomis-ügyben a vizsgálat kiterjedt 1. a terhelt előzetes fogva tartásának kockázatára; 2. a visszaesés kockázatára; és 3. az erőszakos bűncselekmények vonatkozásában külön vizsgálták a visszaesés kockázatát. Az ügyben részint e kockázatelemzési módszer alapján állapította meg a bíróság a vádlott számára legmegfelelőbb büntetést és szabott ki Loomisra hat év szabadságvesztést és öt év szigorított bűnügyi felügyeletet. A büntetéskiszabás során további jelentős tényezőként értékelték Loomis szexfüggőségét, amely alapján Loomis a legmagasabb kockázati kategóriába *(high-risk)* került. Loomis kegyelmi kérvénnyel élt, amelyben arra hivatkozott, hogy a COMPAS eredményeire alapozott ítélethozatal sértette a tisztességes eljáráshoz való jogát. Az indítvány jogi alapjait részletezve Loomis védője külön kiemelte, hogy a COPMAS eredményeinek felhasználása során a bíróság alkotmányellenesen támaszkodott azon, részben faji alapú megkülönböztetést lehetővé tévő adatokra, amelyek a COMPAS kérdésbázisának részei. Ezáltal sérült a terhelt azon joga, hogy megfelelő, egyéniesített büntetésben részesüljön. Másrészt az elítélés alapja nem konkrét tudásbázison nyugvó információ, lévén hogy maga az eljáró bíróság sem ismerte az ítéletkiszabás során alkalmazott algoritmust. Végül a rendszer nemi és szexuális alapon történő megkülönböztetést is tartalmazott, amelyek szintén összeegyeztethetetlenek a törvény előtti egyenlőség és az egyenlő bánásmód követelményével.

A wisconsini legfelsőbb bíróság az egyéniesített ítélethez fűződő jogot a *Malenchik v. State-ügy*ben hozott 2010-es ítéletben megfogalmazott elvek alapján vizsgálta. Ebben az ítéletben a hasonló kockázatelemző módszerek alkalmazásával összefüggésben leszögezte a bíróság, hogy *„a kockázatelemző módszerek segíthetik a bírákat abban, hogy hatékonyabban értékeljék és mérlegeljék a különböző, jogszabályban rögzített, a büntetés kiszabása körében figyelembe vehető bűnösségi körülményeket, mint például a büntetett előéletet, az elzárás vagy rövid tartamú szabadságvesztés alkalmazásának lehetőségét, a feltételes szabadságra bocsátás tényleges valószínűségét és az elkövető ráutaló magatartását, illetve személyi körülményeit, amelyek azt valószínűsítik, hogy nem követ el újabb bűncselekményt”*[20].

Az 1989-es *State v. Skaff-ügy*ben szintén arra az álláspontra helyezkedett a bíróság, hogy a megalapozott adatokon nyugvó ítélethez való jog magában foglalja azt a részjogosultságot, hogy a terhelt megismerheti, befolyásolhatja és módosíthatja az elítélésének alapját képező PSI-jelentést.[21]

20 Malenchik v. State, 928 N.E.2d 564, 574 (Ind. 2010).
21 State v. Skaff, 152 Wis.2d 48, 57-58 (Ct. App. Wisc. 1989).

Mivel a Loomis-ügyben a bíróság nem kizárólag a COMPAS eredményeire támaszkodott a büntetéskiszabás során és mivel Loomisnak a PSI befolyásolásához való joga nem szenvedett sérelmet (hiszen a vizsgálat eredménye részint a terhelti vallomásának adataira, illetve az általa adott válaszokra, amelyeket önként bocsátott a hatóság rendelkezésére, részint pedig a hatóság hivatalos tudomását képező korábbi elítéléseire támaszkodott), így a wisconsini legfelsőbb bíróság bírája, *Ann Walsh Bradley* bíró arra a jogi álláspontra helyezkedett, hogy az ítélet nem volt jogszerűtlen. A bíró kiemelte, hogy Loomis nem bizonyította hitelt érdemlően, hogy a büntetéskiszabás során eljáró bíróságot érdemben befolyásolta volna a faji hovatartozása. Az egyéniesítés kapcsán a bíró azonban azt is elismerte, hogy a visszaesés kockázatának elemzése során a COMPAS meghatározott, a vádlottal azonos társadalmi csoportról szerzett információk halmazára támaszkodott. Az alapügyben eljáró bíróság azonban *nem kizárólag a COMPAS eredményeit vette figyelembe,* hanem a büntetéskiszabás bírói mérlegelése körében egyéb tényezőket is.

Loomis mindhárom érvét elutasították tehát, és a wisconsini legfelsőbb bíróság az adott ügyben a COMPAS használatát jogszerűnek ítélte. A jövőbeni rendszeres alkalmazás tekintetében azonban aggályokat fogalmazott meg. Általánosságban kimondta, hogy a rendszer önállóan nem alkalmazható, csupán egy tényező lehet a bizonyítékok körében. Előnyeit összegezve leginkább ott szabad a módszert hasznosítani, ahol 1. alacsony kockázati százalékkal *(low risk)* jellemezhető terhelt vonatkozásában megelőzhető annak büntetés-végrehajtási intézetbe kerülése; továbbá 2. a közbiztonságot növelő tényező lehet, ha a társadalomra veszélyes elkövetőket folyamatosan felügyeljük akkor is, ha mindez nem a büntetés-végrehajtás keretei között történik; 3. a rendszer segíthet még a feltételes elítélés, a felügyelet és a kezelési modellek megválasztásában is.

A bíróság a kockázatelemző rendszerek alkalmazásával kapcsolatos korlátokat is felállított. Bár álláspontja szerint kétségkívül hasznosak ezek a módszerek az elkövető motivációjának és személyi körülményeinek feltárásában, de nem szabad kizárólag őket használni a konkrét büntetés nemének, mértékének és tartamának megállapítására; továbbá önmagában az elemzés eredménye nem használható fel az ítélkezés során súlyosító vagy enyhítő körülményként sem. Ennek oka leginkább abban keresendő, hogy a COMPAS nincs figyelemmel valamennyi, a büntetés kiszabása során releváns szempontra, hanem többnyire a visszaesés szempontrendszerén keresztül vizsgál egyes tényezőket. Más büntetéskiszabási körülmények (például bűnösség, felróhatóság, elrettentés) nem jelennek meg az algoritmusban. Ezért a bíró-

ság kötelezővé tenné, hogy az ítéletből egyértelműen derüljön ki, milyen szempontok értékelése során támaszkodott az eljáró bíróság kizárólag a COMPAS eredményeire, azaz e vonatkozásban is részletes indokolási kötelezettséget írna elő.

A COMPAS alkalmazása tehát a wisconsini legfelsőbb bíróság döntése értelmében csak a letartóztatás kérdésében történő döntésre korlátozódna. A kockázatelemző módszer alkalmazása kizárt annak eldöntésére, hogy az elkövetővel szemben szabadságvesztés kiszabására kerüljön-e sor, illetve nem determinálhatja a kiszabandó büntetés súlyosságát sem. Az alkalmazási tilalmak mellett a bíróság öt figyelmeztetést fogalmazott meg az algoritmust a jövőben alkalmazni szándékozó bírák számára:

1. a COMPAS szabadalmazott rendszere eleve kizárja a jogalkalmazó felelősségét a rendszer által alkalmazott algoritmusért, mivel annak működése, különösen az egyes tényezők közötti súlyozás mértéke laikusok, illetve szélesebb kör számára ismeretlen;
2. az adatok csoportadatokon alapulnak, amelyek tartalmazhatnak speciális kockázatnövelő tényezőket. Az eredményt így annak tudatában kell mérlegelni, hogy az értékelés csoportvizsgálatok típusjellemzőin, és nem kizárólag egyéniesített vizsgálat adatain alapul;
3. a COMPAS kifejlesztésére az Egyesült Államok teljes lakosságának figyelembevételével került sor, nem tartalmaz Wisconsin-specifikus adatokat;
4. több tanulmány kimutatta, hogy a COMPAS nem objektív az etnikai kisebbségek tagjaival, és az is valószínűsíthető, hogy egyes kisebbségek vonatkozásában lényegesen nagyobb visszaesési arányokkal dolgozik;
5. a COMPAS-t eredetileg nem büntetéskiszabásra tervezték, hanem arra fejlesztették ki, hogy a pártfogó felügyelők munkáját segítse az elítéltek szabadulása után, azok reszocializációja során.[22]

Abrahamson bíró különvéleményében azt javasolta, hogy a COMPAS fejlesztője, a Northpointe adjon tájékoztatást a rendszer működésének lényegéről. Álláspontja szerint ezáltal kizárható lenne az a feltételezés, hogy az algoritmus túlzott mértékben veszi figyelembe az elkövetés (vagy az elkövető) földrajzi helyzetét, illetve az elkövető szociogazdasági státusát. A felvilágosításnak szerinte a következő szempontokra kellene kiterjednie: 1. mely adatok (input tényezők) alapján dolgozik az algoritmus; 2. hogyan súlyoz az al-

22 Danielle Kehl – Priscilla Guo – Samuel Kesser: Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative. Berkman Klein Center for Internet & Society, Harvard Law School, 2017.

goritmus az egyes input tényezők között; 3. e tényezők közül melyek lehetnek problematikusak (például fajra, nemre vonatkozó adatok) az értékelés kapcsán.

Független vizsgálatok azt bizonyították, hogy a Loomis-ügyben használt algoritmus a színes bőrű elkövetők vonatkozásában magasabb visszaesési kockázatot mutatott, mint a fehér tettesek tekintetében. A ProPublica ezért 2016-ban átfogó vizsgálat alá helyezte a COMPAS módszert, és *„alapvetően megbízhatatlannak”* minősítette a visszaesés kockázatának elemzése szempontjából. Legnagyobb hibaként azt emelték ki, hogy az afroamerikai elkövetők vonatkozásában sokkal magasabb arányt (mintegy kétszeres értéket) mutat a rendszer a visszaesés előrejelzése tekintetében, mint az a későbbi, reális adatok vonatkozásában ténylegesen bekövetkezett. A COMPAS kivitelezője, a Northpointe nem zárkózott el a ProPublicával folytatott egyeztetések elől, érzékelve a tényt, hogy mind a jogtudomány, mind a joggyakorlat körében egyre erősebb ellenállás kezdett körvonalazódni a rendszer alkalmazása ellen. A *Washington Post*ban néhány informatikus szakember arra is felhívta a figyelmet, hogy – bár az algoritmusok alkalmazása látszólag növelheti az eljárás hatékonyságát és a döntések megalapozottságát – súlyos etikai és tudományos problémákat vethet fel. Folyamatosan figyelemmel kell kísérnünk alkalmazásukat és alapvetően kritikai hozzáállást kell tanúsítanunk annak lehetősége kapcsán, hogy a büntető igazságszolgáltatásban ezek az algoritmusok egyre jelentősebb szerepet kapjanak.[23]

A kritikus hozzáállás alapja lehet már maga az a tény is, hogy a COMPAS vizsgálatánál helytelen megoldások mutatkoztak az erőszakos bűnelkövetők visszaesési kockázatának meghatározása során: a rendszer mindössze húsz százalékban jósolta meg helyesen a visszaesők helyzetét az erőszakos bűncselekmények elkövetői sorában. Az összes bűncselekmény tekintetében a rendszer már magasabb százalékban adott ugyan helyes választ a visszaesések megjóslásakor, de ettől még nem állíthatjuk azt, hogy általában megbízható lenne. A hibák több okra vezethetők vissza. Egyrészt az egyes államokban lévő adatok nem kompatibilisek egymással, például az adott elkövető másik államban történő elítélését nem feltétlenül mutatja ki a rendszer, másrészt az egyes bűncselekmények súlyozása nem egységes. Például egy gyermekek sérelmére szexuális bűncselekményt elkövető személynél kisebb visz-

23 Sam Corbett Davies et al.: A Computer Program Used for Bail and Sentencing Decisions was Labelled as Biased against Blacks. It’s actually Not that Clear. The Washington Post, October 17. 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2016610/176can-an-algoritm-be-racist-our-analysis-is-more-cautious-than-propublicas/

szaesési kockázatot mutat a rendszer, ha van rendszeres munkaviszonyból származó jövedelme, mint egy korábban garázdaság miatt elítélt hajléktalan ember esetén.

Ezek a problémák addig nem lesznek orvosolhatók, amíg a rendszert működtető algoritmus titkos. Az alkalmazás során ugyanis a bíróságoknak értékelniük kell az algoritmusok által kimunkált eredményt annak tudatában, hogy ismerik a rendszer működésének sajátosságait, különös tekintettel arra, hogy a súlyozás során milyen elveket érvényesít az informatikai bázis. Ezért hiába szögezte le a wisconsini legfelsőbb bíróság a Loomis-ügyben, hogy a kockázatelemző módszerek alkalmazásának feltétele, hogy az eljáró hatóságok folyamatosan ellenőrizni tudják a kockázatelemző rendszerek megbízhatóságát, amíg maguk az értékelés eredményei alapján ítélkező bírák sem látják át a rendszer működését, addig megbízhatóságról nem beszélhetünk.

Algoritmusok a büntető igazságszolgáltatásban[24]

A kockázati tényezők sokfélék lehetnek, de alapvetően az elkövető személyi adottságaihoz köthetők, például: kor, nem, földrajzi környezet, családi háttér, munkahely/alkalmazásban állás vagy munkanélküliség, gazdasági helyzet, baráti kör, végzettség, mentális állapot stb.

Az Egyesült Államokban jelenleg három típusú kockázatelemző rendszer ismert:

– COMPAS (Correctional Offender Management Profiling for Alternative Sanctions);
– PSA (Public Safety Assesment);
– LSI-R (Level of Service Inventory Revised).

A COMPAS fejlesztője – ahogyan arról már volt szó – egy profitorientált cég, a Northpointe. Öt fő szempontot vizsgál: a bűnözői (deviáns) életvitelt, személyes kapcsolatokat/életmódot, az elkövető személyiségét, az elkövető családi körülményeit és szociális kapcsolatait. Az LSI-R, amelyet egy kanadai egészségügyi cég fejlesztett ki, szintén több faktort vizsgál, az elkövető büntetett előéletétől kezdve a személyiségi jellemzőiig. A PSA viszont már kevesebb paramétert használ, csak a terhelt életkorát és korábbi büntetéseit, büntetett előéletét veszi figyelembe.

24 Ellora Israni – Evelyn Chang (eds.): Algorithmic Due Process: Mistaken Accountability and Attribution in State v. Loomis. Harvard Journal of Law and Technology – JOLT digest, no. 8, 2017.

A COMPAS a leggyakrabban alkalmazott kockázatelemző rendszer az Egyesült Államokban, eredményeit a szakemberek általában elfogadják, és nem vitatják azok megbízhatóságát. A gyakorlatban leginkább a következő területeken használják:

– feltételes szabadságra bocsátás kérdésében tartott meghallgatáson;
– szabadlábra helyezés kérdésében tartott meghallgatáson;
– a büntetéskiszabás területén.

A COMPAS-t eredetileg abból a célból hozták létre, hogy segítsék a büntetés-végrehajtási tisztek és pártfogó felügyelők munkáját abban, hogy melyik elítélt számára melyik kezelés, reszocializációs módszer lesz hatásos. Ha az ítélkezésben használják, hátrányosan hathat a vádalkuval lezárt ügyek alakulására, mivel a COMPAS eredményei alapján a bíró gyakran úgy ítéli meg, hogy súlyosabb szankcióval kell illetni a terheltet, mint amiben a vádalku során megállapodtak az ügyfelek.

Az 1980-as években a *New York Times* a büntető igazságszolgáltatás „csendes forradalma”-ként aposztrofálta azt a folyamatot, amely kísérletet tett arra, hogy kiszűrje a társadalom azon elemeit, akik feltehetően hajlamosak erőszakos bűncselekmények elkövetésére és ismételt bűnelkövetésre („karrierbűnözők”).[25] A szelektív kiválasztás célja e bűnözők társadalomtól való távoltartása volt, amely célt azáltal látták megvalósíthatónak, hogy hosszabb tartamú szabadságvesztésre ítélték az érintett személyi kört. A modell alapja annak előzetes feltételezése volt, hogy a karrierbűnözők tehetők felelőssé az Egyesült Államokban elkövetett súlyos bűncselekmények nagy részéért, továbbá az, hogy e személyek konkrétan beazonosíthatók meghatározott személyiségjegyeik és bűnelkövetői előéletük alapján. Az e témában született empirikus kutatások közül kiemelendő *Greenwood és Abrahamse* vizsgálata, akik 2100 női elkövetővel készítettek kockázatelemző interjút Kalifornia, Texas és Michigan államokban. Eredményekben rögzítették, hogy szoros kapcsolatot látnak a visszaesés viszonylatában a fiatalkori elkövetések, a heroin, a munkanélküliség és a korábbi bűnelkövetői életvitel között. A kutatásukba bevont populációt magas, közepes és alacsony kockázatot jelentő elkövetői csoportokra osztották.[26] További kutatások arra az eredmény-

25 Danielle Kehl – Priscilla Guo – Samuel Kesser: i. m.
26 Peter W. Greenwood – Allan Abrahamse: Selective Incapacitation. Rado Corp., Aug. 1982. https://www.rand.org/content/dam/rand/pubs/reports/2007/R2815.pdf

re jutottak, hogy a bírák részéről nagyobb hajlandóság mutatkozik a színes bőrű elkövetők elítélésére.[27]

Az 1970–1980-as években azonban a büntetéskiszabás során fő szabályként az elkövetett bűncselekmény társadalomra veszélyességére voltak tekintettel a bírák, és csak másodlagosan az elkövető személyében rejlő társadalomra veszélyességre. Később – részben a kockázatelemző kutatásoknak köszönhetően is – előtérbe került a bizonyítékon alapuló gyakorlat *(evidence-based practice; EBP),* amely tudományos módszereken alapul, és elfogadja annak lehetőségét, hogy a jövőbeni elkövetői magatartás előre dimenzionálható. A módszer lényege annak felismerése, hogy a visszaesés csökkenthető, ha a konkrét elkövető személyiségjegyeire és bűnelkövetői szükségleteire fókuszálunk, azaz feltárjuk azokat a faktorokat, amelyek őt a jövőbeni elkövetésre motiválják. Ennek megfelelően az elkövetők a későbbi visszaesés szempontjából szintén magas, közepes és alacsony kockázatot jelentő csoportba kategorizálhatók. Ezek a kockázatelemző besorolások az elkövető rehabilitációját is segítik azáltal, hogy meghatározzák, milyen kezelést vagy támogatást kapjon az elítélt a szabadságvesztés végrehajtása alatt.

A kockázatelemzés következő fázisát annak az elméletnek a megjelenése jelentette, amely szerint vannak dinamikus kockázati tényezők, amelyek idővel változnak vagy – akár külső beavatkozás hatására – megváltoztathatók (például foglalkoztatási státus, alkohol-/kábítószer-függőség); és vannak statikus faktorok (például az elkövető életkora, büntetett előélet, az első elítélés időpontja, az elkövető neme, származása), amely kockázati tényezők megváltoztathatatlanok.[28]

A kockázatelemző tudományos módszerek alkalmazási köre az Egyesült Államokban kiterjed 1. az elítélt rehabilitációja során alkalmazandó módszerek, kezelési eszközök megválasztásában történő segítségnyújtásra; 2. a letartóztatás kérdésében való döntéshozatal megkönnyítésére; 3. az ítélkezés, büntetéskiszabás során alkalmazható eljárásokra.

A *rehabilitáció* során annak kimutatására szolgál a módszer *(rehabilitative risk/needs assessment; RNA),* hogy milyen eszközök alkalmasak legin-

27 Josua B. Fischman – Max M. Schanzenbach: Racial Disparaties under Federal Sentencing Guidelines: The Role of Judicial Discreation and Mandatory Minimums. Journal of Empirical Legal Studies, no. 4, 2012, p. 729.

28 Susan Turner et al.: Development of the California Statc Risk Assasment (CSRA): Recidivism Risk Prediction in the California Department of Corrections and Rehabilitation. Center for evidence-based corrections, University of California, Irvine, 2013. https://ucicorrections.seweb.uci.edu/flies/2013/12/Development-of-the-CSRA_Recidivism-Risk-Prediction-in-the-DC-SR.pdf

kább az érintett személy rehabilitációjára. Az elkövetői csoportok létrehozásával intenzívebb kezelést tudnak biztosítani a magasabb kockázati kategóriába tartozó elkövetők vonatkozásában, mint az alacsony kockázati arányú elítélteknél.

A *letartóztatás* kérdésében való döntést megkönnyítendő módszer *(Public Safety Assessment; PSA)* abban segíti a bírót, hogy a kockázati tényezők felmérésével előrevetíti számára az esetleges bűnismétlés (vagy szökés/elrejtőzés) veszélyét.

Az Amerikai Egyesült Államokban az *ítélkezés* kétlépcsős folyamat. Miután az esküdtszék megállapította a terhelt bűnösségét, a büntetés kiszabása már a bíró feladata, külön eljárás keretében. Ebben segíti őt – a már említett – jelentés *(pre-sentence investigation report; PSI),* amely a terhelt előéletéről és szociális körülményeiről ad felvilágosítást. A jelentést általában a bíróságok mellett működő szociális munkások készítik, és az további – a terhelt büntetőjogi felelősségét vizsgáló büntetőperben fel nem használható – bizonyítékot szolgáltat az elkövető büntetett előéletéről, személyi, családi körülményeiről, baráti köréről, korábbi munkaviszonyairól. A PSI-ben rögzített információk általában hozzáférhetők és megismerhetők a terhelt és védője számára is.

Az ítélkezés, büntetéskiszabás során először Virginia államban alkalmazták a kockázatelemzést 1994-ben. Az úgynevezett *virginiai módszer*t arra fejlesztették ki, hogy a társadalomra kevéssé veszélyes elkövetők vonatkozásában segítse a bíróságot a megfelelő – lehetőség szerint szabadságelvonással nem járó – szankció megválasztásában. Ezek az alternatív jogkövetkezmények a büntetőeljárásról való elterelés alkalmazásától a pénzbüntetésen, közérdekű munkán át a legrövidebb tartamú szabadságvesztésig terjednek. A cél a visszaesés megakadályozása mellett a költséghatékonyság növelése volt azáltal, hogy ne kerüljenek büntetés-végrehajtási intézetekbe olyan elkövetők, akiknél a szabadság elvonásával járó büntetések alkalmazásának létjogosultsága nem igazolt.[29] Jelenleg a büntetéskiszabás során arra használják a kockázatelemző módszereket, hogy megválaszolják: *melyik büntetési nem* a legmegfelelőbb az érintett elkövető esetében, és *milyen tartamú büntetés* kiszabására kerüljön sor.[30] A büntetéskiszabásban jelenleg alkalmazott kockázatelemző módszer a *Level of Service Inventory (LSI-R),* amely a statikus és dinamikus tényezők széles skáláját vonul-

29 Sonja B. Starr: Evidence-based Sentencing and the Scientific Rationalization of Discrimination. Stanford Law Review, no. 66, 2014, p. 803.

30 Ebből a szempontból kiemelendő Sonja B. Starr kutatása: kimutatta, hogy nincs szignifikáns összefüggés a hosszú tartamú szabadságvesztés és a bűnismétlés csökkenése között. Sonja B. Starr: Uo.

tatja fel, és amely a büntetéskiszabás során a visszaesés esélyeit is mérlegeli. A másik népszerű eszköz a COMPAS, amely öt fő területről emeli be az értékelési szempontjait: az elkövető kriminális érintettsége/befolyásoltsága; kapcsolatai/életvezetése. Statikus és dinamikus tényezőket egyaránt vizsgál, a visszaesés esélye meghatározó tényező a büntetéskiszabás során.

Amerika öt államában kötelező ezen eszközök alkalmazása a büntetéskiszabás során: Arizonában, Oklahomában, Kentuckyban, Ohióban és Pennsylvaniában. Más államok (például Idaho, Lousiana, Nyugat-Virginia) engedélyezik az alkalmazást.

Kockázatelemzések a magyar büntető igazságszolgáltatásban

Hazai szakirodalmi előzmények

A kibernetika és a matematika jogtudományra gyakorolt hatását *Erdei Árpád* már 1972-ben vázolta, amikor előrevetítette, hogy a technika fejlődésével elkerülhetetlen lesz a kibernetika térnyerése a jogalkalmazás területén is. Írásában ezért a vonatkozó hazai kutatások késedelem nélküli megkezdésére buzdított.[31] A valószínűségnek a büntető igazságszolgáltatásban betöltött szerepével az 1970–1980-as években foglalkozott – többek között – *Kertész Imre, Pusztai László* és *Katona Géza* is.[32] A valószínűségi ítéletalkotás egyes pszichológiai problémáit kutatta *Engländer Tibor,* akinek 1999-ben monográfiája jelent meg a témában.[33]

Alkalmazási lehetőségek

Ha idővel a hazai büntető igazságszolgáltatásban is felvetődik a számítógépes kockázatelemzések alkalmazásának lehetősége, abban a szerencsés hely-

31 Erdei Árpád: A kibernetikai, matematikai és logikai módszerek jogi alkalmazásával kapcsolatos néhány problémáról. In: Gödöny József (szerk.): Kriminológiai és kriminalisztikai tanulmányok. KJK, Budapest, 1972, 241–290. o.

32 Arató Mátyás – Kertész Imre: A valószínűség és a közvetett bizonyíték. In: A valószinűség szerepe az igazságszolgáltatásban. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 1981, 57–69. o.; Pusztai László: A nyomozási verziók, mint a valószínűség megjelenési formái a büntető eljárás kezdeti szakaszában. In: A valószinűség szerepe az igazságszolgáltatásban. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 1981, 69–79. o.; Katona Géza: Az analógia kimutatására irányuló kriminalisztikai vizsgálatok tapasztalataiból. In: A valószinűség szerepe az igazságszolgáltatásban. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 1981, 207–221. o.

33 Engländer Tibor: Viaskodás a bizonytalannal. Akadémiai Kiadó, Budapest, 1999

zetben leszünk, hogy rendelkezésünkre állnak a külföldi példák és tapasztalatok, illetve tanulhatunk azok hibáiból is.

Úgy véljük, hogy az adekvát jogkövetkezmények megválasztásának elősegítésével és alkalmazásuk gyorsításával a számítógépes kockázatelemzések egyértelműen hozzájárulhatnak a büntetőeljárás hatékonyságának növeléséhez. Ezen kívül pozitívan hathatnak az ítélkezési gyakorlat egységességére, valamint növelhetik az objektivitást is. Mindazonáltal ezen eszközök alkalmazása – ahogyan arra a tanulmány is rámutat – nem veszélytelen. Számos, alapjogi – elsősorban a tisztességes eljáráshoz és a törvény előtti egyenlőséghez fűződő – aggály merülhet fel a gyakorlatban, amelyek kizárólag az elmélet alapján nem mindig válaszolhatók meg. Éppen ezért úgy véljük, hogy a számítógépes kockázatelemzések alkalmazásának lehetőségét csak korlátozottan és fokozatosan lehet megteremteni, illetve később meghonosítani a magyar büntetőeljárásban.

Általánosságban is megállapítható, hogy a bűnügyekkel kapcsolatos, azokra vonatkozó ismereteket a bűnmegelőzés, a büntetőeljárás és a büntetés-végrehajtás szereplői egymástól eltérően értékelik. Ez a tétel a kockázatelemzések vonatkozásában is igaznak bizonyul. Mindhárom területen rendelkezésre állnak ugyan kutatási adatok, de gyakorlati eredményeket elsősorban a kriminalisztikai és a kriminológiai terület tud felmutatni[34], ebből kifolyólag a különböző valószínűségszámításon alapuló módszerek egyfelől a nyomozás (egész pontosan a felderítés) oldaláról képezik részét a büntetőeljárásnak, másrészt viszont – a büntetőjogi jogkövetkezmények kapcsán – a büntetés-végrehajtási jog révén kapcsolódnak hozzá. A téma szempontjából elsősorban utóbbi a releváns.

A kockázatelemzések alkalmazása a tágabb értelemben vett magyar büntető igazságszolgáltatás bizonyos területein már nemcsak elfogadott, hanem egyenesen előírt, és kezdetei, csakúgy, mint az Egyesült Államokban, a büntetés-végrehajtási jog területéhez köthetők. A 2013. évi CCXL. törvény, a Bv.-kódex egyik legnagyobb újítása volt a kockázatelemzési és -kezelési rendszer bevezetése, amely megteremtette a jogi keretrendszert a kezdetektől alkalmazott tudományos megalapozottságú reintegrációs módszerek gyakorlati alkalmazásának lehetőségére.[35] A szabadságvesztés végrehajtásáról szóló fejezet értelmező rendelkezései között a jogalkotó meghatározza a kockázat-

34 Orbán József: Bayes hálók a bűnügyi tudományokban. PhD értekezés. PTE Állam- és Jogtudományi Kar Doktori Iskola, 2017, 17. o. http://ajk.pte.hu/files/file/doktori-iskola/orban-jozsef/orban-jozsef-muhelyvita-ertekezes.pdf

35 Schmehl János: A fogvatartottak kockázatelemzési és kezelési rendszere. Börtönügyi Szemle, 2014/I.

elemzési és -kezelési rendszer fogalmát, amely az elítélt visszaesési és fogva tartási kockázatának a felmérése, értékelése és kezelése érdekében kialakított és működtetett szakmai rendszer (82. § 3. pont) és amelyet a Központi Kivizsgáló és Módszertani Intézet működtet és használ az elítéltek kockázatelemző, valamint az egyéb reintegrációs programokat és döntéseket elősegítő vizsgálataihoz [92. § (1) bek.]. Fő szabály szerint az elítéltet szabadulása előtt legalább hat hónapon belül kockázatelemzési vizsgálatnak kell alávetni a módszertani intézetben, az ezt követő záró kockázatértékelési jelentésben pedig rögzíteni kell az elítélt szabaduláskor mért visszaesési kockázatát [93. § (2) bek.].

Figyelemmel arra, hogy a jogszabály szerint a Központi Kivizsgáló és Módszertani Intézet új szakmai módszerek és eljárások kidolgozását is elvégzi [94. § (2) bek.], e körben a döntéshozatalt segítő jelleggel megvalósíthatónak látjuk a COMPAS-hoz hasonló, számítógéppel támogatott kockázatelemző algoritmusok használatát.

Összegzés

A tanulmányból kiderült, hogy az Egyesült Államokban – ha nem is feltétel nélkül, de – általánosan és széles körben elfogadott egy szabadalmazott és titkos algoritmus alkalmazása a büntető igazságszolgáltatásban, ami akár annak befolyásolására is alkalmas lehet. Az Európai Unió számára viszont kiemelten fontos az átláthatóság: *„a nagy adathalmazok elemzése révén nyert információk megbízhatósága az alapul szolgáló adatokon múlik, ezért az elemzés és prediktív algoritmusai eredményeinek megítéléséhez szigorú tudományos és etikai normákra van szükség”*[36]. Továbbá fel kell hívni a tagállamok bűnüldöző hatóságainak figyelmét arra, hogy *„az adatelemzést a legmagasabb színvonalú etikai normák fenntartásával alkalmazzák, és biztosítsák az emberi beavatkozást és elszámoltathatóságot a döntéshozatal valamennyi szakaszában, nem csak az adatok reprezentatív voltának, pontosságának és minőségének értékelése, hanem az adott információ alapján meghozandó minden egyes döntés megfelelőségének értékelése céljából is”*[37].

Mint ahogyan arra a közelmúlt eseményei (például a *Cambridge Analytica-botrány*) és az azokra adott reakciók is rámutattak, a személyes adatok-

36 Jelentéstervezet a nagy adathalmazok alapjogi vonatkozásairól: magánélet, adatvédelem, megkülönböztetésmentesség, biztonság és bűnüldözés (2016/2225(INI).
37 Uo.

kal, valamint azok védelmével kapcsolatos hozzáállás jelentősen különbözik az angolszász, illetve a kontinentális jogrendszerű rendelkező országok esetén. Ez a különbség kihathat a prediktív algoritmusok alkalmazásának lehetőségeire is: míg az Amerikai Egyesült Államok jelentős részében elterjedt ezen eszközök használata, addig az Európai Unió térségében az adatvédelmi irányelvekre (is) tekintettel nem. Utóbbiakkal kapcsolatosan megjegyzendő, hogy bár az általános adatvédelmi rendeletet (GDPR)[38] általában a bíróságok és más igazságügyi hatóságok tevékenységeire is alkalmazni kell, a személyes adatoknak az illetékes hatóságok által bűncselekmények megelőzése, nyomozása, felderítése, a büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából – ideértve a közbiztonságot fenyegető veszélyek megelőzését, illetve az azokkal szembeni védelmet is – végzett kezelése vonatkozásában a természetes személyek védelme, valamint az ilyen adatok szabad áramlása külön uniós jogi aktus tárgyát képezi. Ezért az e célok érdekében végzett adatkezelési tevékenységekre nem az általános adatvédelmi rendelet, hanem a kifejezetten erre vonatkozó külön uniós jogi aktus, az (EU) 2016/680 európai parlamenti és tanácsi irányelv alkalmazandó.[39] A kockázatelemzések eredményeinek felhasználása során olyan megválaszolatlan kérdések vetődnek fel (például a tisztességes eljáráshoz való jog, a nyilvánosság elve, a diszkrimináció tilalma, a törvény előtti egyenlőség és az egyenlő bánásmód követelménye), amely említett alapjogok és elvek, illetve az algoritmus közötti ellentmondás feloldása jelenleg még várat magára. Az Európai Unió tagállamai számára az amerikai minta ezért csupán példaként szolgálhat arra, hogy milyen alapjogi kérdések tisztázása elengedhetetlen a kockázatelemző eszközök alkalmazása során, és ezekre milyen megoldások adhatók. Az adatvédelmi szabályok miatt ezen automatizált döntéshozatali formák ezért jelenleg hazánkban is csak nagyon szűk körben és célból engedélyezhetők.

38 Az Európai Parlament és a tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

39 Az Európai Parlament és a tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

DOI: 10.38146/BSZ.2018.10.2

PARTI KATALIN

Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében

Egyre több bűncselekmény valósul meg informatikai környezetben, éppen ezért az elektronikus hírközlési (telekommunikációs és internet-) szolgáltatók egyre több megkeresést kapnak a felhasználói adatok kiadása iránt.[1] Az elektronikus hírközlési szolgáltatóknak a bűnüldözési célú adatátadással kapcsolatos jogszabályi kötelezettségeiről azért is időszerű említést tenni, mert a 2018. július 1-jén hatályba lépő új büntetőeljárási törvény (a büntetőeljárásról szóló 2017. évi XC. törvény, a továbbiakban: új Be.), valamint az elektronikus hírközlésről szóló 2003. évi C. tv. (a továbbiakban: Eht.) és az elektronikus kereskedelmi szolgáltatásokról szóló ágazati jogszabályok (2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről, a továbbiakban: Ekrtv.) is megerősítik a szolgáltatók bűnmegelőzéssel, felderítéssel és bűnüldözéssel kapcsolatos feladatait. Ezen túl az Európai Bizottság büntetőügyekre vonatkozó, elektronikus bizonyítékok átadásának meggyorsítását célzó európai rendelettervezete is 2018 áprilisában látott napvilágot. A rendelettervezet, a tagállami szabályozás egységesítése mellett, a szolgáltatókra telepítené a külföldről érkező adatmegőrzési és -átadási kérelmek jogszerűségének vizsgálatát és közvetlen teljesítését. Mindezen jogszabályi módosításokra tekintettel a jelen tanulmány célul tűzi ki a szolgáltatók bűnüldözési célú adatkezelési kötelezettségeinek áttekintését a legutóbbi törekvések tükrében.

1 Lásd például a Deutsche Telekom átláthatósági jelentését: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/hungary-363562; továbbá Google and Apple report jump in requests for user data. BBC News, Oct 2, 2017. https://www.bbc.com/news/technology-41442857; valamint Stephen Nellis: Apple sees steep increase in US national security-related data requests. Businessinsider.com, May 25, 2018. http://www.businessinsider.com/apple-nsa-data-request-transparency-report-2018-5

A szolgáltató együttműködési kötelezettsége a büntetőeljárás során

Az elektronikus hírközlési szolgáltatók együttműködési kötelezettségét az adatok átadására a büntetőeljárás során a büntetőeljárásról szóló törvény írja elő [új Be. 244. § (6) bek.]. A büntetőeljárási célú adatkérésen túl létezik még rendészeti (bűnmegelőzési, felderítési) [Rtv. 68. § (1) bek.] és nemzetbiztonsági, honvédelmi célú adatkérés is, amelyek rendjét külön ágazati törvény [Nbtv. 41. § (1) bek. l) pont], valamint az Eht. [Eht. 92. §; 155. § (5) bek.] szabályozza. A szolgáltató együttműködési kötelezettségét a büntetőeljárás során az elektronikus adat ideiglenes hozzáférhetetlenné tétele kényszerintézkedés és az elektronikus adat végleges hozzáférhetetlenné tétele szankció (régi Be. 158/A §; új Be. 335. §; Btk. 77. §) végrehajtásában az Eht. 92/A §-a szabályozza. A szolgáltató és a felsorolt szervek közötti, büntetőeljárási, felderítési, nemzetbiztonsági és honvédelmi célú együttműködés részletes rendjét a 180/2004. (V. 26.) kormányrendelet (a továbbiakban: kormányrendelet) szabályozza[2].

A büntetőeljárásról szóló törvény tartalmazza azoknak a szerveknek a megnevezését, amelyek megkereséssel fordulhatnak a szolgáltatóhoz adatkérés céljából [új Be. 262. § (1) bek.], ezek a következők: a nyomozó hatóság és a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve. Az új Be. rendelkezése, hogy az arra feljogosított szervek kizárólag az ügyészség engedélyével kérhetnek adatszolgáltatást a törvényben meghatározott szervektől, egyebek mellett az elektronikus hírközlési szolgáltatótól [új Be. 262. § (1) bek. c) pont]. Megjegyzendő, a 1998. évi XIX. törvény szerint a nyomozó hatóságnak a büntetőeljáráson belüli adatkéréseihez (nyílt eljárásban) nem volt szüksége ügyészi engedélyre.

A jelen tanulmány elkészítéséhez interjúkat készítettem a Nemzeti Nyomozó Iroda munkatársaival és a nagyobb telekommunikációs szolgáltatókkal. Mind a nyomozó hatóság, mind pedig a szolgáltatók kifejezték szkepticizmusukat a tekintetben, hogy az új Be. által megkívánt ügyészi engedélyezési rendszer teljesíthető lesz anélkül, hogy ez szükségtelenül megnövelné az adminisztrációt és az adatkiadási időt.

---

2 180/2004. (V. 26.) kormányrendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

Az elektronikus hírközlési szolgáltatók *adatmegőrzési és -átadási kötelezettsége,* az általuk kezelt adatok körére, meghatározott célra és időintervallumra az elektronikus hírközlésről szóló törvényben szabályozott (Eht. 159/A §). A nagyobb telekommunikációs szolgáltatók (Magyar Telekom, Vodafone, Pannon, Telenor, UPC) bűnmegelőzési és bűnüldözési célból kötelesek megállapodást kötni a rendőrséggel, ügyészséggel, nemzetbiztonsági célból pedig a Belügyminisztériummal arról, hogy milyen módon engedik a rendszerükön átmenő adatok átadását, azaz milyen módon és feltételekkel (jogszabályi és formai követelmények) működnek közre az automatikus adatkérések teljesítésében (kormányrendelet 3. §). A rendőrség és a titkosszolgálatok kihelyezett tisztek segítségével tartják a kapcsolatot a telekommunikációs szolgáltatókkal. (Ezek olyan titkos megállapodások, amelyek utaló jelleggel sem megismerhetők a nyilvánosság számára.)

Az automatikus adatátadási rendszer

Az *automatikus (elektronikus) adatátadási rendszer* kidolgozására az elektronikus közigazgatás projekten belül került sor – a NAV, a TEK, az ORFK, a BRFK és az ügyészség esetében. De nem minden, nyomozati jogkörrel felruházott hatóságnál van lehetőség automatikus adatkérésre, ezt technikai és szervezeti okok indokolják. Az ügyészséget például direkt interfész köti össze a szolgáltatóval, ezen keresztül az ügyész maga kereshet, közvetlenül a szolgáltató adatbázisában. Ez a nyomozó hatóság automatikus megkeresési rendszerénél (Robotzsaru) is direktebb, gyorsabb keresést tesz lehetővé, elektronikus formanyomtatványok kitöltése nélkül.

Az automatikus adatkérések előtt a nagyobb szolgáltatóknál hozzávetőlegesen ötven-ötven ember kellett az adatok manuális leválogatásához, a papíron és telefaxon érkező adatkiadás iránti kérelmek kiszolgálásához. Ma, az automatikus adatkérések idején a hatósági megkeresésre kiadandó adatok leválogatásához csupán átlagosan öt ember kell szolgáltatónként. Az automatikus adatkérést a nagy szolgáltatók és az ORFK között kiépült dedikált interfészek teszik lehetővé. A rendőrség a Robotzsaru hálózaton keresztül használja ezt a rendszert, itt húsz-harminc adatkérési *template* áll rendelkezésre, ezt kitöltve az adatok lehívhatók a szolgáltató rendszeréből. Ebben a rendszerben nemcsak a lekérés, hanem a keresés is automatikus, emberi beavatkozást nem igénylő tevékenység (telekommunikációs szolgáltatók, nyomozó hatóság, interjúk).

Szükségességi és arányossági generálklauzula az adatkérések teljesítésére

Ilyen generálklauzula az adatkérés ügyészi engedélyezése, amelyet az új Be. vezet be [új Be. 262. § (1) bek.]. [Az új Be. 261. § (1) bekezdése szerint bíróság adatkérése esetén ügyészi engedélyre nincs szükség.] Az új Be. vezeti be a szükségességi és arányossági [új Be. 264. § (4) bek.], a célhoz kötöttségi [új Be. 264. § (4) bek.] klauzulákat is, valamint az adattörlési kötelezettséget [új Be. 264. § (5) bek.] az adatkérés céljával össze nem függő adatra vonatkozóan. Ugyancsak az új Be. szerint az érintettet tájékoztatni kell az adatkérésről, amely tájékoztatás elhalasztható, ha a büntetőeljárás eredményességét veszélyeztetné [új Be. 264. § (7) bek.]. A szolgáltató az adatkérés tényéről és tárgyáról másnak nem, csak az érintettnek adhat tájékoztatást [új Be. 264. § (7) bek.].

A szolgáltatók adatmegőrzési és -átadási kötelezettségének kiterjesztése az alkalmazásszolgáltatókra

A telekommunikációs és internetszolgáltatókat kötelezettség terheli a nemzetbiztonsági és a bűnüldözési feladatokat ellátó hatóságok irányában metaadatok és kommunikációs (tartalmi) adatok kiadására vonatkozóan. Az Ekrtv. 2016-os módosítása következtében a metaadatokat az *alkalmazásszolgáltatók* is kötelesek megőrizni, legfeljebb egy évig, illetve megkeresésre átadni a hatóságoknak (Ekrtv. 13/B §). Ennek megszegése estére szankciók is kiszabhatók (Ekrtv. 16/H §). A módosítás indokolása szerint *„a technikai fejlődés következtében az internet alapú globális kommunikációs rendszerek, valamint ezen szolgáltatások egyre szélesebb körben terjednek el és megfizethető áron vehetők igénybe, így reális veszélyt jelent, hogy az általános kommunikációs szokások megváltoznak, és a hagyományos hírközlési szolgáltatók helyett ezen szolgáltatásokat veszik igénybe a bűnözői körök. Tekintettel arra, hogy a mobiltelefonok kommunikációjának védelmét ellátó rendszernek egyik elemét képező mobiltelefonos alkalmazás az egyes alkalmazásszolgáltatók interneten elérhető, kereskedelmi céllal létrehozott felületén megtalálható, onnan telepíthető, így kivédhető, hogy az egyes országok szolgálatai a kommunikációt, vagy az ahhoz kapcsolódó információkat megszerezhessék, valamint dekódolhassák. A probléma megoldását jelentheti az alkalmazásszolgáltatókra vonatkozó jogi kötelezettségeknek az előírása. […] Az Ekrtv.*

módosításának célja az Ekrtv. hatálya alá tartozó szolgáltatók adatmegőrzési, adatszolgáltatási és együttműködési kötelezettségének megteremtése. Az Ekrtv.-t érintő módosítási javaslat egyrészt megteremti annak a lehetőségét, hogy a szolgáltató köteles legyen megadni mindazokat az adatokat és információkat, amelyek a titkos információgyűjtés eszközeinek, módszereinek alkalmazásához nélkülözhetetlenek, így a titkosítási szintet érintő információkat is, másrészről pedig a módosítás a szolgáltató részére kötelező jelleggel írja elő a Nemzetbiztonsági Szakszolgálattal történő, a titkos információgyűjtés feltételeit érintő megállapodások megkötését."[3]

Szankció a szolgáltatóval szemben

Büntetőeljárásban rendbírsággal sújtható a szolgáltató, illetve minden, *„az adatkérés keretében megkeresett szervezet",* ha a kérelemben foglaltakat határidőn belül (alapesetben harminc, sürgős esetben nyolc nap) nem teljesíti (telekommunikációs szolgáltatók, interjú), annak teljesítését alaptalanul megtagadja, vagy az adatkérésről történő tájékoztatás szabályait megszegi (például a büntetőeljárás eredményességét veszélyeztetve tájékoztatja az adatkéréssel érintett személyt vagy az adatkérésről másnak is tájékoztatást nyújt – tehát túllépi a tájékoztatási jogkörét) [új Be. 265. § (1) bek.]. Ha annak feltételei fennállnak, akkor a szolgáltatóval szemben kényszerintézkedés – a kért adatok lefoglalása, illetve az adatkérések teljesítéséért felelős személy letartóztatása – is alkalmazható [új Be. 265. § (1) bek.].

Amennyiben a hozzáférést biztosító elektronikus hírközlési szolgáltató nem teljesíti kötelezettségét az elektronikus adat ideiglenes vagy végleges hozzáférhetetlenné tétele tekintetében, úgy a felügyeletet gyakorló Nemzeti Média- és Hírközlési Hatóság rendbírságot szabhat ki a szolgáltatóval szemben [Eht. 92/A § (3) bek.].

A szolgáltató titoktartási kötelezettsége

Az elektronikus hírközlési szolgáltatókat titoktartási kötelezettség terheli a titkos információgyűjtéshez nyújtott, törvényben meghatározott közreműködésük mivoltát illetően. Ezt két jogszabály határozza meg: az elektronikus hírköz-

3 Indokolás a T/10307. számú törvényjavaslathoz, a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról. https://itcafe.hu/dl/cnt/2016-04/127478/10307.pdf

lési szolgáltatóknak a titkos információgyűjtésben való közreműködését előíró 180/2004. (V. 26.) kormányrendelet és a 2009. évi CLV. törvény a minősített adat védelméről (Mavtv.). *„A titkos információgyűjtéssel összefüggő tevékenység végzésében, valamint a monitoring alrendszer, berendezés telepítésében, üzemeltetésében, rendszerfelügyeletében, javításában, karbantartásában az a személy vehet részt, aki az Nbtv.-ben meghatározott nemzetbiztonsági ellenőrzésen megfelelt és rendelkezik az elektronikus hírközlési szolgáltató vezető tisztségviselője által az NBSZ egyetértésével kiadott megbízással”* (kormányrendelet 13. §). A biztonsági feltételekről a Mavtv. rendelkezik: *„Elektronikus biztonsági intézkedéseket kell tenni az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében”* [Mavtv. 10. § (7) bek.]. Az adathoz hozzáférő, együttműködő személy „személyi biztonsági tanúsítványt” kap, amelyet a Nemzeti Biztonsági Felügyelet bocsát ki [Mavtv. 17. § (2) bek. a) pont].

Az elektronikus hírközlési szolgáltatónak a titkos információgyűjtésben közreműködő tagja titoktartási kötelezettsége megszegésének esetén „minősített adattal visszaélés” bűncselekményéért felel [Btk. 265. § (3) bek.]: *„Az a minősített adat felhasználására törvény alapján jogosult személy, aki a minősített adattal visszaélést korlátozott terjesztésű, bizalmas, titkos vagy szigorúan titkos minősítésű adatra követi el [...] két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.”* Az előkészület és a gondatlan alakzat is büntetendő.

Az átadott adatok integritásának védelme

Az elektronikus hírközlési szolgáltatás rendszeréből kinyert, avagy „elektronikus adat” többféle módon juthat el a nyomozó hatósághoz: *a)* az automatikus adatkérési rendszerben; *b)* a szolgáltató manuális lekérése, leválogatása esetén adathordozón (régebben CD, DVD, ma már inkább pendrive); *c)* titkos információgyűjtésre kiépített monitoring-alrendszeren keresztül – ilyenkor először a minősített adatok titkosítását fel kell oldani (új Be. 256–260. §). Az automatikus adatkérési rendszerben megszerzett adat időbélyegzővel és elektronikus aláírással ellátva kerül a nyomozó hatósághoz. A szolgáltató által átadott adathordozót és a titkos információgyűjtés során megszerzett adatot tartalmazó adathordozót először lefoglalja a nyomozó hatóság, majd hiteles másolatot készít róla, amelyet eljuttat az informatikai szakértőhöz. A szakértő véleményével ellátott hiteles másolatnak lesz bizonyító ereje a büntetőeljárásban. A bíróság a közvetlenség elve alapján a tárgyalásra beidézhe-

ti az adatszerzésben közreműködőt – a nyomozó hatóságnak a házkutatáskor, lefoglaláskor jelen lévő tagját vagy a Nemzetbiztonsági Szakszolgálat titkos információgyűjtésben részt vevő tagját –, aki szóban, tanúként válaszol a bíróság kérdéseire. A kérdések az adat megszerzését, illetve a megszerzés körülményeit is érinthetik. A bíróság előtt tett tanúvallomás a bizonyítás része, de nem bővíti a bizonyítékok körét (hacsak a vallomással összefüggésben új bizonyítékra nem derül fény).

A dinamikus IP-cím kiadása

Lehetséges dinamikus IP-címek lekérése, mind a szolgáltató megkeresésével, mind pedig az automatikus adatkérés rendszerében. A feltétele, hogy nagyon pontosan meg kell tudni határozni, milyen időintervallumra nézve szeretné leválogatni az adott IP-címhez tartozó felhasználói kört az arra jogosult szerv. Lehetséges, hogy egyetlen dinamikus IP-címet két nap alatt harminc felhasználó használt, ebből a körből hosszadalmas munkával – azonosítás, tanúkutatás stb. – lehetséges leválogatni a büntetőeljárás szempontjából releváns személyeket. Az, hogy a dinamikus IP-cím az automatikus rendszeren keresztül lekérdezhető-e, függ az országrész mobil- és/vagy vezetékestelefon-szolgáltatással való lefedettségétől. Ha egyetlen IP-cím sok felhasználóhoz kapcsolódhat rövid időn belül, akkor az arra jogosult szervek inkább megkereséssel élnek a szolgáltatónál, amely manuálisan teljesíti a leválogatást. Ha a nyomozó hatóság megkeresése a „szokásostól eltérő” széles felhasználói körre vagy „a szokásostól eltérő”, túlságosan hosszú időre vonatkozik, a szolgáltató ezt a kérést is teljesíti, nem bírálhatja felül a hatóság célját. Elegendő a lekérés/megkeresés céljának megnevezése (milyen bűncselekmény miatt, milyen ügyben van szükség a kért adatokra), a szolgáltató nem bírálja felül a hatóság kérését, és nem szűkíti önkényesen az adatok körét (telekommunikációs szolgáltatók, interjúk). A nyomozó hatóság által kért felhasználói adatok nemcsak közvetlen bizonyításra, hanem a nyomozás irányának meghatározására (verzióállítás) is felhasználhatók.

Az adatkérés teljesítésének megtagadása

A gyakorlatban nem jellemző, hogy a bűnüldözési, honvédelmi, vagy nemzetbiztonsági célú adatkérést megtagadja a szolgáltató. Ennek megvan a for-

mája és a tartalmi kellékei (jogszabályi hivatkozás, célhoz kötöttség), amit betart a megkereső. Egy alkalommal azért utasította vissza az egyik nagy telekommunikációs szolgáltató a rendőrség adatkiadás iránti megkeresését, mert azt csak az ügy előadója írta alá és nem a felettese. Az aláírás pótlásával azonban az adatkiadás megtörtént. Ez egy évekkel ezelőtti adatkérés volt, még papíralapon nyújtotta be a nyomozó hatóság a megkeresést – a ma hatályos, automatikus adatkérési rendszer még nem működött. Ahogy a technika fejlődik, egyre inkább marad el a papíralapú ügyintézés, ezzel együtt a nyomozó hatóság olyan adatokat is lekér, amelyek körét a jogszabály (az Eht.) konkrétan nem szabályozza. Erre példa, hogy korábban csak papíralapú ügyfélszerződések köttettek, de ma már elektronikusan is köthető felhasználói szerződés (webshopon keresztül). Az elektronikus úton megkötött szerződéseken nincs ügyfélaláírás, így azok másolata nem szolgál bizonyítékul, csak az IP-címek, amelyeket a szerződés megkötésekor használt az ügyfél. Ezen a ponton egyeztetésre volt szükség a nyomozó hatósággal: a webshopba való belépéskor használt IP-cím vagy a webshopban, navigálással töltött időintervallumban kiosztott dinamikus IP-címekre van-e szükség a bizonyításhoz. Ilyen és ehhez hasonló kérdésekben folyamatos a nyomozó hatósággal való egyeztetés.

A szolgáltató dekriptálási (titkosításfeloldási) kötelezettsége

Az elektronikus hírközlési szolgáltató dekódolási kötelezettségét előírják a jogszabályok. Az együttműködési kötelezettség körébe tartozik a szolgáltató titkosításfeloldó kötelezettsége is, amennyiben a titkosítást a szolgáltató (és nem maga a felhasználó) végezte [új Be. 264. § (2) bek.]. Az új Be. minden, „az adatkéréssel megkeresett szervezetet", tehát az elektronikus hírközlési szolgáltatót is kötelezi az adatok titkosságának feloldására: *„A rejtjelezett vagy más módon megismerhetetlenné tett adatot az adatkérés keretében megkeresett szervezet köteles az átadás vagy a közlés előtt eredeti állapotába visszaállítani, illetve az adatszolgáltatást kérő szerv számára az adat tartalmát megismerhetővé tenni"* [új Be. 264. § (3) bek.].

A szolgáltató a titkos információgyűjtés keretében is köteles biztosítani, hogy a lehallgatás során az arra jogosult szervek az általa titkosított vagy tömörített információt az eredeti formájában ismerhessék meg: *„Amennyiben az elektronikus hírközlési szolgáltató az előfizető által kezdeményezett vagy foga-*

dott kommunikáció tartalmát bármely módon megváltoztatja, kódolja vagy tömöríti, a kommunikáció tartalmán a visszaalakított, dekódolt vagy tömörítés előtti alakot kell érteni” [kormányrendelet 6. § (2) bek.]. A *felhasználó* által titkosított kommunikáció dekódolására azonban a szolgáltató nem kötelezhető.

2016 óta hatályos az Ekrtv.-nek az a módosítása, amely az alkalmazásszolgáltatókat kötelezi a nem végpontok között, hanem a szerveroldalon titkosított üzenetek tartalmának megőrzésére és a titkos információgyűjtésre jogosult szerv megkeresése esetén történő átadására.[4] A törvény értelmében az alkalmazásszolgáltató *„az a természetes, illetve jogi személy vagy jogi személyiséggel nem rendelkező más szervezet, aki, vagy amely elektronikus hírközlő hálózat felhasználásával valamilyen szoftverhez vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen több felhasználó számára [...]”* [Ekrtv. 2. § m) pont].

A törvénymódosítás bevonja a törvény hatálya alá a nemzetközi vállalatok Magyarországon elérhető online szolgáltatásait is [Ekrtv. 2. § g) pont].

A végpontok közötti *(end-to-end)* titkosítást kínáló szolgáltatók kötelesek megőrizni, és a külső engedélyhez kötött titkos információgyűjtésre jogosult szervek megkeresésére átadni a forgalmi (meta-) adatokat és az üzenetek tartalmát is (Ekrtv. 3/B §).

A szabályozás szerint a szolgáltatónak csak akkor kellene dekriptálnia az üzenetek tartalmát, hogyha *nem végpontok* között folyna a kommunikáció (ilyen alkalmazás például a Signal), hanem a szolgáltató szerverén keresztül.[5] Ami az alkotmányosság tesztjének való megfelelést illeti, a szabályozás éppen az előbbiek miatt az alkalmasság tesztjén bukna el, hiszen a bűnelkövetők, a terrorcselekmények megvalósítói nagy valószínűséggel a végpontok közötti titkosító alkalmazásokat veszik igénybe, amely esetben a szolgáltatónak nincs dekriptálási kötelezettsége.

A jogalkotó ezzel a rendelkezéssel gondolhatott például a 2015 novemberében, San Bernardinóban történt terrortámadásra, amelynek során az öngyilkos merénylők iPhone-ját nem sikerült feltörnie az NSA-nak, és ebben a szolgáltató sem segített. Ebben az időszakban történt az az eset, amikor Brazíliában letartóztatták a Facebook egyik dolgozóját, mert a Facebook megtagadta egy WhatsApp-üzenet dekriptálását. Ugyanebben az időszakban az Egyesült Királyságban is olyan törvényjavaslatot nyújtottak be, amely tiltotta volna az ano-

---

4 Megállapította a 2016. évi LXIX. tv. 45. § (3) bek., hatályos 2016. július 17-től.

5 Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle, 2018/2., 115–135. o.

nim és titkosított üzenetváltást lehetővé tevő applikációk alkalmazását. Jellemző azonban, hogy a magyar jogalkotó egyfajta folyamatos visszavonulást végzett a témában, és ennek a következménye volt a hivatkozott szabályozás bevezetése. A magyar jogalkotó első ötlete nagyon merész volt, például bűncselekménnyé nyilvánították volna a végpontok közötti titkos kommunikációt lehetővé tevő alkalmazások (így például a Signal) használatát. Ehhez az eredeti elképzeléshez képest a jogalkotó fél év alatt folyamatosan hátrafelé lépdelve adta fel kezdeti radikális elképzeléseit a kriminalizációra. Volt egy olyan verzió is, amely szerint kötelezték volna a szolgáltatókat a végpontok között titkosan folytatott kommunikáció tartalmának a megőrzésére. Ennek a folyamatnak a végén maradt a jelenleg hatályos, 2016-ban bevezetett, a nem végpontok közötti titkosított üzenetek dekriptálásának a kötelezettsége.[6]

Az elektronikus hírközlési szolgáltatókra az alkalmazásszolgáltatókat érintő szabályozás csak akkor vonatkozhatna, ha maguk is kínálnának csevegőszolgáltatásokat. Jelenleg a hírközlési szolgáltatónak nincs titkosításfeloldó kötelezettsége a rendszerét használó, úgynevezett Over The Top (OTT) applikációszolgáltatások keretében folyó kommunikáció tartalmára. Ezt úgy lehetne kiküszöbölni, ha az OTT applikációszolgáltató szerződést kötne az elektronikus hírközlési szolgáltatóval az infrastruktúrája használatára. A másik lehetőség, hogy az elektronikus hírközlési szolgáltató létrehozná a maga applikációit, és a vele szerződő felhasználóknak csak az általa kínált applikációkat engedné használni a mobilinternet-szolgáltatáson keresztül. Ebben az esetben a szolgáltató az általa kínált applikációk tekintetében is érvényesítené a törvényes lehallgatás és az adatmegőrzési kötelezettségeit, azaz ezekre is vonatkozna az applikációban folyó kommunikációra a titkosításfeloldási kötelezettség. A saját applikációk létrejöttéig és azok letöltésének exkluzív felhasználói jogosultságokhoz kötéséig azonban erre nincs sem technikai, sem jogi lehetőség.

Kölcsönös jogi segítségnyújtás a telekommunikációs adatok átadása terén

Az elektronikus hírközlési szolgáltatás, vagy számítástechnikai eszköz vagy rendszer útján továbbított kommunikációnak az érintett személy tudta nélkül, leplezett módon történő megismerése és rögzítése végett előterjesztett *eljárá-*

6 A Társaság a Szabadságjogokért álláspontja a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló törvény tervezetéről, 2016. https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf

si jogsegély iránti megkeresést az ügyész a Be. bírói engedélyhez kötött titkos adatszerzésre, illetve az egyéb adatszerző tevékenység során végezhető titkos információgyűjtésre vonatkozó szabályai szerint hajtja végre (lásd az Európai Unió tagállamai közötti bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény 69/E §). Az eljárási jogsegély iránti megkeresés akkor teljesíthető, ha tagállami hatóság a saját államának joga szerint engedéllyel rendelkezik. Ha a megkeresésbeli adatszerzés bírói engedélyhez kötött titkos adatszerzés keretében hajtható végre Magyarországon, akkor a megkeresésről az ügyész indítványára a nyomozási bíró határoz. Ha a bíró elutasítja a megkeresési indítványt, akkor az ügyész tájékoztatja erről a tagállami igazságügyi hatóságot. Az eljárás iránti megkeresés eredménye vagy az eljárási cselekmény befejezését követően (rögzített adat formájában), vagy közvetlen továbbítással irányítható át a megkereső állam eszközére, ha annak technikai feltételei megvannak. Az ügyész a megkereső tagállam kérésére itt is elrendelheti az adatok írásba foglalását.

A Magyarországon tartózkodó személy megfigyelésére irányuló eljárási jogsegély iránti megkereséseket a Fővárosi Főügyészség bírálja el a szerint, megvannak-e a magyar jogban a titkos információgyűjtés feltételei. Erről a bíró a kézhezvételtől számított 96 órán belül dönt, de szükség esetén ez a határidő további 8 nappal meghosszabbítható.

Ha a Magyarországon folyamatban lévő büntetőeljárással érintett személy nem tartózkodik Magyarországon, de az elektronikus kommunikációja megfigyeléséhez nem szükséges a tartózkodási helye szerinti tagállam közreműködése, akkor az ügyész az érintett kilétének felfedését követően haladéktalanul tájékoztatja a tartózkodási hely szerinti tagállamot. Ha a tagállam 96 órán belül (vagy határidő-hosszabbítás esetén 12 napon belül) arról tájékoztatja az ügyészt, hogy nemzeti joga szerint nincs lehetőség a titkos megfigyelésre, vagy a már végrehajtott titkos megfigyelés eredménye nem vagy csak meghatározott feltételekkel használható fel, az ügyész a Be. alapján megteszi a szükséges intézkedéseket. Ha az ügyész ezzel nem ért egyet, akkor az Eurojust közreműködésével egyeztetést kezdeményezhet.

A jövő: külföldi nyomozó hatóság adatkérésének közvetlen kiszolgálása?

Az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény 65/A–65/D és 69/E, 65/H § alapján nincs lehető-

ség arra, hogy az elektronikus hírközlési szolgáltató a külföldről érkező adatkéréseket közvetlenül, a nemzeti kontaktpont (Nebek) bevonása nélkül teljesítse. A nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény 4. § (2) szerint a bűnügyi jogsegélyt a miniszter vagy a legfőbb ügyész teljesíti.

Ahhoz, hogy a szolgáltatók közvetlenül ki tudják szolgálni a külföldi hatóságok adatok iránti megkereséseit, egyértelmű és átfogó jogszabályi háttérre lenne szükség. Azonban az állami szuverenitás, a nemzetbiztonsági érdekek elsőrendűsége, valamint az elektronikus hírközlési vagy kereskedelmi szolgáltatók piaci szerepe mind akadályokat gördít a jelen idejű kéréskiszolgálás megvalósulásának útjába.

Az Európai Bizottság 2018. április 17-én terjesztette elő a büntetőügyekre vonatkozó, elektronikus bizonyítékok közlésére és megőrzésére kötelező európai rendelettervezetet[7] (a továbbiakban: rendelettervezet), valamint az ezzel szorosan összefüggő, a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló irányelv tervezetét.[8] A jelen tanulmány készítésének idején folyamatban van a magyar kormányzat álláspontjának kialakítása a két tervezettel kapcsolatban, ezeket a Hírközlési Érdekegyeztetési Tanácson keresztül véleményezésre kiküldték az elektronikus hírközlési szolgáltatást nyújtó vállalatok számára. Jelenleg nincs jogszabályi felhatalmazásuk a hírközlési szolgáltatóknak, hogy a szuverén államok erre feljogosított hatóságai helyett vizsgálják, van-e alapja a külföldi megkereső fél kérésének. Előállhat egy olyan helyzet, amely szerint az európai rendelettervezet előírja a szolgáltatónak, hogy külföldi kéréseket is közvetlenül fogadjon és teljesítsen, miközben a helyi (nemzeti) jogszabályok szerint az adott ügyben erre jelenleg nincs lehetőség, hiszen hiányzik a nemzeti jogalap, vagy egyenesen veszélyezteti a nemzetbiztonságot a külföldi hatóság által kért adatok kiadása (minősített adat). Ehhez járul, hogy a hírközlési szolgáltató piaci szereplő, nem tartozik a szolgáltatása körébe sem a külföldi megkeresés jogalapjának, sem a forrásának (tudniillik hogy a kibocsátójának van-e jogköre az adatkérésre) vizsgálata, ezt jelenleg a kölcsönös jogsegélykérelmeket teljesítő szervek végzik el. A rendelettervezet kikapcsolná a jogsegélykérelmek teljesítéséből a hatóságokat, és a jogalap vizsgá-

7 Javaslat az Európai Parlament és a tanács rendelete a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról COM/2018/225 final – 2018/0108 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

8 Javaslat az Európai Parlament és a tanács irányelve a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról COM/2018/226 final – 2018/0107 (COD). https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vknmikug23z1

latát a szolgáltatókra bízná. Jelenleg ennek nincsenek meg sem a jogi, sem a technikai feltételei. A rendelettervezet által előrevetített hatósági kontroll hiányát nem oldaná meg a hozzá csatolt *Melléklet az adatkiadás közvetlen teljesítéséről szóló formanyomtatványokról* sem.

Konklúzió

A bizonyítékszerzés terén egyre nagyobb szerep hárul az elektronikus kereskedelmi és hírközlési szolgáltatókra, hiszen a rendszerükben kezelt adattömeg akár egy egyszerű bűncselekmény esetén is fontos bizonyítékul szolgálhat. Az Európa Tanács számítástechnikai bűnözésről szóló (budapesti) egyezménye[9], az eddigi legátfogóbb nemzetközi dokumentum a számítástechnikai rendszerben tárolt adatok átadásának rendjét illetően is iránymutatást ad a tagállamok számára. A szolgáltatót érinti egyebek mellett a számítástechnikai adat gyors megőrzésére és részbeni átadására kötelezés szakasza.[10] Az Európai Bizottság jelen tanulmányban ismertetett, új rendelettervezete ennek a szakasznak a nemzetközi bűnügyi együttműködésben való érvényesülését hivatott biztosítani az adatok gyorsabb átadása érdekében. Kérdés, hogy a szolgáltató, piaci szereplőként kötelezhető-e a hatáskörének ilyen mértékű kiterjesztésére, és ha igen, hol marad a jogállamiság *(rule of law)* megvalósulása.

9 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezményének kihirdetéséről

10 17. Cikk, Forgalmi adat gyors megőrzése és részbeni átadása.

DOI: 10.38146/BSZ.2018.10.3

NAGY ZOLTÁN ANDRÁS

A jövő tegnap óta tart

A modern technikai-technológiai folyamatok kihívásai a jog területén

Napjaink rendkívül gyorsan változó világa a társadalmaktól és tagjaiktól állandó alkalmazkodást kíván, folyamatos adaptációkényszerben élünk.

A próbatételek részint globálisak, részint – bár összefügg a globalitással, hatásukat illetően inkább – helyi jellegűnek nevezhetők.

Az adott ország alkalmazkodásának mikéntje (gyorsasága, mélysége stb.) nyilván függ az érintettségétől, de ugyanígy a reagálás nemzetközi és hazai politikai konstelláció érdekharcának függvénye is, nem utolsósorban szellemi és anyagi források megléte is feltétel.

Napjaink legégetőbb feladatai el nem odázható teendőket rónak a társadalmakra.

A *klímaváltozás* globalitására meg kell találni a válaszokat. Ezzel összefüggésben sürgetőnek ítéljük az építészeti szabványoknak és építési technológiáknak az új időjárási viszonyokhoz igazítását, a trópusi betegségekről való tájékoztatást és a felkészülést a terápiájukra az orvosképzésben, a növényi kultúrák váltásának vizsgálatait a mezőgazdaságban, az energiamenedzselést a klímaváltozáshoz igazítani, és más feladatokat.[1] Az alkalmazkodás egyik lehetősége most terjed el az Egyesült Államokban, ahol is a közutakat fehérre festik a nagy meleg ellen.[2]

A *migráció* egyidős az emberiséggel, ahogy *Ernst Georg Ravenstein* szembesítette a világot a vonzás–taszítás *(push–pull)* elméletével, most ennek valóságát éljük ismét.[3] Az elsivatagosodás feltartóztathatatlansága, ezzel az élet lehetőségeinek megszűnte az erősödő ökomigráció folyamatának állandóságát

1 Hankó Márta – Földi László: A klímaváltozás várható nem kívánatos hatásai és a kritikus szektorok. Hadmérnök, 2009. március, 6–15. o.

2 Máth Dávid: Fehérre festett utakkal hűtik Los Angelest. Totalcar.hu, 2017. augusztus 21. https://totalcar.hu/magazin/hirek/2017/08/21/feherre_festett_utakkal_hutik_los_angeles-t/

3 Ernst George Ravenstein: The Laws of Migration. Journal of the Royal Statistical Society, vol. 52. 1889, p. 286. Ha léteznek olyan okok, körülmények (élethelyzetek), amelyek távozásra ösztönöznek személyeket, és ezzel szemben – ennek mintegy alternatívájaként – léteznek olyan valódi vagy vélt vonzó körülmények, amelyek az elvándorlás motivációját jelentik, mind belföldi, mind külföldi vándorlások esetén. Ez az egyszerű magyarázat igaz mind a gazdasági, mind a politikai menekültekre.

vetíti előre. Európa közelsége miatt már látható, hogy a terhek viselése is az „öreg kontinensre” marad.[4] Utóbbira is figyelemmel, nem látszik megoldás.

A *Föld erőforrásainak felélésére, a túlnépesedésre* – különösen a szegény régiókban, közösségekben – sajnos még a válaszokat megelőző kérdésfeltevések sincsenek. Minden év nagyjából hetedik–nyolcadik hónapjában feléljük a Föld tizenkét havi fogyasztásra elegendő erőforrásait, majd folytatódik ezek kizsákmányolása.[5]

„A népességnövekedés és a tőke növeli az emberiség ökológiai lábnyomát, az emberiség terhét a világ ökoszisztémájára, hacsak nincs sikeres erőfeszítés az ilyen növekedés elkerülésére.”[6] Ijesztő az a vélemény, miszerint *„ha mindenki úgy élne, mint a mai észak-amerikaiak, legalább két további Földre lenne szükség az erőforrások előállításához, a hulladék elnyeléséhez és általában a létfenntartáshoz”*[7]. Mindamellett nem lehet a fogyasztást érdemben visszafogni, mert ennek veszélyes következményei lehetnek a társadalomra (munkanélküliség növekedése, költségvetési bevételek csökkentése, multinacionális vállalatok kivonulása stb.). Tehát ez vállalhatatlan bármely most regnáló és a politikai hatalmat a továbbiakban is fenntartani akaró kormány számára. E körben csak hosszabb távon, konszenzus után születhet megoldás – már ha létezik.

Magyarország sajátos problémája a *kivándorlás*. Ha őszintén beszélnénk a magyarországi push–pullról, közelebb kerülnénk az okokhoz és ezzel a megoldásukhoz.[8] Addig is szomorúan konstatálhatjuk, hogy zömében a fiatal, vállalkozókedvű, fogyasztani tudó és akaró, nyelvet, nyelveket beszélő korosztály megy el, amelynek tagjai már külföldön szülnek, és hazatérésük is egyre távolabb kerül. Mivel például Ausztriában ingyenes az egyetemi képzés, egyre többen vannak, akik már az egyetem elvégzésének az idejére sem maradnak itthon. Pesszimista, de realista közelítéssel rövid távon nincs megoldás.[9]

---

4 Hautzinger Zoltán: Büntetőjogi válaszok a tömeges bevándorlás okozta válsághelyzetre Magyarországon. In: Tálas Péter (szerk.): Magyarország és a 2015-ös európai migrációs válság. Dialóg Campus Kiadó, Budapest, 2017, 69–82. o.

5 https://www.overshootday.org/

6 Donella Meadows – Jorgen Randers – Dennis Meadows: Limits to Growth. The 30-Year Update. Eartscan, London, (reprint). 2006, p. 73. [Magyarul megjelent: A növekedés határai – 30 év múltán. Kossuth Kiadó, Budapest, 2005.] Már az 1972-es könyv is óriási vitát váltott ki.

7 Mathis Wackernagel – William E. Rees: Ökológiai lábnyomunk. Hogyan mérsékeljük az ember hatását a Földön? Föld Napja Alapítvány, Budapest, 2001, 29. o.

8 Ha nem beszélünk őszintén erről a problémáról, akkor egyre távolabb kerülünk az okoktól, miközben egyre többen hagyják el az országot.

9 Unyatyinszki György: Exodussá válhat az elvándorlás. MNO.hu, 2018. március 23. https://mno.hu/belfold/exodussza-valhat-az-elvandorlas-2455430

A technikai-technológia kihívások

A technika-technológia gyors ütemű fejlődése is egy próbatétel, de egy olyan próbatétel, amelyben az államok mozgástere – az előbbiekhez viszonyítva – jóval szabadabb. A gyors változással összefüggésben figyelmeztető, hogy mivel a technológiai fejlődés növekedésének üteme exponenciális, azoknak az országoknak, amelyek nem tartanak lépést napjaink fejlődésével, nem alkalmazkodnak a változásokhoz, a lemaradásuk is exponenciális lesz.

Napjaink már a harmadik és ez ebbe belenövő negyedik ipari forradalomhoz köthető technikai-technológiai megoldásainak adaptálása kikerülhetetlen.

Az adaptáció kapcsán az első kérdés, hogy akar-e az adott ország alkalmazkodni. Ez a kérdésfeltevés életidegennek tűnhet, hiszen melyik ország ne akarna modern országgá válni.

A kérdést azonban itt nyitva hagyjuk…

Ez a tanulmány elsősorban a technikai-technológiai fejlődéshez történő adaptáció egyes jogi vetületeit veszi górcső alá, amelyek a leginkább szembetűnők. E körben részint *de lege ferenda* törvényjavaslatokra, részint a jogi képzés helyzetére, hiátusára hívjuk fel a figyelmet. Ezek a ma még fantasztikusnak tűnő technikai-technológiai „csodák” bizony nem a sci-fi körébe tartoznak, hanem a valóság részei, eszközei.

A *jogi szabályozás* kapcsán *Tóth András* hívja fel a figyelmet arra, miszerint a túl korai szabályozás visszafoghatja a technikai fejlődést, tehát káros, ámde a túl kései reagálás pedig azt a veszélyt rejti magában, hogy kicsúszik a kezünkből a technika, a jog és jogász nem tudja kezelni a felvetődő kérdéseket.[10]

Ezt az időtényezőt szem előtt tartva a jellemzően a harmadik ipari forradalom újdonságai tárgyában (például a 3D nyomtatással és a drónok használatával összefüggő) *de lege ferenda* javaslatok már megértek, míg a negyedik ipari forradalom esetében (például robotika, mesterséges intelligencia stb.) még csak az „anyaggyűjtés fázisában” vagyunk. Tegyük hozzá, hogy a technológiai fejlődés mellett a politikai vagy demokráciafelfogás változása is a jogi szabályozást befolyásoló tényező (például változhatnak a *big datá*ra, az *open datá*ra vonatkozó álláspontok, felfogások).

A most *jogalkalmazóként* dolgozók számára a folyamatos továbbképzés alapfeltétel. A mester-, a szakjogász-, szakirányú továbbképzések nyitva áll-

10 Tóth András: A technológia szabályozásának jogi kihívásai. In: Tóth András (szerk.): Technológia jog. Új globális technológiák jogi kihívásai. Károli Gáspár Egyetem Állam- és Jogtudományi Kar, Budapest, 2016, 33–34. o.

nak. A technikai-technológiai fejlődés, az ezt követő jogi szabályozás megismerése, értelmezése az „élethosszig tartó tanulás” igazi példája.

A jogi oktatást érintő teendők kapcsán a következő *jogi karok* törekvéseit ismerem, már most elnézést kérek azoktól a jogi karoktól, amelyeket kihagytam.

Pécsett a fő tárgyak oktatása mellett több szemináriumon is ismerkedhetnek a hallgatók e modern technológiákkal, tudományos diákkör működik e kérdéskör kutatására, konferenciákat is szerveztek, és a hallgatók rendszeresen látogatják a 3D nyomtatás egyik hazai kutatási központját. Három pécsi oktató is részt vesz a Digitális jólét program 2.0 jogi teendőinek kutatására szerveződött csapatban.

Szegeden a fő tárgyak oktatásának keretében, továbbá tudományos diákkörben folyik a modern technológiákkal való ismerkedés, vizsgálódás. Konferenciájuk közül kiemelkedik az *Ember–gép–jog* elnevezésű, amelyen oktatók és az ország különböző részéből érkező hallgatók, doktoranduszok vettek részt. Az ottani agilis kari vezetés olyan tantervi reformokban is gondolkodik, amelynek egyik vezérelve modern technológiák oktatása, a feladatok kutatása, amely a doktori program része. Lehet, hogy ők lesznek a példa a jogászképzés számára?

A *Károli Gáspár Református Egyetem* nívós tanulmánykötetet jelentetett meg e témához kapcsolódva, továbbá a fő tárgyak oktatása keretében történik az új technológiákra vonatkozó ismeretek átadása. Konferenciákat is szerveztek e témában. Kiemelkedő a Digitális jólét program 2.0 jogi teendői kutatásának koordinátori szerepe.

Győrött intézeti háttere lett a modern technológiák kutatásának, és a szponzor céggel nyitott a kapcsolat, sok segítséget kapnak e körben.

Miskolcon a fő tárgyak keretében figyelnek az új technológiákra, továbbá a doktori programuknak is az egyik hangsúlyos témája.

A *Nemzeti Közszolgálati Egyetem* Rendészettudományi Karán a modern technológiák felhasználásával megvalósított bűncselekmények nyomozásához szükséges ismeretek kimagasló szintű oktatására szerveződött tanszék a vezetésemmel. Az államtudományi és közigazgatási karon mesterképzés keretében ismerhetik meg napjaink e problémáját.

A *Nemzeti Közszolgálati Egyetem Rendészettudományi Karán* a Belügyminisztérium támogatásával *kiberbűnözés elleni tanszék* kezdte meg munkáját a vezetésemmel. A fő célkitűzés nemcsak a hagyományos bűncselekmények számítástechnika érintettségével összefüggő nyomozásának, hanem a virtuális térben zajló bűncselekmények, sőt a jövő technológiai eszközei felhasználásával elkövetett bűncselekmények nyomozásának kriminálmetodikai szempontú oktatása.

A tanszék doktori programot is indított a rendészettudományi kar doktori iskolájában.

Mielőtt elégedetten hátradőlnénk, gyorsan fogjuk vissza az optimizmusunkat. 2018. január 1-jétől ugyanis már kötelező a jogi személyek közötti elektronikus ügyintézés. Érthetetlen, hogy ez még nem része a tanterveknek. Nem mellesleg két év volt a felkészülésre. A jogalkalmazásra alkalmassá nyilvánított végzősök az egyetemekről anélkül kerülnek ki, hogy értenének az elektronikus igazgatáshoz, annak jogi és informatikai együtt kezeléséhez. Nem beszélve a modern technológiák jogi nehézségeinek bemutatásáról, oktatásáról.

Mivel a tantervek elég feszesek, a hallgatók leterheltségét nem szabad fokozni, így nincs más út, mint hogy hozzá kell nyúlni a tantervekhez, amihez vezetői belátás, eltökéltség, a helyi érdekek, egyéni ambíciók határozott „kezelése" szükséges. Nagyon fontos lenne az oktatók érdeklődésének a felkeltése, és itt nem csak az idősebb oktatókra kell gondolnunk.

Szemezgessünk egy-egy új technikai-technológiai megoldás közül, amelyek már jelen vannak, és amelyek vonatkozásában a jogalkotás, a jogalkalmazás és a jövő jogalkalmazóinak képzése nem késlekedhet.

3D nyomtatás, amely a magyar iskolákban sci-fi, másutt már gyerekjáték

A 3D nyomtatás a harmadik ipari forradalom vívmánya.[11] A nyomtatás révén olyan tárgyak, eszközök hozhatók létre, amelyek kézzel kivitelezhetetlenek, mára már a betegek számára szükséges implantátumok precizitása is megoldott. Ahogy az első ipari forradalomban a gőzgép felváltotta a helyhez kötött vízenergiát, ilyen mobil megoldás napjainkban a 3D nyomtatás, amely akár a megrendelőhöz is viheti a termelést.

A *bionyomtatás,* vagyis az emberi szervek azonos genetikai állományból történő pótlása nagymértékben csökkenti, remélhetőleg ki is zárja a kilökődés kockázatát. Ez még kísérleti stádiumban van. Pécsett folynak kísérletek lombikban történő sejttenyészet technológiával.[12]

11 Grad-Gyenge Anikó: A modern technológiák szerzői jogi és iparjogvédelmi kihívásai különös tekintettel a fájlcserére, a felhőprogramozásra és a 3D nyomtatókra. In: Tóth András (szerk.): i. m. 98–115. o.; Nagy Zoltán András: A 3D nyomtatás, mint a jogrendszert érintő új kihívás. Magyar Jog, 2017/10., 613–621. o.

12 Tüdőfejlesztés 3D-ben. http://aok.pte.hu/hu/hirek/hir/10388

A 3D nyomtatás kapcsán felvetődő jogi nehézségek közül fontos megemlíteni, hogy mivel a technológia lehetővé teszi tárgyak reprodukálását is, így az magában rejti bármely szabadalmi, mintaoltalmi, termék know-how, szerzői jogi sérelmének a lehetőségét. A költséges befektetés árán létrehozott új találmányok, újítások, alkatrészek is engedélyek nélkül előállíthatók, sorozatgyártásba bevonhatók, majd értékesíthetők. Mivel a beteg terápiájához szabott vagy ritka gyógyszerek előállítása is megoldott, akkor kábítószerek is előállíthatók, bármilyen összetevőkkel és az összetevők módosításával is. Végül, de nem utolsósorban a legmodernebb fegyverek is előállíthatók. A bűnöző és terrorista csoportok birtokába ily módon kerülő eszközök ellenőrizhetetlenek, jól rejthetők, titkolhatók a hatóságok, szakszolgálatok elől.

A *törvényhozás* feladata az iparjogvédelmi jogok megerősítése. Az első lépés azonnali kell hogy legyen, és mivel a 3D tárgyak nyomtatása .CAD kiterjesztésű fájlból történik, célszerű a .CAD-fájlokat nevesítve beemelni a szerzői jogilag védett alkotások közé.[13]

Az iparjogvédelemmel összefüggésben eldöntendő kérdés, hogy maga a .CAD fájl önálló szabadalomnak (mintaoltalomnak stb.) minősíthető-e, vagy sem. A dilemma az lehet, hogy e fájlból már közvetlenül és azonnal létrehozható az újdonság erejével bíró találmány.[14]

Tovább menve, minél több szereplője van a technológiai folyamatnak (tervezés–szkennelés–nyomtatás–sorozatgyártás–logisztika stb.), annál nagyobb a veszélye annak, hogy a tárgy iparjogvédelmi, szerzői joga vagy üzleti titka sérül.

Az már előre látható, hogy ezek a .CAD fájlok, amelyek adott esetben fegyverek, kábítószerek és más eszközök, dolgok előállításának alapjai, az internet sötét bugyraiban bárkinek elérhetők lesznek, aki meg tudja fizetni. Ahogy ma már sajnálattal kijelenthetjük, hogy a szerzői jog „vereséget szenvedett” az interneten, hiszen megbecsülhetetlen nagyságrendben le- és feltölthetők pénzért vagy ingyen a zenei felvételek, filmek, másolt könyvek stb., úgy biztosak lehetünk abban, hogy néhány éven belül bármely 3D-s tárgy (fegyver, gyógyszer, védett szabadalom stb.) nyomtatására alkalmas fájl is szabad prédává válhat.

Érzékeny kérdés lehet az is, hogy a fegyver, kábítószer és más, a közbiztonságra veszélyes tárgyak előállításának lehetősége miatt sor kerüljön-e a 3D nyomtató forgalmazásának, az eszközt birtokló kis- és nagyvállalkozá-

13 1999. évi LXXVI. törvény 1. § (2) bekezdés
14 1995. évi XXXIII. törvény 1. §

sok, háztartások regisztrálására. Ahogy régebben a stencilgépek nyilvántartásba vétele, a nyomtatás dokumentálása, a fokozott ellenőrzés is létezett.[15] Implantátumok létrehozásakor kemény adatvédelmi követelményt támaszt a beteg egészségügyi adatainak védelme.

Az *egyetemi oktatásban* a technológiának, a technológia (hardver és szoftver) eszközigényének a megismerése, lehetőség szerinti láttatása, valamint a potenciális jogsértések megismerése a feladat.

Exkurzus megjegyzendő, hogy Németországban évek óta árulnak 3D nyomtatójátékot. Azaz a német gyerekek már a saját ötleteik (játékok, ajándékok, használati eszközök, oktatási eszközök stb.) megvalósításához játékosan sajátítják el a 3D-s nyomtatás „titkait".

Minden magyarországi gimnáziumban már „tegnap" ott kellett volna lennie egy 3D nyomtatónak, lássák, tanulják, alkalmazzák azt a technológiát, amely nem korlátozza szárnyaló fantáziájukat.

Kötelezővé tenném Magyarországon a kisiskolásoknak is a 3D-s tollal való „rajzolást": lássák, hogy a rajzuknak ott lesz magassága, ahová „pötyögtetik" a tollból kifolyó műanyagot. Ugyanígy fog a számítógép által vezérelt nyomtató „pötyögtetni", folyatni műanyagot, homokot, fémport, porcelánport, téglaport stb., majd ezek különféle módon történő megszilárdítása után jön létre a 3D-s kiterjedésű tárgy, dolog, eszköz, művészeti alkotás, implantátum, gyógyszer, no meg persze fegyver, kábítószer is.

Már előrelátható, hogy szakmák tűnhetnek el, ám a 3D nyomtatáshoz kapcsolódó ipari (például gyártás), kereskedelmi (gépek, alapanyagok eladása), szolgáltatási (például szerviz) tevékenysége lehetőséget kínál a szakmájukból kikerülők számára. Nem is beszélve a kiemelkedően képzett informatikusok, mérnökök, tervezők, szakorvosok előtt megnyíló lehetőségekről.

A drónok[16]

A drónokat illetően többféle elnevezés ismert, például a személyzet nélküli légi jármű *(Unmanned Aerial Vehicle; UAV),* a távolról irányított jármű *[Remotely Piloted (Aerial) Vehicle; RPV],* vagy a kvadrokopter. A drón elne-

15 26/1959. (V. 1.) kormányrendelet.

16 Gyaraki Réka: A drónok használatának hazai szabályozása. Magyar Rendészet, 2016/1., 43–54. o.; Gyaraki Réka – Rottler Violetta: Drónok kora – személy és vagyonbiztonság a XXI. században. In: Bányász Péter – Kiss Dávid – Orbók Ákos (szerk.): A Tudomány kapujában. Konferenciakötet. Magyar Hadtudományi Társaság, Budapest, 2016, 108. o.

vezés alapja az angol *drone* (méh) szó, utalva annak zümmögő hangjára. Ez is katonai kutatás eredménye, ahogy a számítógép, a dzsip, a GPS, a mélytengeri búvárkodás, az éjjellátó kamerák, a mesterséges eső stb.

A katonai kutatás húzta, húzza a technikai-technológiai fejlesztést, sok minden kerül ki onnan civil hasznosításra. Ugyanúgy, ahogy, kisebb volumenben, a Forma–1-es fejlesztések egy része is átkerül a civil autókba.

A drónok a levegőben, távirányítással röpködnek. Ezáltal lehetővé válik fényképek, filmek készítése olyan objektumokról, tevékenységekről, amelyeket falak vagy más védelmi berendezések óvnak a kíváncsiskodó tekintetek elől. Persze a drónokkal a rendezvények, ünnepségek, sportesemények is megzavarhatók.

A katonai felhasználású drónok alkalmasak távközlési kapcsolatok kiépítésére, rádiótechnikai átjátszásra, rádióelektronikai zavarásra, továbbá zavarórepülés végrehajtására és kamikazetípusú célra repüléshez.

A drónokkal kifürkészhetők üzleti titkok (például a fallal körülvett szabad területen gyártási, logisztikai folyamatokat, gépeket, munkaerőt megfigyelve stb.), továbbá magántitkok (emberek birtokának nagyságát, vagyontárgyakat, kastélyokat stb.) vagy a magánszféra (például a teraszokon, erkélyeken, kertekben ruhátlanul napozók, netán intim tevékenység stb.).

Ezenkívül szándékosan vagy gondatlanul is okozhatnak kárt.

Ebben a kérdésben nincs európai uniós jogforrás, állásfoglalás, de kétségtelenül szükséges szabályok közé szorítani a drónhasználatot.

De lege ferenda jogalkotási javaslat a drón- vagy kvadrokopter használatra:

„(1) Magyarországon a drónhasználatot csak e törvény tilthatja illetőleg korlátozhatja.

(2) Tilos a drónhasználat (abszolút tilalom):

a) 100 méteres magasság felett[17]*;*

b) kritikus infrastruktúrák felett,

c) polgári és katonai repülőterek légterében[18]*,*

17 Az Egyesült Államokban 400 láb, kb. 120 méter felett tiltott. Az Egyesült Államokban a Szövetségi Légiközlekedési Hatóság szabályaiban és a pilóta nélküli légijármű-rendszerekre vonatkozó rendelkezések között olvashatunk a drónokról: Federal Aviation Administration Regulations: *§107.51. […] (b) The altitude of the small unmanned aircraft cannot be higher than 400 feet above ground level, unless the small unmanned aircraft: (1) Is flown within a 400-foot radius of a structure; and (2) Does not fly higher than 400 feet above the structure's immediate uppermost limit.*

18 A Federal Aviation Administration Regulations 107.41 §-a az E lajstromú repülőtereknél enged kivételt. Ez már „mély" szakmai ismeretet feltételez.

d) honvédelmi, rendészeti és büntetés-végrehajtási intézetek, továbbá ezen intézetek használatában lévő, az intézetek funkciójához kapcsolódó területek felett,

c) pénzintézetek felett, továbbá az ezen intézetek használatában lévő, az intézetek funkciójához kapcsolódó területek felett,

d) természeti katasztrófák, kivéve rendészeti szervek és katasztrófavédelem által,

e) balesetek helyszíne felett, kivéve rendészeti szervek és katasztrófavédelem által,

f) tűzesetek felett, kivéve rendészeti szervek és katasztrófavédelem által,

g) állatok etetőhelye és méhészeti telepek felett,

h) bejegyzett naturista strandok, kempingek, illetve egyéb strandok ruhátlan napozásra kijelölt helyei felett.

(3) Időlegesen korlátozható a drónhasználat (relatív tilalom): *a rendészeti szervek által meghatározott területeken és időpontokban (például politikai események, ünnepségek vagy sportrendezvények idején). Ez esetben a rendészeti szervek drónhasználata engedélyezhető.*

(4) Aki a drón (kvadrokopter) (jogszerű) használatával kárt okoz, a Ptk. rendelkezései[19] *szerint felel.*

(5) A drónt (kvadrokoptert) regisztrálni kell.[20]

(6) Az (2) bekezdés d), e), f), g) pontjában említett esetekben az érintett hatóság a tudományos, oktatási célból drónról (kvadrokopterről) történő kép- és filmrögzítést ideiglenesen engedélyezheti."

De lege ferenda javaslat a büntető törvénykönyv módosítására:

Btk. 352/A §

„(1) Aki a drón (kvadrokopter) használatára vonatkozó szabályokat megszegi, ha más bűncselekmény nem valósul meg, vétséget követ el, és egy évig terjedő szabadságvesztéssel, vagy pénzbüntetéssel, vagy közérdekű munkával büntetendő.

(2) Elkobzásnak helye van."

---

19 Ptk. 6:519. § [A felelősség általános szabálya]

20 Az Egyesült Államokban az 55 lbs, azaz a 249,48 gramm feletti repülőszerkezeteket kell regisztrálni. Federal Aviation Administration Regulations §107.3.

A bűncselekmény tervezése szubszidárius, mivel a drónokkal súlyosabb bűncselekmények is elkövethetők, így például üzleti titok megsértése[21], rongálás[22], akár célzott emberölés[23], terrorcselekmény[24].

A *jogalkotás* számára itt a javaslat.

Az *egyetemi oktatás* a drónok alkalmazásának lehetőségeire, a drónokra vonatkozó szabályokra, és az e repülőszerkezetek alkalmazása során elkövethető jogsértésekre, azok polgári vagy büntetőjogi tényállásaira kell hogy fókuszáljon.

Az önvezető autók

Az önvezető autók *(connected cars)* szintén a harmadik ipari forradalom termékei, és több országban már a forgalomban is részt vesznek. Sőt nem ördögtől való nemcsak autók, hanem más, elsősorban kötött pályás járművek önvezetővé alakítása, gondoljunk a 4-es metróra.

Az autógyárakban készülnek emberi beavatkozás nélkül is közlekedő járművek, például a felvidéki Zsolnán 2018-tól sorozatgyártásban.

Üzenet a mostani fiataloknak: nagy üzlet lesz az önvezető autók bérlése, hiszen miért vásároljunk saját autót, ha egy mobilapplikáció segítségével ér-tünk jön, és elvisz a célállomásunkhoz, míg az autóban töltött idő alatt dolgozhatunk, akár alkoholt is fogyaszthatunk.

Persze, mint minden közlekedési eszköz, az *önvezető autó is veszélyes üzem*. Történtek és történni is fognak balesetek e járművekkel is, hiszen hosszabb folyamat lesz a teljes átállás az önvezető autókra, vagyis egyidejűleg közlekednek majd az ember által vezetett és az önvezető járművek.

Már ma el kellene gondolkodni azon, hogy milyen okok vezethetnek a balesetekhez. Sok tényező együttes figyelembevételére lesz szükség, így

– az autó programozásába (útirány, sebesség stb.); majd
– útközben annak vezetésébe történt-e emberi beavatkozás (átprogramozta-e vagy átvette-e a vezetést az ember);
– hardver- vagy szoftverhiba okozhatta-e a balesetet, különös tekintettel arra, hogy ezek az autók a rájuk szerelt érzékelőkkel, GPS-ekkel, műholdas irányítással közlekednek;

21 Btk. 418. §
22 Btk. 371. §
23 Btk. 160. §
24 Btk. 314. § a h) pont alapján

– vis maior hiba történt-e (nem volt kapcsolat a műholddal, másik autóval, az utcán a forgalmat segítő érzékelőkkel – például az időjárási, légköri viszonyok, áramszolgáltatás hiánya miatt stb.);
– eltérő lehet a rutinos autóvezető és az önvezető autó „veszélyérzete”. Az önvezető autó már a potenciális veszélynél megáll, míg a rutinos járművezető csak a közvetlen veszélynél (elég a sárga jelzésnél történő megállási kötelezettségre gondolni).

Nos, ezeket a szempontokat és nyilván az általam nem tárgyalt, más tényezőket is különböző kutatásokban végig kellene venni, és a polgári jogi[25], illetve a büntetőjogi[26] felelősségi rendszert e kutatási eredmények alapján kellene újragondolni.

Az oktatás során elengedhetetlen az önvezető autók technológiájának megértetése, és a hallgatók ösztönzése a felelősségi rendszert érintő kutatásokban való részvételre.[27] Továbbá, ha adódik lehetőség, érdemes felkeresni a Zalaegerszeg mellett épülő tesztpályát, hogy a jogalkotók, jogalkalmazók, joghallgatók élőben szemügyre vehessék, hogyan is közlekednek ezek a járművek egymás mellett, egymást kerülgetve, milyen technikai eszközök segítik a balesetmentes közlekedésüket, és miből keletkezhetnek a balesetek, amelyekről nekik jogi véleményt kell alkotniuk.

A felhőszolgáltatás

A harmadik ipari forradalomhoz köthető az adattárolás és -hozzáférés új módszere. A növekvő adatmennyiség tárolása, gyors elérése, nem utolsósorban a hardver méretének csökkenése, az internet egyre nagyobb elterjedtsége, hívta életre azt az ötletet, majd üzletet, amely találkozott a felhasználók igényével is, hogy tudniillik a felhasználók nem saját számítógépeiken tárolják az adataikat, sőt ma már a programjaikat sem, hanem egy úgynevezett felhőszolgáltatónál.

A felhőszolgáltatók több szerveren és más eszközön tárolják a felhasználók által feltöltött adatokat, programokat. A szerverek lehetnek ugyanabban vagy másik országban, távoli szigeteken (általában utóbbi a jellemző). A fel-

25 Ptk. 6:519. § [A felelősség általános szabálya]
26 Btk. 232., 234., 235. §
27 Boóc Ádám: Robotautókkal, közösségi taxikkal és kereskedelmi drónokkal kapcsolatos felelősségi kérdések. In: Tóth András (szerk.): i. m. 214–226. o.

hőszolgáltatók szerverei között az adatkapcsolat élő, hiszen az adatok folyamatos biztonsági mentése a felhőszolgáltató feladata, kötelessége. Az adatokat a felhőszolgáltató titkosítja, a felhasználókon kívül, elvileg más nem ismerheti meg.

A felhőben tárolt adatokhoz (cikkek, tanulmányok, konferencia-előadások stb.) a felhasználó bármikor és bárhol hozzáférhet, ahol van internetkapcsolat. De a felhők közvetítik azt a kommunikációt is, amelyek emberek és emberek, emberek és gépek, gépek és gépek között zajlanak.

Praktikus és kényelmi lehetőségein túl a felhőszolgáltatás nem kevés gondot okoz a büntető igazságszolgáltatásnak.[28]

A felhőszolgáltatónál tárolt, naplózott információk mint digitális bizonyítékok jellemzően dinamikus digitális tartalmak; felhasználói aktivitásokat, folyamatokat, adatok változásait tanúsítják, igazolják.

Hogyan válhat egy büntető- vagy más eljárásban bizonyítékká a „felhőben" (valamely földrész valamely helyén lévő szerveren) lévő inkriminált adatállomány (például egy tiltott tartalom és annak előállítója, közösségi oldalon közlője, blogra feltöltője stb.).

A bűnügyi jogsegély[29] nehézsége felhőszolgáltatás esetében:

– általában a kettős inkrimináció feltétele (tartalomközlés esetében – a véleménynyilvánítás szabadságának eltérő értelmezése miatt – kétséges);
– nem lokalizálható, hogy melyik országban vannak a szerverek;
– nem lokalizálható, hogy az inkriminált tartalom melyik ország mely szerverén található az elkövetés és az elbírálás idején.

Mivel a szolgáltató nem foglalkozik a territoriális elvvel (mert nem érdeke), így a kérdések tulajdonképpen indifferensek. Egy egyesült államokbeli szolgáltató ma bármely országban úgy viselkedik, mint a saját hazájában.

Ha a feltöltött tartalom bűncselekményt valósít meg, a hatóság felhőszolgáltatóhoz fordul az inkriminált elektronikus adatok mint az eljárásban felhasználni kívánt bizonyítékok kiadása iránt. A felhőszolgáltatók válasza a kérés teljesítése, vagy elutasítása.

---

28 Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I–II. Hadmérnök, 2013/3., 184–210. o.; Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária – Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.): Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018, 755–767. o.

29 Az 1996. évi XXXVIII. tv. (62. § és következő szakaszai) és a 2012. évi CLXXX tv. (66/A és következő szakaszai).

A válasz függ a felhőszolgáltatást alapító cég bejegyzése helyének jogszabályi feltételeitől, azaz jellemzően az Egyesült Államok jogszabályai kívánalmaitól (például a véleménynyilvánítási szabadság megítélésétől).[30]

Mindazonáltal, ha a szolgáltató nem adja át a kért információkat, mert például az adott tartalomközlés a szolgáltatóra vonatkozó (azaz az ő hazai) jogszabályok szerint belefér a véleménynyilvánítás szabadságába, akkor gyakorlatilag a „koronabizonyítékait" elzárja a hatóság elől.

Egy tartalomközlést a magyar hatóság által detektált tartalommal és a készítő személyének a feltárásával lehet(ne) bizonyítani.

A politika feladata, mondhatni kötelessége, hogy megteremtse az együttműködés lehetőségeit az egyes tagállamok hatóságainak érdekei és az egyesült államokbeli nagyobb szolgáltatók között. Nem lesz könnyű.

Egy adalék, a GDPR május 25-től tiltja az úgynevezett profilozó reklámokat, amelyeket a felhasználók profilja, érdeklődése (például korábbi böngészései, közösségi oldali posztja, más internetes aktivitása, horribile dictu marketing célú spyware-ek „gyűjtése") alapján generálnak a szolgáltatók programjai. A tiltó szabály a következő: *„Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené"* [GDPR 22. cikk (1) pont]. Ez világos és egyértelmű szabály a profilalkotás és ezzel a profilba illő reklámok megjelenítésére. Ám ha a felhasználó belépett az adott szolgáltató valamely programjába (email, böngésző, felhő stb.), akkor már lehet olyan jogértelmezés, amely szerint lehet a felhasználó profiljába illő reklámokat mutatni. Ugyanígy problémát vet fel, ha a nagy szolgáltatók nem európai, hanem tengertúli vagy ázsiai szervereken tárolják az európai felhasználók adatait.

A dolgok internete

A dolgok internete *(Internet of Things; IoT)* már átmenet a harmadik és a negyedik ipari forradalom fejlesztései között.

Az internet emberi kommunikációra született, de innen már csak egy lépés, hogy a gépek is kommunikálhatnak, kommunikáljanak egymással. A ro-

30 Mezei Kitti: Az informatikai bűnözés elleni küzdelem – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. Jura, 2018/1., 349–360. o.

botok által irányított/végzett termelési, logisztikai folyamatokban a gépek jelzik majd egymásnak, ha e folyamatokban bármilyen probléma adódik, elfogy az alapanyag, az alkatrész vagy a folyamat bármely okból megáll stb.

A smart home-okban a háztartási eszközök irányítására, vezérlésére térben és időben is sor kerülhet egy mobiltelefon segítségével (meghatározott időre, távolról indítható a sütés, a fűtés, vagy a hűtés[31]), a szolgáltatóknak a mérőóráink küldik az értékeket, a hűtőszekrény automatikusan megrendeli a kifogyó vagy hiányzó alapanyagokat.

Az önvezető autó a parkolókkal kommunikálva tudja meg, hol található szabad hely, és mennyibe kerül a parkolás.

A biztonsági kamerák és riasztók már a környékbeli eszközöket is riasztanák, így az elkövetők mozgása, a menekülésükhöz igénybe vett közlekedési eszköz, annak rendszáma és más információk láthatóvá válnának a hatóságok számára.

E rendszerek kiépítése, összekötése, ily módon történő alkalmazása sürgető feladat.

A *jogalkotás* sem ülhet a babérjain, hiszen a számítástechnikai rendszerek működésének megzavarása büntetni rendelt magatartás.[32]

E rendszerek megzavarása azonban a bűncselekmény tárgyi oldalán szereplő eredményt is előidézhet, abban zavart vagy kárt okozhat. Mégpedig olyan rendszerekben, amelyek nem minősülnek közérdekű üzemnek, a károsult valamely vállalkozás, gyár vagy háztartás.

Tehát adott egy „elektronikus betörés” *(hacking),* ami a számítástechnikai rendszer integritását, biztonságát megtöri[33], valamint az adott az e-rendszer működésének megzavarása vagy abban történő károkozás, ha az forintban mérhető.

De lege ferenda e körben a teendő a *Btk. 423. § (2) bekezdés c) ponttal* történő kiegészítése a következő elkövetési magatartással és büntetőjogi jogkövetkezménnyel: *„c) a számítástechnikai rendszerbe történő beavatkozás kárt okoz”.*

Tehetünk-e különbséget emberek és gépek kommunikációja között? Vagy ugyanazon feltételekkel történhet a (törvényes) ellenőrzés?[34]

---

31 Én már az internet közvetítésével kapcsolom ki és be a légkondicionáló berendezésemet.

32 Btk. 423. §

33 Btk. 43. § (1) bekezdés

34 Kovács Zoltán: Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban. Ellentétes vagy egymással megférő követelmények. Hadmérnök. 2016. december, 222–227. o.

Az *egyetemi oktatás* terén e technológia alapjait, logikáját, az e rendszerek megzavarásának lehetőségeit, következményeit kell megismernünk, illetve elengedhetetlen a jogszabályi változások követése.

Az oktatóknak, hallgatóknak, kutatóknak javasolt a tatai magyar „okosváros” modell és a ceglédberceli „okosfalu” meglátogatása.

Robotika, mesterséges intelligencia

Az IoT technológiával összefüggésben már felrémlenek azok a jogi problémák, amelyek a robotokra és a mesterséges intelligenciával bíró (abba beépített) gépekre is vonatkoznak majd. A mesterséges intelligencia kifejezést először *John McCarthy* használta 1955-ben, majd az elnevezés alapján szervezték meg Dartmouth-ban, 1956-ban az első konferenciát erről az izgalmas területről. Abból kell kiindulni, hogy a gépek bizonyos ideig „csak” azt teszik, amire beprogramozták őket, azaz elsődleges a hardvergyártók és szoftverírók felelőssége. Természetesen, ha a folyamatba ember avatkozik be (például átvéve az irányítást egyes gépek, folyamatok felett, átprogramozza őket menet közben, kiiktat kontrollfunkciókat), akkor az ember felelőssége egyértelmű.

Érdekes és érdeklődéssel várt helyzet, hogy a gépek evolúciójában eljuthatunk-e oda, hogy a robotok a külvilággal történő sokrétű kommunikáció révén az információk tömegének feldolgozása, majd a lehetőségek számbavétele alapján képesek lesznek autonóm döntést hozni. A jogászok számára pedig alapvető feladat annak megválaszolása, hogy a gép által hozott autonóm döntés megalapoz-e jogi felelősséget.

Nem kell sok idő, és meglátjuk, milyen eredményt hoz a gépek, sőt a humanoidok „teremtésmítosza”[35].

35 Az ember evolúciója, az ember évmilliók során történt „önfejlődése”, „önfejlesztése” a mainstream gondolat. A paleoasztronautika történelemszemlélet a világ különböző tájain fellelt, a kor technikai tudásával összeegyeztethetetlen tárgyak, építmények, eszközök, technológiák, ábrázolások bemutatásával igyekszik az emberi evolúció és tudás minőségi ugrását „földönkívüliek” beavatkozásával magyarázni. Mielőtt legyintenénk, lássunk néhány zavarba ejtő konkrétumot: az abydosi hieroglifák repülő- és harckocsi-ábrázolásai, a Puma Punktuban használt építési technológiák, a palenquei űrhajós sztélé, az olmék óriásfejek, a maják mainál pontosabb naptára, az égből látható Nazca-vonalak célja, a szakkarai „madár” vagy siklórepülő (?), a kolumbiai miniatűr aranyrepülők, carnaci óriásméretű szobrok, a Costa Rica-i óriási kőgolyók, a moai óriásszobrok, a bagdadi „elem”, az asszuáni 1200 tonnás obeliszk, az 1500 éve nem rozsdásodó delhi „vasból” (?) készült oszlop, a Cargo-kultusz továbbélése, a barlangi rajzok „űrhajóssisakban” lévő furcsa „emberekről”, repülőtárgyak ábrázolása, Ézakiel utazása, a 800 tonnás (!) kőtömbök a római Jupiter-templom romjaiban… Hosszú sora van a mainstreambe

Már nálunk is kapható olyan csúcstechnológiás (kínai) mobiltelefon, amely intelligens, tanulni, alkalmazkodni képes. Ez nyilván még csak a kezdet, de már jelzi a mesterséges intelligencia (AI) felhasználásának számtalan lehetőségét. Nagy várakozással tekintünk a hazai mesterségesintelligencia-koalícióra, amely hetven kormányzat, piaci szereplőt tömörít, és egyebek között a jogi szabályozásra, a technológiai fejlesztésre fókuszál.

A robotokkal kapcsolatos megközelítésben ma még meghökkentő az a kérdés, hogy válhat-e robot munkavállalóvá.[36] Vagy az a kérdés, hogy milyen jogai lehetnek a robotnak. A robotjogokról ír a Microsoft, és az Európai Unió tervei is erre irányulnak.[37] Még bizarrabb az, hogy az egyik legkonzervatívabb iszlám állam, Szaúd-Arábia állampolgárságot adott egy Sophie nevű robotnak.[38]

A big data és az open data

Ez a probléma csak számítógépes környezetben vetődik fel. A 2000-es évektől kezdve a kereskedelmi tevékenységek és szolgáltatások dinamikusan növekedtek a kibertérben. Mi, állampolgárok naponta több tucat, akár százas nagyságrendben „szolgáltatunk" magunkról adatokat, mobiltelefonhívással és azok fogadásával, internetre bejelentkezéssel, böngészésünkkel, e-mail-írással, bankkártyával fizetés helyével, a vásárolt áru- vagy szolgáltatás teljesítésével. Naivan azt hisszük, hogy a Google, a Facebook, a Twitter, a Viber és más szolgáltatások ingyenesek, pedig *fizetünk érte, jóval értékesebb fizetőeszközzel,* mint a pénz – a személyes adatainkkal, sokszor titkaink, vágyaink, érzéseink megosztásával.

Tehát óriási mennyiségű elektronikus adat keletkezik különböző forrásokból a felhasználóktól.

---

nem illeszkedő dolgoknak, épületeknek, amelyek léte még magyarázatra szorul. A múlt nagy kérdése így kapcsolódik a jövő problémájához. Vajon a gépek, humanoidok evolúciójában a minőségi ugráshoz kell-e majd emberi beavatkozás vagy Marvin Minskynek, a mesterségeintelligencia-kutatás egyik nagy alakjának lesz igaza, miszerint, ha megértjük az emberi gondolkodást a célirányultságtól az érzelmekig, akkor ez a folyamat átvihető gépekre is. Marvin Minsky: The Emotion Machine, Simon & Schuster, 2006.

36 https://arsboni.hu/mesterseges-intelligencia-valhat-e-munkavallalova-egy-robot/

37 https://nuus.hu/tech/infotech/0125/microsoft-eppen-robotok-jogait-irja-le-tarsadalomban/ ; https://www.ormosnet.hu/robot-emberi-jog.html

38 http://www.origo.hu/techbazis/20171028-eloszor-kapott-allampolgarsagot-egy-robot-szaud-arabia-sophie.html

A kérdés, hogy mi lesz ezzel a rengeteg adattal. Mivel az adatszolgáltatással az adatgyűjtés megtörténik, kérdés, hogyan történik az adatok további kezelése.

A big data számos társadalmilag helyes és akceptálható célra felhasználható.[39] Az adataink a társadalmi folyamatokról nyújtanak információkat, segítve azok tervezhetőségét, a közigazgatás vagy a tömegközlekedés szervezését stb. Információt nyújthatnak fogyasztásunkról, jövedelmünkről, egészségi állapotunkról, demográfiai helyzetünkről.

Ha az adatok anonimizáltak, akkor adataink ilyen célú felhasználása elfogadható. Ámde bármely adat anonimitása megszüntethető, visszafejthető, és az adatalanyra vonatkozó információk már felhasználhatók. Az adatalany megzsarolható, „listázható", az adataival vissza lehet élni a kárára.

Mindamellett a tárolt információk visszakeresése (például kamerafelvételek, mobilszolgáltatók információi, banki tranzakciók stb.) a nyomozó hatóságokat is segítik a nyomozásban. A terrorizmus ellen is nagyfokú segítséget nyújt a nagytömegű adatgyűjtés.

Még a jövő problémája, hogy a big data hogyan kezelhető (hasznosítható) a GDPR rendelkezései szerint.

Az open data, az úgynevezett nyílt adatok körébe tartoznak azok az információk, amelyek szabadon hozzáférhetők mindenki számára.[40] Ezeket az adatokat nem kötik szerzői, iparjogvédelmi jogok, vagy más jog, illetve ellenőrzési mechanizmus. A nyilvánosság számára szánt adatok a bárki által elérhetők, amelyeket a kormányzatok, államigazgatási, önkormányzati szervek, vállalkozások, hivatalok osztanak meg, tesznek közkinccsé, amelyek figyelembevételével a lakosság cselekvési lehetőségei adottá, tervezhetővé válnak (ügyintézés ideje, mikéntje, építési lehetőség, rendelési idők, előzetes eljárások, papírok, vásárlási lehetőségek stb.).

Az *oktatás területén* a majdan végző jogalkalmazóknak saját és ügyfeleik érdekében érdemes figyelmet fordítaniuk az úgynevezett nyílt forrású hírszerzésre *(Open Source Intelligence; OSINT),* és ennek legális helyeire, technikáira.

---

39 Belényesi Pál: A technológiai piacok versenyjogi vonatkozásai. In: Tóth András (szerk.): i. m. 170. o.

40 Muha Lajos – Négyesi Imre. Nyílt forráskódú rendszerek alkalmazása. NT Nonprofit Közhasznú Társaság, Budapest, 2013, 197. o.

A kiberbűncselekmények oktatásáról

Az interneten is, ahogy a valós térben a legveszélyesebb bűnözési forma a szervezett elkövetés.[41] E bűnözői kör tagjai ugyanazokkal a technikai lehetőségekkel élnek vissza, amelyet más felhasználók tisztességes célra használnak.[42] Hamis vagy azonosíthatatlan IP-címekről, nem forgalmazó e-mail-fiókokban hagyott üzenetekkel kommunikálnak, kép-, szöveg- vagy bármely más fájlba rejtett üzeneteket küldözgetnek, töltögetnek egymástól (például jelszóval védett FTP-hálózatokról). Továbbá tagokat toboroznak tevékenységükhöz, vallási-politikai propagandát folytatnak szöveges, audio- és videoelérhetőséggel, kábítószert, hamis árukat, termékeket forgalmaznak, illegális szerencsejáték-oldalakat üzemeltetnek, pénzt mosnak[43] tisztára alapítványokon, legális vagy illegális szerencsejáték-oldalakon keresztül.

Az Europol 2014 óta adja ki az *Internetes szervezett bűnözéssel kapcsolatos fenyegetésértékelés (Internet Organised Crime Threat Assessment; IOCTA)* című jelentését egy úgynevezett Fehér könyvben. A jelentések évente adnak helyzetjelentést a számítógépes bűnözésről, a megismert fenyegetésekről, a várható tendenciákról. Összegezik a szakemberek, a tagállamok tapasztalatait, a tudományos kutatások eredményeit.

Érdemes áttekinteni az elmúlt két év értékelését *(táblázat)*.

Jó láthatók a két IOCTA-jelentés közötti átfedések, amiből viszont azt a következtetést vonhatjuk le, hogy ezek azok a kibertérhez kötött vagy azzal összefüggő bűncselekmények, amelyek a gyakorlatban mennyiségében és minőségében a legjelentősebbek.

Tovább menve vegyünk észre még valamit. Az Europol szakértői által összeállított listából látható, hogy a bűncselekmények zöme nem a kibertérhez kötött, hanem már előtte ismertek és büntetendők voltak.

Ez viszont azt jelenti, hogy a büntetőjog különös részének bármely szinten történő oktatásában, a bűncselekmények bemutatásakor, elemzésekor e

41 Organised Crime in Europe: The threat of cybercrime. Council of Europe – Octopus Programme, Strasbourg, 2005, pp. 161–170.; Korinek László: Kriminológia II. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2010, 310. o.; Nagy Zoltán: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy S.O.S Magyarország! Magyar Jog, 2016/1., 17–24. o.; Papp Péter: Hi-tech bűnözés napjainkban. Belügyi Szemle, 2011/11–12., 5. o.; Anamaria Cristina Cercel: Criminologie. Editura Hamangiu, 2009, p. 101.

42 Simon Béla: A virtuális világok büntetőjogi szempontból. In: Szelei Ildikó – Berki Gábor (szerk.): Hadtudomány és a 21. század. Budapest, 2015, 265–277. o.

43 Gál István László: A pénzmosás és a terrorizmus finanszírozása. In: Korinek László – Kőhalmi László – Herke Csongor (szerk.): Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2004, 39. o.

Az Europol jelentéseinek összevetése

Az IOCTA 2016-os jelentése[44]	*Az IOCTA 2017-es jelentése*[47]
– a malware-ek (malicous software – rosszindulatú programok összefoglaló elnevezése); – gyermekek online szexuális kizsákmányolása; – fizetési csalások; – social engineering; – adatsértések és hálózati támadások; – a kritikus infrastruktúra elleni támadások[45]; – online bűnös pénzügyek; – a darknet és a rejtett szolgáltatások; – a terrorizmus és a kibertér konvergenciája[46]; – big data, IoT, felhőszolgáltatások.	– kibertérfüggő bűncselekmények; – malware-ek; – adatsértések; – gyermekek online szexuális kizsákmányolása; – fizetési csalások – card present csalások, – card not-present csalások; – online bűnözői piac; – a kibertér és a terrorizmus konvergenciája.

bűncselekmények kibertérben történő megvalósulásának lehetőségeit is említeni kell(ene)[48]. Ez az *oktatók felelőssége*.

Összegzés

A tanulmány elején feltettem az alapkérdést: akar-e a mindenkori hatalom a technikai-technológiai fejlődés útjára lépni?

Ma a fejlett nyugat-európai országokban (Szlovákiával, Szlovéniával[49] is) a DAB *(Digital Audio Broadcasting)* még inkább a DAB+ technológiájú di-

44 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

45 Muha Lajos: A kritikus információs infrastruktúrák védelme. Reinet Technológia Kft., Budapest, 2015, 16–19., 54–58. o.; Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gál Gyula – Hautzinger Zoltán (szerk.): Szent Lászlótól a modernkori magyar rendészettudományig. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2017, 163–168. o.

46 Dornfeld László – Sántha Ferenc: A terrorizmus és a terrorcselekmény, mint nemzetközi bűncselekmény aktuális kérdései. Jog Állam Politika, 2017/3., 69–106. o.

47 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

48 Simon Béla: Csúcstechnológiai bűnözés. Egyetemi jegyzet. Nemzeti Közszolgálati Egyetem, Budapest, 2012, 11. o.; Nagy Zoltán András – Mezei Kitti: Az informatikai bűncselekmények. Egyetemi jegyzet. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2017, 5–8. o.; Deres Petronella: Internetes bűnözés. In: Tóth András (szerk.): i. m. 248–250. o.; Domokos Andrea: Internetes bűnözés. In: Tóth András (szerk.): i. m. 251–260. o.; Mezei Kitti – Tóth Dávid: Információs bűncselekmények. Büntetőjogi Szemle, 2015/1–2., 64–73. o.

49 Szlovéniában jelenleg az ország területének hetven százalékán szólnak digitális rádióadások, terveik szerint 2022-ben lekapcsolják az analóg hálózatokat. http://radiosite.hu/mar-2022-ben-lekapcsolhatjak-az-fm-adokat-szloveniaban/

gitális rádiózás már felváltotta, felváltja az analóg rádiózást. Egyfelől a digitális rádióadások vételére alkalmas rádiók igen sokba kerülnek, ami a magyar átlagjövedelmi viszonyok és a fogyasztási preferenciák mellett meggondolandó kiadás. Másfelől ha lekapcsolnák az analóg magyarországi rádiósugárzást, nem jutnának el a lakosság teljes köréhez (vidéken, peremterületeken, tanyákon, kicsiny falvakban) a hírek és egyéb tartalmak.

A közszolgálati és néhány rádióadó kísérletképpen sugároz digitális rádióadásokat, ma még csupán Budapest vételkörzetében. Látható, hogy Magyarországon a technikai megújulást és egyben tartalombővülést is magával hozó digitális rádiózás áttörésére még várnunk kell.

A lenyűgöző technikai-technológiai fejlődés társadalmi nehézségeinek sokszempontú és beható vizsgálata nem elodázható feladat.

A *jogalkotó* figyelmét hívta fel a Kúria elnöke is, amikor arról beszélt, hogy *„a big data, a közösségi portálok, a felhőalapú szolgáltatások jelentős hatással vannak a szerzői jogokra és az adatvédelemre. Várhatóan jelentős változást eredményez a drónok vagy az önvezető autók alkalmazása a kárfelelősségi szabályokban.”*[50]

Nem vitatható, hogy a *jogalkalmazók* naprakész és szervezett, szakmailag megbízható felkészítése fontos feladat.

Az *egyetemi oktatásban* ugyanez a teendő, nem késlekedhetünk, hiszen egyfelől a technika és a technológia rendkívül gyors ütemben halad előre és nem várja be az országok adaptációját, másfelől ha e területen nem jártas hallgatók végeznek, akkor jogalkotóként, jogalkalmazóként is ugyanilyen ismeretlen marad előttük az a világ, amelyben élnek.

A Nemzeti Közszolgálati Egyetem Rendészettudományi Kar kiberbűnözés elleni tanszéke élen fog járni a modern technika és technológia jogi buktatóinak felszínre hozatalában.

50 http://www.lb.hu/sites/default/files/sajto/ab_darak_ur_beszede_2017._aprilis_10.pdf

DOI: 10.38146/BSZ.2018.10.4

KOLLÁR CSABA

A magyarországi online csalások fontosabb tulajdonságai[1]

A 2013 és 2016 között elkövetett releváns bűnesetek elemzése

A büntető törvénykönyvről szóló 2012. évi C. törvény (Btk.) nevesíti a vagyon elleni bűncselekmények közül a lopást (370. §), a sikkasztást (372. §), a csalást (373. §), a gazdasági csalást (374. §), az információs rendszer felhasználásával elkövetett csalást (375. §), a hűtlen és hanyag kezelést (376. és 377. §), a jogtalan elsajátítást (378. §), az orgazdaságot (379. §), a szellemi tulajdon elleni bűncselekmények közül az iparjogvédelmi jogok megsértését (388. §), a pénz- és bélyegforgalom biztonsága elleni bűncselekmények közül a készpénz-helyettesítő fizetési eszköz hamisítását, illetve a vele való visszaélést (392. és 393. §), valamint a készpénz-helyettesítő fizetési eszköz hamisításának elősegítését (394. §). E bűncselekmények adják a tanulmány jogi keretét. Elméleti szinten igen, saját kutatásomban azonban nem teszek lényeges különbséget a Btk. nevezett tényállásai között, így a csalás fogalmát nemcsak a 373–375. §-ra, hanem kriminológiai értelemben általában használom azokra az esetekre, amikor a csalás (tévedésbe ejtés) módszerével, vagy annak révén, segítségével valósult meg a bűncselekmény.

A digitális korban elkövetett elektronikus bűncselekmények

A digitális kor technikai eszközeinek a használatával megvalósított bűncselekményeket a szakirodalom összefoglaló néven csúcstechnológiai bűnözésnek[2], számítástechnikai jellegű bűncselekménynek[3], számítógépes bűncselekménynek[4], valamint jelenleg általánosságban és leggyakrabban kiberbűnözés-

1 A tanulmány az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I-OE-779/45 kódszámú Új Nemzeti Kiválósági Programjának támogatásával készült.

2 Simon Béla: A csúcstechnológiai bűnözés és nyomozása. Nemzeti Közszolgálati Egyetem, Budapest, 2013

3 Ibolya Tibor: A számítástechnikai jellegű bűncselekmények nyomozása. Patrocinium, Budapest, 2012

4 Gyaraki Réka: Számítógépes bűncselekmények és az ellenük való védekezés. In: Christián László (szerk.): Információvédelem. Nemzeti Közszolgálati Egyetem, Budapest, 2015

nek nevezi. *Simon*[5] az általam említett, és a Btk.-ban is nevesített tényállások szerint osztályozza a bűncselekményeket. *Ibolya*[6] az online csalásokat, a zaklatást, a készpénz-helyettesítő fizetési eszközzel kapcsolatos bűncselekményeket, az e-mailes csalásokat, az adathalászat különböző formáit és módszereit, a wifilopást és a szerzői jogi jogsértéseket különbözteti meg. *Gyaraki*[7] és *Nagy*[8] az online környezetben elkövetett bűncselekmények hazai és nemzetközi tipizálási törekvéseit ismerteti. Nagy többek között svájci, japán, belga, német, osztrák, amerikai, skót szerzők művei alapján megállapítja, hogy a számítógépes környezetben elkövetett bűncselekmények első generációjáról a nyolcvanas évek végéig beszélhetünk. Ebben az időszakban a fontosabb bűncselekmények a következők:

– számítógépes manipuláció;
– titkos kémkedés;
– gépidőlopás és szabotázs;
– adatmanipuláció és adatlopás;
– komputer jogosulatlan használata;
– számítógépes hamisítás;
– rendszerbe történő jogosulatlan behatolás;
– személyes adatokat veszélyeztető támadás;
– mikrochip jogosulatlan másolása;
– szoftverlopás;
– visszaélés az adatfeldolgozási tevékenységgel;
– számítógépes hacking.

Az elektronikus környezetben elkövetett bűncselekmények osztályozására, tipizálására tehát igény mutatkozott nemcsak nemzeti, hanem – ahogy Gyaraki és Nagy leírja – nemzetközi szinten is. Az OECD 1986-ban kibocsátott rendelkezése öt alrendszerbe sorolta ezeket a bűncselekményeket, és megadta az információlopás, a számítógépes szabotázs, az adatok tisztességtelen manipulálása vagy megváltoztatása, a jogosulatlan használat, illetve a jogosulatlan hozzáférés fogalmi kereteit. Az Európa Tanács 1989/9. számú ajánlásában egy olyan minimális listát állított össze, amelyikben a megnevezett cselekmények büntetendővé nyilvánítását javasolja. Ennek első pontja a számítógépes csalás. Nagy közlésében az Európa Tanács ajánlásában defini-

5 Simon Béla: i. m.
6 Ibolya Tibor: i. m.
7 Gyaraki Réka: i. m.
8 Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009

ált számítógépes csalás *„adatok, programok bevitele, megváltoztatása, törlése, elrejtése, vagy más, az elektronikus adatfeldolgozási folyamatok befolyásolását eredményező magatartás, amellyel az elkövető egy harmadik személynek gazdasági, vagy vagyoni hátrányt okoz, illetve amelynek célja az, hogy az elkövető önmaga, vagy más számára gazdasági, illetőleg vagyoni előnyhöz jusson”.* Vagyis *„más személyt vagyonától megfosszon”.*

Gyaraki úgy véli, hogy a *„számítógépes bűncselekmények elkövetői általában magasan képzett, 18-45 éves szakemberek, jellemzően férfiak”*[9]. A tanulmányom második részében ismertetett primer kutatásom alapján megállapítottam, hogy az online csalások elkövetőire csak fenntartásokkal igaz az idézett megállapítás. Ennek legfőbb okát abban látom, hogy az elkövetői fő kategóriák – hacker, cracker, social engineer, kalóz – közül az elkövetők zömében a social engineer, s kisebb részben a kalóz kategóriákba sorolhatók be.

Csalás az elektronikus kereskedelemben és piactereken

Az eNET Internetkutató és Tanácsadó Kft. online kereskedelemre vonatkozó felmérése szerint 2016-ban 427 milliárd forint, vagyis a hazai kiskereskedelmi forgalom 5,2 százaléka bonyolódott le elektronikus környezetben. A piac mérete és forgalmának növekedése mellett a virtuális bevásárlókosarakba átlagosan tizenháromezer forintnyi áru került, ami ezerhétszáz forinttal több, mint a 2015-ös átlagkosár mértéke. A vásárlók száma 2016-ban megközelítette az ötmilliót, ami azt jelenti, hogy a felnőtt internetezők több mint nyolcvan százaléka legalább évente egyszer vásárol online piactereken. A vásárlási aktivitás fokozódása nemcsak a hazai, hanem külföldi webshopoknál is érezhető. A külföldi webáruházakban vásárló magyar vásárlók száma 2015-höz képest (másfél millió fő) 2016-ban további hétszázezerrel gyarapodott. A GKI Digital HVG.hu-n olvasható felmérése szerint[10] a hazai online kiskereskedelem öt legnagyobb szereplője 2017-ben az Extreme Digital, az Emag, a Media Markt, a Mall.hu és a Tesco. Ezek és a rangsorban következő öt vállalat forgalma a hazai online kereskedelem harminc százalékát teszi ki. Az online módon (is) értékesítő vállalatok mellett az online piacterek is népszerűek.

Az említett oldalak üzemeltetőinek/tulajdonosainak nyilvánvalóan jól felfogott gazdasági érdekük, hogy az online kereskedelmi felület, illetve piactér biztonságos legyen, minél több olyan biztonsági elem legyen tudatosítva a (le-

9 Gyaraki Réka: i. m.
10 https://hvg.hu/kkv/20170615_Ezekben_a_boltokban_koltjuk_el_a_legtobb_penzt_a_neten

endő) vásárlóban, ami csökkenti a vásárlás kockázatát, és elősegíti az online környezetben történő vásárlás mint szokás beépülését az emberek rutinjába.

Az online kereskedelemmel foglalkozó vállalkozók a törvény által kötelezően előírt szavatosság, jótállás, elállás tényének és lehetőségének bemutatása mellett a fizikai világhoz képest kedvezőbb árakkal, online akciókkal motiválják a vásárlókat, a nagyobb piactereken pedig az eladó bizalmi indexe (például sikeres vásárlások száma, pozitív értékelés, ötfokú Likert-skálán az ötös gyakorisága, a rendszerben eladóként történő regisztráció időpontja), a csalófigyelő rendszer, pénzvisszafizetési garancia próbálja elősegíteni a biztonságos, csekély kockázattal járó online vásárlást. *Barta és Székely*[11] az online piactereken elkövetett visszaélések felderítésével foglalkozó könyvében bemutatja a Vatera Biztonsági Csoport tevékenységét *(táblázat)*.

A Vatera Biztonsági Csoport tevékenysége

Akciók	Leírás	Cél
Észlelés	Felhasználói inaktivitás, biztonsági adategyeztetés: – személyes okmányok (személyi igazolvány, lakcímkártya, útlevél) másolatának bekérése (faxon, szkennelve); – okmányok adatainak egybevetése a regisztrációs adatokkal	személyellenőrzés, visszaélést megkísérlő felhasználó kizárása a piactérről – megelőzési céllal
Adatgyűjtés	– online piactéren észlelt felhasználói adatok mentése, rendszerezése; – nyílt információgyűjtés, jellemzően közösségi portálokon	nyombiztosítás, az elkövető által hagyott digitális lábnyomok mentése
Felhasználói tájékoztatás	Észlelt visszaélés esetén a csaló felhasználóval kapcsolatba kerülő személyek tájékoztatása – figyelemfelhívás; – tájékoztatás feljelentés lehetőségéről	megelőzés figyelmeztetéssel, egyúttal a sértettek tájékoztatása
Nyomozó hatóság támogatása	– kiemelt ügy észlelése esetén feljelentés megtétele; – adatszolgáltatás; – sértetti igények összegyűjtése, továbbítása (külön kérésre).	felderítés megkönnyítése, sértetti kör és kárérték felmérése

Forrás: Barta Sándor – Székely Gergely: i. m. alapján saját szerkesztés.

11 Barta Sándor – Székely Gergely: Kézikönyv az online piactereken elkövetett visszaélések felderítéséhez. Allegroup.hu Kft., Budapest, 2010

Részint a rendszer biztonsági elemeinek, részint a biztonsági csoport által működtetett, korlátozott hozzáférésű, zárt informatikai rendszernek, a csalófigyelő rendszernek tulajdonítható, hogy bár 2009-ben az átmenő forgalom 17,5 milliárd forint volt, a visszaélésekkel keletkező kár negyvenmillió forint[12].

A tipikus elkövetési magatartások között található a saját kutatásomban külön kategóriaként nem szerepeltetett és a hivatkozott szakirodalomban „ritka esetként" számon tartott jutalékcsalás, amikor az aukciós szolgáltató sérelmére követnek el visszaélést azzal, hogy az eladó hamis adatokkal regisztrál és az aukciós díjat nem fizeti meg.

Primer kutatás

Módszertani alapok

Kutatásom módszertani alapját *Krippendorff*[13], *Langer*[14], *Héra és Ligeti*[15], *Gordon és Langmaid*[16], valamint *Horváth és Mitev*[17] tartalomelemzéssel és (alternatív) kvalitatív kutatási technikákkal és módszerekkel foglalkozó szakirodalma, illetve *Kollár*[18] szakértői kiválasztással és megkérdezéssel foglalkozó tanulmánya adta. A 2017. március 1. és szeptember 1. között végzett kutatásomban a következő módszereket használtam fel:

– szakértői interjúk;
– esetleírásokat tartalmazó dokumentumok szövegelemzése.

Szakértői interjúk

A szakértő fogalmának többsíkú értelmezése (voluntarista, konstruktivista, tudományszociológiai) közül kutatásomban elsősorban a konstruktivista-tudományszociológiai megközelítést alkalmaztam, és a szakértők kiválasztásánál a következő szempontokat vettem figyelembe:

– legalább öt éve dolgozzon nyomozóként vagy vizsgálóként a rendőrségen;

12 Uo.
13 Klaus Krippendorff: A tartalomelemzés módszertanának alapjai. Balassi Kiadó, Budapest, 1995
14 Langer Katalin: Kvalitatív kutatási technikák. Szent István Egyetemi Kiadó, Budapest, 2009
15 Héra Gábor – Ligeti György: Módszertan. A társadalmi jelenségek kutatása. Osiris Kiadó, Budapest, 2005
16 Wendy Gordon – Roy Langmaid: Kvalitatív piackutatás. HVG Kiadó, Budapest, 1997
17 Horváth Dóra – Mitev Ariel: Alternatív kvalitatív kutatási kézikönyv. Alinea Kiadó, Budapest, 2015
18 Kollár Csaba: A szakértővé válás, illetve a szakértői kiválasztás és megkérdezés módszertani kérdései. Vezetéstudomány, 2018/2.

– kiemelkedő szakmai ismerete legyen (az adott munkakörben történő foglalkoztatás feltétele a szakirányú felsőfokú végzettség);
– birtokában legyen a gazdasági-műszaki-informatikai folyamatokhoz kapcsolódó ismereteknek;
– ismereteit folyamatosan bővítse (belső képzések, továbbképzések);
– legyenek értelmező, értékelő, elemző ismeretei, illetve ezeket a módszereket használja (ez ugyancsak a szakmai követelmények közé tartozik);
– a rendelkezésére álló nyomozati anyagok és egyéb források alapján határozott és megalapozott véleményt legyen képes kialakítani;
– véleményét érthetően legyen képes megfogalmazni (rendszerint írásban, ritkábban csak szóban);
– olyan megállapításokat tegyen, amelyek révén a probléma jobban megismerhető.

Tíz, az előbbi feltételeknek megfelelő nyomozóval készítettem félig strukturált szakértői interjút. Az interjúk során kötelező jelleggel hangzottak el a digitális kor próbatételeivel, a bűnözői magatartás megváltozásával, a nyomozás lefolytatásával és a vádemeléssel kapcsolatos kérdések. A kapott válaszok jelentős része kongruált egymással, s a következő öt markáns konzekvencia megfogalmazását tette lehetővé:

1. Erős pozitív korreláció mutatható ki a digitális eszközök (okostelefon, laptop) elterjedése, a rajtuk futó technológiák (3G, 4G, wifi) és alkalmazások (Facebook, online hirdetés) használata, valamint a digitális/elektronikus térben elkövetett csalások száma között.
2. Az elkövetési módszerek egy része nem új, mivel a megvalósítás módja megtalálható a digitális kor előtti időszakban is, igaz, akkor még a szemtől szemben, vagy a nyomtatott médiában megjelenő (apró-) hirdetések révén tévesztették meg sértetteket az elkövetők.
3. A digitális korban elkövetett csalások felderítésénél nehézséget okoz, hogy az esetek egyre nagyobb részénél a) a valódi elkövetők háttérben maradnak (strómanokat használnak fel erre a célra); vagy b) az elkövetők külföldi állampolgárok és/vagy külföldön vannak.
4. Az emberek hiszékenysége nem feltétlenül függ az iskolai végzettségüktől és az életkoruktól.
5. A sértettek általános pszichológiai jellemzői (például nyereségvágy, kapzsiság, manipulálhatóság, érzelmi gyengeség) nem a digitális korban alakultak ki, de a digitális kor hozzájárult bizonyos tulajdonságaik felerősödéséhez.

Az elektronikus csalás bűncselekményekről a szakértői interjúk elemzése révén egy általános képet kaptam, ezután hozzákezdtem a területi és helyi nyomozó hatóságok 2013–2016. évi tevékenységéről szóló beszámolók (kutatói értelemben véve dokumentumok) elemzéséhez.

Esetleírások tartalmi elemzése

Az esetleírásokat tartalmazó dokumentumok szövegelemzésénél a módszertan lehetőségei közül (tartalomelemzés, narratív elemzés, beszélgetéselemzés és diskurzuselemzés) a tartalomelemzést választottam, mivel a területi és helyi nyomozó hatóságok írásos dokumentumai leginkább ebbe a kategóriába sorolhatók be. Célom az volt, hogy egy összetett jelenséget (az online csalások különböző fajtáit) vizsgáljam úgy, hogy a dokumentumok többségében bizonyos eseteket számszerűsítettek ugyan, a dokumentumok tartalma kutatói aspektusból nem tekinthető egységesnek, mivel a megnevezett csalások fajtái nem minden dokumentumban, és nem azonos névvel (besorolás) jelentek meg. Így kutatási vállalásom a csalás jelenségének és fajtáinak bemutatására vonatkozott, és nem az esetek kvantitatív, számszerű, statisztikai módszereket használó elemzésére. A tartalomelemzés lépéseinél Langer[19] ajánlását vettem figyelembe:

1. Kutatási probléma megfogalmazása: a téma alkalmas a tartalomelemzésre, mivel a kapott eredmények révén nevesíteni és így kategorizálni lehet a 2013 és 2016 között elkövetett online csalásokat.
2. Szöveg kiválasztása: az elemzésre szánt szöveg kiválasztásánál két tartalomforrást használtam fel: *a)* a médiában 2013 és 2016 között megjelent, a Magyarországon elkövetett online csalásokkal foglalkozó cikkeket; *b)* a nyomozó hatóságok 2013 és 2016 közötti írásos jelentéseit. Utóbbinál az elkövetők és a sértettek személyazonosságára vonatkozó információkat nem ismertem meg, mivel azonban az esetleírások közel százszázalékos képet adtak a vizsgált időszakban elkövetett online családhoz köthető bűnesetekről, így a két forrást összességében alkalmasnak és elégségesnek találtam a szükséges elemzés elvégzésére.
3. Szöveg átírása: mivel a szövegek leírt formában álltak rendelkezésre, ezért nem kellett az átírással foglalkozni.
4. Kódolás: a szöveg leíró elemzésénél először valamennyi dokumentumot átolvastam, hogy általános képet kapjak, majd az újbóli átolvasáskor már esetkategóriákat alkottam, s arra törekedtem, hogy az adott kategóriához

19 Langer Katalin: i. m.

leginkább illeszkedő leírását adjam meg. Így kaptak az egyes csalásmódok elnevezést, illetve néhány mondatos bemutatást.

A következőkben a dokumentumok tartalmi elemzése során kialakított elkövetési módokat és azok rövid leírását ismertetem.

A fontosabb elkövetési módok

Használati tárgy eladásának ígérete

Az internetes csalás legegyszerűbb esete az, amikor az elkövető valamelyik apróhirdetési oldalon meghirdet egy terméket (rendszerint műszaki cikket, okostelefont, laptopot, tabletet), a sértett a termék vételárát átutalja a megadott bankszámlaszámra, de a megvásárolt terméket soha nem kapja meg, a hirdető pedig megszakít vele minden kapcsolatot (telefonon nem érhető el, e-mailekre nem válaszol).

Webáruházban, apróhirdetési oldalon történő vásárlás

Az esetek egy részében a sértett megkapja ugyan postán a csomagot, amit aláírásával is igazol, de azt csak ezután bontja fel. A csomag tartalma változatos (tégla, sokkal kisebb értékű műszaki, vagy egyéb termék, nem működő, hibás, hiányos termék). Ennél a csalásfajtánál is gyakori, hogy az elkövető – miután a bankszámlájára megérkezik a termék ára – nem elérhető, a telefonszáma nem csöng ki, e-mailekre nem válaszol. Nagyobb értékű, internetes oldalakon hirdetett ingó (gépjármű) és ingatlan (lakásvásárlás, albérlet) vagyonelemek esetében az elkövető előleget, foglalót vesz át, majd miután azt megkapta, nem teljesíti a szerződésben vállalt kötelezettségeit. Bizonyos esetekben megjelenik a jóhiszemű sértett, aki megbízik az ingatlanközvetítőben, akinek átadja a lakás kulcsait, hogy az érdeklődőknek mutassa meg az ingatlant, mivel ő nem ér rá ezzel foglalkozni. Gépjárműveknél a hirdetési oldalon látott fényképek és leírás alapján adja át az előleget/foglalót a sértett az elkövetőnek.

Csereajánlat

Több internetes apróhirdetési oldalon is lehetőség van arra, hogy a termék eladása mellett az eladó/vevő cserében állapodjon meg. Az esetek nem túl nagy

százalékában olyan csalással is találkozni, amikor a sértett a megállapodás értelmében elküldi a terméket, az elkövető azonban vagy nem küld semmit, vagy értéktelen, működésképtelen, sokkal kisebb értékű terméket küld cserébe.

Munkalehetőség ígérete

Ugyancsak az internetes csalások témakörébe sorolhatók azok az esetek, amikor az elkövető – rendszerint külföldi – állást kínál a gyakran az adott nyelvet nem beszélő munkakeresőnek úgy, hogy kiutazás, illetve a munka tényleges megkezdése előtt regisztrációs/közvetítői díjat kér. Az ilyen állások változatosak lehetnek, általánosságban azonban elmondható, hogy végzettséget nem igénylők (például mezőgazdasági kisegítő, építőipari segédmunkás, konyhai kisegítő/mosogató), vagy szakmunkás-bizonyítványhoz kötöttek (például építőipari szakmunkák, mint kőműves, burkoló, tetőfedő, ács, vagy vendéglátóipari szakmunkák, mint szakács, felszolgáló, cukrász, vagy ipari szakmunkák, mint lakatos, esztergályos, marós, hegesztő, gépszerelő). Miután a sértett a regisztrációs/közvetítői díjat befizette, az elkövető vagy nem létező, vagy hamis lehetőségeket küld el neki, vagy ritkábban a sértett csak a kiutazás után szembesül azzal, hogy a hirdetésben közölt feltételek nem vagy csak részben állnak rendelkezésre.

Emelt díjas telefonszám használata

Az emelt díjas telefonszám használatával akkor valósul meg a csalás vétsége, amikor a sértett a telefonszámot felhíva 1. bárki által térítésmentesen elérhető, általános információkat kap; 2. valótlan álláslehetőségeket ajánlanak a számára; 3. szándékosan húzzák a beszélgetés idejét, hogy a sértettnek több telefondíjat kelljen fizetnie. Az emelt díjas telefonszámot korábban nyomtatott, az utóbbi években zömében már online felületen hirdetik.

Javításra adott megbízás

A sértettek az internetes hirdetési felületen megadott címre küldik el a készüléküket (rendszerint okostelefon, tablet, laptop) és gyakran a javítás összegét is, de sem a készüléket, sem a javítási díjat nem kapják vissza. Ennek a csalásnak a másik fajtája az, amikor az elkövető hirdeti magát valamelyik internetes felületen, majd találkozik a sértettel általában valamelyik gyorsétteremben, aki átadja neki a készüléket és a (becsült) javítási díjat. Ezután a csaló nem érhető el.

Sértett hirdet eladásra műszaki cikket

A sértett a műszaki cikket elküldi a megadott címre, az elkövető a fizetési módok közül a banki átutalást javasolja a termék átvétele után. Másik gyakori mód ennél a csalásfajtánál az, amikor a sértett meghirdeti eladásra a telefonját, s olyan hamis igazolást kap, hogy annak ellenértékét a vevő átutalta, de ez nem valósul meg, s időközben ő a terméket már elpostázta. Harmadik ritkább módszer az, amikor az eladó és vevő abban állapodnak meg, hogy a vevő foglalót küld az előadónak (ezt meg is teszi), az eladó válaszul elküldi a terméket, de nem kapja meg a fennmaradó vételárat.

Jegyduplikáció

Az elkövetők az interneten valóban megrendelnek és ki is fizetnek egy jegyet, amivel jogosultak koncerten, vagy egyéb eseményen részt venni. A beléptetőrendszerek úgy működnek, hogy az otthon kinyomtatott jegyen található egyedi azonosító alapján csak egyszeri belépést tesznek lehetővé. Az elkövetők a jegyből több példányt nyomtatnak, amelyet akár az esemény előtt, vagy a (telt házas) esemény helyszínén adnak el a sértetteknek.

Hamis arculati eszközök használata

Bár számukat tekintve ritkább, de tipikusnak tekinthető csalásfajta az, amikor az elkövető megfelelő informatikai tudását használja fel arra, hogy a bűncselekményt megvalósítsa. Ennek egyik legegyszerűbb esete az, amikor valamelyik állami szerv (tipikusan Nemzeti Adó- és Vámhivatal, Országos vagy Budapesti Rendőr-főkapitányság, önkormányzat) arculati elemeinek és eszközeinek (például logó, betűtípus, levélpapír, boríték) felhasználásával – amelyet rendszerint az állami szerv weboldaláról, vagy korábbi hivatalos levelezésből szerez meg – olyan hamis levelet szerkeszt és küld el a sértettnek, amiben felszólítja, hogy az általa elkövetett vétség miatt (például a sértett weboldalán az adatkezelési nyilatkozat nem felel meg a törvényi előírásoknak) fizessen bírságot a megadott bankszámlaszámra.

Hamis bankszámlaszám használata (utalásos csalás)

Az elkövetők rendszerint olyan céget választanak ki, amelyiknél viszonylag nagy összegű, vagy gyakori átutalásos pénzmozgás történik. Az adott pénz-

ügyi osztály munkatársának (nevét, e-mailes elérhetőségét a vállalat nyilvánosan elérhető adataiból, vagy telefonhívás révén szerzik meg) egy céges e-mailt küldenek (rendszerint nem magyarországi doménről, de a vétlen vállalat nevével azonos névvel), hogy a bankszámlaadatok megváltoztak, s a szolgáltatás/termék ellenértékét már az új bankszámlára kérik. Ennél a csalásfajtánál az elkövetők feltérképezik a sértett ügyfélkörét (a vállalat weblapján megtalálhatók), és azt is, hogy a beszállító – akinek nevét kihasználva eljárnak – milyen terméket/szolgáltatást szokott kínálni a sértettnek.

Hamis márkajelzésű termék kereskedelme

Ez is viszonylag gyakori elkövetési módnak tekinthető. Az elkövető online apróhirdetési oldalon, vagy Facebookon nagyon kedvező áron kínál hamis márkajelzéssel ellátott termékeket (rendszerint ruhát, cipőt, órát, divatékszert). A vevő megkapja a terméket, ugyanakkor a hamis márkajelzésű termékek gyártása, forgalmazása, értékesítése már büntetőjogi (például versenytárs utánzása [Btk. 419. §] iparjogvédelmi jogok megsértése [Btk. 388. §]) és szabálysértési következményekkel járhat.

Kedvezőbb hitelkonstrukció ígérete

A banki hitelek kedvezőbb kiváltására, illetve a banki kamatoknál kedvezőbb hitelek felvételére vonatkozó csalás eseteinél megjelenő elkövetési mód az, amikor az adott bank nevében hirdetnek valamilyen apropóból (például a bank születésnapja, EU-s támogatás) hitelfelvételi akciót valamelyik hirdetési oldalon, vagy gyakrabban e-mailben úgy, hogy az akcióban való részvételhez előzetesen közjegyzői/ügyvédi díjat kell átutalni.

Bizalomra épülő csalás

Ritkábban lehet találkozni olyan esetekkel, amikor az elkövetők több sikeres tranzakciót követően válnak bűnelkövetőkké. A kisebb mennyiségű/értékű termékek megbeszélés szerinti leszállításával/postázásával férkőznek az elkövetők a sértettek bizalmába, akiknek idővel rabattot ajánlanak fel, vagy egy drágább terméknél jelentős árkedvezményt adnak, ha viszonylag rövid időn belül (például 12–24 órán belül) a kedvezményes vételárat átutalják a korábban is használt bankszámlára.

Házasságszédelgés, párkapcsolati csalás

Ugyancsak a bizalom kiépítésére és a kapcsolat/ismeretség elmélyítésére alapozzák a csalás vétségét azok az elkövetők, akik különböző internetes társkereső oldalakon regisztrálnak, majd kedves, megnyerő modorukkal a megtévesztett személyek bizalmába férkőznek, s akár több tízmillió forintot is kicsalnak különböző ürüggyel (például beteg szülő, kölcsön a közös lakás megvásárlásához, gépkocsivásárláshoz, amellyel majd egy romantikus kirándulásra mennek).

Hamis személyi adatokkal, vagy személyes adatok klónozásával elkövetett csalás

Az elkövető vagy hamis adatokkal, vagy a sértett digitális lábnyoma (például Facebook) és az ott található tartalmak alapján alkotja meg a személyiségét, majd terméket, szolgáltatást rendel.

Bankkártyával elkövetett csalás

A bankkártyával elkövetett csalások közül a leggyakoribb az, amikor az elkövetők ellopják, vagy a bankkártyatolvajtól megveszik a bankkártyát, majd azzal – még a letiltás előtt – termékeket, szolgáltatásokat vásárolnak. Magyarországon nem annyira jelentős, de több olyan esettel is találkoztam, amikor a bankjegykiadó automata kezelőfelületén helyeztek el olyan, a környezetbe illeszkedő elektronikai-informatikai eszközt, amelyik leolvasta a bankkártya adatait a PIN-kóddal együtt, majd ezek birtokában az elkövetők a bankkártyát klónozták. Az előbbihez hasonlóan jelentős technikai tudást feltételez az az elkövetési mód is, amikor a bankjegykiadó automatát hackelik meg az elkövetők, vagy például az automata billentyűzetének hőmérséklet-változása alapján szerzik meg a kártya PIN-kódját.

Következtetések

A szakértőkkel folytatott interjúk, illetve a közel százszázalékos mintának tekinthető dokumentumok alapján úgy gondolom, hogy az online csalással és annak vázolt, illetve a jövőben megjelenő újabb változataival érdemes és kell is foglalkozni. Az általános, az emberi pszichében és viselkedésben megtalál-

ható jellemvonások alapján egy átlagember is sértetté válhat. Ilyen jellemvonás egyebek között:

– A szűkös jószág megszerzése iránt táplált csillapíthatatlan vágy: amikor valamiből csak egy van (például régiség, festmény), vagy több van ugyan, de az a legolcsóbb (például informatikai eszköz, gépkocsi).
– Kapzsiság, nyereségvágy: az elkövetők a többi termékhez/szolgáltatáshoz viszonyítva kedvezőbb áron kínálják az adott dolgot, rendszerint rövid időtartam alatt, vagy lényegesen nagyobb nyereséggel kecsegtetnek a befektetett pénz után.
– Az ember társas lény, akinek igénye van a társas kapcsolatokra (barátság, szerelem, üzleti kapcsolat), ennek érdekében könnyen belevihető olyan helyzetekbe, ahol a bizalmába férkőznek.
– Figyelmetlenség: a szerzési, birtoklási kényszer miatt az emberek nem figyelnek azokra az árulkodó jelekre (például az eladót még senki nem minősítette, vagy csak negatív minősítést kapott, vagy csak egy-két jó minősítést, a termékleírásban az szerepel, hogy a kép csak illusztráció), amikre egyébként némi figyelem és higgadtság után azonnal rájönnének.
– Kényelem: az emberek többsége törekszik a dolgok (ilyen az online vásárlás) minél gyorsabb, minél egyszerűbb elintézésére, és a kényelem oltárán feláldozza a(z információ-) biztonságot.
– Félelem: még a törvénytisztelő polgárok is feszültté és izgatottá válnak akkor, amikor egy hivataltól levelet kapnak. A tartalmát rendszerint nem kérdőjelezik meg, és a benne leírtak szerint járnak el.
– Hiszékenység: bár a nagyobb online hirdetési oldalak egyre több módszerrel próbálják biztonságossá tenni az ott zajló aukciókat, kereskedelmet, a csalókat – akik például a hamis termékről azt állítják, hogy valódi – nem lehet teljesen kiszűrni. Egy kedves arcú kereskedőnek könnyen elhiszi az ember, hogy a márkatermék valódi, és a pénzért cserébe meg is kapja.

Szinte mindenkivel előfordulhat olyan élethelyzet, amikor nem higgadtan, racionálisan, hanem valamilyen pillanatnyi megérzés, érzelmi érintettség, vagy az átlaghoz képest lényegesen kedvezőbb lehetőség (ígéretének) hatására hoz döntést. Ilyen gyakoribb élethelyzet lehet például

– a munkanélküliség, vagy az az élethelyzet, amikor a munkavállaló nem látja biztosítva a szakmai fejlődését, anyagilag nem becsülik meg, és erősen elgondolkodik azon, hogy munkahelyet váltson. A tömegmédiából és egyéb

forrásokból hallott hírek a kedvezőbb külföldi lehetőségekről (ez igaz egyébként a külföldről rendelt olcsóbb árukra és használt cikkekre is) arra sarkallják az illetőt, hogy külföldön próbáljon szerencsét;
– a különböző banki hitelek miatt eladósodott emberek a kilakoltatástól és teljes anyagi ellehetetlenüléstől való félelem miatt megoldást keresnek a problémáikra. Egyik ilyen megoldás a hitel kiváltása irracionálisan alacsony kamatozású hitellel. A gyakorlatban ilyen hitelt egyik bank sem ad;
– magány, szeretett társ elvesztése, új városba költözés. Az embernek – még az introvertáltabbnak is – szüksége van emberi kapcsolatokra, amelyekre a digitális kor által kínált megannyi platformon is próbál szert tenni.

Összegzés

A tanulmány alapját a Btk. irányadó paragrafusai adják, különösen kriminológiai értelemben a csalásra vonatkozó 373–375. §, mindamellett a csalás fogalmának használatára az egyes tényállásokon túlmutatóan általános értelemben került sor. Az elméleti részben külön kitértem az elektronikus kereskedelemben és online piactereken elkövetett bűncselekményekre, s megállapítottam, hogy ezen oldalak üzemeltetőinek/tulajdonosainak gazdasági érdeke, hogy egy biztonságos online környezetet teremtsenek a vásárlásokhoz, kivéve akkor, ha egyébként a hamis webáruház üzemeltetésével követik el a csalást. Saját kutatásomban két módszert használtam: 1. szakértői interjúk; illetve 2. esetleírásokat tartalmazó dokumentumok tartalmi szövegelemzése. Kutatásom eredményeként megalkottam az online csalás tipikus eseteinek a megnevezését és röviden be is mutattam az egyes eseteket, továbbá megneveztem azokat a fontosabb emberi tulajdonságokat, illetve élethelyzeteket, amelyek okán az emberek könnyen sebezhetővé, kihasználhatóvá válhatnak. A tanulmány célja az volt, hogy az online csalások témakörében rövid áttekintést adjon a téma iránt érdeklődők, vagy azzal foglalkozók számára.

IRODALOM

Barta Sándor – Székely Gergely: Kézikönyv az online piactereken elkövetett visszaélések felderítéséhez. Allegroup.hu Kft., Budapest, 2010

Bogner, Alexander – Littig, Beate: Interviews mit Experten: Eine praxisorientierte Einführung. Qualitative Sozialforschung. Springer, Berlin, 2014

Christián László (szerk.): Információvédelem. Nemzeti Közszolgálati Egyetem, Budapest, 2015

Gordon, Wendy – Langmaid, Roy: Kvalitatív piackutatás. HVG Kiadó, Budapest, 1997

Gyaraki Réka: Számítógépes bűncselekmények és az ellenük való védekezés: In: **Christián László (szerk.):** Információvédelem. Nemzeti Közszolgálati Egyetem, Budapest, 2015

Héra Gábor – Ligeti György: Módszertan. A társadalmi jelenségek kutatása. Osiris Kiadó, Budapest, 2005

Horváth Dóra – Mitev Ariel: Alternatív kvalitatív kutatási kézikönyv. Alinea Kiadó, Budapest, 2015

Ibolya Tibor: A számítástechnikai jellegű bűncselekmények nyomozása. Patrocinium, Budapest, 2012

Kollár Csaba: A szakértővé válás, illetve a szakértői kiválasztás és megkérdezés módszertani kérdései. *Vezetéstudomány,* 2018/2.

Krippendorff, Klaus: A tartalomelemzés módszertanának alapjai. Balassi Kiadó, Budapest, 1995

Langer Katalin: Kvalitatív kutatási technikák. Szent István Egyetemi Kiadó, Budapest, 2009

Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009

Simon Béla: A csúcstechnológiai bűnözés és nyomozása. Nemzeti Közszolgálati Egyetem, Budapest, 2013

INTERNETES FORRÁSOK

http://www.enet.hu/tag/e-kereskedelem

http://hvg.hu/kkv/20170615_Ezekben_a_boltokban_koltjuk_el_a_legtobb_penzt_a_neten

DOI: 10.38146/BSZ.2018.10.5

SIMON BÉLA

Kriptovaluták – rendészeti válaszok[1]

Az optimális rendészeti fellépés érdekében szükséges, hogy legyenek ismereteink a kriptovalutákkal összefüggő jogsértések jelenlegi és prognosztizálható volumenéről.

Az árfolyam meredek emelkedésének az egyik legnagyobb korlátja, hogy a kriptovalutákban nem teljes a bizalom. Időről időre bekövetkeztek olyan tényezők, amelyek megrengették a felhasználók bizalmát. Ezek egy része teljesen független a kriptovalutát fenntartó informatikai hálózatától, de arra jelentős hatással bíró teljesen legális döntés. Ilyenek voltak, amikor számos ország vagy multinacionális vállalkozás elzárkózott a kriptovaluták elfogadásától, vagy betiltotta.

Nem zárható ki azonban, hogy egy-egy kriptovaluta hanyatlásához nem ártó szándékú, hanem helytelen belső piaci döntések vezetnek. Az egyes kriptovaluták nem változatlanul működnek megalkotásuk óta. A bitcoint – mint a legjelentősebb kriptovalutát – fenntartó szoftvernek tizenhat fő továbbfejlesztett verziója készült el 2018 júniusáig. A bitcoin üzemeltetése felett hatalmat gyakorló szervezetek döntésén múlt az is, hogy 2017. augusztus 1-jén az addig önállóan fejlődő bitcoinblokklánc kettéágazott, és kivált belőle a bitcoin cash[2]. Ez a döntés nem ingatta meg a bitcoinba vetett bizalmat, de nem kizárható, hogy a későbbiekben az egyes kriptovaluták kibocsátói, fejlesztői helytelen döntéseikkel viszik hanyatlásba az egyes kriptovalutákat, vagy olyan új kriptovaluták jönnek, amelyek letaszítják a jelenleg értékes digitális pénzeket.

Az egyes kriptovaluták – és a bennük felhalmozott érték – tehát ártó szándék nélkül is könnyen elszenvedhetnek hatalmas árfolyamvesztéseket, elértéktelenedést.

A kriptovaluták árfolyamát nagyon jelentősen visszavető illegális tevékenységek is jelentkeztek a múltban. Volt példa arra, hogy bitcoin kereskedelmével

1 A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, *A jó kormányzást megalapozó közszolgálat-fejlesztés* elnevezésű kiemelt projekt keretében működtetett Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

2 A bitcoin utalási költségeinek és időigényének emelkedése miatt a kis összegű, nagy számú tranzakciók gyors végrehajtását célzó technológiai változtatással egy új kriptovalutát hoztak létre. Akinek az elágazás előtt volt bitcoinja, az ez után ugyanannyi bitcoin casht is kapott a tárcájába.

foglalkozó tőzsde üzemeltetői a kezelésükre bízott bitcoinnal sajátjukként rendelkeztek, és eltérő adatokat mutattak az ügyfeleknek, mint amekkora az összeg valójában volt. Volt arra is példa, hogy egy jelentős forgalmú tőzsde informatikai rendszerét támadás érte, és megsemmisültek a tárcaadatok.

Tekintsük át, hogy összességében milyen illegális folyamatok, cselekedetek vezethetnek a felhasználók, tulajdonosok sérelméhez!

A blokklánc-technológiából adódó veszélyek

A kriptovaluták belső működéséből, a blokklánc-technológiából eredő veszély elméletileg elenyésző.

A blokklánc-technológia – különösen a bitcoin esetében – a matematikai algoritmus, a számítógépes program következtében védve van a visszaélések ellen. A privát kulcs „kitalálásának” esélye a program oldaláról szinte zéró[3]. A kriptovaluták értékét éppen az adja, hogy a tudomány mai állása szerint szinte hamisíthatatlanok, feltörhetetlenek. A blokklánc hamisításához olyan számítási kapacitásra volna szükség, amely erősebb a jelenleg a rendszerben működő összes csomópont teljes számítási kapacitásánál[4]. A technológiából származó sérülékenységek azonban léteznek. Tekintettel arra, hogy ezek a visszaélések olyan szintű informatikai ismereteket igényelnek, amely meghaladja e tanulmány jellegét és kereteit, ezért bemutatásukra csak példálózva és érintőlegesen kerül sor.

Kétszeres elköltés

Visszaélésre ad lehetőséget – jellemzően a bitcoin esetében –, ha valaki a blokklánc véglegessé válása előtt egy újabb transzferálást végez. Mivel az egyes blokkokat a feldolgozó számítógépek nem feltétlenül a beküldés sorrendjében dolgozzák fel, ezért lehetséges, hogy az elkövető egy személyes találkozón a kriptovalutáért kapott pénz átvételekor a telefonján vagy a laptopján elindítja az utalást, majd néhány percen belül átutalja a teljes számlaegyenlegét egy másik tárcára úgy, hogy a kéréseket feldolgozó és a blokkláncot generáló számítógépek számára (mivel erre van lehetőség) na-

3 Bár a kvantumszámítógépek fejlesztésével lehetséges, hogy például egy RSA algoritmussal kódolt adat is rövid időn belül feltörhető lesz.

4 Ez az úgynevezett 51 százalékos támadás, ami egyéb hackertechnikával (a rendszer két részre szakításával) akár 33 százalékos számítási kapacitással is lehetséges.

gyobb összegű felajánlást tesz a blokkba foglalásra és véglegesítésre. Ekkor előfordulhat, hogy a korábban kezdeményezett utalás nem teljesül a tárca üressége miatt.

A decentralizált autonóm szervezet

A bitcoin utáni legnagyobb kapitalizációval bíró altcoin az ethereum, amely egy világméretű decentralizált hálózat létrehozatalán túl lehetőséget teremtett az úgynevezett okosszerződések megkötésére, amikor a tranzakciók valamilyen feltétel bekövetkezésétől teljesülnek[5]. Az ethereumban lehetőség van ICO-k *(Initial Coin Offering)* kibocsátására, ami egy-egy kriptográfiával megtámogatott közösségi finanszírozási modell. Egy ilyen ICO a decentralizált autonóm szervezet *(Decentralized Autonomous Organization; DAO),* ami arra gyűjtött támogatásokat, hogy az abban részt vevők a közvetlen demokrácia eszközével dönthettek, támogatnak-e, vagy sem egy projekteket, és döntéseiknek megfelelően részesülnek a sikerből.

Amiért a decentralizált autonóm szervezet fontos témánk szempontjából, az az, hogy 2017 júliusában az összegyűjtött 170 millió amerikai dollár értékű ethereum kriptopénzből (ether) 53 millió amerikai dollár[6] értékben utalt magának egy személy az algoritmus hibáját kihasználva. A vélemények még abban is eltérnek az eset kapcsán, hogy mennyiben volt szabálytalan/jogellenes az utalás, hiszen nincsenek előírások ezeknek a tranzakcióknak a szabályos lebonyolítására. A tranzakciót megvalósító személy az algoritmusban rögzített feltételek szerint cselekedett, azaz utalta saját részére a kriptovalutákat, így bár az alkotók szándékával ellentétes volt a transzferálás, de nem volt szabályrendszer, amelyet sérteni kellett a művelethez.

A konszenzus elleni támadások

Ezeknél az a lényeg, hogy a blokkláncot létrehozó számítógépek közti megállapodásban érnek el olyan tranzakciókat, amelyek rendes működés mellett nem következnének be. Szükséges hozzá a rendszerben működő eszközök feletti irányítási jog, vagy a kriptográfia feltörése, de mindkettőnek rendkívül kicsi az esélye.

---

5 https://www.ethereum.org/

6 David Siegel: Understanding The DAO Attack. Coindesk.com, Jun 25, 2016. https://www.coindesk.com/understanding-dao-hack-journalists/

Sybil-támadás

Sybil-támadásnál a támadó előállít egy szimulált P2P bothálózatot, amivel megpróbálja a decentralizált konszenzust befolyásolni, azaz a blokkláncot fenntartó számítógépeknek azt a látszatot kelti, hogy az általa irányított hálózat a teljes blokkláncot tartalmazó teljes csomópont, pedig valójában nem.

Maginot-vonal-támadás

E támadási forma nem a számítási kapacitással kapcsolatos, hanem a lekötött kriptovaluta összegétől függ. Ha az összes lekötött összeg 51 százalékát leköti az elkövető, akkor lehetősége van az összeget kétszer elkölteni, ezáltal összeomlasztani a kriptovalutát. Ez a kriptovalutát fenntartó informatikai rendszer működéséből adódik. A lényege, hogy hatalmas összeget kellene arra fordítani, hogy megvalósulhasson, és az eredménye az volna, hogy a kriptovaluta teljesen elértéktelenedik, így megvalósulásának esélye elenyésző.

DDoS-támadás

A blokklánc fenntartásáért felelős hálózati eszközök, számítógépek elosztott túlterheléses támadásával akadályozható a rendszer, de széttagoltsága miatt nem következhetnek be nagy károk, inkább csak a szolgáltatás ideiglenes lassulása[7].

Az előbbieken túlmenően is léteznek elméletben támadási metódusok a blokklánc-technológia ellen, de azok megvalósításának esélyei szintén csekélyek.

Az informatikai eszközökből származó veszély[8]

E körbe sorolhatjuk azokat az elkövetési magatartásokat, amikor nem a blokklánc-technológia esetleges sérüléseit kihasználva, hanem a kriptovalu-

7 Trinh Anh Tuan – Szegő Dániel: Ezek a legvadabb módszerek, amelyekkel kifosztják a bitcoinosokat. Portfolio.hu, 2018. április 24. https://www.portfolio.hu/vallalatok/it/ezek-a-legvadabb-modszerek-amelyekkel-kifosztjak-a-bitcoinosokat.282664.html

8 Természetesen a blokklánc-technológiát működtető hálózat elemei is informatikai eszközök, de a könnyebb megértés érdekében célszerű különválasztani az üzemeltetői oldalt (blokklánc-technológia működtetői) és a felhasználói oldalt (kriptovaluta-tulajdonosok).

ták megszerzésének, tárolásának, transzferálásának folyamata során használt informatikai eszközöket éri támadás.

Ezek a támadások jellemzően olyan sérülékenységeket, kompromittálási lehetőségeket használnak ki, amelyek a kriptovalutáktól függetlenül is léteznek.

Ebben az esetben célszerű az egész folyamatot végigtekintenünk, és kiemelni a gyenge pontokat.

Az átlagos felhasználó a kriptovalutára nem bányászat útján[9] tesz szert, hanem valamilyen formában vásárolja. A vásárláshoz egy tárca alkalmazást használ. A nem megbízható forrásból telepített tárca alkalmazások önmagukban tarthatnak olyan kódokat, amelyek arra szolgálnak, hogy a manipulált tárca alkalmazás által tárolt kriptovaluták felett az elkövetők átvegyék az irányítást.

Ha az alkalmazás megbízható forrásból származik, és a privát és publikus kulcs generálása is szabályosan – egyedi és befolyástól mentes formában – megtörténik, akkor a felhasználó ezt a sérülékeny pontot átlépte. Ha azonban a kulcsok generálását valamilyen nem megbízható forrásra bízza, akkor a beszerzett kulcspárt az elkövetők bármikor felhasználhatják, amikor azt látják a blokkláncon, hogy azon jelentősebb értékű kriptovaluta jelent meg. Például ha egy erre kifejlesztett oldalon az elkövetők naplózzák a magmondatok segítségével, vagy bármilyen módon generált kulcspárokat, akkor nincs más teendőjük, mint folyamatosan ellenőrizni, hogy megjelennek-e a publikus kulcsok a blokkláncon[10].

De a generált kulcspárok bármilyen informatikai eszközön bármelyik létezési formájukban elméletileg megszerezhetők: a vágólapra másolt kódsorokat, a papír tárcaként kinyomtatni szándékozott fájlokat a nyomtatóra küldés előtt, vagy a nyomtatót kompromittálva lehetőség nyílik az ártó szándékú beavatkozásra.

Kriptovalutákat érintő kártékony kódként detektáltak olyan – az operációs rendszer sérülékenységét kihasználó malware-t, amely a háttérben futva folyamatosan figyeli, hogy mikor helyez a felhasználó vágólapra egy publikus kulcsot, majd amikor a beillesztésre kerül sor, akkor a sértett már az elkövetők által meghatározott kódsort – azaz saját publikus kulcsukat – illesz-

9 Nagy számítási kapacitású számítógépek, vagy célhardverek (berendezésorientált áramkör, Application-specific integrated circuit; ASIC) használatával megvalósított eljárás, amelynek eredménye, hogy a blokkláncban megjelenik a bányászatot végző számára bizonyos mennyiségű kriptovaluta.

10 Legálisan is működnek olyan szolgáltatások, amelyek e-mailt küldenek a regisztrált személynek, ha az általa követni szándékolt publikus kulcs megjelenik a blokkláncban.

ti be. Mivel a kódsorok nehezen megjegyezhetők és könnyen összekeverhetők, ezért a sértett már csak a teljesített utalás után észleli, hogy kriptovalutáját nem szándékolt tárcába utalta.

A szolgáltatók igénybevételével használt online tárcák esetében azok az információs rendszereket érő visszaélési formák lehetségesek, amelyek például az internetes bankolásnál megvalósulhatnak.

A különbség azonban nagyon lényeges: egy internetes bankolás során megvalósuló visszaélésnél az illegálisan utalt összeget vissza lehet származtatni, a készpénzfelvételt meg lehet akadályozni, és még a pénzintézet is kártalaníthatja a sértettet. A kriptovaluták világában azonban ez nem így van. Az transzferálás nem visszavonható, jellemzően nem kapcsolható konkrét személyhez, és a szolgáltatók tipikusan nem vállalnak kötelezettséget a kártalanításra.

Bár a kriptovaluták tárolására a hardveres tárcákat tartják az egyik leginkább megbízható formának, mégis előfordulhat ezek sérülékenysége, még ha ennek esélye meglehetősen kicsi is[11].

Az informatikai eszközök kompromittálásával megvalósuló visszaélések között említhető a korábbi terminológia szerinti „gépidőlopáshoz”[12] hasonló elkövetés, amelyben az elkövetők különféle kártékony kódokkal, *script*ekkel arra bírják rá a sértett informatikai eszközeit, hogy azok kriptovalutákat bányásszanak[13]. A tevékenység nem a kriptovaluta-tulajdonosokat sérti ugyan, és nem okoz jelentős kárt, de büntető törvénykönyvünkbe ütköző.

Természetesen nem csak ügyfél oldalon vannak kitéve az értékek a kiberbűnözőknek. Több esetben előfordult, hogy az ügyfeleiknek forró tárcát, vagy tőzsdei kriptovaluta-szolgáltatást nyújtó szolgáltatók informatikai rendszereit kompromittálták az elkövetők, és megsemmisítették a tárcaadatokat, vagy maguknak transzferálták azok állományát.

Utóbbi visszaélésekre az ad lehetőséget, hogy e szolgáltatóknak nincsenek olyan nemzetközi szabványaik, mint például a bankkártya-üzletágban megszokott előírások[14].

---

11 Andriana Gkaniatsou: Bitcoin hardware wallet vulnerability exposes funds to hackers: study. https://www.ed.ac.uk/files/atoms/files/bitcoin_wallet_devices_vulnerable_to_security_hacks_study_shows_23.01.2018.pdf

12 Szathmáry Zoltán: Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2012, 100. o.; Nagy Zoltán: Az informatika és a büntetőjog. Magyar Jog, 1991/1., 21–26. o.; Nagy Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok, 1992/1., 22–26. o.

13 https://news.bitcoin.com/hackers-target-400000-computers-with-mining-malware/

14 PCI DSS bővebben lásd https://www.pcisecuritystandards.org/pci_security/

Tehát a kriptovalutával megvalósított ügyleteknél használt informatikai eszközök (telefonok, asztali számítógépek, laptopok, szerverek, okosórák, pendrive-ok) esetén nagyon fontos azok integritásának megléte[15].

E visszaélések megelőzésére az információbiztonsági tudatosság fejlesztése a leghatékonyabb eszköz. A bekövetkezett visszaélések felderítésére a kimagaslóan képzett nyomozó hatósági munkatársak és a piaci szereplőkkel való szoros együttműködés ad lehetőséget.

Kriptovaluta a bűnös vagyon tárolására és a pénzmosás

Ebben az esetben a konkrét cél jellemzően nem a kriptovaluta megszerzése, hanem a más elkövetésből származó illegális bevételeket az elkövetők kriptovalutába fektetik, majd a későbbiek folyamán saját céljaikra, vagy más jogsértő cselekmények (például terrorizmus) finanszírozására fordítják[16].

Ily módon a bűnelkövető nagy valószínűséggel elvonhatja a hatóságok intézkedései elől a megszerzett illegális javakat, ezáltal csökkenti a nyomozás eredményességét, meghiúsítja a vagyon elvonását, a sértettek polgári jogi igényének kielégítését.

A pénzmosás már a bitcoinnal kapcsolatos legkorábbi tanulmányok során is felvetődött kockázati tényezőként[17], és azóta is az egyik legtöbbször emlegetett veszélyforrásnak tekinthető a kriptovaluták és a kriminalitás kapcsolatát vizsgáló értekezésekben[18]. Mindennek egyik legfőbb oka, hogy az utóbbi huszonöt évben a pénzmosás elleni közös nemzetközi fellépés fő irányvonala az volt, hogy a pénzügyi közvetítő szolgáltatókat ügyfél-azonosítási és gyanús pénzmozgások bejelentésére irányuló kötelezettségekkel terhelték, a kriptovaluták a decentralizáltságukkal pedig elegánsan kiléptek az e szabályok hatóköre alól.[19] Vélhetően jó részben ez is az oka annak, hogy amikor egy-egy jogalkotó rászánja magát manapság kriptovalutákkal kapcsolatos normák megalkotására, ezt mindenekelőtt a pénzmosás elleni küzdelem je-

15 Muha Lajos: A kritikus információs infrastruktúrák védelme. Reinet Technológia Kft., Budapest, 2015

16 Természetesen itt elmosódik a határ azokkal a bűncselekményekkel, amelyek esetében eleve a bitcoin megszerzése a cél.

17 Lásd például Reuben Grinberg: Bitcoin: An Innovative Alternate Digital Currency. In: Hastings Science & Technology Law Journal, vol. 4, no. 1, 2011, p. 204.

18 Gyaraki Réka: Az ördög pénze? A Bitcoin. Detektor Plusz, 2016/23., 1–3. o. http://detektorplusz.hu/index.php?m=23458

19 Robert Stokes: Anti-money laundering regulation and emerging payment technologies. In: Banking & Financial Services Policy Report, vol. 32, no. 5, 2013, p. 3.

gyében teszi[20] (mint ahogy láthattuk ezt az európai pénzmosás elleni irányelv legutóbbi módosítása kapcsán is)[21].

A pénzmosással kapcsolatos vádak vonatkozásában a kriptovalutákkal összefüggésben az azokat támogató személyek érvei között is megjelenik, hogy a készpénz sokkal inkább alkalmas e tevékenység folytatására, de könnyű rejthetősége, gyors és olcsó transzferálása a kriptovalutákat könnyebben alkalmazhatóvá teszi e célra.

A kriptovalutákat pénzmosásra nemcsak anonimitásuk okán érdemes az elkövetőknek használniuk, hanem amiatt is hogy egyre több helyen lehet közvetlenül ellenszolgáltatást teljesíteni általuk[22].

Az ellenőrző/felügyeleti rendszer hiányából adódó veszély

A pénz- és tőkepiacok ártalmas befolyásolásának korlátozására számos jogintézmény kialakítására került sor az elmúlt évszázadokban. Az egyik legfontosabb, hogy a résztvevők körének jellemzően egy szűrésen kell átesnie[23]. A kriptovaluták esetében nem működik ilyen módon a belépési korlát. Jelentős online jelenléttel és marketinggel a hozzáértés szinte pótolható. A másik jelentős veszélyforrás, hogy nincsen jegybanki rendszer és intézkedési lehetőség az árfolyamok befolyásolására. A hatalmas árfolyammozgások akár csalárd szándékkal is előidézhetők, de a rendszer normális működéséből is következhetnek[24]. A kriptovaluták jogi szabályozása nem megoldott. Nem alakult ki egységes jogalkalmazói gyakorlat az esetlegesen fellépő jogviták orvoslására.

---

20 Ne tévesszen meg senkit, hogy a pénzmosás esetén a magyar szabályozás következetesen bűncselekményből származó *dologgal* kapcsolatos cselekményekről rendelkezik. A dolog fogalma itt nem a Ptk.-ban használatos dologfogalommal egyenértékű, hanem a szabályozás az alapját képező, 1990. november 8-án, Strasbourgban aláírt nemzetközi egyezményben szereplő dologfogalmat emelte át. Ez magában foglalja a megfogható és megfoghatatlan dolgokat egyaránt, és a kihirdetésről szóló 2000. évi CI. törvénnyel a magyar jogrendszer részévé is vált. Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. Különös rész. HVG-ORAC, Budapest 2013, 738–739. o.

21 Halász Viktor: Kriptovaluták a bűnüldözésben. Új kihívások és lehetséges válaszok. Diplomamunka. Nemzeti Közszolgálati Egyetem Nemzetközi és Európai Tanulmányok Kar, Budapest, 2018, 40. o.

22 https://coinmap.org

23 Például értékpapírok tőzsdére bekerülése, vagy kereskedelmi bank alapítása számos feltétel teljesítése után lehetséges.

24 A 317 amerikai dollárról 0,1 amerikai dollárra esés a piaci működés következtében. https://blog.gdax.com/eth-usd-trading-update-5d8142b5bdc1

A büntető törvénykönyv számos tényállást tartalmaz, ami a gazdaság jogszerű működését hivatott védelmezni:

– belépési küszöb védelmére hivatott a jogosulatlan pénzügyi tevékenység[25] bűncselekményének pönalizálása[26];
– a bennfentes kereskedelem bűntette[27], bennfentes információ jogosulatlan közzétételének vétsége[28], illetve tiltott piacbefolyásolás bűntettét[29] elkövethetnék mindazon személyek, akik álhírekkel, publikációkkal, egy-egy kriptovaluta dömping jellegű felvásárlásával, értékesítésével olyan módon befolyásolják az árfolyamot, amely tisztességtelen és jellemzően a többi befektető kárából jogtalanul maga vagy a megbízottja tesz szert vagyoni előnyre.

E tényállások azonban csak akkor vehetők figyelembe, ha a kriptovaluták pénzügyi eszközöknek minősülnének. Sem a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló törvény[30], sem a tőkepiacról szóló törvény[31], sem a Magyar Nemzeti Bank pénzügyi eszközök jegyzéke[32] nem minősíti a kriptovalutákat pénzügyi eszközöknek.

Ha azonban a kriptovaluta kibocsátója gazdálkodó szervezet és valaki e gazdálkodó szervezet vagyoni helyzetéről vagy vezető állású személyéről e tevékenységével összefüggésben valótlan adat közlésével vagy híresztelésével, illetve adat elhallgatásával másokat tőkebefektetésre vagy a befektetés emelésére, illetve tőkebefektetés eladására vagy a befektetés csökkentésére rábír – akkor a magatartása tényállásszerű lehet a kriptovalutákra vonatkozóan is, és elkövetheti a tiltott piacbefolyásolás bűntettét[33].

25 A büntető törvénykönyvről szóló 2012. évi C. törvény 408. §.

26 A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény szerinti pénzügyi szolgáltatási vagy kiegészítő pénzügyi szolgáltatási tevékenység körében értékelhető sok olyan tevékenység, amely a kriptovaluták váltásával, kereskedelmével foglalkozik.

27 Btk. 410. §

28 Btk. 410/A §

29 Btk. 411. §

30 2007. évi CXXXVIII. törvény

31 2001. évi CXX. törvény

32 https://www.mnb.hu/felugyelet/szabalyozas/mifid-mifir/penzugyi-eszkozok-jegyzeke/penzugyi-eszkozok-jegyzeke-2018/penzugyi-eszkozok-jegyzeke-2018-marcius

33 Bár e tényállás az elmúlt öt éveben a Belügyminisztérium Bűnügyi Statisztikai Rendszere szerint egyszer sem valósult meg, így nehezen elképzelhető, hogy a kriptovalutákkal összefüggésben a regisztrált bűncselekmények közt megjelenne.

A kiberbűncselekményekkel foglalkozó sajtó az elmúlt évben gyakorta tudósított az ICO-kkal[34] mint startup vállalkozásokkal kapcsolatos visszaélésekről.

A Magyar Nemzeti Bank tájékoztatása szerint *„Akár befektetett tőkéjük egy részét vagy egészét is elveszthetik azok az ügyfelek, akik tokeneket vásárolnak nyilvános ICO forrásgyűjtés keretében tőkebevonásra, cégfejlesztésre hivatkozó személyektől. Az MNB és az Európai Értékpapír-piaci Hatóság is folyamatosan figyelmeztet – az egyre inkább terjedő – befektetés jelentős kockázataira.”*[35] Az ICO-k jelentős kockázatot hordoznak magukban, tekintettel arra, hogy a legtöbbször csak egy ötlet létezik, és semmilyen megvalósítási feltétel nem adott, a befektetők pedig könnyelműen bíznak a projekt sikerében mindenféle ellenőrzés nélkül. Emiatt az ICO-kibocsátások nagy része pénzügyileg bukás a befektetők számára[36].

Sok esetben előfordult, hogy a befektetések összeomlásakor a befektetők hiszékenységét kihasználva és az adott kibocsátó munkatársának kiadva magukat, az elkövetők arra kérték a károsultakat, hogy további regisztrációs díj, vagy a tárca azonosítása céljából küldjenek kisebb összegű kriptovalutát – jellemzően ethert. Ezáltal az egyébként is károsult személyeket további vagyonelemtől fosztották meg.

A visszaélések megakadályozása érdekében szükséges volna megelőzésként széles körű tájékoztatást végezni azon célcsoportok körében, amelyek vélhetően kriptovalutákkal összefüggő üzleti befektetéseket hajtanak végre. Az elmúlt időszak – de leginkább a bitcoin 2017-es szárnyalása – vélhetően Magyarországon is sok olyan embert csábított kriptovaluta vásárlására, akinek a rendszer működésével összefüggésben nincs széles körű tapasztalata. Fontos, hogy az ezzel kapcsolatos konferenciákon, internetes fórumokon jelenjenek meg magyar nyelven is azok az információk, amelyek gyanút ébresztenek például egy-egy rendkívül csábító ICO-val összefüggésben.

Kriptovaluták mint a bűnelkövetés segédeszközei

A kriptovaluták és leginkább a bitcoin egyik legnagyobb visszhangot kiváltó megjelenési formája a darknetes kereskedelemben történő felhasználás. A Silk-

34 Ezekről információt az icodrops.com oldalról is lehet gyűjteni.

35 https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/rendkivuli-kockazatot-hordoznak-az-ico-befektetesek

36 Horváth Ferenc: A kriptovalutákkal történő visszaélések. Szakdolgozat. Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2018, 16. o.

Road nevű platform 2013-as felszámolásakor megállapították, hogy az illegális áruk és szolgáltatások óriási volumenű kereskedelme zajlott, és az ellenérték kiegyenlítésére szinte kizárólag bitcoint használtak. Kriptovaluták hiányában a darknetes kereskedelem semmiképp nem fejlődhetett volna ilyen szintre.

Az elmúlt időszakban számos hasonló szolgáltatás indult a torhálózat[37] által fenntartott internetes felületen. Ezekkel összefüggésben számos olyan eredményes nemzetközi nyomozás fejeződött be, amelyekben a hatóságoknak sikerült az ügyletekben részt vevők széles körét beazonosítaniuk és eljárás alá vonniuk.

Az ilyen jellegű bűncselekményekkel szemben szoros nemzetközi együttműködés, a titkosszolgálati eszközök összehangolt alkalmazása és a legjobb gyakorlatok megosztása vezethet eredményre. Ezek részletes bemutatása azonban nem része e tanulmánynak.

Csalás jellegű veszélyek

Amint említettem, a kriptovalutákkal összefüggésben jelentős online jelenléttel, keresőoptimalizálással, micro-targeting[38] módszerekkel elérhető, hogy a célcsoport folyamatosan olyan hirdetésekkel találkozzon, amelyek látszólag valamilyen kiváló üzleti lehetőségről szólnak, de valójában hólabda-[39] csalások, piramisjátékok[40], vagy egyszerű csalások.

Az elkövetők számos csalási metódust alkalmaznak, amelyek a blokklánc-technológiával kapcsolatos kifejezések használatával hihetővé teszik a sértettek számára a tettes által közvetítetteket.

Például:

– kriptovaluta közös bányászatára vonatkozó felhívás a kezdeti költségek megelőlegezésével valós bányászati kapacitás nélkül;

37 https://www.torproject.org/

38 https://policyreview.info/articles/news/political-micro-targeting-hijacking-european-democracy/753

39 E csalástípusnál a sértettektől jelentős hozam ígéretével gyűjtenek az elkövetők pénzt befektetésre, miközben valós gazdasági lehetőségeik nem adnak alapot a hozam garantálására. Az esetleg kivett összegekre a kezdeti időszakban a többi sértett betétjéből történik hozamkifizetés. Kellően nagy összegű betét összegyűjtése után az elkövetők azzal sajátjukként rendelkeznek.

40 A rendszer működéséhez szükséges, hogy az abba belépők vagyoni hozzájárulást teljesítsenek a rendszerbe, majd újabb személyeket vonjanak be, akik szintén vagyoni hozzájárulást teljesítenek, és beszerveznek további személyeket. A több szintű marketing (Multi Level Marketing) rendszertől az különbözteti meg, hogy piramisjáték esetében a beszervezettek a befizetett összegért nem kapnak értékkel bíró dolgot.

– színleg már működő kriptovaluta-bányászati kapacitás lekötése garantált nyereséggel a kezdetben befizetett költségek megfizetése után[41];
– az elkövető az általa fejlesztett speciális (titokzatos) algoritmus által prognosztizálni tudja a kriptovaluták árfolyammozgását, és garantálja a rendkívül magas hozamot (szintén hólabdacsalás). Erre jó példa a BitConnect esete, amikor egy valós blokklánc-technológiához egy piramisjátékot szerveztek azt ígérve, hogy egy speciális kereskedőalgoritmus segítségével a cég a betett összegek után több ezer százalékos éves hozamot képes elérni, amihez az is szükséges, hogy a befektetők meghatározott ideig ne vegyék ki betéteiket, és további betéteseket szervezzenek be[42];
– valamilyen véleményformáló, vagy gazdag személynek kiadva magát az elkövető arról ad tájékoztatást, hogy mindenkinek küld jelentős mennyiségű kriptovalutát, de a transzferáláshoz szüksége van a sértettek publikus kulcsára, ezért teljesítsenek egy kis értékű kriptovaluta-utalást az elkövető által megjelölt tárcába;
– scamcoinok – csalás jellegű kriptovaluták esetében az elkövetők létrehoznak egy altcoint – egy új kriptovalutát –, majd annak jelentős részét kibányásszák. Ez után megfelelő marketingeszközök használata mellett elkezdenek a saját tárcáik között egyre magasabb árfolyamon kereskedni a kriptovalutával. Ha megfelelően sok külső befektető is vásárol az egyébként értéktelen kriptovalutából, akkor az elkövetők kiszállnak az illegális profittal[43];
– „nigériai levél” jellegű csalások, amikor is e-mailben, vagy más formában arra bírják rá a sértettet, hogy a diktátor mesés vagyonának utalásához, vagy az afrikai szépség kiszabadításához, vagy hatalmas nyeremény, örökség utalásához a szükséges „csekély” értékű kriptovalutát transzferálják az elkövető tárcájába;
– működnek olyan vállalkozások is, amelyek a kriptovaluta látszatát keltve betétet gyűjtenek, és jelentős hozam ígérete mellett buzdítják a betéteseiket újabb betétek fizetésére és további személyek bevonására. Ennek ellenértékeként az elkövetők által kifejlesztett „kriptovalutát” kapják. Valójában a

41 A sértetteknek nem tűnik fel, hogy vajon miért adja át kriptovaluta bányászati kapacitását a felajánló negyven amerikai dollár értékben, ha magának is bányászhatna ez idő alatt százdollárnyi értékűt. Ha azonban megbízható vállalkozás a kapacitása bővítésére gyűjt pénzt, akkor az üzleti megoldás lehet legális és rentábilis is.

42 Az elkövetésben keveredett a hólabda csalás, (amikor csak irreálisan nagy hozamot ígért a befektetőknek valós gazdasági tevékenység nélkül), illetve a piramisjáték szervezése (amikor a várt jutalmat/eredményt más személyek beszervezése, betéte által lehet elérni).

43 Hasonlít a tiltott piacbefolyásolásra, de ebben az esetben az egész altcoin létrehozása a csalást szolgálja.

kibocsátott saját „kriptovalutának” nincs valós értéke, valódi pénzre való átváltása nem lehetséges, és nem a blokklánc-technológiától, hanem csak a kibocsátótól függ, mennyi van belőle[44];

– lehetséges olyan pénzügyi szolgáltatás csalárd indítása is, amelyben az „ál-szolgáltató” azt a látszatot kelti, hogy az ügyfelei által részére utalt valódi pénzből az ügyfelek számára forró tárcát tart fenn – azaz az ügyfél csak a publikus kulcsát látja webes felületen, vagy csak a számlaegyenleget –, majd amikor kellő számú betét gyűlt össze, akkor a virtuálisan létező és egyébként üres tárcákat magukra hagyják, és az ügyfelek befizetéseit sajátjukként használják az elkövetők;

– mint említettem, a kriptovaluták kapcsán ugyanolyan elkövetési magatartások lehetségesek, mint az internetes bankolásnál. A forró tárcák esetében is előfordulhat, hogy az elkövetők e-mailben kérik a sértettet arra, hogy a küldött linken keresztül a publikus kulcs mellett adja meg jelszavát is az azonosításhoz[45];

– lehetséges a csalás elkövetése offline is. Az elkövetők internetes fórumon eladásra kínálnak nagyon kedvező áron kriptovalutát, amelyet személyes találkozó keretében kívánnak értékesíteni. A találkozón az elkövetők a pénz sértettől történő átvétele után látszólag az ügyletben szereplő kriptovalutát transzferálják, majd elhagyják a helyszínt. Az ügylet tárgya azonban soha nem érkezik meg a vevőhöz. Hasonló módon valósulhat meg lopás vagy akár rablás is.

A csalás jellegű bűncselekmények esetében több esetben előfordult, hogy a tettes – felkészülve a csalásból származó javakra – az elkövetés előtt bitcoinvásárlást kezdeményez valamely online kriptovaluta-váltónál, majd a váltó által – általában e-mailben – megküldött bankszámlaszámot a vásárlás azonosításához szükséges közleménnyel úgy küldi tovább a sértettnek, mintha az a sajátja lenne (kéri természetesen a közlemény feltüntetését is). Az összeg beérkezése után a váltó abban a hitben van, hogy a fizetést az elkövető végezte, így a bitcoint elutalja a tettes által megadott címre. Ezek a szolgáltatások nagyban megnehezítik minden bűncselekmény felderítését, amikor is az elkövetők célja a haszonszerzés. Ezzel összefüggésben számos tényállás felvetődhet a sorozatjellegű aukciós csalásoktól a terrorcselekményig. Az a különlegessége, hogy a pénzvál-

44 Például a OneCoin. Bővebben lásd www.onecoin.eu; https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/a-onecoin-elleni-fellepesrol-targyalt-a-piacfelugyeleti-munkacsoport

45 Ezekben az esetekben is a kétfaktoros azonosítás megakadályozhatja a visszaéléseket.

tók tevékenységének pillanatában a bűnös forrásból származó előny egy mozzanatban válik elérhetetlenné a sértett számára és válik a nyomozó hatóság számára nehezen elérhetővé. Mindez úgy valósul meg, hogy az alapügy elkövetője csak nagyon rövid ideig tevékeny az elkövetésben[46].

Mint látható, a csalás jellegű visszaélések közt nincs sok újdonság. Ugyanazok a sémák jelennek meg, de a kriptovalutákba vetett túlzott bizalom, és az a tény, hogy a kriptovaluták az eddig megszokott pénzpiaci folyamatoktól jelentősen eltérnek[47], alkalmas a sértettek józan értékítéletének, kételkedésének legyőzésére.

E visszaélésekkel összefüggésben is a lehetséges sértettek tájékoztatása, a megtörtént visszaélések publikálása okozhatja a bűncselekmények számának visszaesését.

A megvalósított bűncselekményekkel összefüggésben a nyomozó hatóságok a blokkláncok elemzésével és a feltételezett elkövetők feltérképezésével, adatbázisok létrehozásával érhetnek el eredményeket, tekintettel arra, hogy e téren az elkövetői kör megfelelően kvalifikált kell hogy legyen, így lehetőség nyílik az egyes személyek kriminalizálódásának nyomon követésére[48].

Rendészeti válaszok

Azt nehéz megjósolni, mekkora erőforrást kell lekötni a rendészeti szerveknél a kriptovalutákkal kapcsolatos problémák orvoslására. Az azonban tény, hogy 2012 és 2017 között 141 büntetőügy kapcsolódott a kriptovalutákhoz, ami összességében nem sok, de a 2012-es egy büntetőügyhöz képest a 2017-es ötvennyolc ügy exponenciálisan emelkedő görbét mutat.

Vélhetően a következő években sem történnek a kriptovaluták kapcsán olyan bűncselekmények, amelyek érdemben befolyásolnák Magyarország gazdasági érdekét, hiszen nem nagy az ország veszélyeztetettsége. Az azonban valószínűsíthető, hogy sok sértettet érintő jogsértés kerül napvilágra. Ezen túlmenően annak is fontos szempontnak kell lennie, hogy az állampolgároknak a nyomozó hatóságokba vetett bizalmát és az eljáró szervek megbecsültségét nagyon pozitívan befolyásolná, ha az ilyen ügyeket szakértő módon, gyorsan és eredményesen fejeznék be a hatóságok.

---

46 Egy váltságdíj átvétele, vagy az utalt pénz továbbutalása/felvétele, vagy a pénzmosási folyamat számos buktatót tartogat az elkövetők számára, itt azonban ezek egy mozzanatban javarészt megvalósulnak.

47 Például hogy 2017 januárjától egy év alatt huszonegyszeresére nőtt az árfolyama.

48 Fórumnyilatkozatokban, online jelenlétben stb.

A leginkább akut probléma a bűnüldöző szervek számára a büntetőeljárásokban felvetődő kriptovaluták kezelése.

Abban minden szakértő egyetért, hogy az elkövető által használt és a saját tárcáját tartalmazó informatikai eszköz (számítógép, pendrive, telefon stb.) fizikai lefoglalása nem elegendő a kriptovaluta feletti felügyelet megszerzésére.

A kriptovalutákra vonatkozó vagyoni kényszerintézkedések módszertani utasítása jelenleg zajlik.

Az elkövető részéről tulajdonképpen elegendő akár a tárcát zároló privát kulcs ahhoz, hogy a kriptovaluták feletti felügyelet ő, vagy a megbízottja megőrizze oly módon, hogy azt transzferálja egy általa létrehozott és a hatóság által nem ismert tárcába.

Éppen ezért a hatóság részéről is elsődleges feladat a kényszerintézkedéssel érintett tárca tartalmának lefoglalásaként egy a hatóság felügyelete alatt álló tárcába transzferálása. Ez a tranzakció azonban összetett hatósági intézkedés esetén nem kívánt módon információt szolgáltat az elkövetőtársaknak, hiszen ők a blokkláncból rájöhetnek erre.

A hatósági tárcába történő átutalás azonban számos további problémát vet fel.

Az egyik ilyen a hatósági tárca kompromittálása[49]. Erre jó válasz lehet a több jelszóval védett *(multisig)* tárca és a hardvertárca.

A másik nehézség az elvont kriptovaluták tárolása, kezelése, értékesítése. Megítélésem szerint a lefoglalást szenvedőt nyilatkoztatni kell arra vonatkozóan, hogy kívánja-e a kriptovaluta értékesítését. Ennek célja annak elkerülése, hogy a terhelt felmentése és a kriptovaluta neki való visszaszolgáltatása esetén kár érje az eljárás időtartama alatti esetleges árfolyamcsökkenéssel. Ha az értékesítés mellett dönt a lefoglalás szenvedője, akkor az új büntetőeljárási törvényben van egy újítás előzetes az értékesítésre vonatkozóan, miszerint az általános feltételtől eltérést engedve, az értékesítés egy opcionális esetét is bevezeti a 319. § (4) bekezdésben. Ha a lefoglalt dologgal kapcsolatban bejelentettek megalapozott igényt és az értékesítéshez a megalapozott igény bejelentője hozzájárult, a lefoglalt dolog értékesítése elrendelhető.

49 A bitcoinnal kapcsolatos, eddigi legnagyobb sajtófigyelem mellett zajló büntetőügyben (Ross Ulbricht DPR, bővebben: Andy Greenberg: Silk road creator Ross Ulbricht loses his life sentence appeal. https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/) megtörtént, hogy szövetségi ügynökök lopták el a bűnös forrásból származó bitcoinokat. Bővebben lásd https://www.wired.com/2016/11/ross-ulbrichts-lawyers-point-another-corrupt-agent-silk-road-case/

Az elmúlt időszakban a kapcsolódó kutatások középpontjában sokkal inkább a technológia és a funkcionalitás állt, míg javarészt figyelmen kívül hagyták az értékteremtő tevékenységeket és az irányítás kérdését[50]. Azt mindenképpen fontos leszögezni, hogy a blokklánc-technológia multidiszciplináris megközelítést követel.

E tanulmány célul tűzte ki, hogy megvizsgálja a kriptovaluták tekintetében fennálló jelenlegi problémákat, és becsléseket ad a rendészeti szervek szükséges intézkedéseire.

Operatív szinten szükséges a blokklánc-technológiához kapcsolódó ismeretek elmélyítése a bűnüldöző és titkosszolgálati szervek állományában.

Fontos kiaknázni a bűnüldözési célú nemzetközi együttműködésből származó lehetőségeket, megismerni a legjobb gyakorlatokat, esettanulmányokat, részletszabályozási megoldásokat, használni a közös erőforrásokat[51].

Ki kell dolgozni a kriptovalutákkal kapcsolatos kényszerintézkedések módszertani utasítását, valamint azok értékesítésének módját.

Stratégiai szinten jó tudni, hogy a visszaélések nem elkerülhetők egy-egy ország jogalkotásának, végrehajtó hatalmának elszigetelt megoldásaival. Szükséges az átfogó szabályozás. Erre azonban meglehetősen kicsi az esély, hiszen mindig vannak ellenérdekelt felek és kapcsolódó nem kívánt hátrányok.

Ha csak arra gondolunk, hogy a rendészeti szervek sok éves küzdelem után sem tudták elérni, hogy legyen egy egységes bankszámla-nyilvántartás[52] belföldi pénzintézetektől, akkor elég csekély annak az esélye, hogy életre hívható egy regiszter arról, milyen kriptovalutával kapcsolatos szolgáltatók működnek a világban, és kik az ügyfeleik.

Egyre valószínűbb, hogy nem lehet megakadályozni a kriptovaluták fokozott térnyerését a pénzügyi szektorban. Egymással szemben áll azonban két állami/társadalmi érdek: az innovatív technológiák szárnyalásának lehetővé tétele és a vagyonmozgások átláthatóságának, korlátozhatóságának érdeke. Minden bizonnyal azokon a pontokon lehetséges megteremteni a kriptovaluták átláthatóságát, ahol a hatósági ellenőrzés és felügyelet álló pénzügyi szolgáltatók és személyek megjelennek. Ha olyan szabályozás kidolgozására kerülne sor, amely szerint egy vállalkozás (bizonyos limit felett) csak akkor érhet el profitot a kriptovalutákból származó ügyletből (kriptopénzváltók, online-tárca-szolgáltatók, kriptopénz-ATM-üzemeltetők stb.), hogyha az ügy-

50 Marten Risius – Kai Spohrer: A Blockchain Research Framework. Business & Information Systems Engineering, vol. 59, no. 6, 2017, pp. 385–409. https://doi.org/10.1007/s12599-017-0506-0

51 Például az Europol EC3 blokkláncelemző platformja.

52 Bár e cikk írásakor is vannak kedvező jelek arra, hogy ez megvalósul.

felét beazonosította, az jelentős korlát volna azzal szemben, hogy a kriptopénzeket a bűnös vagyon eredetének elrejtésére, legalizálására, vagy felhasználására alkalmazzák. Ezek a rendelkezések a pénzmosás elleni normákból is következnének, de ezek betartatása, kikényszerítése jelenleg nem történik meg.

A kriptovaluták sorsát nagyon jelentős részben a kapcsolódó jogi szabályok határozzák meg, azazhogy az egyes államok milyen mértékben tiltják, korlátozzák a használatukat.

Korábbi kutatási eredményekből jól látható, hogy a kriptovalutákat nagy arányban használják bűncselekmények elkövetéséhez[53], illetve bűnös forrásból származó javak mozgatására, elrejtésére. Megítélésem szerint bizonyosan maradnak olyan államok – jellemzően offshore területen –, amelyekben a kriptovaluták konvertibilis valutákra történő átváltása megoldható marad, így nem vonhatók ki a kriptovaluták a pénzmosás eszköztárából. Sokkal célszerűbb szélesebb körben lehetőséget adni nekik, és a saját jogrendszerünkben a törvényes és ellenőrizhető működés keretein belül tartani. A tiltásokkal és súlyos korlátozásokkal ellentétben célszerűbb az enyhe korlátozások és szabályozott keretek megteremtése. Hasonlóan a kriptográfiai megoldásokhoz, vagy a torhálózathoz: a szellemet nem lehet visszazárni a palackba, így meg kell próbálnunk kordában tartani és a lehetőségekhez mérten felügyelni.

53 Sean Foley – Jonathan R. Karlsen – Tālis J. Putniņš: Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

DOI: 10.38146/BSZ.2018.10.6

VIGH ANDRÁS

A drónok rendészeti alkalmazási lehetőségei[1]

Talán megkockáztatható az a kijelentés, hogy napjaink kutatási témái között kiemelt szerephez jutott a drónokkal[2] kapcsolatos fogalmi kérdések és alkalmazási lehetőségek tisztázása, a jogszabályalkotással összefüggő paraméterek kidolgozása. Ezt a tényt a vonatkozó konferenciák, tanulmányok és internetes híradások növekvő száma is alátámasztja. Az ok abban keresendő, hogy az elmúlt években robbanásszerű növekedés figyelhető meg a drón eszközök terjedésében. Annak fizikai jellemzőitől, felszereltségétől és kialakításától függően nőttek a felhasználási lehetőségek és területek (honvédelmi, rendészeti, illetve civil szféra). Az Amerikai Egyesült Államokban kormányzati felmérések alapján számuk a 2016-os 1,1-ről 2021-re több mint három és fél millióra fog nőni.[3] A siker titka az, hogy a gyártó cégek is igyekeznek minél jobban kiszolgálni az állami, állampolgári, kereskedelmi és kutatási igényeket, a növekvő termelés mellett egyre sokoldalúbb és változatosabb eszközöket egyre kedvezőbb áron dobnak piacra, illetve a versenyben fontos szempontta vált a megbízhatóság. Az is látható, hogy bár sokoldalúan elemzett témáról van szó, ennek a területnek a fejlődése olyan gyors ütemű, hogy az aktuális információk tudományos igényű feldolgozása nehezen tud lépést tartani a változásokkal. Ezért – jellemzően a technika világára – sok információ az internetes felületeken érhető el, ott kutatható.

Mivel a drónok honvédelmi, hadászati jellegű használata alapvető mértékben elkülönül a rendészeti, illetve a polgári célú alkalmazásoktól, valamint más jellegű kérdésfelvetéseket és kutatási módszereket követel meg, a tanulmány további része eltekint ennek a területnek a bemutatásától és elsősorban az egyéb állami, rendészeti feladatokhoz köthető problémakörökre koncentrál. Ennek okán a tanulmány a tárgyául szolgáló eszköz megnevezésére a hazai és külföldi írott sajtóban, szakanyagokban a mindennapi szóhasználatban

1 A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, *A jó kormányzást megalapozó közszolgálat-fejlesztés* elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

2 A drón a repülés közben kiadott jellegzetes zümmögő hangjáról kapta a nevét (drone angolul: [méh]zümmögés).

3 David Shepardson: U.S. commercial drone use to expand tenfold by 2021: government agency. Reuters, March 21, 2017.

lassan gyűjtőfogalomként elterjedt és általánossá vált „drón” kifejezést használja az egyéb, mint például személyzet nélküli légi jármű *(Unmanned Aerial Vehicle; UAV)* elnevezések helyett.

A drónok előnyei

A drónok folyamatosan növekvő népszerűségének hátterében számos előnyük áll, amelyeket egyik oldalról a széles körű felhasználási lehetőségek, másik oldalról a nagyfokú típusvariáció és változatos felszerelhetőség alapoz meg. Ezek közül néhány, általánosnak tekinthető tulajdonságra világít rá a tanulmány, semmiképpen sem törekszik, a technikai sokoldalúság miatt nem is törekedhet, a teljességre.

„A pilóta nélküli repülőgép kezdetekben elsősorban katonai feladatokra alkalmazott olyan repülőeszköz, mely valamilyen ön- vagy távirányítással (leggyakrabban a kettő kombinációjával) rendelkezik, emiatt fedélzetén nincsen szükség pilótára.”[4] A kisebb méretű, sokszor játékjelleggel, szórakozás céljából használt drónok egyik legnagyobb előnyének tekinthető, hogy repetésükhöz nem kell hosszadalmas és drága tanfolyamokon, képzéseken elsajátítani az ismereteket. Ezek az eszközök, adott esetben akár tablet segítségével is egyszerűen, bárki által üzemeltethetők. Az internetes oldalakon számos cég hirdeti magát és kínál kedvező áron, csoportos, drónkezelő tanfolyamokat mindössze 2 × 4 órában. Négy óra elmélet, négy óra gyakorlat. Akár pilóta nélküli kvadrocopter (négy forgószárnyú eszköz) szinten is, és nincs szükség egészségi, pszichikai-fizikai alkalmassági vizsgára sem, bárki lehet „drónpilóta”. Ezzel szemben a nagyobb követelményeknek megfelelő pilóta nélküli, távirányított eszközök állami, rendészeti célú alkalmazásának érdekében a Nemzeti Közszolgálati Egyetem indított egy négyhetes, 150 tanórás, intenzív tanfolyamot, amelynek hallgatói egyebek között a repülések megtervezéséhez és végrehajtásához szükséges aerodinamika, jogszabályi, célirányos meteorológiai ismereteket, felhasználói szintű elméleti és gyakorlati tudást szerezhettek. Megismerhették a drónok alapvető üzemeltetési és karbantartási követelményeit, a hatósági eljárásokat, a repülésbiztonsággal kapcsolatos tudnivalókat és a munkavégzéshez szükséges angol nyelvű kifejezéseket is.[5] Látható, hogy az alkalmazás céljától, helyétől, idejétől, az alkal-

4 https://hu.wikipedia.org/wiki/Pilóta_nélküli_repülőgép
5 https://www.honvedelem.hu/cikk/52252

mazott eszközök tulajdonságaitól és a használt légtértől függően a felhasználók között markáns eltérések mutathatók ki mind a drónok reptetéséhez szükséges ismeretanyag, mind a felelősségteljes használathoz kapcsolódó követelményszintek területén.

A jogi szabályozatlanság is elősegíti a drónok számának növekedését, mert csak szűk körben léteznek olyan előírások, amelyek betartása következetesen megkövetelhető lenne. A *„drónhasználat rendkívül összetett tevékenység, hiszen a gépek irányításakor sok egyéb mellett repülés-, köz- és nemzetbiztonsági kérdésekre éppúgy felelni kell, mint a frekvenciahasználati és etikai felvetésekre”*[6]. Mivel azonban Magyarországon nem létezik közvetlenül rájuk vonatkozó jogszabály, így a légteret használó drónokra áttételesen a légi közlekedésről szóló 1995. évi XCVII. törvény előírásai alkalmazhatók. A magyar légtér igénybevételének feltételeit pedig a magyar légtér légi közlekedés céljára történő kijelöléséről szóló 26/2007. (III. 1.) GKM–HM–KVVM együttes rendelet írja le. E jogi keretek szükség esetén jelenleg csupán analóg módon alkalmazhatók a drónok használata esetén, mivel azok alapvetően nem tartoznak a közlekedési eszközök közé.

Reptetésük, felszállásuk, típustól függően, viszonylag kis helyet igényel, így parkokból, mezőkről, szükség esetén kézből is könnyedén indíthatók, nincs szükség célirányosan kiépített felszállópályára. Ugyanez igaz a leszállás, landolás feltételeire is.

Az optikai rendszerekkel felszerelt, kamerájuk által közvetített kép segítségével irányítható drónok népszerűségének oka, hogy a környezet a magasból, akár száz-százötven méterről, esetleg még magasabbról, úgymond madártávlatból látható vagy magasban lévő tereptárgyak is látótávolságba hozhatók, valamint a drón képes olyan helyekről is képet közvetíteni, amelyek nehezen megközelíthetők vagy veszélyesek például kirándulás, vártúra alkalmával, ezáltal segíthet az esetleges veszély mértékének felmérésében. Ez a perspektíva olyan értékű információkat hordozhat a használó számára, amelyek a földön járva nem észlelhetők. Többletként említhető, hogy infra-, hőkamerával felszerelve rossz látási viszonyok között is (szürkület, köd, éjszaka) hasznos segítség lehet a drón. Ezt a speciális észlelési képességet használják ki a szórakozni vágyók, használják fel munkafolyamataikban a gazdasági, kereskedelmi, az állami területek vagy akár a kutatók.

A drónok növekvő közkedveltségét segíti elő a felszerelhetőség nagyfokú variációs lehetősége, amelynek köszönhetően összetettebb feladatok megol-

6 Lázin Miklós András: Pro és kontra a drónhasználatról. Magyar Hírlap, 2014. október 30.

dására is sikerrel igénybe vehető. Olyannyira, hogy egy számunkra talán szélsőségesnek tűnő példa szerint az Észak-dakotai Rendőrség felhatalmazást kapott arra, hogy drónokat szereljen fel nem halálos fegyverekkel *(non-lethal weapons),* úgymint sokkoló, könnygáz, gumilövedék.[7]

Mindenképpen előnyként említendő, hogy szemben a pilótaigényes repülő járművekkel, a drón spórol az emberi erőforrással, a fenntartási költsége jóval alacsonyabb. Egy esetleges műszaki meghibásodás okozta baleset, lezuhanás esetén nem kell a pilóta személyi sérülésével számolni.

Típustól függően nagyon fontos tulajdonságuk, hogy az irányító távközlési kommunikáció megszűnése, meghibásodása esetén GPS-koordinátákat használva képes visszatérni a kiindulási pontra.

A rendészeti, polgári célú felhasználás lehetséges területei

Ha a drónok alkalmazásának lehetséges területeit szeretnénk megjelölni, azt látjuk, hogy az igen szerteágazó, és többfajta rendszer szerint lehetséges. Szempont lehet például a drónok jellemzői alapján történő csoportosítás vagy a felhasználók szerinti kategorizálás. A legegyszerűbb azoknak a nagyobb, átfogó területeknek a megjelölése, amelyek egyre növekvő mértékben alkalmaznak dróneszközöket. Ebből kiindulva megkülönböztethetjük egymástól

– az állami, ideértve a honvédelmet és a közszolgálatot;
– a gazdasági, kereskedelmi;
– a tudományos, kutatási; és
– a magáncélú területeket.

A tanulmány a számos alkalmazási terület közül a elsősorban a közszolgálat, a rendészet és kismértékben a magáncélú használat területén megjelenő lehetőségekre koncentrál.

Katasztrófavédelem

Mind a természeti, mind az ipari katasztrófák esetében jelentős segítséget jelenthet a magasból készített, távlati megfigyelés, a teljes terület átfogó képé-

7 https://www.theverge.com/2015/8/26/9211165/north-dakota-armed-drones-tasers

nek közvetítése. Segítségével lehetőség nyílik a helyszínen a katasztrófa sújtotta terület pontos helyének és kiterjedésének felmérésére, a veszélyeztetett területek védelmének érdekében teendő intézkedések célirányosabb megtervezésére. Átlátható, elemezhető egy esetleges árvíz, netán veszélyes anyag (zagy) terjedési iránya és sebessége, figyelembe véve a fentről szembetűnő domborzati adottságokat vagy a beépített területek sajátosságait. Igény szerint a veszélyes anyagokból drón segítségével mintavétel végezhető, és az gyorsan egy vizsgálati helyre szállítható. Eldönthető, hol és milyen erőkkel célszerű a védekezés, végső esetben szükséges-e a lakosság kitelepítése. Akár emberi életeket is menthet a drón.[8] Kihasználva ezeket az előnyöket, a katasztrófavédelem 2014 szeptemberében drónt is bevetett a Zala megyei árvízhelyzet felmérése érdekében.

Felmérhető, hogy katasztrófa esetén milyen mértékű a károkozás, esetleg mely utak lezárására van szükség. 2014 decemberének első napjaiban a Pilis hegységben az ónos eső soha nem látott mértékű pusztítást okozott, nagy területen veszélyhelyzet alakult ki, erdőlátogatási tilalmat kellett elrendelni. A felülnézeti képeken jól kivehető a körülbelül húszezer hektáron kialakult jégképződés. Az ilyen esetekben a jövőben is hathatós segítséget jelenthet a drónok használata.

Jégzajlás esetén a drónra szerelt képtovábbító eszköz képes magát a zajlási folyamatot és annak terjedését, kiterjedését figyelemmel kísérni, arról informálni. Képes a veszélyes, nem megközelíthető helyeken is felvételeket készíteni, például hídlábak, vagy a jég által körülzárt hajók, építmények állapotáról. Egyáltalán nem zárható ki, hogy a drónok segíthetnek a jégtorlaszok felrobbantásában, akár úgy, hogy a robbanóanyagot a megfelelő veszélyes helyekre szállítják.

Tömegszerencsétlenség esetén gyorsan a helyszín fölé küldhető egy drón, így pontosabb kép alakulhat ki arról, milyen erőket és eszközöket igényel a segítségnyújtás, milyen személyi sérülések ellátására van szükség, a káreny-hítés során milyen intézkedések teendők. Szükséges-e kórházak sürgősségi értesítése az ellátandó személyek számának és az ellátás fokának függvényében, esetlegesen gyógyszer, kötszer küldhető a helyszínre.

8 http://www.origo.hu/techbazis/20150703-dronokkal-mentettek-eletet-tuzoltok-dron-kopter-aradas.html

Vízügy

Ezen a területen sokszor alakulhat ki olyan szituáció, amely akár katasztrófavédelmi intézkedéseket is követelhet, ahol, mint láttuk, a drón hasznos segítő lehet.

A folyógátak ellenőrzésére folyamatosan szükség van. Ez kiemelt feladatnak minősül áradás esetén, amikor fokozottabb, gyakoribb a kontroll szükségessége, sokszor óráról órára változhat a vízállás. A gátőrök tevékenysége mellett ilyenkor nyújthat segítséget a drón, amely nagy területeken, percre lebontva követheti a kialakult helyzetet. Pontosan megállapítható a veszélyeztetett gátrészek helye, az esetleges buzgárok kialakulása, így kellő időben, még egy esetleges gátszakadás előtt megtehetők az árvízvédelmi intézkedések.

Áradás esetén a folyószakaszokon ellenőrizhető annak levonulása, esetleg a víz által elöntött területek állapota. Felmérhető, van-e ott veszélyeztetett emberi lakhely, és annak védelme érdekében hol, milyen mértékű védelmi intézkedésekre van szükség.

Az áradó víz vagy esetleg nagy mennyiségű hó által elzárt településekre ivóvíz, élelem, kommunikációs eszközök, egyéb segélyszállítmányok juttathatók el. A jeges ár veszélyessége miatt sokszor annak közvetlen emberi megfigyelése nem megoldható, de drón segítségével a kialakult helyzet nyomon követhető, katasztrófahelyzet esetén az emberi beavatkozás megtervezhető.

Szándékos gátátszakítás esetén a tervezetten elárasztani kívánt terület előzetesen a magasból ellenőrizhető, például nem tartózkodik-e ott illetéktelen személy. Későbbiekben felmérhető az ár mozgása, a belvíz kiterjedése.

Áradás, jégzajlás következtében elhullott, fertőzésveszélyt jelentő állati tetemek a magasból könnyebben észlelhetők.

A drónok által készített felvételek nagy előnye, hogy azok a pillanatnyi helyzetről informálnak, nagy felbontásúak, így a kevésbé feltűnő, viszonylag gyorsan kialakuló változások is észlelhetők, például a gátak állapotának ellenőrzésekor.

Környezetvédelem, környezetkárosítás

A minket körülvevő természetes élettér védelme egyre kiemeltebb feladat nemcsak az egyén, de az állami szervek szintjén is. Emlékezetes eseményként marad meg a „habzó Rába”, a Körös-vidéki folyóvizeket érintő, Romániából származó ciánszennyezés. A szennyezés jelentős károkat okozott a

környezetben, az élővilágban, látványos hal- és növényzetpusztulást okozva. Manapság már adott a technika, hogy esetleges ismételt bekövetkezés esetén ezeket a folyamatokat mihamarabb észlelni lehessen, a szennyezés mértékét, terjedését drónok alkalmazásával a magasból, távlati felvételek segítségével figyelemmel lehessen kísérni, így célirányosabban és idejében megszervezhető az ellenintézkedések rendszere, helye és mértéke, valamint pontosan felmérhető a veszélyeztetett területek nagysága.

Hulladékként fölbe ásott vagy akár a felszínen hordóban tárolt veszélyes, mérgező anyagok talajba szivárgása esetén, a felszínen a növényi populáció elváltozása, megváltozása vagy akár a talaj elszíneződése jelezheti a szennyezés meglétét, annak kiterjedését és mérgező hatását.

Sajnos manapság sem ritka, hogy a környezetet jelentősen szennyező nagyobb mennyiségű építési vagy egyéb ipari hulladék engedély nélküli lerakása lakott területektől távolabb, akár természetvédelmi területen történik meg. A rejtettség következtében a tevékenység sokáig észrevétlen maradhat, a szennyezéssel okozott kár növekedhet, egyben az idő múlásával az elkövető kilétének megállapítása is egyre nehezebbé válhat. A magasból, nagy területek láttatására alkalmas drónok segíthetnek ezeknek a helyeknek a relatív rövid időn belüli felfedezésében, ideális esetben a cselekmény akár meg is szakítható, az elkövető tetten érhető.

Határőrizet, határrendészet

Ebből a célból elsősorban a határterületek zónáiban kerülhet sor drónok akár éjjel-nappali alkalmazására, a határőrizeti munkát ellátó humán erők állandó segítségeként.

Mivel a drón a magasból átlát a határvonalon, bizonyos keretek között lehetőség nyílik a menekültcsoportok figyelemmel kísérésére, összetételük megállapítására, határ menti mozgásuk nyomon követésére, a létszámadatok ellenőrzésére, kapcsolataik észlelésére és felfedésére is. Az információk alapján az illetékes szervek felkészülhetnek az esetleges illegális határátlépés helyének és valószínű idejének meghatározására. Adott esetben felfedhetők az embercsempészeti tevékenységek.

Jelenleg a rendőrség részt vesz egy európai uniós fejlesztési projektben, amely határőrizeti célú, autonóm, heterogén robotrajok kifejlesztését tűzte ki célul. A raj légi, földi, vízi és víz alatti egységekből áll, amelyek koordináltan működnek együtt az embercsempészés, a határzár jogosulatlan átlépése

vagy megrongálása, a tiltott határátlépés és a határon átnyúló környezetszennyezés felderítése érdekében, a reagáló erők támogatásában. A koncepció alapja a *Robotok rendvédelmi célú alkalmazása* című, a Nemzeti Közszolgálati Egyetemen folyó kutatás.[9]

Biztonságtechnikai terület

Az állami szintű feladatok ez irányú csökkenésével párhuzamosan egyre nagyobb jelentőséghez jut az úgynevezett magánszektor, ahol az őrzésvédelem területén, elsősorban az objektumok védelmekor is jól használható eszköznek bizonyulhat a drón. Bár az esetek többségében a biztonsági céllal fixen telepített videokamera elegendő információs képi hátteret nyújthat, bizonyos esetekben a magasból történő képtovábbítás plusz adalékot jelenthet. Olyan helyekről, amelyeket a kamera nem lát, folyamatos és mobil képi információ szerezhető egyrészt nagyobb területet átfogva, másrészt más látásszögből, akár éjjel is. Például egy többemeletes épület védelme során az emeletek külső ellenőrzése minden gond nélkül megoldható drón segítségével a nap bármely időszakában.

Közlekedés

A drónok által a magasból közvetített képek segíthetnek az aktuális forgalmi helyzet elemzésében, a sűrűn terhelt utak, a dugók felmérésében, így a közlekedés megszervezésében, lezárt, elzárt utak esetében alternatív útvonalak kijelölésében. A balesetek helyszínére elsőként érkező drón informálhat annak mértékéről, a veszélyhelyzet nagyságáról, arról, fennáll-e azonnali közveszély-elhárítási feladat, adatot szolgáltathat a balesetben részt vevő járművek és a sérültek számáról. Ezen információk alapján személyi és tárgyi vonatkozásban pontosabban tervezhető a későbbi helyszíni tevékenység.

A mindennapok vonatkozásában a költséghatékony drónok alkalmazhatók lennének például az utak állapotának felmérésére, a hibás útszakaszok képi rögzítésére, egyben megállapítható lenne a sérülések és kijavítandó úthibák száma, relatív helyzete és a javítandó útszakasz hossza is.

---

9 Székely, Zoltán: Application of Robotics for Enhanced Security: European Research on Security Robots. In: Péter Korondi (ed.): Proceedings of ARES'14: Workshop on Application of Robotics for Enhanced Security. Budapest, 2014. 06. 13. – 2014. 06. 14. BUTE, Budapest, 2014, pp. 11–15.

A közlekedési vállalatok, a vasút felső vezetékeinek ellenőrzése a már leírt módon történhet.

Energiaszolgáltatás

Elsősorban azok a szolgáltatók alkalmazhatják sikerrel a dróntechnikát, amelyeknek jelentős szabadtéri eszközkészletük van, mint például a villamosenergia-szolgáltatók, amelyek egy-egy természeti anomália következtében jelentős káreseményeknek vannak kitéve. A villanyvezetékek rendkívüli ellenőrzésére is alkalmasak a drónok. Pontosan megállapítható, melyik helyen következett be a káresemény, így az elhárítási munkálatok célirányosan tervezhetők.

Természetesen a szabadtéri hálózatok mindennapi rendszeres felülvizsgálatai során is sikerrel alkalmazhatók a drónok, mind a vezetékek, mind a tartóoszlopok ellenőrzésére.

Mezőgazdaság

A termények felülnézeti vizsgálata sajátos lehetőségeket kínál a termelők, a gazdák számára. Fentről észlelhető, ha egy-egy termőterület a környezetétől eltérő növekedési szintet, pusztulást, eltérő színhatást mutat, ami valamely betegség vagy kártevő által kiváltott hatás folyománya lehet. A még idejében felfedezett kárjelenség negatív hatásai az észlelés következtében csökkenthetők, elháríthatók, a szükséges permetezés, trágyázás hatásfoka a későbbiekben ellenőrizhető, a rágcsálók elleni védelem eszközei bevethetők.

Az időjárási körülmények nagyban befolyásolják a terméshozamot. Drónok segítségével lehetőség nyílik a várható termés mennyiségének és minőségének becslésére, a termény-előrejelzésre.

Erdőgazdálkodás

Az erdőket fenyegető legnagyobb veszélyek egyike a tűz. Erdészeti drónok rendszeres ellenőrző vagy mások általi véletlenszerű reptetése lehetővé teszi egy esetleges tűzfészek mielőbbi észlelését, így az oltási munkák azonnali megkezdését, a tűz elterjedésének megakadályozását, a kár csökkentését. Ké-

sőbbiekben a magasból nézve könnyebben behatárolható a tűz által érintett terület nagysága és pontos helye, felmérhető a lehetséges továbbterjedés iránya. A humán erőforrást igénylő költséges helikopteres felderítéssel szemben a drónok segítségével végzett *„képi felderítés is hasonlóan kielégíti a hatékonyságot elősegítő kritériumok teljesülését”*[10].

A lenti viszonyok között megszemlélve egységesnek ható erdőrészek magaslati látképe olyan információkat nyújthat, amelyek a földről nem mindig észlelhetők. Az eltérő színképek és lombozati jellemzők alapján jól behatárolhatók az elöregedett, megbetegedett területek.

Felfedezhetők az engedély nélküli fakivágások és az azok megközelítésére, illetve a szállításra szolgáló útvonalak, amelyek a későbbiekben jól követhetők.

A magaslati képek alapján jobban tervezhetővé válik a fakitermelés mértéke és helye, felmérhető az erdőújítás, a fatelepítés szükségessége.

Vadgazdálkodás

Ezen a területen többes funkciót is elláthat a drón. Fentről könnyebben észlelhetők az illegálisan kihelyezett csapdák, a csapdába esett állatok, az elhullott tetemek. Könnyebben felfedezhető a vadkár helye is. A vadállomány vagy az esetleg városba tévedő vadállatok, például vaddisznók, mozgása nyomon követhető, utóbbiak befogása könnyebben tervezhető.

A határon túli területekről védett vagy ritka állatok is megjelenhetnek erdeinkben, például medvék, farkasok, hiúz, ezek megkeresése, nyomon követése az olykor nehéz terepviszonyok miatt – például szurdok, meredek sziklafal – a bejárással nehezen megközelíthető erdőrészeken szinte megoldhatatlan feladat, ebben segíthet a magaslati, nagyobb területeket átfogó látásmód.

Az orvvadászok elleni küzdelemben kiemelt jelentőségű lehet a rossz látási viszonyok között is dolgozó infrakamera, amelynek segítségével állatok és személyek mozgása követhető nyomon.

---

10 Restás Agoston: Vegetációtüzek felderítésének támogatása pilóta nélküli repülőgépek alkalmazásával. Repüléstudományi Közlemények, 2015. különszám repulestudomany.hu/kulonszamok/2005_cikkek/restas_agoston.pdf

Régészet

A felső talajszint által elfedett, ezért a földön járva nem, de a magasból a növényzet vagy a talajréteg eltérő színei alapján észlelhető történelmi emlékek, romok, esetleg temetkezési helyek felfedezését teszi lehetővé a légi felvétel. Nagyobb területeket átfogó építkezési munkák helyén vagy nyomvonalán, például útépítés esetén, a fenti nézet segíthet abban, hogy ne semmisüljenek meg régészeti értékeink, azok feltárhatók, kutathatók legyenek.

Térképészet

A domborzati elemek és a tereptárgyak (idesorolva az ember által alkotott építményeket is) formája, mérete, egymáshoz viszonyított helyzete és távolsága a drón által készített, pontos mérések elvégzésére is alkalmas légi felvételek segítségével hitelesen megállapítható, naprakészen nyomon követve az aktuális változásokat is. A drón így nemcsak a térképészek, de a földmérők munkáját is nagymértékben segítheti.

Posta

Talán az egyik legdinamikusabban fejlődő területnek tekinthető a postai csomagküldési szolgáltatás. Ez egyrészt annak tulajdonítható, hogy a nehezen megközelíthető helyekre, például a tanyákra is könnyűszerrel eljuttatható a nem túl súlyos küldemény, másrészt a sűrűn lakott városokban a légvonalban repülő drón esetében nem kell számolni a forgalmi akadályokkal, egy közlekedési dugóban történő araszolgatással, így a szállítás, a címzettel való esetleges telefonos egyeztetés után, rövid időn belül elvégezhető. Előnyt jelenthet a tetszőleges időben, kora reggel, késő este történő szolgáltatás, valamint a sürgősséget, gyorsaságot igénylő csomagkézbesítés lehetősége is. A drón ezenkívül spórol a humán erőforrással, ezáltal költségkímélő. A posta az egyéb állami feladatainak végzése során is kihasználhatja a „csomagküldés drón segítségével” lehetőséget. Bár Magyarországon még erőteljes a lemaradás ezen a téren, a svájci posta már teszteli az alkalmazás módjait.[11]

11 https://www.engadget.com/2015/07/08/swiss-mail-delivery-drone-test/

Kereskedelem

Az internetes kereskedelem mértéke rohamléptekkel növekszik, ennek egyik nagy szelete az online rendelt termékek házhoz szállítása. Hasonlóan a postai szolgáltatásokhoz, a vállalkozások szintén egyre nagyobb mértékben a GPS-koordinátákat használó, relatív olcsón üzemeltethető drónokkal oldják meg a csomagküldés feladatait. Nehézséget jelenthet a kézbesítés során, ha olyan címre kell eljuttatni a küldeményt, amely nem alkalmas drónok leszállására. Ellenben akár egy parkba is rendelhetünk pizzát.

Egészségügy

Balesetek helyszínére, kórházak, rendelőintézetek, egyéb egészségügyi intézmények számára sürgősségi vér-, gyógyszerszállítás céljából mindenképp hasznos eszköznek tekinthető a drón, mert forgalomfüggetlen, gyors, pontos. Rövid időn belül többször is fordulhat.

A drónok támogathatják a speciális mentők tevékenységét is.[12] A nehezen megközelíthető terepek, szurdokok könnyen felderíthetők a levegőből.

Építőipar

Építkezések megkezdése előtt a látható talaj- és a környezeti viszonyok felmérésében, építkezési területeken a munkafolyamatok megszervezésében, magasépítmények állapotának ellenőrzésében vagy akár az őrzés-védelemben jelenthetnek segítséget a drónok által készített felvételek.

Statikai szempontból bizonytalan, nehezen megközelíthető, illetve magasra nyúló építmények, például gátak, hídlábak vagy rekonstrukciós vizsgálatok előtt álló épületek – például a Füzéri vár falainak – állapotfelmérésében[13] jól hasznosítható eszköznek számíthat a drón. Emberi életek veszélyeztetése nélkül nyújthat olyan képi információt a vizsgálat tárgyáról, amely később akár 3D-s látványként is elemezhető.

---

12 Petrétei Dávid: A drónok krimináltechnikai és rendészeti felhasználása. Magyar Bűnüldöző, 2015/1–3.

13 http://kiralyiudvar.lapunk.hu/?modul=oldal&tartalom=1218209#.WsYdcNRMT4Y

Hírközlés

Napjainkban a különböző hírközlő csatornák számára elengedhetetlen követelmény a gyorsaság. Fontos, hogy a közérdeklődésre számot tartó eseményekről az információk minél hamarabb és részletesebb formában, minél látványosabb módon „tálalódjanak”, ezért a helyszínről közvetített „élőkép” fontos elemévé vált a tájékoztatásnak, a híradásnak. A nemzeti ünnepségekről, a felvonulásokról, a fesztiválokról a drón által közvetített kép mindenképpen emeli a tudósítások színvonalát és hitelességét.

Szórakoztatás

A sportközvetítések során[14], valamint a filmiparban is egyre növekvő mértékben használják ki a drónokkal készített légi felvételek előnyeit, csakúgy, mint a kirándulók, akiknek segíthet a túraútvonal nehézségi szintek alapján történő megtervezésében, míg a sziklamászóknak segíthet a függőleges felületek előzetes felmérésében. Míg az első két esetben a drága eszközöket, utóbbi esetekben elsősorban játék kategóriájú, könnyű és kis méretű multikoptereket alkalmaznak.

Bűnüldözés

A bűnüldözés során a drónt elsősorban a rá felszerelt fényképezőgép, videokamera teszi hasznossá. Véleményem szerint ebből a szemszögből megvizsgálva a jogszabályokat, az eszköz használatára vonatkoztathatók a fényképfelvételre, valamint az egyidejű kép- és hangfelvételre vonatkozó előírások, hiszen légi felvételek készítésekor sem találkozunk mással, mint a régóta alkalmazott fényképkészítéssel és a – sok esetben hang nélküli – folyamatos mozgóképrögzítéssel. Általános jogi háttérként a rendőrségről szóló 1994. évi XXXIV. törvény 42. § (1) bekezdése lehetőséget nyújt arra, hogy a rendőrség a rendőri intézkedéssel, illetve az ellátott szolgálati feladattal összefüggésben az intézkedéssel érintett személyről, a környezetéről, illetve a rendőri intézkedés szempontjából lényeges körülményről, tárgyról képfelvételt,

14 http://www.origo.hu/techbazis/20150707-magyar-dron-balaton-kekszalag-arkad-nagydij-vitorlas-verseny-hajo-oktokopter-skyviewair-panoramafoto.html

hangfelvételt, kép- és hangfelvételt készíthessen. A halaszthatatlan, halasztást nem tűrő feladatok esetén a levegőből, a légtérből történő felvételek készítését teszi lehetővé a magyar légtér légi közlekedés céljára történő kijelöléséről szóló 26/2007. (III. 1.) GKM–HM–KVVM együttes rendelet 5. § (4) bekezdése, amely a rendészeti vagy bűnüldözési feladat céljából végzett repülés esetén engedélyezi a korlátozott légtér előzetes kérelem nélküli igénybevételét. Mivel drón alkalmazására azokban az esetekben lehet reálisan szükség, amikor a felülnézeti, madártávlati képi információ plusz adalékot jelenthet egy intézkedés vagy egy bizonyítási cselekmény során, elsősorban ezeket az eseteket érdemes kiemelni és górcső alá venni. Véleményem szerint itt is elsősorban a dinamikusabb, sok mozgással, helyváltoztatással járó tevékenységet igénylő cselekmények végrehajtása során vagy nagyobb kiterjedésű területek áttekintése, átvizsgálása esetén lehetnek hasznosak a drón által rögzített, közvetített felvételek. A büntetőeljárásról szóló 2017. évi XC. törvény 206. §-a szerint *„Bizonyítási cselekmény különösen a szemle, a helyszíni kihallgatás, a bizonyítási kísérlet, a felismerésre bemutatás, a szembesítés és a műszeres vallomásellenőrzés”.* A felsorolt bizonyítási cselekmények mellett egyéb rendőri intézkedések esetén is sikerrel használható a drón, mint például csapaterő alkalmazása során.

1. Szemle – a Be. 207. § (2) bekezdése szerint a szemle tárgyáról, ha lehetséges és szükséges, kép-, hang-, illetve kép- és hangfelvételt kell készíteni. Azokban az esetekben, ha a szemle nem fedett, hanem nyílt helyszínen folyik, a drón használata segíthet egyebek között
   – a releváns terület kiterjedésének pontos meghatározásában;
   – az esetleges közelítési, menekülési útvonalak megállapításában;
   – elhagyott, eldobott tárgyak, eszközök felfedezésében;
   – rejtő szándékkal megbolygatott helyek észrevételében;
   – a szemle során rögzített bizonyítási eszközök helyének, relatív helyzetüknek pontos jelölésében;
   – többes helyszín esetében a vizsgált helyek egymáshoz viszonyított helyzetének felmérésében.

   Mivel a drónra szerelt kamerák által közvetített képek folyamatosan nyomon követhetők és kiértékelhetők, tervezhetőbb és szervezhetőbb lesz a helyszíni tevékenység.
2. Helyszíni kihallgatás – a legdinamikusabbnak tekinthető bizonyítási cselekmény, amikor is a vallomást tevő elmondása, információi határozzák meg az eljáró hatóság konkrét lépéseit. Helyszíni vallomástételre akkor lehet szükség, ha a szükségessé válik az elkövetett cselekmény lefolyásának

rekonstruálása, vagy a helyszíni környezet segíthet az emlékképek felszínre hozatalában, mert például a terhelt, a tanú a négy fal közti vallomás során nem tudja pontosan felidézni az elásott, elrejtett, eldobott tárgyak vagy az elkövetés pontos helyét. Mivel ez a bizonyítási cselekmény minden mozzanatában nem tervezhető előre, és menetét nagymértékben befolyásolja a vallomást tevő személy tevékenysége, megfelelő személyi, technikai feltételek megteremtésével fel kell készülni a váratlan helyzetekre is. A magasból közvetített kép segítségével több releváns helyszín megmutatása esetén a vallomást tevő személy mozgása plasztikusan nyomon kísérhető. Ha a megszerzett adatok alapján adott helyszínen szemle tartása válik szükségessé, a drón a leírtak alapján segítheti a bűnüldöző szervek munkáját.

3. Bizonyítási kísérlet – amennyiben cselekmény elkövetési lehetőségének vizsgálata, esemény lefolyásának rekonstrukciója vagy időtartam tisztázása céljából a bizonyítási kísérlet során egyidejű kép- és hangfelvétel készítése szükséges, figyelemmel kell lenni arra, hogy a láttathatóság érdekében esetenként több nézőpontból is szükséges folyamatában rögzíteni az eseményeket. A tökéletes rögzítés esetenként megkívánná két vagy több videokamera egyidejű, más kameraállásból történő alkalmazását, de erre kevés lehetőség nyílik.[15] Mivel ennél a bizonyítási cselekménynél a mozgásnak, a helyváltoztatásnak kiemelt szerepe lehet, hasznos vizuális információt nyújthat a nagyobb látószöget átfogó, magasból közvetített kép.
4. Biztonsági intézkedés, személy- és létesítménybiztosítási intézkedés – a rendőrség ez irányú intézkedéseit elsősorban a területek ellenőrzése, biztosítása során segítheti a drón alkalmazása. A folyamatosan közvetített információk alapján a hirtelen változó helyzetek, veszélyforrások észlelhetők, a kellő intézkedések megtehetők.
5. A csapaterő alkalmazása – nagyobb rendőri erők igénybevétele során akár a terepkutatás, akár az elfogás megszervezését is segítheti a drón, ha például nagyobb kiterjedésű, egyenetlen terepszakaszokat vagy nehezen megközelíthető helyeket kell átvizsgálni körözött bűnöző helyének megállapításához. Segítheti eltűnt személyek megtalálását is. De alkalmazása az Rtv. 58. § (1) bekezdésében felsorolt egyéb esetekben sem kizárt, például nagyobb területű helyszínek biztosításakor, személyvédelem megszervezésekor, végrehajtásakor, a lakosság ellátása szempontjából kiemelten fontos létesítmények őrzése, védelme esetén, katasztrófahelyzetekben, rendezvénybiztosítás során.

15 Vigh András: Videotechnika kriminalisztikai alkalmazása. Rendvédelmi Füzetek, 2006/1–2.

6. Egyéb tevékenység – épületek, építmények környezettanulmánya során, vagy házkutatás előzetes tervezése esetén, ha például fennáll a gyanú, hogy illegális kábítószerlabor működik az adott épületben, a terület észrevétlen felderítése, megfigyelése végezhető drón segítségével. Azonban ügyelni kell a megfelelő magasság elérésére, hogy a drón működési zaja ne legyen árulkodó jelzés a megfigyeltek számára.
   Lehetőség nyílik kenderültetvények felfedezésére, amelyet sokszor más haszonnövények közé elrejtve ültetnek, így, míg a földről nehezen észlelhető az illegális növény termesztése, addig a levegőből jól láthatóvá válik az eltérő növényi kultúra.

Alapvetően a biztonságtechnikai területhez tartozó, de a rendőrség feladatkörét is érintő személyvédelem esetén a nyílt területek drón segítségével elvégzett naprakész felmérése segítheti az útvonal előzetes megtervezését, valamint a védett személy mozgásának biztosítását, a váratlanul kialakuló esetleges veszélyforrások idejében történő észrevételét.

Általánosságban elmondható, hogy az optikai képrögzítő eszközök bűnügyi célú használata során kiemelt figyelmet kell fordítani arra, hogy a drón nagy felbontású képrögzítő eszközökkel legyen felszerelve, különben a relatív nagy távolságból készített, alacsony pixelszámú felvételeken a megörökített téma nem lesz kivehető.

Látható, hogy a drónok rendészeti, illetve a magáncélú felhasználási, alkalmazási területei széles spektrumot fognak át. Ebben a változatosságban, a nem mellékes alacsony üzemeltetési költség mellett, szerepet játszik az is, hogy a drón a rászerelt felvételkészítő és az azt rögzítő, illetve továbbító rendszertől függően speciális célokra és körülmények között is igénybe vehető. Számuk erőteljes növekedése ellenére azonban hátráltató tényezőként kell figyelembe venni, hogy a repülési idejük típustól függően korlátozott, illetve minél magasabbról készül a felvétel, annál nagyobb felbontású, jobb, drágább és valószínűleg nehezebb eszközökre van szükség. Párhuzamosan már nagyobb teherbírású drón is kell, aminek a reptetésére adott esetben már a korábbitól eltérő szabályozás vonatkozhat. A szép képet tovább árnyalja, hogy a reptető és a drón közötti kommunikációs infrastruktúra fejlődése nem képes követni a felvetődő igényeket, így a közeljövőben nem kell azzal számolni, hogy a légtér telítődik drónokkal, tehát egy ideig még nem kell félnünk, hogy „légi forgalmi dugók” alakuljanak ki és a drónok egymást akadályozzák.

A drónhasználat veszélyei

Bár széles körű felhasználásuk szempontjából láthatóan számos hasznos lehetőséget kínálnak, a drónok alkalmazása legalább olyan fokú negatívumokat is rejt.

Reptetésük szabályozatlansága forrása lehet azoknak a veszélyeknek, amelyek mind a gondatlan használatból, mind a tudatos bűnös szándékból eredeztethetők. *„Pilóta nélküli légijárművet gyakorlatilag bárki vásárolhat magának, így a felhasználók többsége nem is tudja elképzelni, hogy milyen helyet foglalnak el az ilyen eszközökkel végrehajtott repülések a repülés rendszerében.”*[16] A repülések végrehajtása során, a kis mérete és kevés fém alkatrésze miatt a radar által nem érzékelhető drón helyzete általában nem ismert a légiforgalmi szolgálatok előtt, így rejtve marad, általános veszélyforrást jelentve a többi légi közlekedő számára. Ne felejtsük el, hogy alapvetően a reptetők felelőssége, mikor, hol, mire, hogyan használják repülő tárgyaikat, betartják-e az annak működését szabályozó jogi kereteket és észszerű viselkedési normákat. Mindezeket figyelembe véve állapítandó meg, milyen mértékben terheli őket a felelősség egy esetleg kialakult veszélyhelyzet, bekövetkezett baleset, netán szándékos bűnelkövetés esetén.

A felelőtlen légtérhasználat súlyos veszélyek forrása lehet. A repterek környezetében történő drónreptetés veszélyeztetheti a repülés biztonságát, zavarhatja a légi forgalom normális működését, könnyen okozhat akár tragikus végkimenetelű balesetet is. A katasztrófaturisták által kis területen, nagy számban használt drónok hátráltathatják, veszélyeztethetik és tönkre is tehetik a helyszínen feladatokat ellátó hatóságok, szervek saját eszközeit. Egy kaliforniai erdőtűz oltásakor a vízszállító helikopterek tizenöt-húsz percig nem fértek oda a lángokhoz a rossz helyen lebegő civil drónok miatt.[17] Az összevissza repkedő drónok villanyvezetékeket, távközlési kábeleket rongálhatnak meg.

A sűrűn lakott területek felett, például tömegrendezvények alkalmával reptetett drónok esetében veszélyforrás az esetleges lezuhanás. Ennek oka lehet az eszköz meghibásodása vagy a kommunikációs rendszer valamilyen zavara is, de drón lezuhanása bűnös céllal is kiváltható, így *„bárkire rázuhanhat egy meghackelt drón”*[18].

---

16 Székely Zoltán: A pilóta nélküli és a pilóta által vezetett légijárművek lehetséges konfliktusai, a konfliktus feloldás lehetőségei. In: A nyílt információgyűjtés fejlődő területei. Tanulmánykötet. Belügyi Tudományos Tanács, Budapest, 2015

17 http://www.bbc.com/news/technology-33593981

18 http://www.origo.hu/techbazis/20150130-egy-uj-kartevotol-lezuhan-a-dron.html

Egyre több gondot okoznak az alacsony magasságban a magánterületek felett repkedő, valamint a magánszférát megsértő, „kukkoló” drónok. A magasban lévő kamera belát a zárt kertekbe, az emeleti lakásokba és kéretlenül rögzítheti a magánélet perceit. Az internetes bulvársajtót böngészve sokszor bukkanhatunk olyan tudósításokra, amelyek a drónok magánszemélyek általi lelövéséről[19] vagy egyéb módon történő hatástalanításáról szólnak.

A drón alkalmas arra is, hogy büntetés-végrehajtási intézetekbe cigarettát, mobiltelefont vagy akár drogot csempésszen, ahogy az egy Ohio állambeli börtönben megtörtént.[20]

Mivel a drónok a hagyományos radarokkal nehezen észlelhetők, különleges veszélyeket rejt magában, ha terrorista célokból fegyverként kívánják használni. Egy robbanóanyaggal megpakolt drón tömegrendezvényen történő szándékos tömegbe irányítása és felrobbantása számos emberéletet követelhet.

Védett személyek elleni célzott támadás eszköze is lehet, mert a kis távolságból indított repülő eszközök hatékony támadást tesznek lehetővé, például nyílt területen tartott állami ünnepségek esetén. Az ellenük való védekezés jókora feladatot ad a biztosítást végző szerveknek. Általános jelenség, hogy a fejlesztésekkel párhuzamosan a drónok reptethetőségi ideje és sebessége is növekszik. A sebesen repülő drón pedig az ellenreakciókra, az elhárításra rendelkezésre álló időt rövidíti le.

A drónokkal szembeni védekezés lehetőségei

Makkay Imre professzor a *Drónok háborúja* című tanulmányában részletesen bemutatja a drónok felderítésének és azonosításának lehetséges eszközeit.[21] Ezek közül kiemelhető az akusztikai felderítés, amely azon alapul, hogy drón jellegzetes zümmögő hangja a háttérzajoktól jól elkülöníthető és általa az eszköz akár egyedileg is azonosítható. Figyelhetők továbbá a pilóta nélküli repülő eszközök által használt kommunikációs frekvenciák, így már a fogyasztók számára is kifejlesztett észlelő-védelmi rendszerek jelzik a drónok közeledtét.[22] A drón működése közben keletkezett hő Thermal Infra Red op-

19 https://www.cnet.com/news/man-shoots-down-drone-hovering-over-house/#ftag=CAD590a51e

20 https://www.theguardian.com/us-news/2015/aug/04/drone-drug-delivery-ohio-prison-fight-heroin-marijuana-tobacco

21 Makkay Imre: Drónok háborúja. In: A nyílt információgyűjtés fejlődő területei. Tanulmánykötet. Belügyi Tudományos Tanács, Budapest, 2015

22 https://www.huffingtonpost.com/2013/03/20/domestic-drone-countermeasures_n_2916974.html

tika segítségével észlelhető. A drónok elleni harcban számos felhasználható technikai lehetőség és eszköz áll rendelkezésre, az elektronikai ellentevékenységtől kezdve a lézeren át az irányítható lövedékekig. E módszerek mellett enyhébb megoldást kínál, ha nagyobb drónnal leszállásra kényszerítik a fenyegetést jelentő kisebb méretű eszközt, vagy akár felülről hálót dobnak rá. Kísérleti jellegűnek tekinthető a genfi rendőrség azon megoldása, hogy francia és holland tapasztalatok alapján sasokat vet be drónok ellen. A nehezen tanítható vadon élő állatok esetében azonban a siker nem garantált.[23]

Jó megoldásnak tűnik és a gondatlan bűnelkövetések, szabálysértések számát is csökkenthetik a drónba épített és rendszeresen frissített szoftveres megoldások, amelyek automatikusan távol tartják az eszközt a tiltott helyektől (például repülőterek, állami létesítmények, állam által védett objektumok).

Látható, hogy a védekezéshez szükséges berendezések használata alapvetően speciális ismereteket, képzettséget és szakszerűséget követel meg. Megállapítható tehát, hogy – bár a „magánakciók” megjelenése teljeséggel sosem zárható ki – a gondatlan és bűnös szándékú drónhasználat következtében kialakuló veszélyhelyzetek elhárítása, megszüntetése egyértelműen rendészeti feladat kell hogy legyen, és megfontolandó, hogy az adott szituációban mely módszerek alkalmazhatók kockázatmentesen. Érvényesnek tekinthető az a szlogen is, hogy drón ellen drónnal lehet védekezni!

A jövő

A drónok száma minden bizonnyal növekedni fog, gondoljunk csak a játék kategóriájú multikopterekre vagy akár a cégek által használt komolyabb eszközökre. A jövő drónjai a maiakhoz képest azonban gyorsabbak, halkabbak, célszerűbbek lesznek, hosszabb időt tölthetnek a légtérben. A felszerelhető eszközök minősége is javulni fog, típusválasztékuk szélesedik. Egyszerűsödik az irányíthatóság. Mindezzel együtt egyre szélesebb rétegek számára lesz elérhető és használható egy ilyen távirányítással reptethető eszköz. Nincs messze az az idő, amikor a drónok a személyszállításból is kiveszik a részüket, Kínában például már túl van az első nyilvános repülésén a világ első önvezető és egyben utasszállító drónja. Egy szingapúri cég már 3D nyomtatóval is készít drónokat, amelyek felszállótömege két kilogramm alatti, két órát

23 http://www.origo.hu/itthon/20180226-a-genfi-rendorseg-sasokat-vet-be-a-dronok-ellen.html

képes a levegőben tölteni, és maximális repülési sebessége óránként hatvan kilométer. Megjelentek a piacon olyan szimulátorjátékok, amelyek segítségével szórakoztatóan sajátíthatók el a drónreptetés fogásai, anélkül hogy a használó összetörné a saját gépét, vagy veszélyeztetne másokat.

A drónok elleni védekezés céljából, az elhárítás lehetőségeit mérlegelve, sürgősséggel létre kellene hozni olyan területeket, amelyeknek állandó az légtérvédelmük, és megakadályozzák az illetéktelen drónok terület fölé repülését, mintegy függönyt hozva létre a terület határain. Az így kialakított „légifüggöny” minimalizálná például a drónbombák hatékony használatának lehetőségét, jelentősen csökkentené az egyéb veszélyeket.

Látható, hogy a drónok tekintetében a fejlődés rohamléptékű, mielőbb szükséges és hiánypótló tehát a drónreptetés szakmai szempontjainak kidolgozása, a vonatkozó jogszabályok megalkotása, a drónalkalmazás kereteinek meghatározása.

DOI: 10.38146/BSZ.2018.10.7

NYITRAI ENDRE

Az interoperabilitási e-nyomozás alapjai[1]

A hazai szakirodalom szerint a kriminalisztika belső rendszere két fő ágra bontható: általános (kriminalisztikai elmélet, krimináltechnika, krimináltaktika, a kriminalisztika története, kriminálstratégia) és különös részre (kriminálmetodika), azonban mindkét részhez kötődik a bűnügyi szolgálati ismeretek – titkos információgyűjtés.[2] Az elmúlt években (évtizedekben) újabb területek jöttek létre, fejlődtek ki, így a kriminalisztika általános és különös része tovább bővíthető.

Fontosnak tartom a titkos információgyűjtés és az elektronikus nyomozás (a továbbiakban: e-nyomozás) létjogosultságát kiemelni és elhelyezni a kriminalisztika rendszerében. A titkos információgyűjtés szerepét, önállóságát a kriminalisztikán belül már több kriminalista kiemelte, és utalt kulcsfontosságú szerepére. A titkos információgyűjtés nélkül a felderítés sok esetben (például a kiemelt, súlyos ügyekben, a szervezett bűnözés vagy a terrorizmus elleni küzdelemben) szinte lehetetlen lenne, vagy akadályokba ütközne, ami szintén veszélyeztetné az eredményes nyomozást, ezért fontos szerepet kaphatnak a különleges eszközökkel titokban, konspiráltan beszerzett információk, amelyek később, a bizonyítás során bizonyítékként jelenhetnek meg. A titkos eszközök, erők és módszerek alkalmazása nélkül előfordulhat, hogy lehetetlenné válik egyes kiemelt bűncselekmények felderítése és bizonyítása, valamint az elkövetők felelősségre vonása. A társadalom védelme indokolja a bűncselekmény felderítését, az elkövető felkutatását.

A technikai fejlődés eredménye az úgynevezett „okos” elektronikus eszközök, továbbá a digitalizálás megjelenése az egészségügyben vagy a közigazgatásban. Az elektronikus eszközök használata nélkül már el sem tudnánk képzelni a mindennapjainkat, az egészségügyet és a közigazgatást sem. Bárhová megyünk a világban, elektronikus-digitális nyomokat hagyunk magunk után, s mivel ezek életünk részévé váltak, segítik a napi tevékenységün-

1 A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, *A jó kormányzást megalapozó közszolgálat-fejlesztés* elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

2 Balláné Füszter Erzsébet – Lakatos János: A kriminalisztika ágai, belső rendszere, tudományos kapcsolatai. In: Lakatos János (szerk.): Kriminalisztika I. A kriminalisztika egyes elméleti kérdései. Rendőrtiszti Főiskola, Budapest, 2012, 41. o.

ket. Az elektronikus térben való szűrő-kutató tevékenység csaknem nélkülözhetetlen a bűnüldöző szervek munkájában.

A titkos adatgyűjtés, kriminalisztikai nyomozás, e-nyomozás

A hatósági adatgyűjtés formája nyílt és titkos is lehet.[3] Fontosnak tartom a 2017. évi XC. törvény előtti titkos információgyűjtési metódusok ismertetését, kiemelve létjogosultságát a kriminalisztikán belül. A titkos információgyűjtést és a titkos adatszerzést gyakran operatív kriminalisztikaként vagy a titkos felderítés kriminalisztikájaként is emlegetik. A bűnügyi titkos információgyűjtés és a titkos adatszerzés – összefoglalón: operatív kriminalisztika vagy a titkos felderítés kriminalisztikája – nyílt szabályozásával[4] felvetődik a kérdés, hogy ez önálló tudomány-e, vagy a kriminalisztika része.[5] A titkos információgyűjtés ajánlásainak elhelyezése a kriminalisztikán belül a rendszerváltozás után vált aktuális feladattá, mivel korábban minősített normákon alapult.[6] A titkos felderítés kriminalisztikája olyan területe a kriminalisztikának, amely a titkos információk keletkezésének törvényszerűségével és a megszerzésük, valamint az ajánlások kidolgozásával foglalkozik.[7] A titkos felderítés kriminalisztikájának tárgya a titkos információgyűjtés, illetve a titkos adatszerzés, amelynek célja annak eldöntése, hogy szükséges-e a nyomozás formális megindítása, illetve hogy a vádemelés megalapozására elegendő információ várható-e.[8] A titkos információgyűjtés az egyik nézőpont szerint a kriminalisztika általános és különös részében helyezhető el.[9] A titkos információgyűjtés során egyes krimináltechnikai, -taktikai és -metodikai ajánlások speciális alkalmazásáról beszélhetünk, és ez adja a kriminalisztikával va-

3 Fenyvesi Csaba: A védő és a titkos adatgyűjtés. Belügyi Szemle, 2001/11., 66. o.
4 A titkos információgyűjtést a rendőrségi, a titkos adatszerzést a büntetőeljárási törvény kodifikálta.
5 Ballané Füszter Erzsébet – Lakatos János: i. m. 49. o.
6 Katona Géza: A kriminalisztika belső tagozódása. In: Bócz Endre (szerk.): Kriminalisztika I. BM Duna Palota és Kiadó, Budapest, 2004, 63. o.
7 Finszter Géza: A titkos felderítés kriminalisztikája. In: Tóth Éva – Belovics Ervin (szerk.): A büntetőeljárás segédtudományai I. Pázmány Press, Budapest, 2015, 133. o.
8 Finszter Géza: A titkos információgyűjtés szabályozása a hatályos jogban. In: Irk Ferenc (szerk.): Kriminológiai Tanulmányok 37. Országos Kriminológiai Intézet, Budapest, 2000, 101–122. o.
9 Lakatos János: A kriminalisztika. A titkos információgyűjtés – a bűnügyi szolgálati ismeretek. In: Balláné Füszter Erzsébet – Kunos Imre – Lakatos János: Bevezetés a kriminalisztikába. Egyes kriminalisztikai tételek és kérdések. Rejtjel Kiadó, Budapest, 1999, 24–26. o. [Kriminalisztikai jegyzetek és tanulmányok]

ló kapcsolat alapját.[10] *Katona Géza* álláspontja, hogy a magyar kriminalisztikai szakirodalomban megjelentek olyan célkitűzések, amelyek a titkos információgyűjtésnek a kriminalisztikai rendszerbe történő integrálását célozták meg. Ez egyrészt a tudományág egysége, másrészt a *„gyakorlati bűnüldözési tevékenység törvényessége szempontjából fontos”*. A tudományos feldolgozás szükségességét alátámasztja a titkos információgyűjtéssel, a titkos adatszerzéssel összefüggő társadalmi megítélés és a szervezett bűnözéssel összefüggő érdekviszonyok megváltozása.[11] *Bócz Endre* a titkos információgyűjtés és a titkos adatszerzés keretében alkalmazott taktikai módszereket tárgyaló ismeretanyagot a krimináltaktika sajátos területének tekinti.[12] Véleményem szerint a titkos információgyűjtés és a titkos adatszerzés (összefoglalóan titkos adatgyűjtés) a kriminalisztika önálló részének tekinthető, amely a kriminalisztika általános és különös részében foglal helyet.

Fontos azonban kiemelni, hogy a büntetőeljárásról szóló 2017. évi CX. törvény (a továbbiakban: új Be.) a kérdéses témakörben jelentős változásokat vezetett be, mivel az új szabályozás megszünteti a titkos információgyűjtés és a titkos adatszerzés kettőségét. A titkos információgyűjtés és adatszerzés eszközeit és módszereit egységesen szabályozza a törvény. Az új Be. egyik legfontosabbnak tekinthető újítása *a bűnüldözési célú titkos információgyűjtés szabályainak a büntetőeljárásba integrálása,* amellyel a büntetőeljáráson kívüli és a büntetőeljárás keretében folytatott *titkos információszerzés szabályozásának elkülönüléséből fakadó gyakorlati,* jogalkalmazási probléma *elháríthatóvá válik.*[13]

A kriminalisztikai gondolkodás elemei (jogi normákhoz kötött; rekonstruktív gondolkodás; verziók alkalmazása; logikai módszerek; intuíció és fantázia; empátia; kételkedés; ügytípusismeret, tapasztalatok; kollektív bölcsesség; önértékelés; véletlen) már a büntetőeljárás megkezdése előtt is érvényesülhetnek, amikor a rendőrség a bűncselekmény elkövetésének megelőzése céljából titkos információgyűjtést folytat, vagy amikor a büntetőeljárás az előkészítő eljárással megindul. Az említett kriminalisztikai gondolkodás elemeit szem előtt tartva, valamint az új Be. rendelkezéseit elemezve (illetve a titkos információgyűjtés és a titkos adatszerzés kettőségének a meg-

10 Balláné Füszter Erzsébet: Kriminalisztikai ismeretek. NKE Szolgáltató Kft., Budapest, 2014, 11. o.

11 Katona Géza: A kriminalisztika és a bűnügyi tudományok. Gondolatok a 21. század kriminalisztikájáról. BM Kiadó, Budapest, 2002, 119–122. o.

12 Bócz Endre – Finszter Géza: Mi a kriminalisztika? In: Bócz Endre: Kriminalisztika joghallgatóknak. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2008, 13–14. o.

13 A 2017. CX. törvény indoklása. https://uj.jogtar.hu/#doc/db/4/id/A1700090.TVI/lr/chain39

szűnésével, a nyomozást megelőző eljárási szakasz bevezetésével) felvetődik a kérdés, hogy a kriminalisztikai szempontból definiált *nyomozás* fogalom – mint megismerő tevékenység – kiegészíthető-e újabb fogalmi elemekkel. A kriminalisztikai nézőpontból elfogadott fogalmak alapján a nyomozás

– *a múltbeli releváns esemény igazságnak megfelelő rekonstruálására* és az eljárási célok elérésére irányuló sokoldalú szellemi és gyakorlati tevékenység, amely a szükséges és lehetséges cselekvések tervszerű, tudatos, a vonatkozó eljárási szabályoknak megfelelő végrehajtása útján valósítható meg[14];
– *a múltban lejátszódott esemény rekonstruálására irányuló* sokoldalú szellemi és gyakorlati tevékenység, amely a vizsgált eseményre vonatkozó eljárási céloknak és szabályoknak megfelelően a szükséges és lehetséges cselekvések tervszerű és tudatos végrehajtásával az objektív igazság megállapítására irányul.[15]

A kriminalisztikai értelemben vett nyomozási fogalmak legtöbbször a múltbeli releváns esemény megismerését és rekonstruálását emelik ki, ami helytálló, de kiegészíthető azzal, hogy *a nyomozás kriminalisztikai nézőpontból a jelenben zajló és a jövőben elkövetni kívánt esemény megismerésére irányuló tevékenység is.* A sorozat-bűncselekmények (például gépjárművek eltulajdonítása) esetén a kriminalisztikai alapkérdésekre alapozva – a tervezés és az elemző-értékelő tevékenység nyomán – a bűncselekménnyel kapcsolatba hozható személyek figyelemmel kísérhetők (megfigyelhetők). Továbbá a nyomozó hatóság célja *az érintett személyek tettenérése, elfogása, azonosítása és az általuk a jövőben megvalósítani kívánt események (bűncselekmények) meghiúsítása, illetve a kimenetelének a befolyásolása.*[16] Az új Be. 215. § (7) bekezdése alapján *„a leplezett eszközök alkalmazására feljogosított szerv a bűncselekmény megszakítása, a bűncselekmény elkövetőjének azonosítása, illetve a bizonyítás érdekében az információ forrásának leplezésével a leple-*

14 Balláné Füszter Erzsébet – Lakatos János: A nyomozás, a felderítés és a bizonyítás. In: Lakatos János (szerk.): Kriminalisztika I. A kriminalisztika egyes elméleti kérdései. Rendőrtiszti Főiskola, Budapest, 2012, 97. o.

15 http://ibolyatibor.atw.hu/Sajat/11.doc

16 A bűncselekmény-sorozat megszakítása, felderítése és az elkövetők leleplezése érdekében kriminalisztikai csapda mint adatgyűjtési módszer alkalmazható (például csapdagépkocsi telepíthető). Az adatgyűjtés során megismerhetjük egyrészt a múltbeli releváns eseményt (például ha az adatgyűjtésig ismeretlen volt az elkövetési mód és az elkövetésben részt vevő személyek) vagy a különleges eszköz használatával (telefonlehallgatással) a folyamatban lévő bűncselekmény elkövetésének, vagy a jövőben tervezett bűncselekménynek a részleteit.

zett eszköz alkalmazásával érintett személlyel valótlan vagy megtévesztő információt közölhet. Az információ továbbításához a leplezett eszközök alkalmazására feljogosított szerv titkosan együttműködő személyt is igénybe vehet."[17] A törvény indoklása kiemeli, hogy *„...a törvény emellett új eszközként határozza meg a megtévesztő információk közlését, amelynek alkalmazását szigorú tilalmak keretei között teszi lehetővé. A törvény által meghatározott tilalmak egyrészt biztosítják a tisztességes eljárás garanciális folytatását, másrészt azt hivatottak megakadályozni, hogy a leplezett eszköz a bizonyítást ne torzítsa. Hangsúlyozni kell továbbá, hogy a leplezett eszközök alkalmazásának általános szabályai ebben az esetben is irányadók, azaz a megtévesztő információk közlése nem járhat az alkalmazás céljához képest aránytalan és szükségtelen következményekkel…"*

Véleményem szerint a jelenlegi 215. § (7) bekezdése szükséges és elengedhetetlen, de kiegészítésre szorul, mivel a *„valótlan vagy megtévesztő információ"* közlésével egyrészt sérülhet a tisztességes eljárás, másrészt a bizonyítás torzulhat, ha *„a valótlan vagy megtévesztő információ"* a bűnügyre vonatkozó adatokra épül. Álláspontom szerint kizárólag csak olyan valótlan információ közölhető, amely nem függ össze az üggyel, nem tartalmaz téves információt a bűnügyre (a rendelkezésre álló adatokra) vonatkozóan, és az adatszolgáltató nem szerez tudomást arról, hogy az adott bűnügyre irányult az adatgyűjtés. Nem szabad befolyásolni a kérdéses üggyel kapcsolatban az adatszolgáltatót, mivel a befolyásoló, megtévesztő információknak rengeteg negatív hatásuk lehet: a bűncselekmény felderítése megakadhat; hamis nyilatkozattételre késztetheti az adatszolgáltatót, és megnehezítheti nyilatkozata ellenőrzésének lehetőségét. A keletkezett információ hatással lehet a bizonyítási eljárásokra, amely során szintén hamis adatok születhetnek, és összeállhat egy olyan hamis adatokra épülő bizonyítási láncsorozat, amely látszatra azt mutatja, hogy a hamis adatok megfelelnek a valóságnak. Befolyásolják a látottakat, a hallottakat; olyan információ rögzítésére kerülhet sor, amelynek tartalma nem felel meg a valóságnak, ez pedig justizmordhoz is vezethet. Szükséges lenne az új Be. 215. § (7) bekezdését kiegészíteni azzal, hogy a büntetőeljárás során keletkezett (rendelkezésre) álló adatokkal összefüggésben valótlan vagy megtévesztő adatokat nem közölhet.

---

17 Míg a 215. § (8) szerint a (7) bekezdésben meghatározott leplezett eszköz: terhelt vagy tanú kihallgatása, illetve bizonyítási cselekmény során nem alkalmazható; nem tartalmazhat a törvénnyel össze nem egyeztethető ígéretet; és nem valósíthat meg fenyegetést vagy felbujtást, továbbá nem terelheti az érintett személyt annál súlyosabb bűncselekmény elkövetése irányába, mint amelyet eredetileg elkövetni tervezett.

A kriminalisztika struktúráját nagymértékben befolyásolják a technikai változások, a digitális adatok, az interoperabilitási e-nyomozási ismeretek. Napjainkat erősen jellemzi az elektronikus eszközök használata, ezek igénybevételével „elektronikus, digitális nyomokat” hagyunk magunk után. A „digitális nyomok” verziók felállításához, nyomozási cselekmények foganatosításához vagy azok elősegítéséhez vezethetnek. A kriminalisztika új ágazattal bővíthető – figyelembe véve a tudomány és a technika fejlődését –, mégpedig az úgynevezett raszternyomozással (kriminalisztikai interoperabilitási e-nyomozási) ismeretekkel, amely általános és különös részi tartalommal bír *(táblázat)*.

A kriminalisztika ágai

Kriminalisztika	
Általános rész	Különös rész
Kriminálatechnika Krimináltaktika Kriminálstratégia	Kriminálmetodika
(bűnügyi szolgálati ismeretek) Raszternyomozás (e-nyomozási ismeretek)	

Az interoperabilitási e-nyomozás a kriminalisztika új kutatási területének is tekinthető. Az interoperabilitás eddig a Netzsaru vonatkozásában valósult meg. Jelenleg az interoperabilitási e-nyomozás alapjáról, a raszternyomozásról beszélhetünk.[18] Az interoperabilitási e-nyomozás keretében meg kellene teremteni az átjárhatóságot a közigazgatási, egészségügyi, pénzintézeti, elektronikus hírközlési, illetve egyéb nyilvántartások között, így a nyomozó részletes dokumentumot kapna az ellenőrzésben érintett személy kapcsán keletkezett elektronikus adatokról. A rövid idő alatt beszerzett információ egy láncfolyamatot, információáradatot indíthatna el.

Az interoperabilitás a különböző informatikai rendszerek együttműködésre való képességét jelenti.[19]

Az e-nyomozás azt jelenti, hogy a nyomozó hatóság a közvetlenül vagy a közvetetten elérhető adatbázisokból kér információt a felderítés és a bizonyí-

18 Az interoperabilitás, az adatbázisok közötti átjárhatóság megteremtéséhez nemcsak eljárásjogi garanciákat, illetve kriminalisztikai ajánlásokat kell megfogalmazni, hanem informatikailag is meg kell teremteni a szükséges háttérbázist. Az e-nyomozás célja, hogy minél több elektronikus információt rövid idő alatt el lehessen érni, erőfeszítés nélkül, ehhez egy virtuális tér létrehozása szükséges.

19 https://fogalomtar.aeek.hu/index.php/Interoperabilit%C3%A1s

tás érdekében, amikor is taktikai ajánlásokat alkalmaz a nyomozás sikeressége érdekében.

A közvetlenül elérhető nyilvántartások olyan nyilvántartások, amelyekbe a nyomozó hatóság tagjainak joguk van belépni, és a rendszerbe bármikor lehetséges a belépés anélkül, hogy megkereséssel kellene fordulni a nyilvántartást létrehozó – természetes vagy jogi – személyhez. A közvetetten elérhető nyilvántartások olyan adatbázisok, amelyekhez a nyomozó hatóság (rendőrség) tagjainak nincs belépési jogosultságuk, így az adatbázisban rögzített információkat külső megkeresés útján érhetik el.

A nyilvántartások jelentősége a nyomozásban

Sallai János szerint a világ összekapcsoltságából adódóan felerősödik, valamint folyamatosan új lehetőségek előtt áll a szervezett bűnözés, amelynek az a célja minél rövidebb idő alatt a lehető legtöbb, anyagi haszonszerzés céljára használható adat megszerzése különböző módon. Így a XXI. század globalizált világában a bűnüldözés kockázatok és próbatételek előtt áll. A globalizáció főbb jellemzői közé tartozik például a világ összekapcsoltsága, az információs és kommunikációs technológiák fejlődése, gyorsulása. A Föld bármely részén tartózkodó személy könnyedén elérhető a mobiltelefon, illetve az internet segítségével. A legtöbb embernek van telefonja, laptopja, internet-összeköttetése, amelyen keresztül pénzügyi és hivatali ügyeit és vásárlásait intézi. Ugyanezek a felületek azonban egyben a bűnözés melegágyai is. A technikai eszközök jelentős segítséget nyújtanak a szervezett bűnözői köröknek a céljaik eléréséhez.[20]

Sallai János véleménye nem vitatható. A bűnüldöző szerveknek azonban lépést kell tartaniuk a bűnözéssel. Szintén a lehető legrövidebb idő alatt kell megszerezni a (digitális) adatokat a felderítés és a bizonyítás érdekében. Több mint két évtizede egyeztetések zajlanak a világban az igazságügyi informatikai vizsgálatokkal kapcsolatos szabványkövetelmények kialakítása tekintetében, továbbá a papíralapú nyomokat felváltják az elektronikusak.[21]

A bűnözés elleni küzdelem nélkülözhetetlen forrásai az adatbázisok. A digitális világ robbanásszerű fejlődése során rengeteg elektronikus információ

20 Sallai János: A globalizáció rendészeti kihívásai. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok A változó rendészet aktuális kihívásai című tudományos konferenciáról. Pécs, 2013, 38–39. o. [Pécsi Határőr Tudományos Közlemények XIV.]

21 Fenyvesi Csaba: A digitális adatok jelentősége a kriminalisztikában. Jura, 2016/2., 52–53. o.

keletkezett. A bűnözők által elkövetni kívánt bűncselekmények és a terrorizmus terjedésének megelőzéséhez, a bűnszervezetek felderítéséhez elengedhetetlen a nyilvántartásokban szereplő információk feldolgozása, elemzése és értékelése. A digitális ismeretek hiányában az állam védelmi feladata és működtetése nehezen kivitelezhető, ehhez megfelelő információkra, ismeretekre van szükség, ami hatékony fellépést tesz lehetővé a bűnözéssel szemben.

A kriminalisztikai információ aktuális problémái című tanulmányukban *Julian Vlagyimirovics Szolopanov* és *Szemen Szemjulovics Ovcsinszkij* már a hetvenes évek elején említést tesznek a kriminalisztika és az informatika kapcsolódásáról és az így létrejött ismeretkomplexumról, a kriminalisztikai informatikáról mint önálló tudományágról.[22]

Tremmel Flórián már 1974-ben megfogalmazta, hogy *„aligha kétséges, hogy éppen a kibernetikai módszerek és eszközök felhasználása lesz a jogtudományok és a bűnügyi tudományok fejlődésének egy fő mozgató rugója”*[23]. Több év elteltével a feltételezés beigazolódott: az informatika valóban meghatározó szereplővé vált a bűnözés elleni küzdelemben. A Pécsi Tudományegyetem Állam- és Jogtudományi Karának büntetőjogi tanszéke – a Magyar Tudományos Akadémia Pécsi Bizottsága és a Baranya Megyei Rendőr-főkapitányság támogatásával – 1974. április 25–27. között egy kerekasztal-konferenciát szervezett, amelyen *Déri Pál* kifejtette, hogy a nyomozó folyamatosan harcol az információveszteség ellen, azonban a küzdelemben nagy segítséget nyújthat a gépi adattárolás és annak elmélete, az informatika. Déri álláspontja szerint az integrált bűnüldözés elősegítheti a nyomozás hatékonyságát (például az utazó és városi bűnözőkkel szemben), mivel a helyi információk mellett fel kell használni központi számítógépekben tárolt információt is.[24] Déri már 1971-ben megfogalmazta a számítógép és a nyilvántartások fontosságát. Álláspontja, miszerint *„minél gazdagabb »adatbankokat« hozunk létre, annál kevesebb feladat marad a hagyományos nyomozói munka számára, illetve több idő jut a kriminalisztikai gondolkodásra […]”*[25] helytálló. A nyilvántartások hozzásegíthetnek a bűnelemzéshez, a nyomozás megtervezéséhez és a verziók pontosításához.[26]

---

22 J. V. Solopanov – S. S. Ovčinskij: A kriminalisztikai információ aktuális problémái. IX. Nemzetközi Kriminalisztikai Szimpózium. Berlin, 1973. február 5–10. Belügyi Szemle, 1973/7., 34. o.

23 Tremmel Flórián: Az információ kriminalisztikai szerepéről. Belügyi Szemle, 1974/11., 60–61. o.

24 Uo.

25 Déri Pál: A nyomozás-szervezés korszerűsítésének távlatai. Belügyi Szemle, 1971/7., 30. o.

26 Bócz Endre – Finszter Géza: A rendészeti adatkezelés és a bűnügyi nyilvántartási rendszer. Rendőrségi adattárak, gyűjtemények. In: Bócz Endre: Kriminalisztika joghallgatóknak. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2008, 274. o.

A bűnözői körök kihasználják a digitális technológia vívmányait, ezért a kriminalisztikának folyamatosan nyomon kell követnie a technikai változásokat, valamint dolgoznia kell a megelőző és felderítő eszközökön. Az internet kommunikációs eszközzé vált a szervezett bűnözők és a terroristák számára.[27] A bűnözés különböző formái kevésbé függenek bizonyos földrajzi területektől (például számítógépes bűnözés).[28] Egyre inkább növekszik a virtuális térben létrejövő bűnözői csoportok száma.[29] A kormányok, a bűnüldözés, az akadémiai kutatók és a kiberbiztonsági szakemberek felhívják a figyelmet arra, hogy a bűnözői csoportok egyre inkább részt vesznek a digitális bűnözésben, az elkövetői csoportok kiterjesztik a tevékenységüket a digitális világra.[30] A szervezett bűnözés, illetve a terrorizmus elleni küzdelemben fontos szerepet tölt be a digitális felderítés, és a digitális adatoknak a bűnüldözés érdekét is szolgálniuk kell.[31] A világot a technológiai átalakulás jellemzi, több milliárd ember használja az internetet mint infokommunikációs infrastruktúrát, továbbá üzleti tevékenységet is folytatnak. Még a kormányok is kapcsolatba kerülnek egymással, ezért fontos a kiberbiztonság, a biztonságos internet megteremtése is. Mindez műszaki és egyben politikai kezdeményezéseket is követel.[32]

Ahhoz, hogy a kriminalisztikai gondolkodás betölthesse szerepét, nem elegendő annak ismerete, hogy léteznek különféle nyilvántartások. Azt is tudni kell, hogy azokból mit lehet lekérni. A digitális adatok nélkülözhetetlenek a kriminalisztikai alapkérdések megválaszolásához. A digitális adatokkal végzett vizsgálat (elemző-értékelő tevékenység) során rekonstruálni lehet a bűncselekményeket, így választ kaphatunk a *mi történt?* kérdésre is.[33] Fontos

27 Friedrich W. Korkisch: Organized crime, the enlargement of the EU, and the public. AARMS, vol. 4, no. 2, 2005, p. 358.

28 Fredrik Fors – Dan Hansén: Pressured to learn? Swedish police experiences of curbing organized crime. Journal of Scandinavian Studies in Criminology & Crime Prevention, vol. 15, issue 1, 2014, pp. 19–20.

29 Anita Lavorgna – Anna Sergi: Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom. International Journal of Cyber Criminology, vol. 10, issue 2, 2016, pp. 170–175.

30 Roderic Broadhurst – Peter Grabosky – Mamoun Alazab – Brigitte Bouhours – Steve Chon – Da Chen: Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working paper, 15. 05. 2013, pp. 19–20.

31 Marcus K. Rogerss – Kate Seigfried: The future of computere forensics: a needs analysis survey. Computers & Security, no. 23, 2003, pp. 12–16.

32 Aaron Kleiner – Paul Nicholas – Kevin Sullivan: Linking Cybersecurity Policy and Performance. Microsoft Corporation, 2013, pp. 3–27.

33 Eoghan Casey: Digital Evidence and Computer Crime, Forencis Science, Computers and The Internet. 3rd Edition. Maryland, 2011, pp. 14–26.

a tudásanyag folyamatos bővítése, a tudományos-technikai követelmények, eredmények feldolgozása.

Raszternyomozás

Napjainkat már elképzelni sem tudnánk számítógép nélkül. A rendvédelmi szervek a nyomozás folyamán beszerzett adatok egy részét rögzítik (az erre vonatkozó jogszabályi felhatalmazások alapján), nyilvántartják, mint ahogy az egyén esetén az egészségügyi intézmények, vagy akár a pénzforgalmi adatokat rögzítő számlavezető bankok.

A nyomozó hatóság munkáját, illetve a nyomozás eredményességét (a nyomozási feladatok végrehajtását) nagymértékben befolyásolja, hogy milyen mennyiségű és minőségű adatok állnak rendelkezésre. A raszternyomozás továbbfejlesztése következtében az adatbázisok közötti átjárhatóság és az együttműködés kiépítésével, valamint a taktikai ajánlások megfogalmazásával beszélhetünk interoperabilitásról.

Hazánkban a raszternyomozás keretében csak egyes adatbázisokat tud közvetlenül elérni a nyomozó hatóság tagja, így adatelemző munkát csak részben tud közvetlenül végezni.[34] A szervezett bűnözői körök legtöbbször a konspiráció következtében utolérhetetlenek, de elektronikus nyomot azért hagynak maguk után, így elengedhetetlen a raszternyomozás jelentőségének, ismeretanyagának elsajátítása és a hiányzó jogszabályi környezet megalkotása.

Ha szeretnénk elhelyezni a raszternyomozást az adatgyűjtés rendszerében, a helye a meglévő adatgyűjtési módszerek körében lenne, a puhatolás, a környezettanulmány, a megfigyelés, a lakosság bevonása az adatgyűjtésbe, a kriminalisztikai csapda és a megkeresés mellett. Bár így elég szűk kategóriáról beszélhetünk, hiszen az adatgyűjtés magában foglalja a nyomozást az elrendeléstől egészen az iratismertetésig.

A jövő nyomozását jelenti az e-nyomozás, mivel így idő takarítható meg. Az íróasztal mögül gyorsan és könnyen, számítógépen keresztül lehetne információhoz jutni, az információáradat felgyorsulna, és a tudomásra jutó adatok elősegítenék a kriminalisztikai gondolkodást.

---

34 Az új Be. a kérdéses témakörben jelentős változásokat hoz, mivel az új szabályozás logikus rendszerbe helyezi a büntetőeljárás során eljáró szervekre irányadó ágazati jogszabályokban szabályozott adatgyűjtő tevékenységet, továbbá a megkeresést. 2017. évi XC. törvény indokolása a büntetőeljárásról. https://uj.jogtar.hu/#doc/db/4/id/A1700090.TVI/lr/261

Egyetértek Fenyvesi Csaba álláspontjával, amely szerint a raszternyomozás fogalma, illetve ismérvei a hagyományos nyomozási módszerektől a következők alapján különböztethetők meg: *„adattárakban való olyan keresést, kutatást jelent, amely mintegy szitaként (magyarosan raszterként, azaz hálóként) működik és a bűncselekményekhez kötődő lehetséges elkövetőket tudja kigyűjteni, leszűkíteni, akár egyetlen személyre is. A hagyományos nyomozási módszerektől három ismérv különbözeti meg:*

1. *a számítógépes keresést, kutatást adattárakban (nem az utcákon, nem a határoknál stb.) folytatják,*
2. *a kutatás rendőrségi-bűnügyi adatokon túlmenően más nyilvántartásokra is kiterjed,*
3. *meghatározott személyek után nyomoznak, akik bizonyos kritériumoknak megfelelnek. (A kiválasztott személyek semmit nem sejtenek arról, hogy adatellenőrzés alatt állnak.)”*[35]

Véleményem szerint a raszternyomozás olyan adatgyűjtési módszer, amelynek során a kutatás közvetetten vagy közvetlenül elérhető adatbázisokban történik, és az elektronikusan rögzített adatok a nyomozás előbbre vitelét szolgálhatják. Az adatok többsége azonban a felderítést, és nem a bizonyítás tárgyát képezi, amely irányulhat ismert vagy ismeretlen személyazonosságú egyénekre.

A raszternyomozás szinte korlátlan lehetőséget ad a bűnüldöző szolgálatnak, de az elmúlt években a személyes adatok védelmére hivatkozva szót emeltek ellene. A World Trade Center elleni 2001. szeptember 11-i merénylet óta azonban előtérbe került az alkalmazása.[36] A nyilvántartásokban rögzített adatok a személy megismeréséhez szükséges információkat tartalmazhatnak (például a Netzsaruban rögzített iratban, szakértői véleményben, a személy jellemére vonatkozó információ felhasználható a kihallgatási taktika kialakításában), vagy olyan adatokat, amelyek a nyomozási cselekmények végrehajtásához szükségesek (például a házkutatás esetén az ingatlan-nyilvántartás Takarnet rendszerének segítségével az objektum alaprajza alapján meghatározhatók a behatolás lehetőségei).

35 Fenyvesi Csaba: Kriminalisztika, In: Tremmel Flórián: Bűnügyi nyilvántartás. Dialóg Campus Kiadó, Budapest–Pécs, 2009, 236. o.

36 Fenyvesi Csaba: A bűnmegelőzés és a Határőrség. In: Hautzinger Zoltán (szerk.): Tanulmányok a Határőrség szerepe a bűnmegelőzésben című konferenciáról. Pécs, 2003, 183. o. [Pécsi Határőr Tudományos Közlemények II.]

A szerb nyomozó hatóság megkülönbözteti az úgynevezett pozitív vagy negatív raszterkeresést. A pozitív megerősítheti, hogy kik azok a személyek, akik elkövetőként számításba jöhetnek bizonyos jellemzők alapján (például ha a közlekedési baleset helyszínéről az elkövető egy ritka típusú gépkocsival menekül, akkor az ilyen járművek vezetői potenciális elkövetőként szóba kerülhetnek, amit ellenőrizni kell), míg a negatív raszterkeresés egyes személyi köröket kizár.[37]

Az interoperabilitás és az e-nyomozás

A szervezett bűnözésnek a bűnözésen belüli részaránya nem elhanyagolható, továbbá a szervezett bűnözés területén jelentős látencia vélelmezhető. *Az adatbázisokban folytatható információszerző tevékenység megkönnyítené a szervezett bűnözés elleni küzdelmet,* lehetővé válna a büntetőeljárásban szereplő személyek, tárgyak felkutatása, kihallgatása, bizonyítási eszközök beszerzése, értékelése, a nyomozási feladatok elvégzéséhez szükséges adatok összegyűjtése, a nyomozási tervben foglaltak (például nyomozási cselekmények, verziók ellenőrzése) végrehajtása.

A bizonyítást mint átfogó megismerési folyamatot is megkönnyíti az informatikai eszközök használata. Jelenleg a nyomozó hatóságnak írásos megkeresést kell küldenie egyes nyilvántartást vezető szervekhez (például pénzintézetek) annak érdekében, hogy megtudja, rögzítettek-e olyan elektronikus adatot (információt), amely a nyomozás eredményességéhez hozzájárulna. Ezt az adatgyűjtési módszert, amikor a nyomozó adatbázisból kér információt, raszternyomozásnak nevezik. A válasz megérkezése azonban több napot is igénybe vehet, ezzel veszélyeztetve a nyomozás kimenetelét is. A papíralapú ügyintézés nehézségeit – a nyomozás hatékonysága szempontjából – a digitális ügyintézés tudja áthidalni. Egy olyan koncepció kialakítása szükséges, amellyel a nyomozó hatóság kihasználhatná a nyilvántartási rendszer lehetőségei. Elengedhetetlen a hatékony nyomozás érdekében az adatbázis kínálta lehetőségek kihasználása, amivel a nyomozó hatóság időt nyerne, valamint az eddigi legalább nyolc-, legfeljebb harmincnapos határidőkorlát nélkül gyorsabban jutna a releváns adathoz, és így javulna a nyomozás eredményessége. A felvetődő időveszteség is alátámasztja az elektronikus nyomozás alapjainak lefektetését, és meggyorsítja az adatok áramlását.

37 Aleksandar Bošković – Zoran Pavlović: Special Evidentiary Actions in the Function of Combating Organized Crime in Serbia. Journal of Eastern European Criminal Law, no. 1, 2015, pp. 52–53.

Az új tudományos eszközök és módszerek lehetővé teszik a megismerés tételeinek fejlesztését, az e-nyomozás továbbfejlesztését, amelynek az elektronikus közigazgatás és az elektronikus egészségügy mintájára kellene felépülnie.

Interoperabilitás figyelhető meg a Netzsaru programban is, mivel a nyomozó az adatbázisba történő belépése után bármelyik nyomozás (büntetőeljárás) irataiba betekinthet, illetve adatot vihet fel (belépési jogosultságtól függően) anélkül, hogy az ügy előadóját személyesen vagy írásban meg kellene keresnie. Azonban az adatbázisok közötti interoperabilitás megteremtése számos akadályba ütközik, ez legtöbbször *az adatok háttérkörnyezetéből,* valamint *a nem egységesen értelmezett adatformátumokból* adódik. *Szükséges lenne a kommunikációs rendszerek összekapcsolása* (egy *központi adatbázis létrehozása*), ez *számos akadályba ütközhet* az információs *interoperabilitás hiányában.* Az információs interoperabilitás *„különböző szereplők kölcsönös képessége információk közös értelmezésen alapuló, a hatékony együttműködéshez szükséges cseréjére”,* tágabb értelemben magában foglalja a környezeti jelenségek, hatások azonos módon történő értelmezését is.[38] A nyomozás megköveteli a különböző forrásokból származó információk felhasználását, összekapcsolását, ennek alapvető feltétele az adatbázisok közötti információcsere interoperabilitása. *A rendészeti (bűnügyi) nyilvántartásoknak, informatikai rendszereknek kompatibiliseknek, interoperábilisoknak kellene lenniük a közigazgatási és egészségügyi informatikai rendszerekkel,* illetve meg kellene felelniük az interoperabilitás követelményrendszerének.

Napjainkban a szervezett bűnözés elleni küzdelem, illetve a terrorizmus elleni védelem egyre inkább függ a rendelkezésre álló információktól, valamint az informatikai rendszerektől. Bár az informatikai támogatás színvonala javul, ezzel párhuzamosan egyre nagyobb gondot okoz az informatikai rendszerek közötti információcsere, információmegosztás.[39] Egyes szükséges információk *különböző szervezetek* különböző informatikai rendszereinek *egymástól eltérő adatbázisaiban állnak rendelkezésre, és legtöbbször ezek az informatikai rendszerek nem képesek horizontálisan* (azonos szinten lévő szervezetekkel), vagy *vertikálisan* (helyi, regionális vagy központi szervekkel) *információt cserélni, így a szükséges információk nem jutnak el az érintett szervhez,* vagy csak késve, más úton. Továbbá az egyes szervezeteknél keletkező, terrorista személyre, bűnszervezetre vonatkozó információ nem

38 Munk Sándor: Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései. MTA doktori értekezés, 2007, 41. o.
39 Uo. 100. o.

mindig jut el a másik szervhez, valamint az egyes államoknak olyan bűnszervezetre vagy terrorizmusra vonatkozó nyilvántartásaik vannak, amelyeket a másik állam nem ér el.[40] Az ilyen akadályok leküzdéséhez együttműködés lenne szükséges, amelynek előfeltétele lenne a nyilvántartási rendszerek között az interoperabilitás megteremtése, azaz egy interoperabilitási stratégia megalkotása.

Az e-nyomozás megvalósulásával a nyomozó hatóság közvetlenül hozzáférhetne a különböző intézmények adatbázisaihoz, mintha nála keletkezett volna az információ.

A bűnözés ellen a klasszikus módszerekkel csak részben lehet küzdeni, tehát új e-nyomozási ismeretek kidolgozására van szükség. A korszerű nyomozás megköveteli, hogy a digitalizált információ elérhető legyen a nyomozó hatóság tagja számára, ami egy információs lánc kialakításához, körforgásához járulhat hozzá, és a cseréjével elősegíti a kriminalisztikai gondolkodást. Továbbá leküzdi a személyforrásoknál felvetődő veszélyt, az idő múlását, amely az emlékképek halványulásához vezethet.

Összegzés

A bűnözői kör tagjai által elkövetett bűncselekmények, illetve egyéb bűncselekmények nyomozásakor segítségül szolgálhatnak az e-nyomozási ismeretek. Ha a nyilvántartásokat nem használja a bűnüldöző szerv, mert például nem ismeri azoknak a tartalmát, akkor adatveszteség állhat be, amely kockázati tényezőként a nyomozás eredményességét veszélyezteti. Ezért lenne fontos az adatbázisok teljes körű használata, illetve a gyakorlati gondolkodás formálása, valamint ajánlások megfogalmazása. Az így beszerzett információk elősegíthetik például az eljárási cselekmények (vagy különleges eszközök, mint például a lehallgatás) bevezetését, valamint a kényszerintézkedések végrehajtását, továbbá fontos szerepet képviselhetnek a kriminalisztikai gondolkodásban, illetve a verziók felállításában.

40 Uo.

DOI: 10.38146/BSZ.2018.10.8

FOGARASI MIHÁLY – GERZSENYI EGON – VARGA CSILLA LAURA

A morálisan elítélt viselkedésmódok perspektívafelvételre gyakorolt hatásai rendőrök és civilek körében[1]

Mindazon esetekben, amikor az egocentrikusperspektíva-felvétel[2] a másik személy informáltsága, ismeretei, vélekedései kapcsán jelenik meg, a *„tudás átka”*[3] néven ismert jelenséggel állunk szemben. A tudás átka nem más, mint a saját tudásunk irányában létrejövő elfogultság. A megítélő ilyenkor a számára rendelkezésre álló információkból indul ki, azt feltételezve, hogy amit ő tud, azt a másiknak is biztosan tudnia kell.

Az egocentrikusperspektíva-felvétel – közte a „tudás átka” jelenségének – veszélye általában a bűnüldözési tevékenység, de különösen a vallomások felvétele során jelentős mértékben van jelen. Hatása adott esetben súlyos lehet, megalapozatlan szakmai döntésekhez, téves ténymegállapításokhoz vezethet. Ezért meglepő, hogy tudomásunk szerint ezt az összefüggést a rendészettudományok még nem tették kutatásaik tárgyává.

1 A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, *A jó kormányzást megalapozó közszolgálat-fejlesztés* elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* működése során, a Nemzeti Közszolgálati Egyetem felkérésére készült.

2 Jean Piaget – Bärbel Inhelder: The child’s conception of space. Routledge–Kegan Paul, London, 1956; Simon Baron-Cohen – Alan M. Leslie – Uta Frith: Does the autistic child have a “theory of mind”? Cognition, no. 21, 1985, pp. 37–46.; Boaz Keysar – Shuhong Lin – Dale J. Barr: Limits on theory of mind use in adults. Cognition, no. 89, 2003, pp. 25–41.; Boaz Keysar – Dale J. Barr – Jennifer A. Balin – Jason S. Brauner: Taking perspective in conversation: The role of mutual knowledge in comprehension. American Psychological Society, vol. 11, no. 1, 2000, pp. 32–38.; Boaz Keysar – Dale J. Barr – Jennifer A. Balin – Timothy S. Paek: Definite reference and mutual knowledge: Process models of common ground in comprehension. Journal of Memory and Language, no. 39, 1998, pp. 1–20.; Susan A. J. Birch – Paul Bloom: Understanding children’s and adults’ limitations in mental state reasoning. Cognitive Sciences, vol. 8, no. 6, 2004; Susan A. J. Birch – Paul Bloom: The Curse of Knowledge in Reasoning About False Beliefs. Psychological Science, vol. 18, no. 5, 2007

3 Colin Camerer – George Loewenstein – Martin Weber: The curse of knowledge in economic settings: an experimental analysis. Journal of Political Economy, no. 97, 1989, pp. 1232–1254.

A felnőttkori egocentrikusperspektíva-felvétel alakulását befolyásoló tényezők alapkutatása már az eddigiek során is számos, annak elfogultságához vezető tényezőt tárt fel.[4]

Azonban, tudomásunk szerint *a morális szempontból eltérően súlyozott jelentést hordozó helyzetek perspektívafelvételre gyakorolt lehetséges hatását még nem vizsgálták.* Fontosnak tartjuk annak kimunkálását, hogy a morális megítélés szempontjából különböző súlyú bűncselekmények felderítésével összefüggésben a nyomozóknál mennyire sikeres a gyanúsítottak perspektívájának felvétele, ami ez utóbbiak tényleges informáltsága megítélésében alapvető szerepet játszik.

A bűnfelderítés, mert tárgya valamely elkövetett bűncselekmény, a morális megítélés szempontjából éppen ilyen, többé-kevésbé súlyozott kontextusban zajlik. Ez a körülmény indokolja, hogy vizsgálat tárgyává tegyük azt, hogy a nyomozati cselekmények során felhalmozódó információk elfogulatlan értelmezését, megítélését számos alkalommal döntő mértékben befolyásoló perspektívafelvétel alakulására vajon milyen hatást gyakorol a nyomozás tárgyát képező aktuális bűnügy közmegítélés szerint egyértelműen értelmezhető erkölcsi súlya. E megfontolásból következik a kutatás első kérdésfeltevése: a morális megítélés szempontjából különböző súlyú bűncselekmények nyomo-

---

4 Boaz Keysar – Shuhong Lin – Dale J. Barr: i. m.; Boaz Keysar – Dale J. Barr – Jennifer A. Balin – Jason S. Brauner: i. m.; Boaz Keysar – Dale J. Barr – Jennifer A. Balin – Timothy S. Paek: Definite reference and mutual knowledge: Process models of common ground in comprehension. Journal of Memory and Language, no. 39, 1998, pp. 1–20.; Daniel R. Ames: Inside the mind-reader's toolkit: projection and stereotyping in mental state inference. Journal of Personality and Social Psychology, no. 87, 2004, pp. 340–353.; Nicholas Epley – Boaz Keysar – Leaf van Boven – Thomas Gilovich: Perspective taking as egocentric anchoring and adjustment. Journal of Personality and Social Psychology, no. 287, 2004, pp. 327–339.; Adam D. Galinsky – Joe C. Magee – M. Ena Inesi – Deborah H. Gruenfeld: Power and perspectives not taken. Psychological Science, no. 17, 2006, pp. 1068–1074.; Susan A. J. Birch – Paul Bloom (2007): i. m.; Susan A. J. Birch – Paul Bloom (2004): i. m.; Shali Wu – Boaz Keysar: Cultural effects on perspective taking. Psychological Science, no. 18, 2007, pp. 600–606.; Fenna M. Krienen – Pei Chi Tu – Randy L. Buckner: Clan mentality: Evidence that the medial prefrontal cortex responds to close others. Journal of Neuroscience, no. 30, 2010, pp. 13906–13915.; Shuhong Lin – Boaz Keysar – Nicholas Epley: Reflexively mindblind: Using theory of mind to interpret behavior requires effortful attention. Journal of Experimental Social Psychology, no. 46, 2010, pp. 551–556.; Kenneth Savitsky – Boaz Keysar – Nicholas Epley – Travis Carter – Ashley Swanson: The closeness communication bias: Increased egocentrism among friends versus strangers. Journal of Experimental Social Psychology, no. 47, 2011, pp. 269–273.; Andrew R. Todd – Karlene Hanko – Adam D. Galinsky – Thomas Mussweiler: When focusing on differences leads to similar perspectives. Psychological Science, no. 22, 2011, pp. 134–141.; Dana Schneider – Rebecca Lam – Andrew P. Bayliss – Paul E. Dux: Cognitive load disrupts implicit theory-of-mind processing. Psychological Science, no. 23, 2012, pp. 842–847.; Jennifer R. Overbeck – Vitaliya Droutman: One for all: Social power increases self-anchoring of traits, attitudes, and emotions. Psychological Science, no. 24, 2013, pp. 1466–1476.; Shali Wu – Dale J. Barr – Timothy M. Gann – Boaz Keysar: i. m.

zókra gyakorolt eltérő hatásai hogyan befolyásolják e szakemberek bűnfelderítési tevékenység során megjelenő perceptuálisperspektíva-felvételét? Tudatelméleti keretbe helyezve ugyanezt oly módon fogalmazhatjuk meg, hogy miként alakul annak az *elsőrendű intencionális szinten zajló*[5] *elmeteóriának*[6] a működése, amely ez esetben a másik személy informáltságáról alkotott metareprezentáció, azaz a *vélekedéstulajdonítás alakulását öleli fel.*

A súlyos morális megítélésű normasértésekkel való találkozás érthetően intenzívebb felháborodást válthat ki az enyhébbnek tartható esetekhez képest. A morális elítélés hátterén megjelenő düh, azaz a felháborodás tapasztalata a düh élményének egyik sajátos megnyilvánulási formája.

Tudjuk, hogy az oksági attribúció folyamatában az indukált düh a helyzeti tényezők figyelmen kívül hagyása mellett diszpozicionális attribúcióhoz vezet.[7] Ekkor hajlamosak vagyunk a cselekvő személyt hibáztatni. Egyúttal kísérleti eredmények támasztják alá azt is, hogy a dühös állapotba hozott nyomozók a tanúvallomások megbízhatóságának megítélésekor nem veszik figyelembe a másik személy (a tanú) észlelésének helyzeti jellemzőit.[8] Megítélésünk szerint e fejlemény úgy is értelmezhető, hogy *a dühös állapotba hozott nyomozók nem vették figyelembe a tanú perceptuális perspektíváját.*

Ám ha a düh/nincs szituatív tényezők figyelembevétele összefüggés, és ezen belül a másik észlelési perspektívájának figyelmen kívül hagyása tetten érhető a tanúvallomások megbízhatóságára vonatkozó ítéletek alakulásában, ez a tény felveti annak lehetőségét, hogy ha egy perspektívafelvételt megkívánó élethelyzetben, dühös állapotban a másik perspektíváját nem sikerül felvenni, az egyúttal a saját perspektíva felvétele iránti elfogultságot, azaz az egocentrikusperspektíva-felvételt alapozhatja meg. Ennek ellentmondani látszik ugyan *Todd és*

---

5 A kifejezés nem keverendő össze az elsődleges reprezentációk *(primary representations)* fogalmával (Daniel C. Dennett: *Brainstorms: Philosophical essays on mind and psychology.* Harvester Press 1978). Az elsőrendű *intencionális szintű (first-order intentional level)* elmeteória-funkció a dennetti értelemben már a másodlagos (vagy meta-) reprezentációk *(second-order representations)* körébe tartozó jelenség.

6 Például David Premack – Guy Woodruff: Does the chimpanzee have a “theory of mind”? Behaviour and Brain sciences, no. 4, 1978, pp. 515–526.; Heinz Wimmer – Josef Perner: Beliefs about beliefs: Representation and constraining function of wrong beliefs in young children’s understanding of deception. Cognition, no. 13, 1983, pp. 103–128.

7 Dacher Keltner – Phoebe C. Ellsworth – Kari Edwards: Beyond simple pessimism: Effects of sadness and anger on social perception. Journal of Personality and Social Psychology, no. 64, 1993, pp. 740–752.

8 Karl Ask – Par Anders Granhag: Hot Cognition in Investigative Judgments: The Differential Influence of Anger and Sadness. Law & Human Behavior, no. 31, 2007, pp. 537–551.

munkatársai[9], valamint *Bukowski és Samson*[10] eredménye, amely szerint az indukált düh élménye nincs hatással az egocentrikusperspektíva-felvételre. Azonban mindkét kutatás az incidentális düh szerepét vizsgálta egy a dühöt generáló kiinduló helyzetet követő, de önmagában érzelmileg semleges teszthelyzetben. Eredményeik ezért nem zárják ki annak lehetőségét, hogy a súlyos morális megítélésű esetek *a releváns helyzetekben* egocentrikusperspektíva-felvételi hatást idézzenek elő, más szóval, hogy az elsőrendű intencionális szinten végbemenő vélekedéstulajdonítás elfogultságot okozó módon torzuljon.

E megfontolásokból kiindulva úgy véljük, hogy a súlyos morális konnotációjú események észlelése kapcsán megjelenő felháborodás élménye lehet az a lehetséges közvetítő tényező, amely szerepet játszhat a perceptuális perspektíva felvételének esetlegesen bekövetkező egocentrikus irányú elmozdulásában. Várakozásunk szerint *a morálisan súlyos megítélés alá eső bűncselekmények kontextusában nagyobb mértékű lesz a nyomozók perceptuálisperspektíva-felvételének az egocentrikus pólus felé történő eltolódása,* mint a morális értelemben enyhébb megítélésű cselekményekkel találkozás esetén.

Annak érdekében, hogy az iménti kérdésre választ kapjunk, a három elvégzett kísérlet közül az első kettőben személyeinknek olyan, fiktív bűnelkövetés kontextusába ágyazott videójelenetet mutattunk be, amelyek morális megítélése a közvélekedésben egymástól élesen és egyöntetűen eltérő. Így az enyhébb súlyú feltételt egy bolti lopással; míg a súlyosan elítélt körülményt egy pedofil elkövetéssel összefüggésben álló tematika jelentette. A való életben utóbbi bűncselekmény-kategória mindenhol, és minden ép erkölcsi érzékű ember szemében rendkívül súlyos megítélés alá esik. Különösen a rendőrök számára, akik időről időre hivatásukból fakadóan is kénytelenek e súlyos bűncselekményformával szembesülni. Kérdés, hogy ez a szakmából fakadó, feltételezhető „élménytöbblet” létrehoz-e valamilyen rendőr- (nyomozó-) specifikus perspektívafelvételi hatást. E körülmény szükségessé tette, hogy a szakemberektől kapott eredményeket egy civilekből összeállított mintával hasonlítsuk össze (első és második kísérlet). E kísérletek eredményeinek értelmezését célozta a harmadik kísérlet. Az ismertetendő empirikus munkánkban tehát nyomozók és a velük összehasonlított laikus civilek perceptuálisperspektíva-felvételének alakulását tartottuk kontroll alatt.

9 Andrew R. Todd – Alison W. Brooks – Matthias Forstmann – Pascal Burgmer – Adam D. Galinsky: Anxious and Egocentric: How Specific Emotions Influence Perspective Taking. Journal of Experimental Psychology, vol. 144, no. 2, 2015, pp. 374–391.

10 Henryk Bukowski – Dana Samson: Can emotions influence level-1 visual perspective taking? Cognitive Neuroscience, 2015, pp. 1–10.

A kísérletek együttes áttekintése

Az első kísérlet során bemutatott ingeranyagok egy-egy rövid utcai jelenetet foglaltak magukban, míg a második kísérletben ezeket kiegészítette egy imitált szembesítési mozzanat.

Az első és a második kísérlet résztvevői kihallgatási gyakorlattal felvértezett hivatásos állományú rendőrök és laikus civilek voltak.

Az első két kísérlet civilektől kapott eredményei között megjelenő eltérés okainak tisztázása szükségessé tette egy harmadik kísérlet végrehajtását. Ez utóbbi kizárólag civil résztvevőinek már csak egy a súlyos morális megítélést involváló pedofil elkövetéssel kapcsolatos ingeranyagot mutattunk be.

Az első két kísérlet adatait ugyanazon két kontrollcsoport eredményeivel hasonlítottuk össze.

Első kísérlet

Módszerek

Személyek

A kísérletben 76 személy vett részt (61 férfi [80,3 százalék], 15 nő, életkori átlag = 30,76 év; s = 6,5; min. 20; max. 51). A rendőri minta résztvevői kihallgatások lebonyolításában tapasztalt, elsősorban bűnügyi területen dolgozó tiszthelyettesek vagy rendőrtisztek közül kerültek ki. A civilekből álló mintát az Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Kar és a Budapesti Műszaki és Gazdaságtudományi Egyetem hallgatói alkották.

Négy kísérleti csoportot alakítottunk ki. Mind a rendőri, mind a civil minta közelítőleg fele az enyhébb morális megítélés alá eső cselekmény tematikáját magában foglaló lopási feltételben (*Rendőri LOP* csoport; N = 20, *Civil LOP* csoport; N = 16); a másik hányada a súlyos megítélésű elkövetés fiktív kontextusába helyezett pedofil feltételben vett részt (*Rendőri PED* csoport; N = 20, *Civil PED* csoport; N = 20). A kísérleti csoportok korra, valamint nemre illeszkedtek (korra: W = 0,94; n. sz.[11]; U = 2,92; n. sz., nemre: V = 0,204; n. sz.).

A kontrollminta (N = 95; 73 férfi [77 százalék], 22 nő, életkori átlag = 28,89, s = 4,59, min. 19, max. 43) személyeinek mindegyike a Nemzeti Közszolgálati Egyetem Rendészettudományi Karának akkori hallgatója

11 n. sz. = nem szignifikáns.

volt. A két kontrollcsoportot a *LOP kontroll* (N = 48); és a *PED kontroll* (N = 47) alkotta. A kontrollcsoportok korra és nemre egymáshoz (korra: t = 0,11; n. sz., nemre: χ^2 = 0,015; n. sz.), illetve a kísérleti csoportokhoz egyaránt illeszkedtek (Rendőri LOP/LOP kontroll korra: t = 1,39; n. sz., nemre: χ^2 = 0,0; n. sz., Rendőri PED/PED kontroll korra: t = 0,16; n. sz., nemre: Fisher-egzakt próba p = 0,32; n. sz., Civil LOP/LOP kontroll korra: t = 1,39; n. sz., nemre: χ^2 = 0,0; n. sz., Civil PED/PED kontroll korra: t = 0,16; n. sz., nemre: Fisher-egzakt próba p = 0,32; n. sz.).

A személyek Magyarországon élő, magyar anyanyelvű kaukázusiak voltak. Részvételükért díjazást nem kaptak.

Miután a kísérleti személyekkel megismertettük a kísérlet célját és a kísérlet menetét, a résztvevők tájékozott beleegyezésüket adták a részvételükhöz.

Ingerek

Mind a „lopási”, mind a „pedofil” feltétel során bemutatott ingeranyag egyetlen mozzanattól eltekintve ugyanazon, 34 másodperc hosszúságú videófelvételből állt,[12] amely a két kísérleti feltételnek megfelelően csupán a jelenet végén elhangzó mondat szövegében különbözött egymástól.

A *lopási feltétel* során a „vádat” megfogalmazó személy az alábbi mondatot kiáltja a tőle huszonhat méter távolságban, az utcasarkon álló társának: *„Erre a kazettára felvettem, amikor egy hete az üzletből loptál.”*

A *pedofil feltétel* esetén elhangzó mondat így hangzott: *„Erre a kazettára felvettem, amikor egy hete megerőszakoltad a kisfiút.”*

Eszközök

Az ingeranyagot egy 44 centiméter (17,32 coll) átmérőjű számítógép-monitoron mutattuk be. A két hangszóró közvetlenül a monitor két oldalán helyezkedett el, a részt vevő személy felé fordítva.

A kísérlet menete

A kísérletben a személyek egyenként vettek részt. A résztvevők egy karosszékben ültek, testtartásuk függvényében megközelítőleg 80-100 centiméter távolságra a számítógép képernyőjétől.

12 Részletesen lásd Fogarasi Mihály – Máthé Izabella: A „tudás átka” és a nyomozati cselekmények. Érzelmi tényezők hatása a rendőrök perceptuálisperspektíva-felvételére. Belügyi Szemle, 2018/1.

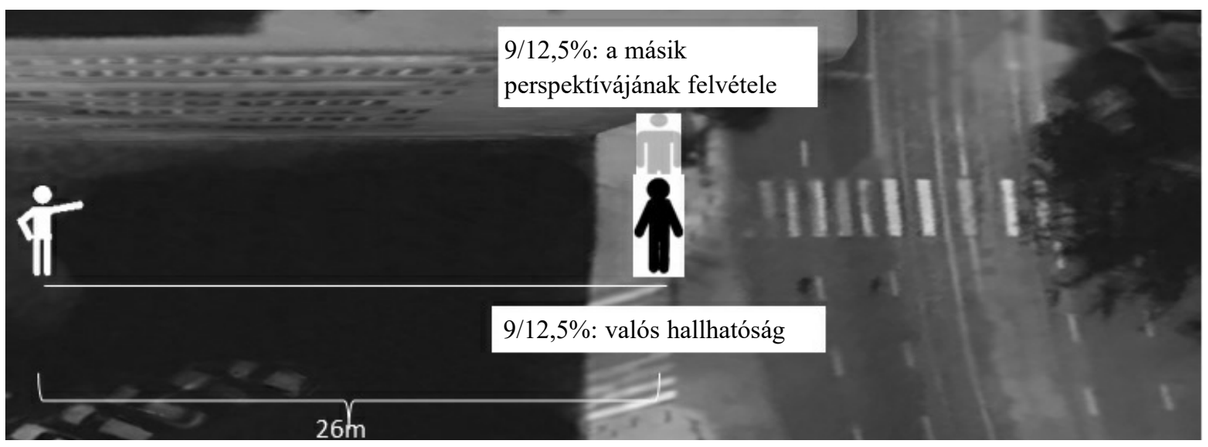
Az instrukció a következőképpen hangzott: *„Egy rövid videójelenetet fog majd látni, melynek két fiatalember a szereplője. Kérem, hogy figyelmesen tekintse meg a jelenetet, majd azzal kapcsolatban egy szubjektív becslést fogunk kérni. A becslésnek nincs se jó, se rossz megoldása.”*

Az ingeranyag bemutatása után a résztvevők válaszlapon jelölték, hogy becslésük szerint a „megvádolt” személy (a „gyanúsított”) mekkora valószínűséggel hallotta meg a felé küldött üzenetet. Az így kapott becslési adatok a *perceptuálisperspektíva-felvételi (= PF) változó* operacionalizált értékei *(1.* és *2. számú ábra).* A skála mérési tartománya 0–100 százalék közötti értékeket vett fel, tízszázalékos valószínűségi léptékű skálán megadva.

A „pedofil” feltétel kilenc- és a „lopási” feltétel 12,5 százalékos tényleges hallhatósági átlagértékeit figyelembe véve[13] a *már inkább* a saját perspektívá-

1. számú ábra

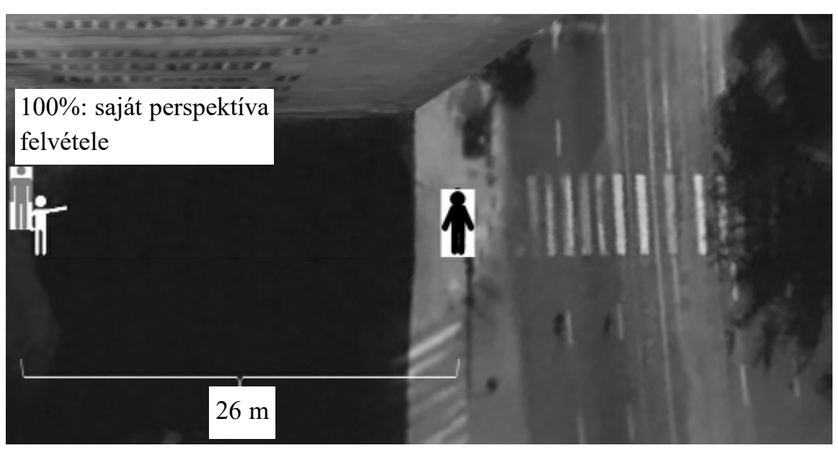
A másik személy perspektívájának sikeres felvétele



Jelmagyarázat: fekete figura: a „megvádolt” személy; fehér figura: a „vádló” személy; szürke figura helyzete: a kísérleti személy virtuális perspektívafelvételi pozíciója.

2. számú ábra

Egocentrikusperspektíva-felvétel



13 Egy utóvizsgálatunk során a videófelvétel eredeti helyszíni feltételeinek pontosan megfeleltetett mo-dellhelyzetben a „megvádolt” személy pozícióját felvevő résztvevők (N = 30) a lopási feltétel szövegéből átlagosan 12,5 (s = 15,3), a pedofil feltétel üzenetéből átlagosan 8,9 százalék (s = 6,1) szövegrészt hallottak. Tehát a szövegeket valójában nem lehetett érteni.

ból származó tudás alapján történő vélekedés tulajdonítás (= a perspektívafelvétel egocentrikus irányú eltolódása) alsó határa rendre a becsült 54,45 és 56,25 százalékos hallhatósági valószínűségi értékektől felfelé kezdődik.

A kontrollcsoportok esetében Az ingeranyag egy mozzanat kivételével megegyezett a kísérleti csoportoknak bemutatott videófelvételekkel. Az egyetlen eltérés az volt, hogy az elhangzó üzenet „vádat" megfogalmazó utolsó három szavát nem foglalta magában. A kontrollcsoportok résztvevői tehát ezt az üzenetrészt hallhatták: *„Erre a kazettára felvettem, amikor egy hete."* Tekintettel arra, hogy mind a bolti lopásról, mind a pedofil elkövetésről szóló vád egymondatos hanganyagát utólag vettük fel, ezért tartalmi egyezőségük ellenére az ingeranyagokat egy-egy elkülönülő kontrollcsoporttal kellett megítéltetnünk.

Az ingeranyag bemutatásának körülményei, valamint az instrukció azonosak voltak a kísérleti feltételek során követett elrendezéssel. Az instrukció elhangzása után bemutattuk az ingeranyagot, majd a résztvevők a kísérleti csoportokéval megegyező skálán jelölték az üzenet meghallhatóságára vonatkozó becsült valószínűségi értékeiket.

Eredmények

Leíró statisztikai eredmények

A kísérleti valamint a kontrollcsoportok alapstatisztikai eredményeit az *1. számú táblázat*ban foglaltuk össze.

1. számú táblázat

A kísérleti és kontrollcsoportok alapstatisztikai eredményei

	Perceptuálisperspektíva-felvétel	
	átlag (%)	szórás
LOP kontroll	48,23	23,85
PED kontroll	44,04	24,22
Rendőri LOP	49,50	22,82
Rendőri PED	61,00	22,92
Civil LOP	48,13	21,36
Civil PED	48,00	20,67

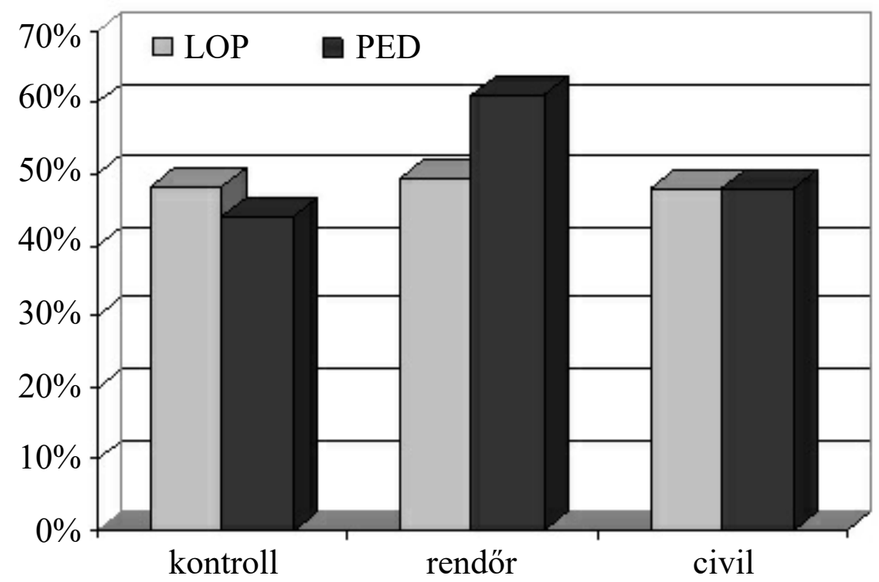
A LOP és PED kontrollcsoport adatainak összehasonlítása

Bár a két kontrollcsoport *perspektívafelvételi* adatai között statisztikailag nincs különbség (z = 0,91; rt = 0,91; n. sz.), mégis, a hibahatáron belül maradva ugyan, de a kontrollminták átlagos PF-értékei nem teljesen egyeznek meg: a LOP kontrollcsoport résztvevői a PED kontroll személyeihez képest átlagosan bő négy százalékkal magasabb valószínűségi becslést adtak. E fejlemény arra int, hogy a kontrollminták numerikusan nem teljesen megegyező, becsült „hallhatósági" átlagértékei miatt a két *kísérleti csoport perspektívafelvételi* adatait *közvetlenül* egymáshoz mérni értelmetlen és indokolatlan lenne.

A kísérleti csoportok perspektívafelvételi eredményeinek összehasonlítását mutatja a *3. számú ábra.*

3. számú ábra

A perspektívafelvétel alakulása a kontroll- és kísérleti csoportokban



Míg a Rendőri PED csoport, valamint a PED kontrollcsoport összehasonlítása szerint a *pedofil feltételben részt vevő rendőrök jelentősen nagyobb hallhatósági értéket tulajdonítottak a „megvádolt" karakternek* (z = 2,45; rt = 2,54; mindkettő p < 0,05), addig a Rendőri LOP és a LOP kontroll perspektívafelvételi adatai között nincs különbség (z = 0,37; rt = 0,37; mindkettő n. sz.).

Ezzel szemben a Civil LOP és a Civil PED csoport becsült, átlagolt valószínűségi értékei a megfeleltetett kontrollcsoportok adataitól sem a lopási (z = –0,05; rt = –0,06; mindkettő n. sz.); sem a pedofil feltétel (z = 0,57; rt = 0,57; mindkettő n. sz.) kapcsán nem tértek el.

Mint azt jeleztük, a lopási és pedofil feltétel mellett az egyes mintákon belül bekövetkezett perspektívafelvételi értékek közvetlen egymáshoz viszonyí-

tása nem lehetséges. Azonban megnyílik erre a lehetőség, amennyiben az egyes kísérleti csoportokat alkotó résztvevők perspektívafelvételi értékeinek a nekik megfeleltetett kontrollcsoport átlagértékétől számított eltéréseit hasonlítjuk össze. Tehát a két kísérleti feltételben a kontrollcsoportok átlagértékeitől mért különbségi értékeket vetjük össze. A kísérleti és kontrollcsoportok adatainak *különbségi értékeire* alapozott kétváltozós ANOVA (Kísérleti feltétel [lopási/pedofil] x Minta [rendőrök/civilek]) eredményei szerint a varianciáért a Kísérleti feltétel változója tendenciaszinten felel (Kísérleti feltétel = 3,79; $p < 0,1$, Minta = 2,12; n. sz., Kísérleti feltétel x Minta = 1,41; n. sz.).

A rendőri mintán belül a különbségi értékekre épülő számítási metódus alkalmazása eredményeképpen azt látjuk, hogy míg a Rendőri PED csoport és a PED kontroll átlagolt perspektívafelvételi értékkülönbsége 17,04 százalék, addig ugyanez a Rendőri LOP csoport/LOP kontroll összehasonlításakor mindössze 1,3 százalék volt. A pedofil feltétel mellett kapott különbségi érték a lopási feltétellel összehasonlítva jelentősen nagyobbnak bizonyult ($z = 2,23$; $rt = –2,35$; mindkettő $p < 0,05$). A civil csoportoknál ugyanebben a viszonyítási dimenzióban nem találtunk eltérést ($z = –0,54$; $rt = –0,54$; mindkettő n. sz.).

A rendőri és civil kísérleti csoportok személyeinek perspektívafelvételi eredményeit összegezve azt tapasztaljuk, hogy kizárólag a *pedofil feltétel mellett részt vevő nyomozói csoport* az, amely a „megvádolt” karakternek tulajdonított informáltság (vélekedés) terén a kontrollcsoporthoz képest szignifikáns elfogultsági hatást mutat: *a perceptuális perspektíva felvétele elmozdult az egocentrikus irányba (4. számú ábra)*. A civil résztvevőknél ugyanakkor egyik kísérleti feltétel esetén sem jelentkezett ez a hatás.

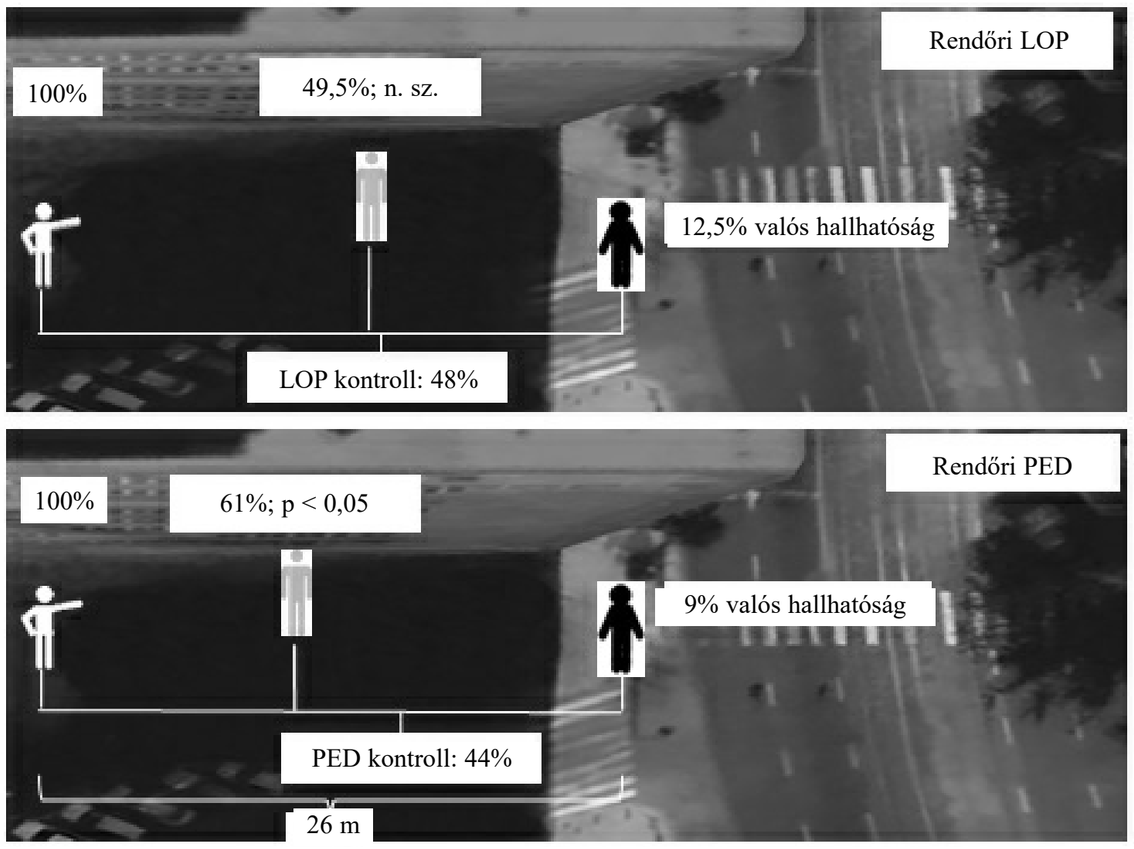
Mindezek után kevéssé meglepő fejlemény, hogy amikor a rendőri és civil csoportokat egymással hasonlítottuk össze, csak a pedofil feltétel esetében kaptunk gyenge, de már értékelhető különbséget: a Civil PED csoporthoz viszonyítva a Rendőri PED csoport tendenciaszinten magasabb hallhatósági értéket becsült ($z = 1,71$; $rt = 1,75$; $rW = 1,75$; mindhárom $p < 0,1$).

Megvitatás

Eljárásunk lehetővé tette, hogy a perceptuálisperspektíva-felvétel alakulását viszonylag finom bontásban vizsgálhassuk. Ebből következően nemcsak annak azonosítására vállalkozhattunk, hogy a résztvevők perspektívafelvétele egocentrikusnak bizonyult-e – a maga teljességében megjelent-e a „tudás

4. számú ábra

A kontrollhoz viszonyított perspektívafelvétel a rendőri csoportokban



Jelmagyarázat: fekete figura: a „megvádolt” személy; fehér figura: a „vádló” személy; szürke figura helyzete: a kísérleti személyek átlagolt virtuális perspektívafelvételi pozíciója.

átka”[14] –, vagy sem, de arra is, hogy az egocentrikus irányba történő elmozdulás graduális jellegéről kapjunk információt. A dichotóm és az egyikünk által *(Fogarasi)* kidolgozott mérési technika alkalmazásából eredő különbséget jól érzékelteti, hogy míg az ingeranyag „megvádolt” szereplőjének perceptuális perspektíváját felvenni egyáltalán nem képes, azaz a szó szoros és szokásos értelmében egocentrikus módon saját magából kiinduló, elfogult személyeink aránya a teljes mintában 2,6 százalékot tett ki, addig az *inkább már* egocentrikus jellegűnek tekinthető perspektívafelvétel megjelenése a résztvevők 47,4 százalékát érintette. Az előbbi esetben arra a kérdésre, amely szerint a „megvádolt” karakter mekkora valószínűséggel hallotta meg a felé intézett üzenetet, a résztvevők a százszázalékos opciót választották – így teljes mértékben a saját észlelői perspektívájukra támaszkodtak, míg az utóbbi, graduális megközelítés kapcsán a korábban ismertetett 55/56 százalékos értékektől induló valószínűségi ítéletek jelezték a saját észlelői pozíció felvételének már hangsúlyosabb szerepét.

14 Colin Camerer – George Loewenstein – Martin Weber: i. m.

Ellentétben a laikus civilek körében kapott eredménnyel, a *rendőröknél* a súlyos morális tartalmat magában foglaló *pedofil feltétel során megjelent a perceptuálisperspektíva-felvétel egocentrikus irányú eltolódása.* A két minta közti különbség azt valószínűsítette, hogy a nyomozók saját informáltságuk irányában megnyilvánuló elfogultabb vélekedéstulajdonításának hátterében talán a szakmai előéletükből szerzett tapasztalataik hatása rejlik. Feltételezésünk szerint az egyik lehetséges tényező az lehetett, hogy míg a professzionális résztvevők számára a pedofil feltétel során bemutatott jelenet már önmagában nyilvánvalóvá tehette, hogy a valóságban rendőri eljárást igénylő, és súlyos következményeket maga után vonó bűnügyről lenne szó, addig a laikus minta tagjai az ingeranyagot talán nem értelmezték ebben az összefüggésében. A felvetés tesztelése érdekében a kísérleti elrendezést oly módon változtattuk meg, hogy a laikusok is egyértelműen felismerhessék a modellált esetbe foglalt jelentés büntetőjogilag is értelmezhető jelentőségét. Célunk tehát az volt, hogy a laikus résztvevőkből összeállított minta tagjai számára bizonyosan kiderüljön, hogy a kísérleti feltételek során bemutatott rövid jelenetek nem pusztán két fiatalember közötti esetleges konfliktus semmire sem kötelező, pillanatnyi megnyilvánulását tárják eléjük, de a való életben azoknak – eltérő mértékű – *morális súlyuk, jelentőségük* lenne. A megfogalmazott vád hitelességét rendőrségi/büntetőjogi következmények támasztják alá, amelyet a „vádló” karakter által hangoztatott bizonyíték – a videófelvétel – tényleges létezése nyomatékosít.

Második kísérlet

A második kísérlet fő kérdésfeltevése annak tisztázására irányult, hogy az előbbiekben jelzett többletinformációkkal kibővített súlyos morális konnotációjú ingeranyag hatására a civilek perceptuálisperspektíva-felvétele vajon változike, és ha igen, a professzionális mintával összehasonlítva miképpen alakul. Várakozásunk szerint, mivel a rendőrök számára az ingeranyag jelentését, értelmezését e pótlólagos információk érdemben már nem befolyásolják, ezért esetükben arra számítunk, hogy az első kísérletben kapott perceptuálisperspektíva-felvételi eredményeik nem fognak megváltozni. A civilek kapcsán viszont azt valószínűsítjük, hogy a tartalmában morálisan súlyosan terhelt feltétel mellett, a rendőri mintához hasonlóan, a kontrollhoz viszonyítva szintén megjelenik az elfogultabb jellegű vélekedéstulajdonítás.

Módszerek

Személyek

A kísérletben 122 személy vett részt (91 férfi [74,6 százalék], 31 nő, életkori átlag: 30,23 év; s = 3,75, min. 23; max. 43). A rendőri mintát 88; a laikus civilekből álló mintát 34 résztvevő alkotta.

Az első kísérletben bemutatott lopási és pedofil feltételt módosított formában megtartottuk. Az ezek alapján kialakított négy kísérleti csoport a következő volt: Rendőri LOP1 (N = 39), Rendőri PED1 (N = 49), Civil LOP1 (N = 17) és Civil PED1 (N = 17).

A kísérleti csoportoktól kapott perspektívafelvételi értékeket az első kísérletben is szerepet kapott két kontrollcsoport adataival vetettük össze (LOP kontroll, PED kontroll).

A négy kísérleti csoport egymáshoz (korra: W = 1,03; n. sz., nemre: χ^2 = 0,198; n. sz.) valamint a kontrollcsoportokhoz (korra: Civil LOP1/LOP kontroll: d = 1,57; n. sz., Civil PED1/PED kontroll: t = 1.61; n. sz., Rendőri LOP1/LOP kontroll: t = 1,53; n. sz., Rendőri PED1/PED kontroll d = 0,91; n. sz., nemre: Civil LOP1/LOP kontroll: p = 0,48; n. sz., Civil PED1/PED kontroll: p = 0,54; n. sz., Rendőri LOP1/LOP kontroll: χ^2 = 0,005; n. sz., Rendőri PED1/PED kontroll: χ^2 = 0,004; n. sz.) illeszkedett. A személyek Magyarországon élő, magyar anyanyelvű kaukázusiak voltak. Részvételükért díjazást nem kaptak.

Ingerek

Az ingeranyag mindkét kísérleti feltétel mellett egy-egy 47 másodperc időtartamú videófelvételből állt. Az első, 34 másodperces részük megegyezett az első kísérlet során bemutatott ingeranyagokkal, amelyet „utcai jelenet” elnevezéssel azonosítunk. Az ingeranyagok második részére „szembesítési jelenet” megnevezéssel hivatkozunk.

Az „utcai jelenet” végén, a képernyő közepén három másodpercig volt látható a „Másnap” felirat. Ezt követte a szembesítési jelenet. Ekkor a nézőnek háttal ül egy nyomozót alakító fiatal férfi, tőle balra, a nézővel szemközt egy asztalnál az utcai jelenet „vádló” karaktere, jobbra a „megvádolt” személy foglal helyet.

Mindkét feltétel során a rendőr a „vádló” felé fordulva megszólal:

„Rendőr”: *„Kérem, mondja a szemébe!”*

A lopási feltétel mellett a „megvádolt” szemébe mondott szöveg:

„Vádló”: *„Tudod, hogy felvettem mindazt, amit az üzletből elloptál.”*
A pedofil feltételben elhangzó mondata pedig a következő:
„Vádló”: *„Tudod, hogy felvettem mindazt, amit a kisfiúval csináltál.”*
Végül mind a két kísérleti feltételben a „megvádolt” ugyanazt válaszolja:
„Megvádolt”: *„Eddig nem tudtam róla.”*

A szembesítési jelenet rövid párbeszédével kívántuk elérni, hogy a résztvevők bizonyosságot kapjanak a vádban foglaltak „valóságosságáról”. A szembesítések elválaszthatatlan része a másik fél válasza, ez indokolta a „megvádolt” karakter megszólalását. Állítása nem a vádban megfogalmazott cselekmény elkövetését tagadja, hanem azt, hogy az „utcai jelenet” során meghallotta a hozzá intézett mondatot. Így a résztvevők perspektívafelvétele nyitott maradhatott, hiszen a válasz hazugság is lehetett. Az ellenkező tartalmú megnyilatkozás – „igen, *már* tudok róla (mert tegnap hallottam)” – lényegében értelmetlenné tette volna azt a résztvevőktől kért megítélést, hogy mindezek után szerintük a „megvádolt” szereplő hallotta-e, és mekkora valószínűséggel az utcai jelenet üzenetét.

A kísérlet menete

A kísérlet helyszíni elrendezése és az eljárás módja megegyezett az első kísérlet körülményeivel.

Eredmények

A második kísérlet alapstatisztikai eredményei a *2. számú táblázat*ban követhetők nyomon.

Szemben az első kísérletben kapott eredménnyel, e kibővített ingeranyagot tartalmazó elrendezésben, a PED kontrollcsoporthoz viszonyítva a *Civil PED* csoport *már jelentősen elfogultabb* vélekedést tulajdonított a „megvádolt” karakternek ($z = 2{,}25$; $p < 0{,}05$, $rt = 2{,}33$; $p < 0{,}05$). A lopási feltétel mellett viszont továbbra sem következett be számottevő mértékű elmozdulás ($z = 1{,}04$; n. sz., $rt = 1{,}04$; n. sz.).

A rendőri mintánál ugyanezt a megoszlást kaptuk (Rendőri LOP/LOP kontroll: $z = 0{,}96$; n. sz., $rt = 0{,}96$; n. sz., Rendőri PED/PED kontroll: $z = 3{,}25$; $p < 0{,}01$, $rt = 3{,}43$; $p < 0{,}01$).

2. számú táblázat

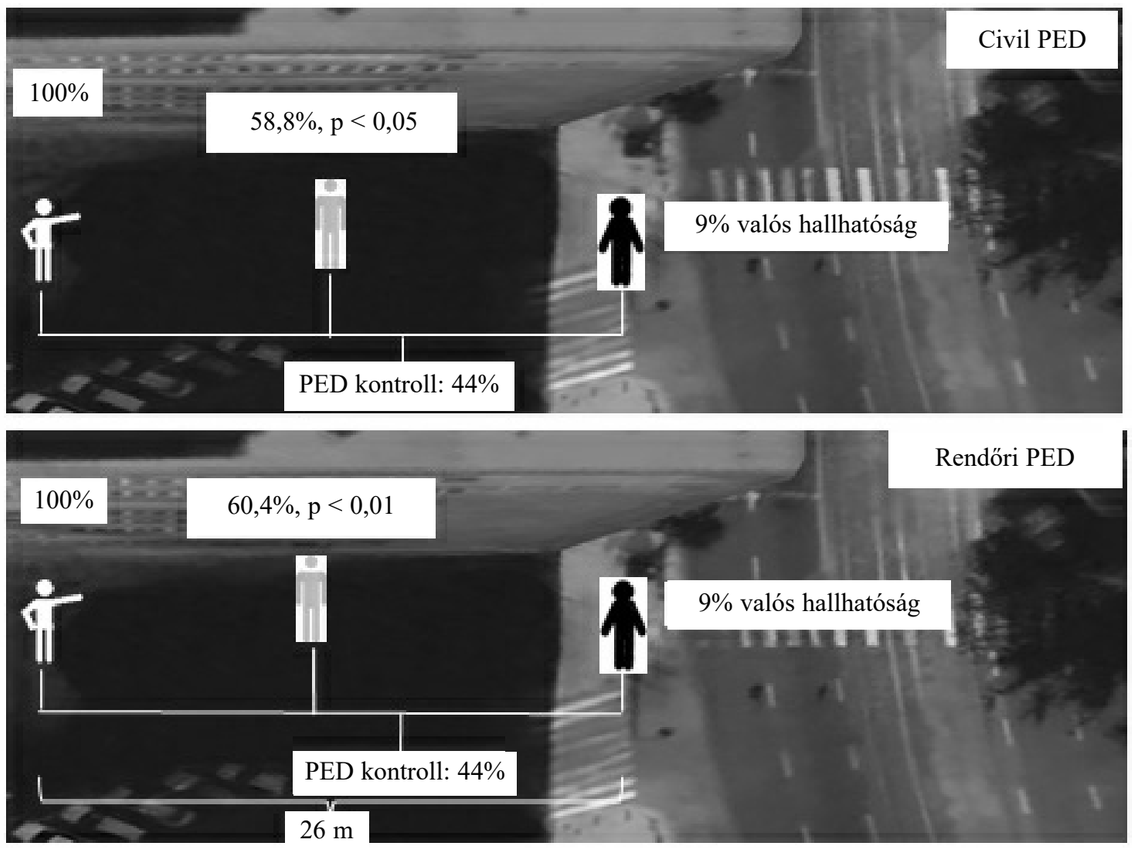
A rendőri és civil kísérleti csoportok perceptuálisperspektíva-felvételi adatai a második kísérletben

	Perceptuálisperspektíva-felvétel	
	átlag (%)	szórás
Rendőri LOP1	52,80	28,74
Rendőri PED1	60,40	20,90
Civil LOP1	55,90	24,25
Civil PED1	58,80	16,16

A rendőri és civil csoportok perspektívafelvételi eredményei között egyik feltétel mellett sem található eltérés (Rendőri LOP/Civil LOP: z = –0,2; n. sz., Rendőri PED/Civil PED: z = 0,44; n. sz.). A pedofil feltétel mellett kapott eredményeket tettük szemléletesebbé az *5. számú ábrá*n.

5. számú ábra

A Rendőri PED1 és a Civil PED1 csoport perceptuálisperspektíva-felvétele a második kísérletben



Jelmagyarázat: fekete figura: a „megvádolt” személy; fehér figura: a „vádló” személy; szürke figura helyzete: a kísérleti személyek átlagolt virtuális perspektívafelvételi pozíciója.

Megvitatás

Mindkét várakozásunk beigazolódott: a második kísérlet *pedofil feltétele* során a kontrollhoz viszonyítva a laikus minta a rendőrivel *már megegyező, és szignifikáns mértékben tolódott el az enyhén elfogult perceptuálisperspektíva-felvétel irányába.* Eközben a Rendőri PED1 csoport perspektívafelvétele az első kísérlet „utcai jelenetéhez" képest (61 százalék) változatlan maradt, tehát a „szembesítési" mozzanat a nyomozókra valóban hatástalannak bizonyult.

Mindebből azonban önként adódott egy további kérdés: vajon a szembesítési jelenet egésze, netán valamely része/részei felelős(ek) azért, hogy a második kísérlet pedofil feltétele mellett a civileknél is megjelent a perspektívafelvételi eltolódás jelensége? A kérdést megfordítva, rendészeti szempontból úgy fogalmazhatjuk meg, hogy a hatás megjelenésének milyen, csak a civilek számára nélkülözhetetlen feltétele(i), van(nak), amely(ek) viszont a rendőri minta esetében irrelevánsnak bizonyul(nak)?

A szembesítési jelenet első mondatának elhangzása *(„Kérem, mondja a szemébe")* nyilvánvalóvá teszi, hogy az „utcai" jelenet nem csupán egy ember üres fenyegetőzése volt, hanem az súlyos *rendőri-büntetőjogi következmények*et vont maga után. Ennél fogva a résztvevőknek az „utcai" jelenetet most már bizonyosan ebben a rendőrségi-hivatalos jelentési kontextusban kellett értelmezniük.

A „vádló" karakter *hatóság előtt* megismételt állítása *(„Tudod, hogy felvettem mindazt, amit a kisfiúval csináltál")* pedig azt tette egyértelművé, hogy valóban *van bizonyíték* a cselekményről (a „felvétel").

A „szembesítési" jelenet zárómozzanatában a „megvádolt" karakter azt jelenti ki, hogy *nincs tudomása arról, hogy a „vádló" korábban már informálta volna őt a bizonyíték létezéséről.* Nem az elkövetés tényét tagadja, hanem ahhoz képest egy meglehetősen elhanyagolható részletkérdésben nyilvánul meg. Könnyen lehetséges, hogy a „megvádolt" személlyel kapcsolatban a résztvevőkben egy olyan benyomás alakulhat ki, amely szerint, ha a már bűnösként észlelt karakter – kifogásolható modorral – egy periferikus jelentőségű állítással képes szembeszállni, akkor talán *kétségbe vonható a szavahihetősége.* Azaz, ha tagadja azt, hogy meghallotta az utcán neki címzett üzenetet, akkor lehet, hogy ennek épp az ellenkezője az igaz.

Az utcai jelenetbe foglalt tartalmakhoz képest a szembesítési jelenet e három, különböző jelentési többletet hordozó mozzanatának bármelyike, sőt azok együttese épp úgy okozhatta a második kísérlet civil résztvevőinél a súlyos morális helyzet megítélésével kapcsolatban tapasztalt elfogultabb vélekedéstulajdonítás jelenségét.

A kérdés megválaszolása érdekében e lehetséges tényezők hatását a harmadik kísérletben szisztematikus vizsgálat tárgyává tettük.

Harmadik kísérlet

Az előbbi megfontolások alapján a következő, egymással nem átfedő előzetes értelmezési lehetőséget fogalmaztuk meg:

1. Ha a szembesítési jelenet első mondatáig *(„Kérem, mondja a szemébe”)* bemutatott ingeranyag hatására a perceptuális perspektíva felvétele nem különbözne a második kísérlet „szembesítési” jelenete után kapott eredménytől (Civil PED csoport: 58,8 százalék), akkor ebből arra következtethetnénk, hogy a laikus minta számára az utcai jelenet vádjában elhangzottak rendőri-büntetőjogi kontextusba helyezése már megadja a fiktív *cselekmény hihetőségét, és ezen keresztül morális súlyát.* A rendőri minta tagjai számára szakmaiságuk miatt viszont erre feltehetően nem volt szükség: ők minden bizonnyal, és magától értődőn már az utcai jelenetet is ugyanezzel a jelentéssel ruházhatták fel.
2. Ha a második kísérlet Civil PED1 csoportjának eredményével a statisztikai egyezés csak a „szembesítési” jelenetben elhangzó első két mondat hatására következne be, az arra utalna, hogy az elfogultabb perceptuálisperspektíva-felvétel megjelenéséhez a civilek számára ahhoz, hogy a vádban foglaltakat hitelesnek tartsák, önmagában nem elégséges a jelenet rendőrségi kontextusba helyezett értelmezése, ehhez még a bűnösséget alátámasztó *bizonyíték* meglétéről szóló információra is szükségük van. Ennek hiányában (csak a szembesítési jelenet első mondatát hallják) az utcai jelenetben elhangzó „vád” továbbra is vádaskodásnak számítana, tehát nem lehetne szó morálisan súlyosan elítélhető cselekmény elkövetéséről.
3. Ha a szembesítési jelenet második mondatának elhangzása után sem sikerülne a második kísérlet Civil PED1 csoportjának eredményét reprodukálni, abból az következne, hogy a civilek egocentrikusabb vélekedéstulajdonítása megjelenéséhez a „megvádolt” karakter szembesítési jelenet végén elhangzó, tagadó válaszára, és az abból következtetett attribúciós hatás megjelenésére lenne szükség. Más szóval, a második kísérlet pedofil feltételében bemutatott ingeranyag egészére.

Természetesen e három „tiszta” opció bármely keveréke, mint a kérdéses jelenséget létrehozni képes hatótényező, éppúgy igazolódhat.

Módszerek

Személyek

A harmadik kísérletben 49, semmilyen rendőri tapasztalattal nem bíró, Magyarországon élő, magyar ajkú, kaukázusi személy vett részt (életkori átlag: 28,92 év, s = 2,97; min. 22, max. 35 év; férfi 80, nő 20 százalék). A minta egyetemi hallgatókból és középiskolai tanárokból állt. A második kísérlet Civil PED1 csoportjához korra (d = 1,71; n. sz.) és nemre (p = 0,52; n. sz.) illeszkedett.

A résztvevőkből két kísérleti csoportot alakítottunk ki: az első (N = 27) és a második kísérleti csoportot (N = 22).

Ingerek

Az első kísérleti csoport ingeranyaga az első és második kísérlet pedofil feltételének utcai jelenetét, az azt követő „Másnap” feliratot, valamint a második kísérlet szembesítési jelenetének első, a rendőrt alakító szereplő által elmondott mondatát *(„Kérem, mondja a szemébe!”)* magában foglaló videófelvétel volt.

A második kísérleti csoportnak bemutatott ingeranyag az előbbieken túl a szembesítési jelenet második mondatát, a „vádló” karakter rendőr előtt tett állítását is tartalmazta: *„Tudod, hogy felvettem mindazt, amit a kisfiúval csináltál.”*

Eljárás

A harmadik kísérletben követett eljárás, valamint a kísérlet feltételei és körülményei megegyeztek az első és második kísérlet során leírtakkal.

Eredmények

A második és harmadik kísérlet releváns eredményeinek összehasonlíthatóságát segíti elő, hogy azokat egy közös táblázatban foglaltuk össze *(3. számú táblázat)*.

Az első és a második kísérleti csoport, valamint a második kísérlet Civil PED1 csoportjának perceptuálisperspektíva-felvétele egyaránt megegyezik (első csoport/ Civil PED1: z = 0,21; n. sz., rt = 0,21; n. sz., második csoport/ Civil PED1: z = 0,46; n. sz., rt = –0,46; n. sz.).

3. számú táblázat

A harmadik kísérlet csoportjainak és a második kísérlet Civil PED csoportjának perspektívafelvételi eredményei

3. kísérlet		
	átlag	szórás
1. Csoport	58,5	18,95
2. Csoport	57,7	25,62

2. kísérlet		
	átlag	szórás
Civil PED1	58,8	16,16

A harmadik kísérlet két csoportja a függő változó alakulásában szintén nem különbözik egymástól (FPW = –0,39; n. sz., rW = –0,39; n. sz.).

Megvitatás

Úgy véljük, hogy a harmadik kísérlet egyértelmű választ adott a tisztázandó kérdésre: a második kísérlet pedofil feltételében részt vevő laikus civilek perceptuálisperspektíva-felvétele azért tolódhatott el az egocentrikus pólus felé, egyszersmind azért „zárkózhattak fel” a nyomozók saját tudásuk irányában megnyilvánuló, enyhe fokú elfogultságához, mert a pedofil elkövetés bemutatott fiktív helyzetét immár annak súlyos, rendőrségi következményeivel együtt értelmezték. Utóbbi körülményből adódhatott a civilek értelmezésében feltételezhetően bekövetkezett változás: a szóban forgó eset a fiktív valóságban ténylegesen megtörténhetett, ezért *már van súlyos morális jelentése és jelentősége,* és ennek felismerése tolta el egocentrikus irányba a perceptuálisperspektíva-felvételüket.

Mivel a harmadik kísérlet két feltételének eredménye megegyezik, ebből arra következtethetünk, hogy a „szembesítési” jelenet további mozzanatai (a „vádló” mondata és a „megvádolt” válasza) a rendőri/büntetőjogi értelmezési keret hatásához képest nem játszott szerepet abban, hogy a civilek tudatelméleti működése az elfogult vélekedéstulajdonítás irányába mozduljon el.

Általános megvitatás

A kutatás mindenekelőtt azokra az összefüggésekre keresett választ, amelyek a tudatelméleti (elmeteória) folyamatok elsőrendű intencionális szintjén végbemenő perceptuálisperspektíva-felvétel sajátosságainak a nyomozati cselekmények végrehajtásában betöltött lehetséges szerepéből következhetnek: a

morális megítélés szempontjából élesen eltérő súlyosságú bűncselekmények közegében zajló bűnfelderítési tevékenység nyomozókra gyakorolt hatásai vajon eltérően jelennek-e meg a gyanúsítottak észlelési perspektívájának felvételében? Amennyiben pozitív kapcsolatot találunk a cselekmények általános erkölcsi megítélésének súlyossági foka és a perspektívafelvétel egocentrikus irányba történő eltolódása között, az egyúttal felhívná a figyelmet arra, hogy már a szociálkognitív folyamatok eme alapszintjét is érintheti a nyomozók elfogultsága. Miként azt *Birch és Bloom*[15] általában a mások tudásáról alkotott elfogult feltevések kapcsán kifejtette, mindez egyaránt elhibázott várakozásokat gerjeszt a szociális kogníció és a viselkedés számos lényegi területén: a partnernek tulajdonított érzésektől a rá vonatkozó attitűdök alakulásán keresztül a tőle várt viselkedés mikéntjéig terjed az elfogultság e formájának torzító hatása. Ezért is tulajdonítunk különös jelentőséget a nyomozati cselekmények során az esetlegesen tetten érhető egocentrikus vélekedéstulajdonítás nyomozói elfogultsághoz vezethető szerepének.

Az első kísérlet eredményei várakozásunkat alátámasztották: a kihallgatási gyakorlattal bíró résztvevők perceptuálisperspektíva-felvétele a *morális értelemben súlyos megítélést involváló helyzetben jelentős mértékben mozdult el az egocentrikus*perspektíva-felvételi pólus felé. A morális tartalmát illetően semleges helyzethez képest bekövetkezett jelentős eltolódás, ennek elenére, abszolút értelemben csak *enyhe fokú elfogultságot* testesített meg.

Felvetődött a kérdés, hogy a fejlemény hátterében vajon a nyomozói/vizsgálói tevékenységből fakadó szakmai faktorok állhatnak-e, vagy ellenkezőleg, az ilyen jellegű professzionális tapasztalattal nem bíró, ebben a vonatkozásban tehát laikus populáció esetében szintén megjelenik-e a hatás. A második és harmadik kísérlet eredményei adták meg a választ. Ezek szerint abban az esetben, ha a laikus civilek és a professzionális hivatásos állományúak a morálisan súlyozott helyzeteket *egyformán értelmezik,* azok jelentése mindkét vizsgált populáció számára megegyezik, akkor a függő változó értékeinek alakulása terén *nincs köztük eltérés.* Ami azt jelenti, hogy a morális színezetét tekintve enyhébb közmegítélés alá eső cselekményekkel összefüggésben mind a rendőrök, mind a civilek képesek felvenni a kifogásolható cselekedetű személy – rendőri szempontból a lehetséges vagy tényleges gyanúsított – perceptuális perspektíváját, más szóval, elfogulatlanok maradnak. Mindazonáltal *a súlyos morális konzekvenciával terhelt helyzetekben a pro-*

15 Susan A. J. Birch – Paul Bloom: Understanding children's and adults' limitations in mental state reasoning. Cognitive Sciences, vol. 8, no. 6, 2004

fesszionális és laikus minta azonos mértékben bizonyult a saját informáltsága irányában enyhe fokban elfogultnak.

A rendőri hivatásból eredő szakmai tapasztalatok hatása a helyzetek értelmezésében játszik szerepet. Úgy tűnik, a rendőrök számára ahhoz, hogy valamely általuk megfigyelt szituáció elnyerje negatív morális jelentését, a civilekhez viszonyítva kevesebb információ szükséges. A cselekményre vonatkozó vád felbukkanása ennek *már elégséges feltétele.* A laikus civilek mintha több megerősítést igényelnének: hiába jelenti ki valaki, hogy szerinte egy másik személy elkövetett valamely súlyosan elítélhető cselekményt, és erről még bizonyíték is van a kezében, ha mindebből és mindezek után nem következik semmi, akkor számukra a helyzet önmagában csak vádaskodás; nincs alapja, nem hiteles, ezért a vád(akodás)ban megfogalmazott cselekményt még a kísérletben bemutatott fiktív valóságban sem értékelik reálisnak. Ennélfogva annak nem is tulajdonítanak morális súlyt. Azonban amint a vád hihetővé lesz, az akkor már ténylegesen elkövetettként értelmezett cselekmény nyomban elnyeri morális színezetét.

A talán legfontosabb kérdés mégis az, hogy az elvégzett kísérlet nyomán kapott eredmények alapján milyen következtetéseket vonhatunk le a gyanúsítottaktól kapott információk szakemberek által történő értelmezése, feldolgozása kapcsán. Az információk kiértékelése során lehetnek-e elfogulatlanok a bűnüldözők?

Noha észlelési helyzetben vizsgáltuk meg a perspektívafelvétel alakulását, de máshol[16] amellett érveltünk, hogy a perceptuális dimenzió alapján feltárt összefüggések valószínűsíthetően a fogalmi perspektíva felvételére szintén érvényesek lehetnek. Ennek figyelembevételével úgy látjuk, hogy eredményeink szerint a kihallgatási gyakorlattal bíró rendőrök – természetesen egyénenként változó mértékben, de – a súlyos morális konzekvenciával együtt járó cselekmények kontextusában zajló bűnfelderítési tevékenységük során hajlamosak lehetnek arra, hogy inkább a saját informáltságukra alapozva, abból kiindulva, mérsékelten elfogultan értelmezzék a gyanúsítottaktól származó nyomozati információkat. A morális értelemben kevésbé súlyos megítélésű esetekben azonban képesek felvenni a gyanúsítottak nézőpontját; a szakemberek nem tulajdonítanak nekik olyan tudást, amely csak a nyomozó előtt ismert, de a gyanúsítottak által nem.

16 Fogarasi Mihály – Máthé Izabella: i. m.

A kutatás korlátai és lehetséges további irányai

Bár úgy gondoljuk, hogy többféle megközelítésből származó érv is alátámasztja azt a vélekedésünket, amely szerint a kísérletben a perceptuális perspektíva felvételével összefüggésben kapott eredmények egyszersmind megfelelő indikátorai lehetnek a fogalmi perspektívafelvétel lehetséges alakulásának is, ebbéli álláspontunk mindaddig hipotetikus jellegű, amíg annak empirikus bizonyítéka nem áll rendelkezésre. E megfontolásból kiindulva tartjuk elkerülhetetlennek, hogy a nyomozati cselekmények során az érintett szakemberek fogalmi perspektívafelvételét közvetlenül tartsuk kontroll alatt, tehát a bemutatott kísérleti elrendezést úgy módosítsuk, hogy az elősegítse e cél megvalósítását.

Vajon a morálisan súlyosan kifogásolható cselekménnyel történő kényszerű szembesülés helyzete, valamint annak a perspektívafelvételre gyakorolt egocentrikus jellegű hatása között valóban a bevezető fejezetben említett felháborodás tölti be a közvetítő mechanizmus szerepét? Mivel az ismertetett kutatás kérdésfeltevése nem erre irányult, így az összefüggés empirikus igazolása további erőfeszítéseket igényelt. Ennek eredményeiről korábban már beszámoltunk.

HIVATKOZÁSOK

Ames, Daniel R.: Inside the mind-reader's toolkit: projection and stereotyping in mental state inference. *Journal of Personality and Social Psychology,* no. 87, 2004

Ask, Karl – Granhag, Par Anders: Hot Cognition in Investigative Judgments: The Differential Influence of Anger and Sadness. *Law & Human Behavior,* no. 31, 2007

Baron-Cohen, Simon – Leslie, Alan M. – Frith, Uta: Does the autistic child have a "theory of mind"? *Cognition,* no. 21, 1985

Birch, Susan A. J. – Bloom, Paul: Understanding children's and adults' limitations in mental state reasoning. *Cognitive Sciences,* vol. 8, no. 6, 2004

Birch, Susan A. J. – Bloom, Paul: The Curse of Knowledge in Reasoning About False Beliefs. *Psychological Science,* vol. 18, no. 5, 2007

Bukowski, Henryk – Samson, Dana: Can emotions influence level-1 visual perspective taking? *Cognitive Neuroscience,* 2015

Camerer, Colin – Loewenstein, George – Weber, Martin: The curse of knowledge in economic settings: an experimental analysis. *Journal of Political Economy,* no. 97, 1989

Dennett, C. Daniel: Brainstorms: Philosophical essays on mind and psychology. Harvester Press 1978

Epley, Nicholas – Keysar, Boaz – Van Boven, Leaf – Gilovich, Thomas: Perspective taking as egocentric anchoring and adjustment. *Journal of Personality and Social Psychology,* no. 287, 2004

Galinsky, Adam D. – Magee, Joe C. – Inesi, M. Ena – Gruenfeld, Deborah H.: Power and perspectives not taken. *Psychological Science,* no. 17, 2006

Keltner, Dacher – Ellsworth, Phoebe C. – Edwards, Kari: Beyond simple pessimism: Effects of sadness and anger on social perception. *Journal of Personality and Social Psychology,* no. 64, 1993

Keysar, Boaz – Barr, Dale J. – Balin, Jennifer A. – Paek, Timothy S.: Definite reference and mutual knowledge: Process models of common ground in comprehension. *Journal of Memory and Language,* no. 39, 1998

Keysar, Boaz – Barr, Dale J. – Balin, Jennifer A. – Brauner, Jason S.: Taking perspective in conversation: The role of mutual knowledge in comprehension. *American Psychological Society,* vol. 11, no. 1, 2000

Keysar, Boaz – Lin, Shuhong – Barr, Dale J.: Limits on theory of mind use in adults. *Cognition,* no. 89, 2003

Krienen, Fenna M. – Tu, Pei Chi – Buckner, Randy L.: Clan mentality: Evidence that the medial prefrontal cortex responds to close others. *Journal of Neuroscience,* no. 30, 2010

Lin, Shuhong – Keysar, Boaz – Epley, Nicholas: Reflexively mindblind: Using theory of mind to interpret behavior requires effortful attention. *Journal of Experimental Social Psychology,* no. 46, 2010

Overbeck, Jennifer R. – Droutman, Vitaliya: One for all: Social power increases self-anchoring of traits, attitudes, and emotions. *Psychological Science,* no. 24, 2013

Piaget, Jean – Inhelder, Bärbel: The child's conception of space. Routledge–Kegan Paul, London, 1956

Premack, David – Woodruff, Guy: Does the chimpanzee have a "theory of mind"? *Behaviour and Brain sciences,* no. 4, 1978

Savitsky, Kenneth – Keysar, Boaz – Epley, Nicholas – Carter, Travis – Swanson, Ashley: The closeness communication bias: Increased egocentrism among friends versus strangers. *Journal of Experimental Social Psychology,* no. 47, 2011

Schneider, Dana – Lam, Rebecca – Bayliss, Andrew P. – Dux, Paul E.: Cognitive load disrupts implicit theory-of-mind processing. *Psychological Science,* no. 23, 2012

Todd, Andrew R. – Hanko, Karlene – Galinsky, Adam D. – Mussweiler, Thomas: When focusing on differences leads to similar perspectives. *Psychological Science,* no. 22, 2011

Todd, Andrew R. – Brooks, Alison W. – Forstmann, Matthias – Burgmer, Pascal – Galinsky, Adam D.: Anxious and Egocentric: How Specific Emotions Influence Perspective Taking. *Journal of Experimental Psychology,* vol. 144, no. 2, 2015

Wimmer, Heinz – Perner, Josef: Beliefs about beliefs: Representation and constraining function of wrong beliefs in young children's understanding of deception. *Cognition,* no. 13, 1983

Wu, Shali – Keysar, Boaz: Cultural effects on perspective taking. *Psychological Science,* 18, 2007

Wu, Shali – Barr, Dale J. – Gann, Timothy M. – Keysar, Boaz: How culture influences perspective taking: Differences in correction, not integration. *Frontiers in Human Neuroscience,* no. 7, 2013