
Nyitrai Endre
A DIGITÁLIS ADATOK
ÉS A MODERN
TECHNIKAI ESZKÖZÖK JELENTŐSÉGE
A KRIMINALISZTIKÁBAN
LUDOVIKA
UNIVERSITY PRESS

Nyitrai Endre

A digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában

Nyitrai Endre

A digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában

A deepfake és a fake news jelenségek

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2025

Szakmai lektor
Balláné Füszter Erzsébet

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Fülöp Éva
Korrektor: György László
Tördelőszerkesztő: Fehér Angéla

DOI: https://doi.org/10.36250/01198_00

ISBN 978-963-531-129-4 (elektronikus PDF)
ISBN 978-963-531-130-0 (ePub)

© A szerző, 2025
© A kiadó, 2025

Minden jog védve.

Tartalom

Bevezetés

A digitalizáció rohamos fejlődésének köszönhetően a jelen és a jövő legnagyobb befektetési területének az *adat* tekinthető. Az adatrobbanás egyúttal a digitális állam és a digitális állampolgárság létrejöttének is a mozgatórugója. A digitalizáció fontos szerepet tölt be a világon az államok versenyképességében is.

Az adat okkal tekinthető a gazdaság új hajtóanyagának, mivel az adatipar évente 40%-os növekedést mutat.[1] Az Európai Bizottság adatközpontú gazdasági stratégiáját megalapozó dokumentumai szerint[2] percenként 1,7 millió gigabájt adat keletkezik. A tudományos újdonságok és az online-elektronikus világ nemcsak a társadalom tagjait – magát az egyént – vagy a gazdasági folyamatokat formálják, hanem a kriminalisztikát is.

A digitalizáció új fejezetet nyitott a kriminalisztika fejlődésében, mivel majdnem minden tevékenységünkkel adatokat hagyunk magunk után. Ezek egyrészt értéket képviselnek az adatvagyon tekintetében, másrészt a digitális nyomok elemzése és értékelése egyes esetekben lehetővé teszi az elkövető azonosítását, valamint elősegítheti a bűncselekmények megelőzését, megszakítását, felderítését és bizonyítását. A bűnüldözés szempontjából a digitális lábnyomok folyamatos létrejötte miatt elengedhetetlenné vált a digitális közigazgatási és a kriminalisztikai nyilvántartásokban keletkezett adatok vizsgálata, elemzése, valamint a kapcsolódási pontok és az összefüggések feltárása.

A tudományos-technikai fejlődés új elkövetési módszerek kialakulására, valamint az elkövetők kapcsolattartási módjaira is hatással van. Az elkövetők és az események, cselekmények közötti látható és láthatatlan összefüggések, illetve a szétszórtan vagy különböző adathalmazokban található adatkataszterek elemzése és értékelése a hálózatkutatás eszköztárával valósítható meg. A technikai fejlődéssel megjelennek a mesterséges intelligenciával támogatott technikai eszközök. Ezek az adatrobbanás egy másik pillérét alkotják, mivel az eszközök használatával újabb adatok keletkeznek, ami információs áramlást indíthat el, illetve hozzájárulhat bizonyítási cselekmények és kényszerintézkedések foganatosításához.

Digitalizált társadalmunkban a hírek gyorsabban jutnak el az emberekhez, ugyanakkor a valótlan hírek száma is növekedésnek indult. A valótlan hírek

[1] *Fehér könyv a nemzeti adatpolitikáról* 2016: 6.
[2] *Fehér könyv a nemzeti adatpolitikáról* 2016: 4.

közlése az elektronikus térben a társadalom befolyásolásának rendkívül hatékony és olcsó eszközének számít. Az álhírek *(fake news)* mellett megjelent a *deepfake* jelenség (módszer), amely a mesterséges intelligenciára épül, és a befolyásolás még hatékonyabb módszerének tekinthető. A deepfake lényege olyan digitális technológia alkalmazása, amivel teljes mértékben valódinak tűnő multimédiás tartalmakat lehet előállítani.

Az álvideók esetén összemosódik a valóság és a fikció, ezért tekinthető veszélyesnek az új technológia, amelynek segítségével egy ember arca, hangja vagy mozgása is újrateremthetővé válhat. Szükségessé vált az álhírek és álvideók elemzése, valamint az igazságügyi (forenzikus) nyelvész igénybevétele a nyomozások során, mivel a nyelvész szakértőnek kiemelkedő szerepe van az álhírek, a *deepfake* jelenség felderítése során.

Meg kell teremteni a bűnügyi nyomozási ökoszisztémát, és a nyomozó hatóságnak a modern elektronikus eszközök használatára, valamint a szolgáltatások nyilvántartási adatainak beszerzésére kell törekednie. 2022 végén jelent meg hazánk *Nemzeti Digitális Stratégiá*ja, amely szerint az elektronikus eszközök és szolgáltatások elérhetősége, illetve a fejlett informatikai háttér javíthatja a bűnmegelőzéshez és bűnüldözéshez kapcsolódó tevékenységek hatékonyságát, valamint csökkentheti a bűnüldöző szervek reakcióidejét, míg az igazságszolgáltatás működését gyorsíthatja.[3]

A *Nemzeti Digitális Stratégia* szempontjából fontos a digitális ökoszisztéma fejlődése. A digitális ökoszisztéma nélkülözhetetlen elemeként jelenik meg a folyamatos fejlődés alatt álló bűnügyi nyomozási ökoszisztéma kialakítása is.

[3] Miniszterelnöki Kabinetiroda 2002: 21.

1. A digitális közigazgatás kriminalisztikai megközelítésből

Az elektronikus közigazgatás mellett a másik gyakran használt kifejezés napjainkban az elektronikus kormányzás.

> „Az elektronikus kormányzás legszélesebb értelemben a digitális információs és kommunikációs technológiák alkalmazását jelenti a kormányzat és a társadalom közötti kapcsolatrendszerekben. Az elektronikus kormányzat megvalósítása az igazgatás minden szintjét érintő olyan modernizációs folyamat, amelyben a technológiai fejlődésre alapozva végső soron a kapcsolatrendszerek minőségi átalakulása megy végbe."[4]

Az Információs és Kommunikációs Technológiák (a továbbiakban: IKT) jelentése: „olyan eszközök, technológiák, szervezési tevékenységek, innovatív folyamatok összessége, amelyek az információ- és a kommunikációközlést, feldolgozást, áramlást, kódolást elősegítik, gyorsabbá, könnyebbé és hatékonyabbá teszik."[5]

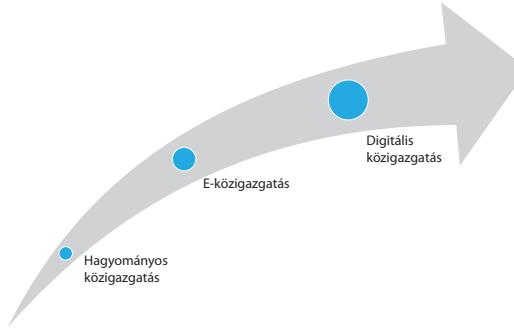
Az infokommunikációs eszközök átformálták életünket és mindennapjainkat. Korábban a pizzát telefonon rendeltük, parkolóórát kerestünk, és volt nálunk aprópénz, az ügyintézés pedig egyet jelentett azzal, hogy sorban állunk.[6] Mára ez megváltozott, mivel applikációkat használunk és töltünk le az okostelefonunkra. Az egyiken keresztül rendeljük meg és fizetjük ki a pizzát. Egy másik a telepített szenzoroknak köszönhetően megmutatja, hol vannak szabad parkolóhelyek. Nem parkolóórákba dobáljuk az érmét, hanem sms-ben vagy applikáción keresztül fizetünk. A mobiltelefon nélkül – kis túlzással – már el sem tudnánk képzelni az életünket.[7] Ez bűnüldözés szempontjából is jelentős, mivel ily módon rengeteg digitális nyomot hagyhatnak maguk után az elkövetők is.

A negyedik ipari forradalom már zajlik, és talán észre sem veszik az emberek, hogy a mindennapi életünket a digitális technológia szinte teljesen átalakítja.[8] A digitális technológiai fejlődésnek köszönhetően folyamatos változásnak vagyunk szemtanúi, és ez a változás a fogalomhasználatban is megjelenik:

4 Dósa–Polyák 2003: 246.
5 *Nemzeti Infokommunikációs Stratégia 2014–2020* 2014: 134.
6 Czékmann–Cseh 2021: 221.
7 Lásd részleteseben a *4.4. alfejezet*et.
8 Krasznay 2022a: 29.

– a bürokratikus, zárt, hagyományos közigazgatást – az ügyféligényeket szem előtt tartva, az IKT-eszközöket és alkalmazásokat igénybe véve – az e-közigazgatás;
– míg az e-közigazgatást (és e-kormányzatot) a digitális állam (közigazgatás) váltja fel,

amelyre jellemző, hogy nyílt és felhasználó által vezérelt (1. ábra).[9]



1. ábra: A közigazgatás evolúciója
Forrás: a szerző szerkesztése

> „Digitális állam: a kormányzat működését támogató belső IT, a lakossági és vállalkozói célcsoportnak szóló elektronikus közigazgatási szolgáltatások, illetve az állami érdekkörbe tartozó egyéb elektronikus (például egészségügyi, oktatási, könyvtári, kulturális örökséghez kapcsolódó vagy az állami adat- és információs vagyon megosztását célzó) szolgáltatások, valamint e szolgáltatások biztonsági hátterének biztosítása."[10]

1.1. Az elektronikus ügyintézés

A 21. század technikai fejlődésre építkezve az Országgyűlés megalkotta az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényt (a továbbiakban: E-ügyintézési tv.), aminek az okai a következők voltak:

[9] Orbán 2021: 27, 29.
[10] *Nemzeti Infokommunikációs Stratégia 2014–2020* 2014: 5.

– az elektronikus ügyintézés széles körű elterjedése;
– az eljárások gyorsítása és az adminisztratív terhek csökkentése;
– a magánjogi jogviszonyok, továbbá az állam és polgár közötti jogviszonyok szélesebb körű elektronizálása;
– az elektronikus ügyintézést nyújtó szervek együttműködésének biztosítása;
– a lakosság számára a korszerűbb és hatékonyabb közszolgáltatások nyújtása.[11]

Az E-ügyintézési tv. alapján az elektronikus ügyintézést biztosító szerv: az államigazgatási szerv; a helyi önkormányzat; a törvény vagy kormányrendelet által közigazgatási hatósági jogkör gyakorlására feljogosított egyéb jogalany; az Országos Bírósági Hivatal és a bíróság; az alapvető jogok biztosa; az ügyészség; a közjegyző; a bírósági végrehajtó, az önálló bírósági végrehajtó iroda; a hegyközségek kivételével a köztestület; a közüzemi szolgáltató; a törvényben vagy kormányrendeletben elektronikus ügyintézés biztosítására kötelezett közfeladatot ellátó vagy közszolgáltatást nyújtó jogalany; valamint a meghatározott ügyek (E-ügyintézési törvény szerint) elektronikus intézését önkéntesen vállaló. Az ügyfél négyféle elektronikus azonosítási szolgáltatást vehet igénybe:
– tároló elemet tartalmazó személyazonosító igazolvány útján biztosított elektronikus azonosítási szolgáltatás;
– ügyfélkapu;
– részleges kódú telefonos azonosítás, valamint
– videotechnológiával történő azonosítás.[12]

Az elektronikus ügyintézési szolgáltatások, valamint a központi elektronikus ügyintézési szolgáltatások vonatkozásában a mesterséges intelligencián alapuló technológia is felhasználható. A központi elektronikus ügyintézési szolgáltatás mesterséges intelligenciával az alábbiakra képes:

> „a) a mesterséges intelligenciával támogatott hangképzés szolgáltatás, amely az elektronikusan rendelkezésre álló szöveget gépi úton hangalapú beszéddé alakító szolgáltatás;
> b) a mesterséges intelligenciával támogatott hangleiratozási szolgáltatás, amely az élő beszédet, valamint az archív-mentett médiaanyagokban a digitálisan rögzített beszédet írásos szöveggé alakító szolgáltatás és

[11] E-ügyintézési tv.
[12] 2015. évi CCXXII. törvény 35. §.

> c) a mesterséges intelligenciával támogatott kommunikációs asszisztens, amely olyan szoftvermegoldás, amely képes az emberek között megvalósuló párbeszédhez rendkívül hasonló beszélgetés lefolytatására és interaktív kommunikációra valós személy közreműködésével kollaboratív módon, illetve valós személy beavatkozása nélkül, automatizáltan, és képes gépi öntanuló folyamat révén a fejlődésre."[13]

Az e-ügyintézési törvény szerint az ügyfélkapu egyike a kormány által kötelezően biztosított elektronikus azonosítási szolgáltatásoknak.[14] Az ügyfélkapun keresztül az azonosítást követően számos hivatalos, munkahelyi vagy magánjellegű ügyet tudunk intézni. Az ügyfélkapu platform a *magyarorszag.hu* oldalon érhető el, ahol a lakosság be tud kapcsolódni az elektronikus szolgáltatások világába. Az ügyfélkapu az „az eszköz, amely biztosítja, hogy az ügyfél egyedileg azonosított módon, biztonságosan léphessen kapcsolatba a központi rendszer útján az elektronikus közigazgatási ügyintézést, illetve az elektronikus közigazgatási szolgáltatást nyújtó szervekkel".[15] Az ügyfélkapu megkerülhetetlen lett az elektronikus eljárásokban. Biztosítja, hogy az ügyintézési folyamat biztonságosan történjen.[16]

Informatizált világunkban a kibertér biztonsága az élet összes területén egyre inkább meghatározóvá válik.[17] Hazánkban 2005. április 1-jétől az ügyfélkapu a legelterjedtebb ügyfél-azonosítást biztosító rendszer az állami elektronikus ügyintézés keretében. Igénybevételével a felhasználók a személyazonosság igazolása mellett, egyszeri belépéssel, biztonságosan kapcsolatba léphetnek az elektronikus ügyintézést és szolgáltatást végző szervekkel.[18] Az első ügyfélkapu létrehozása ingyenes, érvényessége határozatlan idejű, a regisztráció során megadott jelszó legfeljebb két évig érvényes.[19]

A www.ekormanyzat.hu portálon 2001-ben indult az elektronikus ügyintézés, amelyen több alkalommal végeztek fejlesztést, és 2003-tól *magyarorszag.hu* néven érhető el. A webes felületen azonosítás nélküli publikus szolgáltatások is elérhetők, úgymint az általános jellegű információk, ügyleírások.

[13] 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól 134/I. §.
[14] Czékmann–Cseh 2019: 85.
[15] Pócsi 2020: 168.
[16] Czékmann–Cseh 2019: 77, 81.
[17] Krasznay 2022b: 407.
[18] Tarpai 2020: 140.
[19] Király 2018: 134.

Továbbá a felületen több mint 300 elektronikus szolgáltatás érhető el, amelynek körülbelül harmada igényel előzetes – ügyfélkapus – regisztrációt.[20]

Az elektronikusan tárolt információ biztonsága általánosabban véve a kiberbiztonság feladatkörébe tartozik, amely az egyik legnagyobb kihívás a 21. században.[21] A kiberbiztonság külön kutatási terület, ezért külön vizsgálandó.

A *magyarorszag.hu* internetes honlapon az elektronikusan intézhető ügyek egy egységes felületen érhetők el, azonban a SZÜF-portál – azaz a személyre szabott ügyintézési felület – a már megszokott *magyarorszag.hu* oldal megújítása. Az oldalról nagyjából 3700 hivatali szervet lehet elérni. Az úgynevezett e-Papír szolgáltatás is működik, amelyen keresztül havonta 80 ezer kérelem érkezik.[22]

1.2. Az elektronikus ügyintézés nyilvántartásai

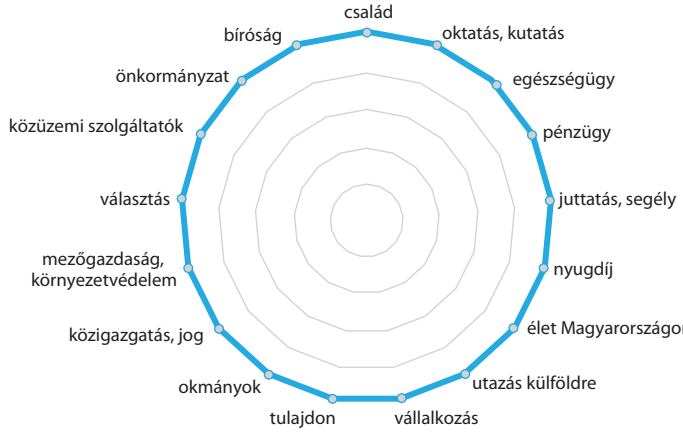
A *magyarorszag.hu* portálon (a továbbiakban: ügyintézési portál) a különböző szervek elektronikus ügyintézési szolgáltatásait vehetjük igénybe. A szolgáltatás megkönnyíti az ügyintézést, illetve a keletkezett adatok egy későbbi időpontban történő elérése adott esetben akár az ügyfél életét is megmentheti. Ezeknek az adatoknak a nyilvántartása (adatbázisa) azonban kriminalisztikai szempontból is kulcsfontosságú. Az ügyintézési portál az elektronikus ügyintézés előszobájaként megnyitotta annak a lehetőségét a bűnüldöző szervek számára, hogy az elkövetőre vonatkozó digitális adatokat, jelen esetben akár digitális nyomokat hivatalos úton történő megkereséssel beszerezzék. A büntetőeljárásról szóló 2017. évi XC. törvény 261. § (1) bekezdése alapján „a büntetőeljárásban a bíróság, az ügyészség és a nyomozó hatóság, illetve – törvényben meghatározott esetben – az előkészítő eljárást folytató szerv bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől adatszolgáltatást kérhet".

A fejezet célja, hogy bemutassa a digitális közigazgatásnak azt az oldalát, amelyikből a kriminalisztika profitálni tud, mivel az elektronikus ügyintézés során keletkezett adatok hozzájárulhatnak a nyomozás eredményességéhez, ezáltal egyaránt lehetővé válhat a bűncselekmények megelőzése, felderítése és megszakítása is.

[20] Orbán 2019: 117.
[21] Krasznay 2020a: 43.
[22] Molnár–Sasvári–Tarpai 2021: 6–7.

Az ügyintézési portálon 17 fő ügycsoport található, amelyek további alnyilvántartásokra, alegységekre tagozódnak (2. ábra). A 17 fő ügycsoport: család; oktatás, kutatás; egészségügy; pénzügy; juttatás, segély; nyugdíj; élet Magyarországon; utazás külföldre; vállalkozás; tulajdon; okmányok; közigazgatás, jog; mezőgazdaság, környezetvédelem; választás; közüzemi szolgáltatók; bíróság; önkormányzat összes ügyleírása. A menüpontnak azért van jelentősége, mert az ügyintézési kérelmek otthonról is könnyedén és gyorsan kitölthetők, és nem kell sorban állni az ügyfélszolgálati ablakoknál.

A nyilvántartásokban szereplő adatok közvetlen elérése[23] a terrorizmus elleni küzdelemben, bűnmegelőzési, bűnfelderítési célú feladatok végrehajtásában, a bűncselekményből származó vagyon visszaszerzésében, valamint az idegenrendészeti és menekültügyi feladatok ellátásában is segítségül szolgálhatna.



2. ábra: Ügyintézési portál
Forrás: a szerző szerkesztése

[23] A lekéréshez (adatszerzéshez) az ügyészi engedélyt be kell szerezni, amennyiben a jogszabály (Be.) előírja. Továbbá van olyan nyilvántartás, amelynek eléréséhez nem kell ügyészi engedély, például a TakarNetből a helyrajzi szám alapján bárki megnézheti (lekérheti) a tulajdonlapot.

1.2.1. A család

A „család” menüpont 8 alkategóriára tagozódik: születés; házasság és egyéb partnerkapcsolatok; elhalálozás; gyámság és gondnokság; örökbefogadás; gyermekvédelem; névviselés; anyakönyvi kivonat (3. ábra).

3. ábra: A család

Forrás: a szerző szerkesztése

A „születés” kategória két adathalmazra tagozódik: a csecsemőgondozási díjra és a születés bejelentésére, anyakönyvezésre. A csecsemőgondozási díj olyan pénzbeli ellátás, amely biztosítotti jogviszonyhoz kötődik, a kiesett jövedelem pótlását szolgálja a gyermek születésekor, és a szülési szabadság időtartamára jár.[24] A születést anyakönyvezés céljából az illetékes anyakönyvvezetőnél be kell jelenteni, a bejelentőnek a közlés során igazolnia kell a szükséges adatokat. A bejelentésről jegyzőkönyv készül, és kiállítják a születési anyakönyvi kivonatot.

A bűncselekményt elkövető személy azonosításában sokszor segítségül szolgálhatnak a családtagjairól beszerzett információk. A születési anyakönyvi kivonaton keresztül is el lehet jutni esetenként a célszemélyhez. Például a hatóság látkörébe kerül egy díler,[25] aki rendszeresen jelentős mennyiségű kábítószert (marihuánát, kokaint stb.) hoz be az országba saját gépkocsival, alkalmanként több millió forint értékben, heti rendszerességgel, kereskedelmi célból. A rendelkezésre álló adatok alapján a célszemélyt – a kábítószer-terjesztőt – „Gipsz Jakabnak”

[24] A *magyarorszag.hu* weboldal Család kategóriája.

[25] Kábítószerrel kereskedő (terjesztő) személy.

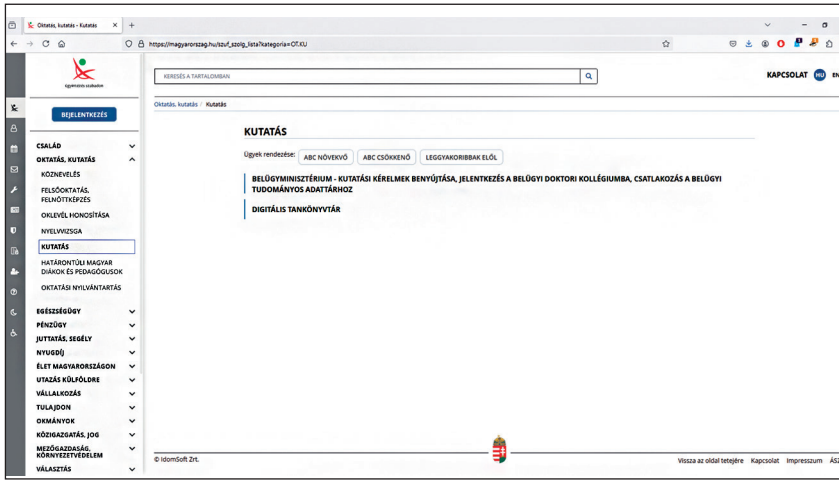
hívják, ám egyéb személyes adata nem ismert. Gyerekei személyes adatai viszont ismertek, mivel a rendőrséggel titkosan együttműködő személy közölte azokat. Szűrő-kutató munka indul: ellenőrzik, hogy a gyerekei lakcímére kik vannak bejelentve. Ám erre a címre a személyi és lakcímnyilvántartás alapján a célszemély nincs bejelentve, tehát még mindig csak a neve ismert.[26] Ilyenkor megoldásként szolgálhat, ha a születési anyakönyvi kivonatból fejtjük vissza az adatokat, mivel abban az apa személyes adatai is megtalálhatók. Innentől kezdve a személyi és lakcímnyilvántartásban már címeket is fogunk tudni társítani a célszemélyhez (az elkövetőhöz). De a gépjármű-nyilvántartásból a tulajdonában vagy birtokában lévő járművek rendszámait is megtudhatjuk. Ez információs láncsorozatot indíthat el, akár kapcsolattérképező figyeléshez vagy bírói engedélyhez kötött leplezett eszköz bevezetéséhez, pontosabban lehallgatáshoz járulhat hozzá. Jelen esetben az anyakönyvi adatokon keresztül jutottunk el az elkövetőhöz. Ez a példa is alátámasztja, hogy milyen jelentősége lehet egy kriminalisztikai szempontból látszólag jelentéktelennek tűnő nyilvántartásnak. Azonban ahhoz, hogy idáig el tudjunk jutni, háttérismeretekre és kriminalisztikai gondolkodásra van szükség.

1.2.2. Az oktatás és a kutatás

Az „oktatás” panel 7 elemet tartalmaz: köznevelés; felsőoktatás, felnőttképzés; oklevél honosítása; nyelvvizsga; kutatás; határon túli magyar diákok és pedagógusok; oktatási nyilvántartás (4. ábra).

4. ábra: Az oktatás és kutatás
Forrás: a szerző szerkesztése

[26] Megjegyzés: ilyenkor az oktatási nyilvántartást is célszerű megnézni, azonban itt sem szerepelt releváns adat.



5. ábra: Kutatási engedély

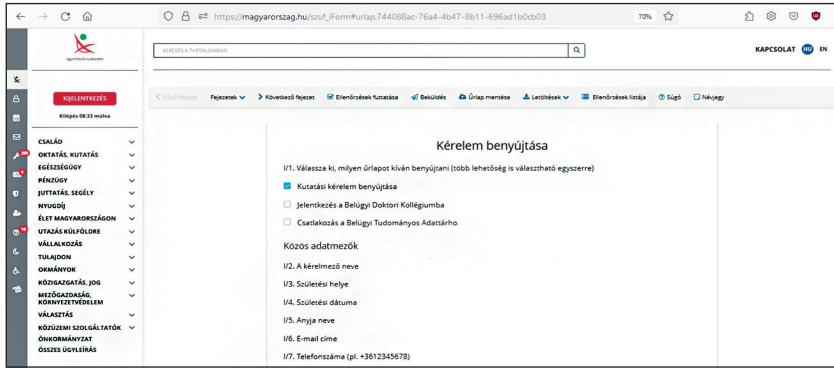
Forrás: magyarorszag.hu weboldal, Kutatás kategóriája

A 7 alegységben szintén „megszámlálhatatlan” ügyet tudunk intézni. Számos kriminalisztikai példát lehetne mondani, hogy a 7 alegység hogyan tudja segíteni a felderítést.

Egy újabb példában tegyük fel, hogy csak ennyi információnk van: a pénzmosás egyik fő szervezője egy egyetemi tanár, aki nemrég „valamilyen tudományos kutatásban” egy kérelmet adott le a Belügyminisztériumba.[27] Ebben az esetben célszerű a kutatási almenüben a „Belügyminisztérium – kutatási kérelmek benyújtása” pontot tanulmányozni, és megtudhatjuk, hogy a kutatási kérelmet az ügyfélkapun keresztül kell benyújtani (5. ábra).

A kérelem formai elbírálásában a Belügyminisztérium Tudománystratégiai és -koordinációs Főosztály Koordinációs Bizottsága is részt fog venni. A kérelembenyújtási lapon a személyes adatokat: születési hely, idő, anyja neve, telefonszám, e-mail stb. is meg lehet adni (6. ábra).

[27] Az adat forrása lehet akár lehallgatás anyaga, együttműködő által közölt információ, tanúkihallgatás stb.

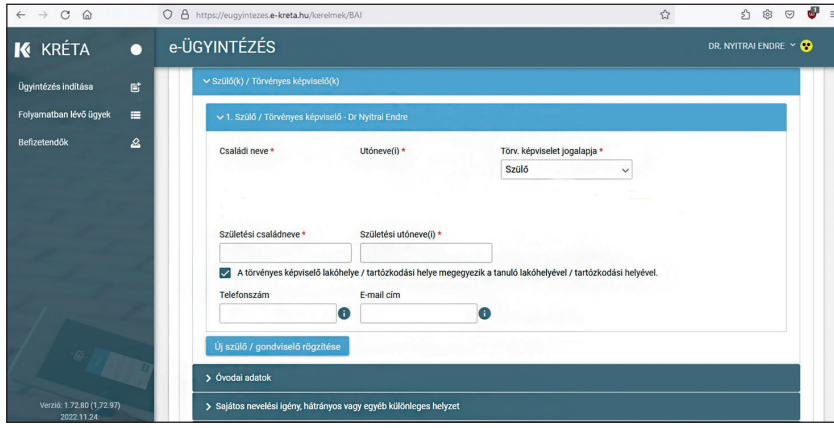


6. ábra: Kérelem benyújtása

Forrás: magyarorszag.hu weboldal, Kérelem benyújtása űrlap

A célszemélyről adatokat egyrészt ügyfélkapujának menüjéből, másrészt a kérelemből tudhatunk meg. Ez azért is fontos, mert lehetőség nyílik arra, hogy újabb nyilvántartásban ellenőrizzük a célszemélyt.

Egy korábbi példában említettem, hogy a célszemélyhez (szülőhöz) a gyerek adatain keresztül is el lehet jutni. A *magyarorszag.hu* portál az oktatás menüpontból a KRÉTA e-ügyintézési felületére irányít. Itt meg kell adni a szülőknek a lakó/tartózkodási helyét, telefonszámát, e-mail-címét (7. ábra).



7. ábra: E-ügyintézés

Forrás: e-ügyintézés az *e-kreta.hu* weboldalán

Ezek az adatok már elegendőek ahhoz, hogy egy hiteles nyilvántartásban, például személy- és lakcímnyilvántartásban be lehessen azonosítani a célszemélyt, ami a rendelkezésre álló adatok függvényében akár megalapozhatja, hogy a célszemélyhez tartozó címeken kutatást lehessen foganatosítani. Jelen esetben ajánlott adatgyűjtést – puhatolást – folytatni a gyermek iskolájában, mivel a szülők elérhetőségként újabb adatokat adhatnak meg az iskolában (például az osztályfőnöknek).

1.2.3. Az egészségügy

Az egészségügy menüpont 3 részből áll: egészségbiztosítás egészségügyi szolgáltatásai; egészségbiztosítás pénzbeli ellátásai; egészségügyi nyilvántartás.

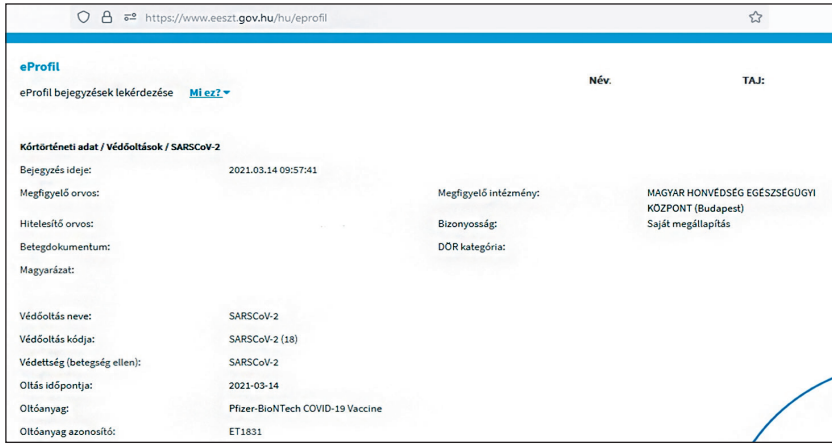
Napjainkban már kulcsfontosságú szerepet tölt be az Elektronikus Egészségügyi Szolgáltatási Tér (a továbbiakban: EESZT), mivel a rendszer elősegíti az információáramlást. Az ide feltöltött adatok, egészségügyi dokumentációk egyszerűen és gyorsan juthatnak el a kezelőorvoshoz, ami adott esetben a beteg életét is megmentheti.

Az egészségügyi ellátás során keletkező adatok rögzítése az EESZT-ben az alábbi módokon történik:

- Központi eseménykatalógus;
- Egészségügyi dokumentáció nyilvántartása (EHR);
- Egészségügyi profil (eProfil);
- eRecept (elektronikus vénynyilvántartás);
- Elektronikus beutalók (eBeutaló) nyilvántartása;
- Időpontfoglalások nyilvántartása;
- Elektronikus szolgáltatásrendelés-nyilvántartás és időpontfoglalás.[28]

Az EESZT-hez csatlakoztak járó- és fekvőbeteg-ellátó intézmények, gyógyszertárak, háziorvosi szolgálatok, nem közfinanszírozott egészségügyi szolgáltatást nyújtó egészségügyi szolgáltatók és az állami mentőszolgálat, valamint minden orvosi vagy fogorvosi működési engedéllyel rendelkező magánfinanszírozott egészségügyi szolgáltató.[29]

[28] EESZT 2021.
[29] EESZT 2021.



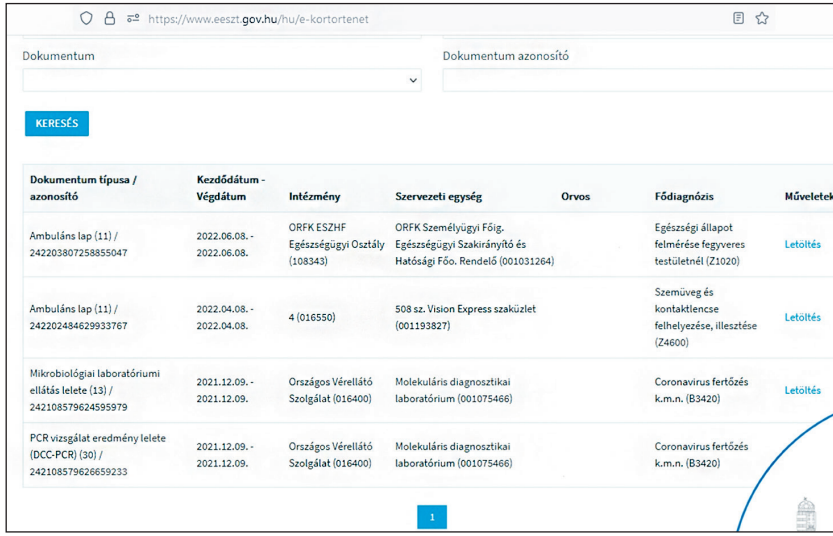
8. ábra: Egészségügyi profil

Forrás: e-profil az *EESZT Lakossági Portál*on

Az EESZT-ben a betegről egészségügyi profil készül, amely tartalmazza az általános egészségügyi állapotát, pontosabban aktuális betegségeit, általános egészségügyi adatait. A profil célja, hogy a kezelőorvos naprakész egészségügyi adatokkal rendelkezzen (8. ábra).

Látható, hogy a rendszer napra, órára, másodpercre pontosan megadja, mikor rögzítették a dokumentumot, melyik egészségügyi intézményben, ki volt a megfigyelő vagy kezelőorvos (9. ábra).

Ezek az adatok kriminalisztikai értelemben azért is fontosak, mert ha tudunk időpontot és helyet, akkor akár olyan kamerafelvételt is beszerezhetünk, amely a szolgáltatást igénybe vevő személyről készült az egészségügyi objektum területén. A kamerafelvétel egy arcképelemző program segítségével összehasonlítható a bűncselekmény helyszínén készült felvétellel, amelyen az ismeretlen személyazonosságú elkövető látható. Ha több időpont és helyszín is rendelkezésre áll, például az ellátás helyei, a receptkiváltás helye (az eRecept nyilvántartásából), úgy az elkövető telefonszáma akkor is beszerezhető (mobiltársaságok segítségével), ha nem adta meg a regisztráció során. Ha több időpont és helyszín áll rendelkezésre, akkor az adott időpontra (időintervallumra) kérhetünk a mobilszolgáltatóktól adatszolgáltatást, hogy a kérdéses területen található mobil cellaazonosítóra milyen telefonszámok jelentkeztek fel. Elemző szűrő-kutató munka keretében kikövetkeztethető, hogy melyek azok a számok, amelyek az adott területen és időpontban előfordultak.



9. ábra: E-kórtörténet
Forrás: EESZT Lakossági Portál, e-kórtörténet

Az eRecept (elektronikus vénynyilvántartás) célja a gyógykezelés, az, hogy például a gyógyszertár hozzáférjen az elektronikus úton kiállított vények adataihoz, és a terméket át tudja adni.[30] Az eRecept kiváltása a körözött személy elfogását is segítheti, továbbá az érintett telefonszámának és e-mail-címének megismerésére is lehetőség nyílik.

A NEAK (Nemzeti Egészségbiztosítási Alapkezelő) nyilvántartása a védőnői szolgálatok tekintetében is lehetőséget ad nyomozási cselekmények végrehajtására. A védőnő feladata a várandós, gyermekágyas és szoptató anyák gondozása, valamint a gyermekek gondozása az újszülött kortól a tanulói jogviszony megkezdéséig. A védőnői gondozási lapok tartalmi követelményei közé tartozik például személyi adatok, védőnői látogatások, tanácsadások, intézkedések dokumentációja stb. A szülők tartózkodási helyüket, telefonszámukat a szülést megelőzően és azt követően a védőnői tanácsadás, illetve családlátogatás céljából közölhetik, valamint a változásokat is jelzik, amelyeket rögzítenek. Így a körözés alatt álló vagy szökésben lévő szülő (apa, anya) aktuális tartózkodási

30 EESZT 2021.

helye, amennyiben azt változtatja, a NEAK védőnői szolgálatok által rögzített adatok segítségével egy megkereséssel megismerhetővé válhat a hatóság előtt.

Az EESZT-ben rögzített adatok a gyanúsított munkahelyének, lakcímének, egészségügyi szolgáltatás igénybevételi helyének (kórház, orvosi rendelő) meghatározásában segíthetnek. Az elkövető tajszámából megtudható, hogy ki, milyen munkáltató fizeti az egészségügyi hozzájárulást.

Az egészségügyi adat fogalma az általános adatvédelmi rendelet 4. cikkének 15. pontja szerint: „egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról."[31] Míg az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény[32] 3. § *a)* pontja alapján egészségügyi adat: „az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőkkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (például magatartás, környezet, foglalkozás)."

Miért fontos kriminalisztikai nézőpontból az egészségügyi adat fogalma? Azért, mert ha tudjuk, mit jelent a fogalom, ismerjük annak elemeit, akkor arra építkezve szükség esetén kérdéseket is meg tudunk fogalmazni.

A gyanúsított alibijének ellenőrzése vagy az elkövető beazonosítása, illetve a bűncselekmény felderítése és bizonyítása érdekében célszerű lehet megkeresni az ügyfél-regisztrációs szervet.[33] A megkeresés arra irányul, hogy az érintett személy milyen szolgáltatást, mikor, hol és milyen elérhetőségekkel vett igénybe.

[31] 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).

[32] Szeretném megjegyezni, hogy a törvény már nem hatályos, de figyelemmel arra, hogy meghatározza az egészségügyi adat fogalmát, célszerűnek láttam feldolgozni.

[33] Az ügyfél ügyeinek intézése során a Kormány által kötelezően biztosított elektronikus azonosítási szolgáltatások közül igénybe veheti az ügyfélkaput.

1.2.4. A pénzügy, a juttatás, segély, a nyugdíj, a vállalkozás és a tulajdon

A pénzügy, juttatás, segély, nyugdíj, vállalkozás és tulajdon kategóriákba tartozó ügyintézési lehetőségeket szemlélteti az 1. táblázat.

1. táblázat: Pénzügyi és egyéb modulok

Pénzügy	Juttatás, segély	Nyugdíj	Vállalkozás	Tulajdon
– Magánszemélyek adózása – Egyéni vállalkozók adózása – Társaságok adózása – Kiemelt adózók – Illetékek – Vám – Befektetések, megtakarítások, hitelek – Pályázatok, közbeszerzés – Központosított illetményszámfejtés	– Családok támogatása – Szociális ellátás – Foglalkoztatás elősegítése és a munkanélküliek ellátása – Fogyatékkal élő személyek támogatása – Megváltozott munkaképességű személyek ellátásai	– Ellátások igénylése – Ellátások igénylése (nemzetközi) – Adategyeztetés, megállapodás – Ellátások folyósítása – Egyéb ügyintézés – Foglalkoztatói ügyintézés – Egyéb szolgáltatások	– Engedély- és bejelentéskötelés vállalkozások – Cégek működtetése – Egyéni vállalkozás – Kereskedelem – Munkavállalókat érintő ügyintézés	– Gépjármű – Ingatlan – Társasházak – Építésügy – Szellemi tulajdon

Forrás: a szerző szerkesztése

Az ügyészség és a nyomozó hatóság az eljárás során minden szükséges intézkedést köteles megtenni az elkobozható vagy a vagyonelkobzás alá eső dolog vagy vagyon felderítése és biztosítása érdekében.[34]

A büntetőeljárás során azonosítani kell valamennyi, a bűncselekményből származó vagyon átvételével, tárolásával, elrejtésével, átalakításával, átruházásával, elidegenítésével vagy abban történő részvétellel, felhasználásával, azzal összefüggésben végzett pénzügyi vagy gazdasági tevékenységgel, ilyen igénybevételével összefüggésbe hozható természetes vagy jogi személyt, jogi személyiséggel nem rendelkező szervezetet.[35]

Ebben nyújthatnak segítséget a tárgyalt menüpontok.

[34] 2017. évi XCI. törvény a büntetőeljárásról 353. § (1).

[35] 32/2022. (X. 25.) ORFK utasítás a vagyonvisszaszerzéssel kapcsolatos feladatokról 8. pont.

A 1. táblázatban szereplő panelek a bűnügytől (a rendelkezésre álló adatoktól) függően segítségül lehetnek, mivel minden ügy egyedi. Például a gépjárművel kapcsolatos bűncselekmények esetében fontos információként szolgálhatnak az alábbiak:

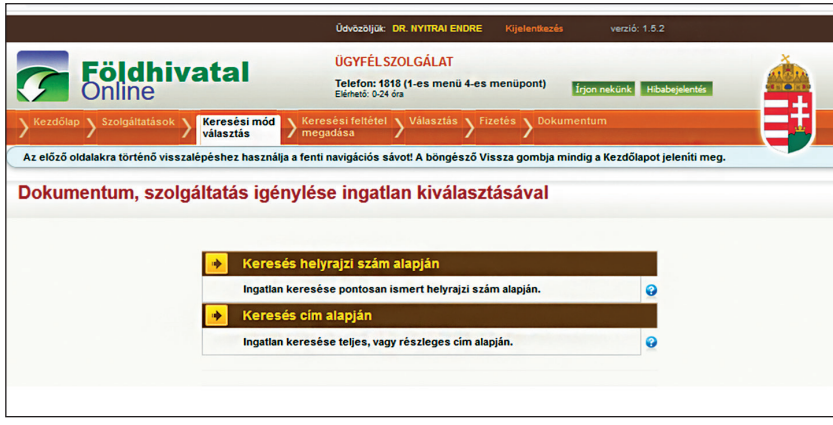
- űrlapon szereplő adatok,
- a tulajdonjogváltozást igazoló teljes bizonyító erejű magánokirat (például adásvételi szerződés, ajándékozási szerződés) beszkennelt képe. A táblázat „gépjármű" panele szintén információkat szolgáltathat.

A portálon lehetőség nyílik e-hiteles és nem hiteles tulajdoni lap lekérésére. A hiteles tulajdoni lap másolatának lekérdezése (szemle, teljes) évente két alkalommal ingyenes, ellentétben az e-hiteles tulajdoni lappal, amely minden esetben költséggel jár. A rendszerben lehetőség van többféle keresésre (10. ábra):

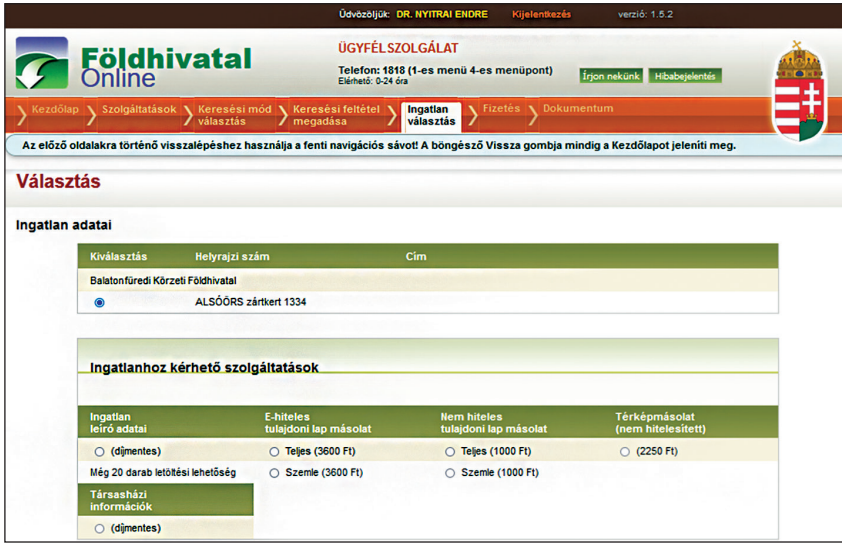
- keresés helyrajzi szám alapján;
- keresés cím alapján.

Ha találatunk van, akkor további keresési menüpont nyílik meg (11. ábra):

- ingatlan leíró adatai;
- térképmásolat;
- társasházi információk.



10. ábra: Földhivatali nyilvántartás
Forrás: Földhivatal Online weboldal



11. ábra: Keresési pontok

Forrás: Földhivatal Online weboldal

A bűnüldöző szerveknek a nyilvántartás segítséget ad ahhoz, hogy a személyekhez ingatlant tudjanak kötni, ahol szükség esetén kutatást tudnak foganatosítani. Az elkövető adatai alapján, valamint a már meglévő cím vagy helyrajzi szám alapján a hatóság tud ingatlanra keresni. A kutatásra való felkészülésben segítségül lehet a „társasházi információ", mert megadja, hogy hány albetét (például lakás, üzlethelyiség, pince) tartozik az épülethez, ezek milyen nagyságúak, melyik emeleten helyezkednek el, illetve ki a tulajdonosuk. Így feltérképezhető, hogy egy szinten hány lakás található, milyen menekülési útvonalak vannak. A társasházi információk a nyomozó hatóság figyelmét arra is felhívhatják, hogy az érintett lakáshoz tartozik-e pince vagy egyéb helyiség. Ilyenkor a kutatást erre a helyiségre is ki kell terjeszteni, mivel az elkövetéshez használt eszközök vagy egyéb tárgyi bizonyítási eszköz is lehet ide elrejtve. Célszerű általában helyrajzi számra keresni, mivel jóval pontosabb a találati arányok tekintetében, mintha címre keresnénk. Nagyobb városokban általában már a főbejárati ajtó fölött egy táblán megtalálható a helyrajzi szám, amely alapján az ingatlan-nyilvántartásban a társasházi információk menüponton keresztül leszűkíthető (beazonosítható) a keresett objektum (lakás).

1.2.5. Az élet Magyarországon, az utazás külföldre, a közigazgatás, jog és a választás

A portál élet Magyarországon; utazás külföldre; közigazgatás, jog, választás alpontjai szintén az ügyfelek ügyintézését könnyítik meg (2. táblázat).

2. táblázat: Élet Magyarországon és egyéb modulok

Élet Magyarországon	**Utazás külföldre**	**Közigazgatás, jog**	**Választás**
– Tartózkodás Magyarországon – Magyar állampolgárság – Menekültként Magyarországon	– Utazási információk – Vízumügyek – Külföldi tartózkodás és letelepedés	– Adatkezelés, adatszolgáltatás – Kérelem benyújtása – Ügyfélbeadványok megindult eljárásban – Döntés, jogorvoslat, kártérítés – Bíróság, ügyészség – Rend- és honvédelem – Időpontfoglalás kormányablakba – Fogyasztóvédelem	– Általános információk – Szavazással kapcsolatos kérelmek – Regisztráció – Adatvédelem – Segítség a fogyatékossággal élők szavazásához

Forrás: a szerző szerkesztése

Ha például egy ügy vizsgálata (nyomozása) kapcsán olyan információ merül fel, hogy jogerős ítélet előtt a terhelt ki akarja vonni magát az eljárásból, és olyan országba akar menekülni, ahová kötelező a vízum, akkor célszerű megkereséssel élni és ellenőrizni az információt az „utazás külföldre” menüpontban.[36]

[36] Azonban nem utazhat külföldre, akit végrehajtandó szabadságvesztésre ítéltek, illetve akinek felfüggesztett vagy részben felfüggesztett szabadságvesztése végrehajtását utóbb elrendelték, az ítélet jogerőre emelkedésétől a szabadságvesztés végrehajtásának utolsó napjáig [1998. évi XII. tv. 16. § (1) *c)* pontja].

1.2.6. Az önkormányzat, az okmányok, a mezőgazdaság, környezetvédelem és a közüzemi szolgáltatók

A portálon még megtalálhatók az önkormányzat; okmányok; mezőgazdaság, környezetvédelem; közüzemi szolgáltatók által nyújtott ügyintézési lehetőségek is (3. táblázat).

3. táblázat: Önkormányzatok és egyéb modulok

Önkormányzatok	**Okmányok**	**Mezőgazdaság, környezetvédelem**	**Közüzemi szolgáltatók**
– E-önkormányzat portál	– Személyazonosító igazolvány – Lakcímigazolvány – Útlevél – Vezetői engedély – Gépjárművel kapcsolatos okmányok – Erkölcsi bizonyítvány – Adóigazolvány – Őstermelői igazolvány – Mozgásában korlátozott személy parkolási igazolványa – Oktatási igazolványok	– Vidékfejlesztés – Mezőgazdaság – Környezet- és természetvédelem – Élelmiszerbiztonság – Közös agrárpolitika	– Alföldvíz Zrt. – Bakonykarszt Zrt. – Budapesti Közművek – Duna Menti Regionális Vízmű – Dunántúli Regionális Vízmű – EON – Északdunántúli Vízmű Zrt. – Északmagyarországi Regionális Vízművek – Fővárosi Csatornázási Művek – Fővárosi Vízművek – Magyar Posta – MVM Next – Tiszamenti Regionális Vízművek

Forrás: a szerző szerkesztése

A szolgáltatók szintén fontos adatokat nyújthatnak bűnüldözési szempontból, mivel sok esetben a bérlő egy büntetőeljárásban érintett mint elkövető, és egy hatóság szeretné megtudni, hogy hol tartózkodik életvitelszerűen, vagy adott esetben arra irányul a kérdés, hogy a bűncselekmény helyszínén (például egy kábítószer-lerakat, -elosztó lakásban) ki lakik, ki az, aki bérli. A tulajdonossal vagy a szomszédokkal nem célszerű minden esetben beszélni, mert a nyomozás elején akár felmerülhet a dekonspiráció veszélye is.[37] A szolgáltatóknál a tulajdonosok a közüzemi számlákat egyre több alkalommal íratják át a bérlőkre.

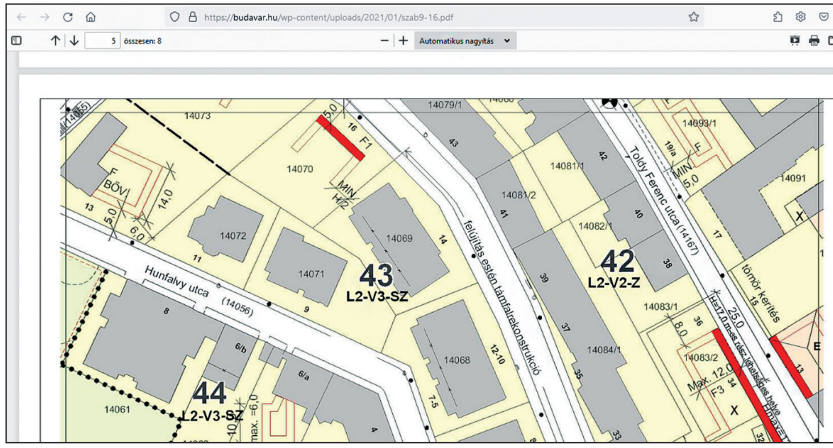
[37] Az ügy előadója dönti el, hogy a releváns címen és annak a környezetben mikor célszerű adatgyűjtést folytatni.

Előfordulhat, hogy olyan információt kell leellenőrizni, hogy a kérdéses lakásban marihuánaültetvény található-e. Első lépésként az objektummal kapcsolatosan ellenőrizni kell az energetikai/villanyszámlát, mivel egy ültetvényen a nap 24 órájában használhatják a villanyt, a szellőztető berendezéseket stb. Így az ültetvény esetén a villanyszámla általában kirívóan magas szokott lenni. A szolgáltatók tájékoztatni tudnak a fogyasztott kWh-ról és arról, hogy kinek a nevén van a szolgáltatás.

Az önkormányzatok portáljain megtalálható „információk gyűjteménye" kriminalisztikai értelemben szintén segítségül szolgálhat. Ha felmerül a gyanúsított vagy szökésben lévő személy tartózkodási címe, vagy más ügyben a cím a felderítés szempontjából releváns, de az ingatlan-nyilvántartásban „nincs találat" eredményt kapunk, akkor a helyrajzi számra kell keresnünk. Ha csak a társasház címe áll rendelkezésre, azonban belül kellene egyesével lekérni az albetéteket/lakásokat, de szintén „nincs találat" jelzést kapunk, akkor célszerű a helyrajzi számot megtudni, az alapján az összes albetétre lehet majd keresni. A helyrajzi számot pedig általában megtalálhatjuk az önkormányzatok portálján „a kerület építési szabályzatának" pontjában (12–13. ábra).

12. ábra: A helyrajzi szám keresése

Forrás: Kerületi Építési Szabályzat a Budavári Önkormányzat weboldalán



13. ábra: Helyrajzi térkép
Forrás: Mű-Hely Zrt. 2021: 13.

A 13. ábrán példaképpen Budapest I. kerületének (KÉSZ) szabályozási terve látható. A terven az utcanevek, házszámok és helyrajzi számok is szerepelnek. Ha az ingatlan-nyilvántartásban nem sikerül címre keresni, akkor a helyrajzi számot kell megtudni, amelynek a legegyszerűbb módja az önkormányzati portál felülete.

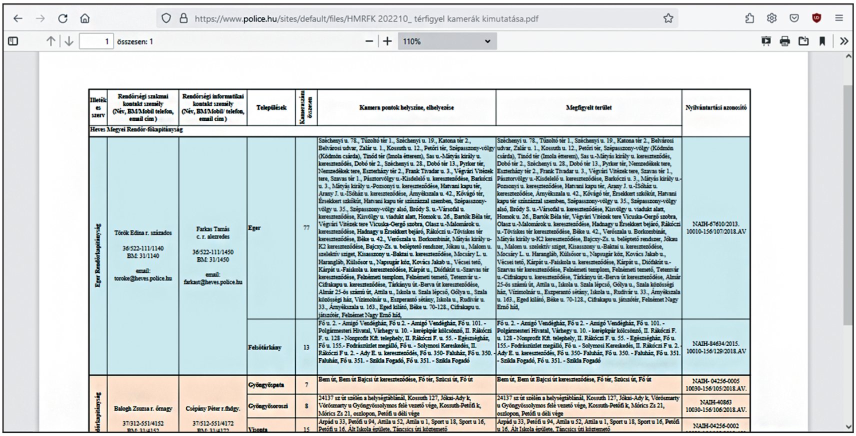
Bűncselekmény helyszínén, illetve a tágabb környezetében mindig fontos, hogy vannak-e térfigyelő kamerák. Ha vannak, azoknak a felvételeit általában lefoglalják. Az adatgyűjtés keretében nem biztos, hogy sikerült észrevenni az adott térfigyelő kamerát. Ezért célszerű az illetékes önkormányzat oldalán megtekinteni a kimutatást a közterületet megfigyelő kamerákról.[38] Például Budapest I. kerületében a megfigyelő kamerákat az önkormányzat portálján két típusra bontják:

– Budavári közterület intelligens megfigyelő kamerák helyszínei;
– Budavári közterület megfigyelő kamerák helyszínei.

[38] Az önkormányzatnak és a rendőrségnek fel kell tüntetni a térfigyelő kamerák helyét.

Mindként esetben részletesen leírják a kamerák elhelyezkedését, például 1014 Budapest, Szentháromság tér 6. Magyarság Háza Homlokzat Fortuna utca felőli oldal.[39]

Továbbá meg kell még említeni, hogy a rendőrség is vezet kimutatást a térfigyelő kamerákról (14. ábra).



14. ábra: Térfigyelő kamerák kimutatása

Forrás: térfigyelő kamerák kimutatása a *Police.hu* weboldalon

A rendőrség kimutatása a kamerákról, illetve azok elhelyezkedéséről elnevezésű linken belül szintén részletesen feltüntetik a kamera helyszínét, elhelyezkedését, továbbá kitérnek a megfigyelt területre, illetve kontaktszemélyt is feltüntetnek elérhetőséggel, akihez kérdés esetén lehet fordulni.

1.3. A nemzeti adatvagyon és adatgazdálkodás

Az adatot egyre gyakrabban a 21. század olajaként szokták emlegetni, amely a társadalom, a gazdaság és a nyomozás hajtóereje, motorja is egyben. A szervezetek, intézmények és szolgáltatók rengeteg adatot halmoznak fel és tárolnak,

[39] *Budavári Önkormányzat közterületet megfigyelő automatikus és intelligens kamerák helyszínei* 2021.

amelyek megismerése és kiaknázása elengedhetetlen. Az adatok megismerésével, feldolgozásával (elemzésével és értékelésével) hatékonyabbá válhat a nyomozás.

A nemzeti adatvagyonról szóló 2021. évi XCI. törvény alapján a nemzeti adatvagyon „a közfeladatot ellátó szervek által kezelt közérdekű adatok, közérdekből nyilvános adatok és kutatási adatok (a továbbiakban együttesen: közadatok) és személyes adatok összessége". Az adatvagyon fogalmának tágabb értelmezését fogalmazza meg a *Digitális Megújulás Cselekvési Terv 2010–2014:* „Mindazok az adatok és információk a nemzeti adatvagyon elemeit képezik, amelyek a társadalom, a gazdaság, az állam működéséhez, a nemzethez és annak kultúrájához tartoznak." A terv a nemzeti adatvagyont a nemzet legfőbb kincsének tekinti, kiemelve, hogy nem azonos a kormányzat által kezelt adatokkal, azoknál sokkal bővebbnek tekinti.[40]

A nemzeti adatvagyon körébe tartozó néhány ismertebb állami nyilvántartás:

- A polgárok személyi adatainak és lakcímének nyilvántartása;
- Elektronikus anyakönyvi nyilvántartás;
- Ingatlan-nyilvántartás, az állami ingatlan-nyilvántartási térképi adatbázis;
- Nyugdíjbiztosítási nyilvántartás;
- Egészségbiztosítási nyilvántartás;
- Központi útiokmány-nyilvántartás;
- Szabálysértési nyilvántartási rendszer;
- Közúti közlekedési nyilvántartás;
- Nemzeti Adó- és Vámhivatal által kezelt adóhatósági és vámhatósági adatok nyilvántartása;
- Cégnyilvántartás;
- Az egyéni vállalkozók nyilvántartása;
- Bűnügyi nyilvántartási rendszer;
- Fizetésképtelenségi nyilvántartás.[41]

Ha a kisebb nyilvántartásokat is figyelembe vennék, akkor a tízezret is meghaladná a számuk.[42]

A mesterséges intelligencia alkalmazásához nagy mennyiségű adatra van szükség, ezért ebből a szempontból is fontos, hogy a keletkezett adatok

[40] *Digitális Megújulás Cselekvési Terv 2010–2014* 2010: 66.

[41] A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet melléklete.

[42] Infostart/Inforádió – Király 2020.

hozzáférhetők legyenek. Így lehetővé válhat, hogy a nyomozásokba és az elemző-értékelő munkafolyamatokba a mesterséges intelligencia nyújtotta lehetőségeket bevezessék.

1.3.1. A Nemzeti Adatvagyon Ügynökség és a Nemzeti Adatvagyon Tanács

Elengedhetetlenné vált egy olyan intézményrendszer létrehozása, amely figyelembe veszi a korszerű digitális államkormányzás és gazdaság megvalósítását; a mesterséges intelligencián és adatelemzésen alapuló technológiák elterjedését; a nemzeti adatvagyon széles körű hasznosításának megvalósítását, az állampolgárok államba vetett bizalmának további erősítését.[43] A nemzeti adatvagyonról szóló 2021. évi XCI. törvény kettős céllal született:

- egyrészt a nemzeti adatvagyon hasznosításának elősegítése miatt, ezért megalkotta a Nemzeti Adatvagyon Ügynökséget (a továbbiakban: NAVÜ) és a Nemzeti Adatvagyon Tanácsot, valamint meghatározta ezek főbb feladatait;
- másrészt egységes szerkezetbe foglalja a nemzeti adatvagyon gazdálkodásával és védelmével kapcsolatos szervezeti normákat, beemelve a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló rendelkezéseit is.[44]

A NAVÜ olyan közfeladatot ellátó szerv, amely

- a nemzeti adatvagyon hasznosításával kapcsolatos állami feladatokat látja el és ennek keretében elősegíti és támogatja a Közadat tv. végrehajtását;
- elkészíti a Közadat tv. szerint újrahasznosítás céljából rendelkezésre bocsátható közadatokat tartalmazó nyilvántartások és adatbázisok jegyzékét, valamint folyamatosan figyelemmel kíséri azoknak a változását;
- az általa működtetett internetes honlapon közzéteszi az elkészített jegyzéket, továbbá a honlapon keresztül tájékoztatja a közfeladatot ellátó szerveket és a Közadat tv. szerinti igénylőket az őket megillető jogokról és őket terhelő kötelezettségekről;
- erre vonatkozó megkeresése esetén közreműködik a Közadat tv. szerinti újrahasznosítás céljából történő rendelkezésre bocsátás megvalósításában,

[43] 2021. évi XCI. törvény a nemzeti adatvagyonról.

[44] 2021. évi XCI. törvény végső előterjesztői indokolása a nemzeti adatvagyonról.

ha a közfeladatot ellátó szerv vagy az igénylő megkeresi, ideértve a kérelem előkészítésében, a díj megállapításában, az újrahasznosítási megállapodás előkészítésében és a rendelkezésre bocsátás módjának meghatározásában való együttműködést, valamint az együttműködő szerv által kezelt nyilvántartásból származó személyes adatnak az anonimizálását követően adatelemzést végez.[45] A NAVÜ háromféle szolgáltatást nyújt: általános kormányzati tájékoztató; kormányzati tájékoztatási, valamint piaci tájékoztatási szolgáltatást.

A Nemzeti Adatvagyon Tanácsot az adatvagyon-gazdálkodással összefüggésben hozták létre. Kormánybizottságként működik, tagjai a kormány adatgazdálkodásban érintett miniszterei. A Tanács a Nemzeti Adatvagyon Ügynökség tevékenységével kapcsolatban iránymutatásokat és alapelveket határoz meg, valamint dönt a piaci tájékoztatási szolgáltatásra vonatkozó igény teljesítése tárgyában.

1.4. A digitális állampolgárság

A Digitális Magyarország Ügynökség Zártkörűen Működő Részvénytársaság kijelöléséről és egyes feladatainak meghatározásáról, valamint a nemzeti informatikai és e-közigazgatási tevékenység összehangolt biztosításával összefüggő részletszabályokról szóló rendelettel a kormány a Digitális Magyarország Ügynökség Zártkörűen Működő Részvénytársaságot (a továbbiakban: DMÜ) jelöli ki az e-közigazgatással, az informatikával, az e-közigazgatási és informatikai fejlesztések egységesítésével, a kormányzati célú elektronikus hírközlési tevékenységgel, valamint a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításával kapcsolatos állami feladatok ellátására, amelyeket közfeladatként lát el.[46]

A DMÜ a feladatok végrehajtása során

- közreműködik a szükséges költségvetési források megtervezésében;
- előkészíti és lebonyolítja a kezelő szervi megállapodásban rögzített fejezeti kezelésű előirányzatok javára történő költségvetési megállapodások megkötését, az azokhoz kapcsolódó beszámoltatási és elszámoltatási feladatokat;

[45] 2021. évi XCI. törvény a nemzeti adatvagyonról 4. § (1).

[46] 307/2022. (VIII. 11.) Korm. rendelet 2. §, 3. §.

– megtervezi, előkészíti és lebonyolítja a releváns fejezeti kezelésű előirányzatok terhére történő közszolgáltatási, támogatási vagy egyéb finanszírozási szerződések megkötését, az ahhoz kapcsolódó beszámoltatási és elszámoltatási feladatokat;
– beszámol a rendelkezésére bocsátott források felhasználásáról.[47]

A Kormányzati Tájékoztatási Központ tájékoztatása szerint a Digitális Magyarország Ügynökség fő tevékenysége a kormányzati digitalizáció, valamint a digitális állampolgárság megteremtése, továbbá célja az átláthatóság, a kiszámíthatóság, a hatékony és gyors ügyintézés biztosítása.[48]

Az információs és kommunikációs technológiák fejlődése életünk gyökeres átalakulását eredményezi, ezért az Országgyűlés az állam és a társadalom kapcsolatának digitális térbe helyezése, a modern kormányzati digitális felületek és szolgáltatások létrehozása érdekében megalkotta a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvényt.[49] A törvény célkitűzésként a digitális állampolgárság létrehozását jelölte meg, értelmező rendelkezése szerint a „digitális állampolgárság: az állampolgárok azon joga, amellyel digitálisan ügyet intézhetnek, szolgáltatást vehetnek igénybe."[50] A DMÜ tájékoztatása alapján így a felhasználók mobilalkalmazás segítségével igazolhatják majd a személyazonosságukat, illetve egyes piaci szolgáltatók ügyintézési felületeire is digitális azonosítással léphetnek majd be az állampolgárok.[51]

A *Digitális állampolgárság kutatás* weboldala szerint

> „a digitális állampolgársághoz kapcsolódó tevékenységek olyan tudatosan átgondolt, az egyén és a közösség számára értékes cselekvést és viselkedést jelentenek, amelyek magukban foglalják a 21. századhoz illeszkedő, digitális kommunikáció és eszközhasználat modelljét, az online felületeken végzett értékteremtő tevékenységet és annak hatásait,

47 307/2022. (VIII. 11.) Korm. rendelet 4. §.
48 Kormányzati Tájékoztatási Központ 2022.
49 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól.
50 A 2023. évi CIII. törvény 8. § 8. pontja.
51 Magyarország Kormánya 2023.

> valamint a digitális eszközökkel végzett cselekvés etikai, jogi, valamint a mentális és fizikai egészségi állapothoz fűződő aspektusait is. A digitális állampolgárság fogalma alapján az egyén a közösség által kialakított – és folyamatosan formálódó – normák szerint, az egyén és a közösség jogainak és becsületének tiszteletben tartásával, annak védelmében és művelésében végzi mindennapi, hétköznapi és szakmai tevékenységét."[52]

Azonban a digitális állampolgárságnak a köztudatban kétféle fogalmi meghatározása él egymással párhuzamosan: az egyik értelmezés magában foglalja az állampolgárok tevékenységének digitális támogatását, kiegészítését, a másik meghatározás pedig a digitális és az online világban állampolgárrá váló egyének tevékenységére összpontosít.[53]

A digitalizációt, a digitális állampolgárságot, valamint az e-közigazgatási folyamatokat fogja elősegíteni az önkiszolgáló mesterséges intelligenciával támogatott ügyintézési pontok, úgynevezett kiosk eszközök országos lefedettségű üzembe helyezése, amely segítségével az állampolgári ügyintézési folyamatok automatizálódnak. A KIOSK kiváltja a hivatali dolgozó személyes beavatkozását. A projekt közérdekű célja, hogy az állampolgárok az automatizálható feladatokat önállóan, de a hatósági környezetben, valamint az ügyintézők nélkül is el tudják kezdeni, vagy adott esetben teljesen önállóan le tudják folytatni. Ezáltal az elektronikus ügyintézés lehetősége azok számára is elérhető, akik nem rendelkeznek megfelelő technikai eszközzel.[54] Az úgynevezett MIA Pontokon (Mesterséges Intelligencia Asszisztens) elhelyezett eszközöket bárki kipróbálhatja.

A kiosk eszköz telepítése lehetővé teszi, hogy az állampolgárok 12 ügyet intézzenek (okmányokkal, járművekkel kapcsolatosan, illetve lakcímbejelentéseket is tehetnek). Az intelligens oszlopok előnye, hogy a nap 24 órájában elérhetők.[55] A személyazonosítás okmány- és arckép-azonosításon alapul. Az arckép-azonosítás során az állampolgárról a videokommunikáció során rögzített képet a szoftver összeveti a közhiteles nyilvántartásban tárolt fotóval, amely az utolsó személyes megjelenéskor készült.[56]

[52] *Digitális állampolgárság kutatás* weboldala.
[53] Ollé et al. 2013: 12.
[54] NISZ 2020.
[55] Magyarország Kormánya 2021.
[56] Az e-közigazgatásban is hasít a mesterséges intelligencia (x) 2022.

Az önkiszolgáló Mesterséges intelligenciával támogatott ügyintézési pont, az úgynevezett kiosk eszköz telepítése nagymértékben hozzá fog járulni akár elkövetők beazonosításhoz, vagy az általuk használt telefonszámok megismeréséhez is. A digitalizált állampolgársággal növekedni fog a magunk után hagyott digitális adat mennyisége, amelynek megismerése és elemzése, értékelése nélkülözhetetlen lesz a kriminalisztikában. Fontos, hogy a bűnüldöző szervek az így keletkezett digitális adatokat (nyomokat) megismerjék. Azonban a megismerés önmagában nem elegendő, mivel kriminalisztikai ajánlásokat is meg kell fogalmazni, amelyek segítségével lehetővé válhat, hogy nyomozási cselekményeket tudjunk foganatosítani, és megismerjük a múltbeli, a jelenben zajló vagy akár a jövőben tervezett cselekményeket.

Az arckép-azonosítás hozzájárul az automatikus határátlépési pont kialakításához is, amely a határforgalom gyorsítását és egyszerűsítését fogja elősegíteni, az ott szolgálatot teljesítő állomány tevékeny közreműködése nélkül.[57] A biometrikus azonosítás a mesterséges intelligenciával párosulva számos lehetőséget fog megnyitni, amelyeket nemcsak az állampolgároknak kell kihasználniuk az e-közigazgatási ügyintézési folyamatoknál, hanem a hatóságnak is a felderítés és a bizonyítás során.

1.5. Az e-nyomozási ökoszisztéma megvalósítása

A kriminalisztikai gondolkodás jelen van a nyomozás folyamatában, a nyomozás tervezésekor és szervezésekor, amely során a múltbeli eseményt gondolatban kell rekonstruálniuk a bűnüldöző szerveknek, fel kell tárni az oksági összefüggéseket, valamint meg kell állapítani az anyagi vagy alaki igazságot. Ezekben segítségül lehet a nemzeti adatvagyon mesterséges intelligenciával történő újrahasznosítása. A nemzeti adatvagyon megismerése választ adhat valamely kriminalisztikai alapkérdésre. A bűnüldözés szempontjából a nemzeti adatvagyon, az interoperabilitási e-nyomozás, valamint a mesterséges intelligencia kapcsolatát szemlélteti az *E-nyomozási ökoszisztéma* című 15. számú ábra.

[57] A mesterséges intelligencia területén megvalósult fejlesztések, a Belügyminisztérium tájékoztatása. Lásd részletesebben: Hajzer 2021.

15. ábra: E-nyomozási ökoszisztéma
Forrás: a szerző szerkesztése

Az e-nyomozás azt jelenti, hogy a nyomozó hatóság a közvetlenül vagy a közvetetten elérhető adatbázisokból kér információt a felderítés és a bizonyítás, valamint a bűncselekményből származó vagyon felkutatása érdekében, eközben taktikai ajánlásokat alkalmaz a nyomozás sikeressége *ügyében*.[58]

Egy uniós rendészeti (e-bűnügyi) ökoszisztéma kialakítására van szükség, amely segíti az e-nyomozási folyamatokat, így csökkenthető a nyomozó hatóság reakcióideje. Ezáltal idő és pénz is megtakarítható, valamint az eljárások gyorsabban lefolytathatók, mindez gyorsítja a felderítő munkát.[59]

Az e-nyomozás során beszerzett adatok a hálózatkutatási elemzések alapját is szolgálhatják, az így megállapított eredmények a bűnügyi digitális ökoszisztéma kialakításához is hozzájárulhatnak.

[58] Nyitrai 2020a.
[59] Nyitrai 2022: 75.

2. A kriminalisztikai nyilvántartások

Napjainkban az eredményes bűnüldözés nem képzelhető el a különféle nyilvántartások és adatbázisok használata nélkül, amelyek a digitalizációnak köszönhetően egyre szélesebb körben válnak hozzáférhetővé a bűnüldöző szervek számára, s amelyek hozzájárulnak a nyomozás felgyorsításához is. Egyes nyilvántartások, például a bűnügyi nyilvántartások adataihoz vagy a Netzsaru rendszer elektronikus adatbázisához jogosultsági szinttől függően a bűnüldöző szervek munkatársai közvetlenül hozzáférhetnek. A nyilvántartás fogalmára többféle definíció található. Kárpáti Orsolya szerint

> „a nyilvántartás adott feladat ellátásának biztosításához, előre meghatározott célból és szempontok szerint összegyűjtött és rögzített, tehát rendszerezetten nyilvántartott adatok összessége, mely áttekintést biztosít a nyilvántartott objektum(ok) fölött, elősegítve a pontos, gyors és valósághű adatokra alapozott döntéshozatalt".[60]

Napjainkban a „nyilvántartás" és az „adatbázis" fogalmát szinonimákként használják.

2.1. A bűnügyi nyilvántartási rendszer egységei, részei

Az állam működése szempontjából az alap- és szaknyilvántartások rendkívül fontosak amelyeknek az elektronizálása megtörtént (például elektronikus anyakönyv, személyiadat- és lakcímnyilvántartás, bűnügyi nyilvántartás, ingatlan-nyilvántartás).[61] A hatósági nyilvántartásokkal szembeni alapkövetelmény, hogy a bennük tárolt adatok hitelesek és naprakészek legyenek. Ezek a legmodernebb informatikai alkalmazások, amelyek könnyítik a hivatalos ügyintézést, meg kell felelniük az adatvédelmi és a biztonsági követelményeknek.[62] A nyilvántartások használata a nyomozás során elősegíti verziók felállítását, a nyomozati terv elkészítését, a felkészülést a kihallgatásra (az ügyből és a személyből),

[60] Kárpáti 2018: 8.
[61] Kárpáti 2018: 14.
[62] Samu Nagy 2020: 1.

bűnelemzésre, stb. Széles skálán mozognak az adattárak nyújtotta lehetőségek. Napjainkban a nyomozásokat nyilvántartásokban történő szűrő-kutató munka nélkül már el sem tudnánk képzelni. A nyilvántartások használata (az azokban való lekérdezés) természetesen szakértelmet követel.[63]

A bűnügyi nyilvántartások a bennük szereplő adatok tekintetében közhitelű hatósági nyilvántartások, így a bejegyzett adatok, tények fennállását, a törölt adatok fenn nem állását – ellenkező bizonyításig – vélelmezni kell.[64] A bűnügyi nyilvántartások törvényességi felügyeletét a legfőbb ügyész látja el.[65]

A bűnügyi nyilvántartási rendszert adattartalma szerint két fő részre lehet osztani: a személyazonosító adatok és fényképek nyilvántartására, illetve a bűnügyi nyilvántartásokra. A bűnügyi nyilvántartási rendszer több nyilvántartásra tagozódik: a bűntettesek nyilvántartására; a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartására; a büntetőeljárás hatálya alatt állók nyilvántartására; valamint a külföldre utazási korlátozás hatálya alatt állók nyilvántartására.

2.1.1. A személyazonosító adatok és fényképek nyilvántartása

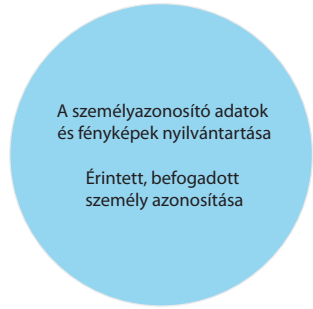
A személyazonosító adatok és fényképek nyilvántartásában szereplő adatok kezelésének célja a bűnügyi nyilvántartásokban, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásában szereplő adatok tekintetében az érintett, valamint a büntetés-végrehajtási intézetbe és a rendőrségi fogdába befogadás során a befogadott személyek azonosítása (16. ábra).[66]

[63] Finszter 2006: 58.

[64] 2009. évi XLVII. törvény indokolása a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról 1. §.

[65] 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról 1. §.

[66] 2009. évi XLVII. törvény 4. § (1).



16. ábra: Az azonosítás
Forrás: a szerző szerkesztése

A személyazonosító adatok és fényképek nyilvántartásában az érintett arcképmását nyilván kell tartani, ha bűncselekmény megalapozott gyanúja miatt büntetőeljárás alá vonták, vagy a bíróság vele szemben bűnösséget megállapító jogerős ügydöntő határozatot hozott.[67] Továbbá az elítéltet befogadó büntetés-végrehajtási intézet a bűncselekmény miatt jogerősen végrehajtandó szabadságvesztés büntetésre ítélt személy arcképmását az érintett befogadását követően megküldi a bűnügyi nyilvántartó szervnek.

2.1.2. A bűnügyi nyilvántartások

A bűnügyi nyilvántartások 4 fő nyilvántartásra tagozódnak:

a) a bűntettesek nyilvántartása;
b) a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartása;
c) Büntetőeljárás hatálya alatt állók nyilvántartása;
d) a külföldre utazási korlátozás hatálya alatt állók nyilvántartása.

Ezeket a 17. ábra szemlélteti.

[67] 2009. évi XLVII. tv. 6. § (1).

17. ábra: Bűnügyi nyilvántartások
Forrás: a szerző szerkesztése

2.1.2.1. A bűntettesek nyilvántartása

A bűntettesek nyilvántartási rendszerébe való bejegyzés nem tekinthető konstitutív hatályúnak, mivel a büntetőjogi felelősségre, a kiszabott büntetésre vagy alkalmazott intézkedésre vonatkozó tényeket nem a nyilvántartásba való bejegyzés (vagy törlés) keletkezteti, hanem a bíróság jogerős határozata.[68] A bűntettesek nyilvántartásának célja a büntetett előélet tényének igazolása, valamint a bűnösséget megállapító ítéletben foglalt büntetés és intézkedés végrehajtásának elősegítése. A büntetett előélet tényének igazolása történhet bűnmegelőzési, bűnüldözési, igazságszolgáltatási és nemzetbiztonsági érdekek védelme; az érintett jogai gyakorlásának elősegítése, valamint mások jogainak és biztonságának védelme érdekében. A bűntettesek nyilvántartásában annak a személynek az adatait kell nyilvántartani, akivel szemben a bíróság bűnösséget megállapító jogerős ügydöntő határozatot hozott, és aki annak jogerőre emelkedése napján az 1978. évi IV. törvény vagy a Btk. alapján nem mentesült.[69]

[68] BH2018. 303.
[69] 2009. évi XLVII. tv. 10. §.

2.1.2.2. A hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartása

A hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyekre vonatkozó adatok nyilvántartásának célja egyrészt a büntetőügyben eljáró bíróság ügydöntő határozatában foglalt büntetés és intézkedés végrehajtásának elősegítése, másrészt a hátrányos jogkövetkezmények végrehajtásának biztosítása. A hátrányos jogkövetkezmények végrehajtásának biztosítása történhet a bűnmegelőzési, bűnüldözési, igazságszolgáltatási és nemzetbiztonsági érdekek védelme; az érintett jogai gyakorlásának elősegítése, valamint mások jogainak és biztonságának védelme érdekében. A nyilvántartásban annak a személynek az adatait kell rögzíteni,

„*a)* akinek az adatait a bűntettesek nyilvántartásából a mentesítés folytán törölték;

b) akivel szemben a bíróság bűnösséget megállapító jogerős ügydöntő határozatot hozott, és annak jogerőre emelkedésének napján mentesült;

c) akivel szemben a bíróság bűnösséget megállapító jogerős ügydöntő határozatot hozott, de büntetés kiszabását mellőzte;

d) akivel szemben a bíróság megrovás, próbára bocsátás, jóvátételi munka vagy kényszergyógykezelés intézkedést, illetve akivel szemben a bíróság terheltként elkobzás, vagyonelkobzás vagy elektronikus adat végleges hozzáférhetetlenné tétele intézkedést alkalmazott, valamint

e) akivel szemben az ügyészség megrovást alkalmazott.”[70]

2.1.2.3. A büntetőeljárás hatálya alatt állók nyilvántartása

A büntetőeljárás hatálya alatt állók nyilvántartásában annak adatait kell nyilvántartani, akivel a büntetőeljárásban megalapozott gyanút közöltek. A nyilvántartásban szereplő adatok kezelésének a célja kettős:

– a büntetőeljárások gyors és hatékony lefolytatásának elősegítése, törvényességének biztosítása;
– az érintett és mások jogainak, biztonságának védelme.[71]

[70] 2009. évi XLVII. tv. 14, 15. §.
[71] 2009. évi XLVII. tv. 21–22. §.

A büntetőeljárás hatálya alatt állók nyilvántartásában a büntetőeljárást folytató hatóságok ellenőrizhetik, hogy az általuk büntetőeljárás alá vont személy ellen más hatóság folytat-e büntetőeljárást. Megnyílik a lehetőség arra, hogy az ügyeket egyesítsék, egyben elősegítve a sorozat-bűncselekmények felderítését és a párhuzamos büntetőeljárások kiszűrését.

2.1.2.4. A külföldre utazási korlátozás hatálya alatt állók nyilvántartása

A külföldre utazási korlátozás hatálya alatt állók nyilvántartásában szereplő adatok kezelésének célja, hogy elősegítse a külföldre utazási korlátozás érvényesülését, és megelőzze a külföldre utazási korlátozás ellenére történő külföldre utazást.

A külföldre utazási korlátozás hatálya alatt állók nyilvántartásában annak a személynek az adatait kell nyilvántartani:

„*a)* aki letartóztatásban, kiadatási letartóztatásban, ideiglenes kiadatási letartóztatásban, átadási letartóztatásban, ideiglenes átadási letartóztatásban, ideiglenes végrehajtási letartóztatásban van, valamint aki előzetes kényszergyógykezelés alatt áll;

b) akivel szemben kiadatási bűnügyi felügyeletet, ideiglenes kiadatási bűnügyi felügyeletet vagy ideiglenes átadási bűnügyi felügyeletet rendeltek el, illetve olyan bűnügyi felügyeletet vagy ideiglenes végrehajtási bűnügyi felügyeletet rendeltek el, amelynek során a bíróság a terhelt számára előírta, hogy meghatározott területet, lakást, egyéb helyiséget, intézményt vagy ahhoz tartozó bekerített helyet engedély nélkül nem hagyhat el;

c) akit végrehajtandó szabadságvesztésre ítéltek, illetve akinek felfüggesztett vagy részben felfüggesztett szabadságvesztése végrehajtását utóbb elrendelték;

d) akivel szemben a bíróság felmentő ítélet mellett kényszergyógykezelést alkalmazott;

e) akinek a bíróság a javítóintézeti nevelését rendelte el, illetve akit javítóintézetből ideiglenesen elbocsátottak, valamint

f) akinek az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló törvény alapján megtiltották Magyarország területének elhagyását, és úti okmányának átadására kötelezték."[72]

2.2. Az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartása

Az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásában rögzített adatok kezelésének célja a tagállami ítéletekben foglalt adatoknak:

„*a)* a tagállamok közötti – az Európai Unió tagállamaival folytatott bűnügyi együttműködés keretében folytatott – kölcsönös cseréjének elősegítése;

b) az elítélttel szemben más bűncselekmény megalapozott gyanúja miatt folytatott büntetőeljárásban való figyelembevétele, illetve

c) a büntetett előélet igazolásának, illetve a hátrányos jogkövetkezmények végrehajtásának az elősegítése."[73]

Annak a magyar állampolgárnak az adatait kell nyilvántartani az adatbázisban, akinek bűnösségét az Európai Unió más tagállamának bírósága jogerősen megállapította.[74]

A bűnügyi nyilvántartó szervnek a tagállami ítéletek nyilvántartásába vételekor, módosításakor vagy javításakor automatikusan össze kell hasonlítania a bejegyzendő tagállami ítélettel kapcsolatos adatokat a bűnügyi nyilvántartási rendszerben (a bűntettesek, illetve a hátrányos jogkövetkezmények hatálya alatt álló, büntetlen előéletű személyek nyilvántartásában) kezelt adatokkal. Az összehasonlítás alapján kiderülhet a magyar hatóságok számára, hogy olyan külföldi bírósági döntés született, amely hatással lehet valamely magyar bíróság által kiszabott büntetőjogi szankció folyamatban lévő végrehajtására. A bűnügyi nyilvántartó szerv ellenőrzést végez, találat esetén az ügyészség útján kezdeményezheti a megfeleltetési eljárás lefolytatását.[75]

[72] 2009. évi XLVII. tv. 30/A–30/B. §.
[73] 2009. évi XLVII. tv. 31. §
[74] 2009. évi XLVII. tv. 31–32. §
[75] 2009. évi XLVII. törvény indokolása 33/B. §.

2.3. A bűnügyi és rendészeti biometrikus adatok nyilvántartása

A daktiloszkópiai, valamint DNS-profil-nyilvántartások összefoglaló neve a bűnügyi és rendészeti biometrikus adatok nyilvántartása. Ezeket szakértői nyilvántartásokként is szokták emlegetni, mivel különleges szakértelmet igénylő feladatok elvégzését követően az érintettek személyazonosságának pontos megállapítását szolgálják.[76]

A biometrikus adatok nyilvántartásának két alapnyilvántartása a daktiloszkópiai nyilvántartás, valamint a DNS-profil-nyilvántartás.

2.3.1. A daktiloszkópiai nyilvántartás

A daktiloszkópiai nyilvántartás három részre tagozódik:

- a bűncselekmény helyszínén és a bűncselekmény elkövetésének nyomait hordozó tárgyon rögzített ujj- és tenyérnyomatok nyilvántartására;
- a büntetőeljárás alá vont személyek ujj- és tenyérnyomatainak nyilvántartására;
- a bűncselekmény elkövetése miatt jogerősen elítélt személyek ujj- és tenyérnyomatainak nyilvántartására.

A daktiloszkópiai nyilvántartást az alábbi célok elérése érdekében hozták létre:

- a bűncselekmény helyszínén és a bűncselekmény elkövetésének nyomait hordozó tárgyon rögzített ujj- és tenyérnyomat alapján a bűncselekmény elkövetésével összefüggésbe nem hozható;
- a bűncselekményt elkövető;
- a rendkívüli haláleset miatt folyó közigazgatási hatósági eljárásban az ismeretlen személyazonosságú elhunyt;
- a büntetés-végrehajtási intézetbe, valamint a rendőrségi fogdába befogadás során a befogadott;
- a személyazonosság igazolásának megtagadása esetén az igazoltatott, valamint
- a külföldi bíróság által elítélt személy azonosítása.[77]

[76] 2009. évi XLVII. törvény indokolása 1. §.

[77] 2009. évi XLVII. tv. 37. §. Azonban figyelembe kell venni, hogy a büntetőeljárás alá vont személynek az ujj- és tenyérnyomatát és a DNS-profilját a 2009. évi XLVII. tv. 44. § (1) bekezdése és az 59. §-a alapján lehet nyilvántartani.

Azonban figyelembe kell venni, hogy a nyilvántartásban rögzített nyomok többségében még nem állapították meg, hogy az kihez tartozik. Nem lehet tudni, hogy az elkövetőt azonosítják-e vagy olyan személyt, akinek nincs köze a bűncselekményhez, csak a kérdéses helyszínen járt és rögzítették az ujj- és tenyérnyomatát. A büntetőeljárás alá vont személyek ujj- és tenyérnyomatainak nyilvántartásában, valamint a bűncselekmény elkövetése miatt jogerősen elítélt személyek ujj- és tenyérnyomatainak nyilvántartásában ezzel szemben már ismert, azonosítható, büntetőeljárás alá vont vagy elítélt személyek ujj- és tenyérnyomatait kell rögzíteni.[78]

2.3.2. A DNS-profil-nyilvántartás

A DNS-profil-nyilvántartás további három-három részre tagozódik aszerint, hogy a felvett biometrikus adatot a bűncselekmény helyszínén és a bűncselekmény elkövetésének nyomait hordozó tárgyon rögzítették, olyan személytől vették le, akivel szemben meghatározott bűncselekmények miatt büntetőeljárás indult, vagy akit meghatározott bűncselekmény elkövetése miatt jogerősen elítéltek. A DNS-profil-nyilvántartás céljai szintén három csoportba bonthatók, úgymint a bűncselekmény helyszínén és a bűncselekmény elkövetésének nyomait hordozó tárgyon rögzített anyagmaradvány alapján a bűncselekmény elkövetésével összefüggésbe nem hozható; a bűncselekményt elkövető, valamint a rendkívüli haláleset miatt folyó közigazgatási hatósági eljárásban az ismeretlen személyazonosságú elhunyt személy azonosítása.[79]

2.4. A vétlen nyomszennyezés kizárására szolgáló nyilvántartás (eliminációs nyilvántartás)

A nyomozás – kiemelten a szemle – során fennállhat a kontamináció, a vétlen nyomszennyezés kockázata, amely miatt az igazságügyi szakértői vizsgálat a személyi állomány eljáró tagjának mintáját idegen mintaként fogja azonosítani, ami téves eredményt fog adni. Ezt meg kell előzni, ezért létrehozták az úgynevezett eliminációs nyilvántartást, így a biometrikus mintával a vétlen szennyeződés

[78] 2009. évi XLVII. törvény indokolása 38. §.
[79] 2009. évi XLVII. tv. 52. §.

kiszűrhető, és az elkövető azonosítása elősegíthető. Az eliminációs nyilvántartásnak az a célja, hogy a büntetőeljárás során rögzített ujj- és tenyérnyomat, illetve DNS-profil meghatározására alkalmas minta vétlen szennyeződését kiszűrje, és ennek egyszerűsítésével elősegítse az elkövető azonosítását.

Az eliminációs nyilvántartás azon személyek biometrikus adatainak nyilvántartására ad lehetőséget, akik a foglalkozásuk vagy hivatásuk okán hordozzák a nyomszennyezés kockázatát.

Azonban figyelembe kell venni, hogy ha az érintett személy tiltakozik az ellen, hogy a személyes adatait nyilvántartásban rögzítsék, úgy a személyes adatai nem továbbíthatók az eliminációs nyilvántartás részére, illetve a már nyilvántartásba vett személyes adatai nem kezelhetők az eliminációs nyilvántartásban.[80]

2.5. Az Elektronikus Modus Operandi Nyilvántartás (eModus)

A *modus operandi* kifejezés esetén a *modus* módszert, az *operae* pedig munkát, tevékenységet jelent, pontosabban kriminalisztikai értelemben az elkövetés módszeréről (módjáról) beszélhetünk.[81]

Az eModus a modus tárgyú bűncselekmény (például emberölés, emberrablás, emberkereskedelem, erőszakos közösülés, visszaélés kábítószerrel) vonatkozásában tartalmazza

- a felderítetlenül maradt bűncselekmény kriminalisztikai szempontból fontos jellemzőit;
- az Rtv. 91/A. § (1) bekezdés *c)* pontjában meghatározott adatok közül a szándékos bűncselekmény elkövetésének megalapozott gyanúja miatt kihallgatott személy adatait, személyleírását, fényképét;
- az Rtv. 91/A. § (1) bekezdés *e)* és *g)* pontjában meghatározott adatokat;
- az ügyszámot, a tényállás megnevezését, elévülési idejét, az adatállományba kerülésének idejét és az ügyben eljáró szervet.[82]

[80] 2009. évi XLVII. tv. 66/A §.

[81] Juhász 2022: 60.

[82] 12/2021. (IV. 30.) ORFK utasítás az elektronikus Modus Operandi Nyilvántartás működtetésével kapcsolatos feladatokról.

Az eModus a szándékos bűncselekmény elkövetésének megalapozott gyanúja miatt kihallgatott, tetoválással rendelkező személy tekintetében tartalmazza a személyleírási és fényképadatok közül a tetoválás képét és leírását.

A rendőrség munkáját segítik szintén a sorozat-bűncselekmények felderítése szempontjából az adatbázisokra épülő programok, úgymint a NOVA Kajtár sorozatkereső alkalmazás. A program a Modus Operandi kódszótáraira építkezve a bűncselekmények elkövetésének legfőbb kriminalisztikai jellemzőit elemzi. A programot a sorozat-bűncselekmények felismerése, a sorozat tagjainak megtalálása érdekében a rendőrségen belül fejlesztették ki.[83]

Az eModus rendszerét kutatási potenciálnak tekintik, mivel elemezni lehetne a bűnözői karrierek mintázatait, valamint vizsgálni lehetne, hogy a nemzetközi kutatásokban felfedezhető trendek mennyire jelennek meg a magyar bűnelkövetőknél.[84]

2.6. A körözési nyilvántartási rendszer

A körözés normatív definíciója a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról szóló 2013. évi LXXXVIII. törvény (a továbbiakban: Körtv.) 1. § *d)* pontja alapján:

> „körözés: személy esetén törvényben, holttest és dolog esetén jogszabályban meghatározottak szerinti döntés, a Schengeni Információs Rendszerben rejtett ellenőrzésre irányuló figyelmeztető jelzés elhelyezése, valamint az elfogatóparancs, az európai elfogatóparancs és a nemzetközi körözés."

A körözési nyilvántartási rendszer közhiteles, hatósági nyilvántartás, amely öt nyilvántartásból épül fel:

- a körözött személyek nyilvántartása;
- a körözött dolgok nyilvántartása;
- az ismeretlen holttestek, holttestrészek nyilvántartása;
- a talált tárgyak nyilvántartása;
- a nyilvántartás használatára jogosultak nyilvántartása.[85]

[83] Ipsits–Oszlánszki 2020: 716.
[84] Baráth 2022: 28.
[85] Körtv. 2. § (2).

A körözött személyek nyilvántartásában kiemelkedő helyet foglalnak el az eltűnt személyek, ezért fontosnak tartom azoknak a kérdéseknek a tárgyalást, amelyeket egy eltűnés alkalmával szükséges feltenni. Az eltűnés bejelentéséről jegyzőkönyvet kell felvenni, a bejelentő személyt részletesen meg kell hallgatni, s a beszélgetés során az alábbi kérdésekre ajánlott kitérni:

- a bejelentő személyes adatainak rögzítésekor célszerű az összes kommunikációs elérhetőséget dokumentálni (például mobiltelefonszámait, vezetékes számait, e-mail-címét), tisztázni, hogy magával vitte-e mobiltelefonját;
- tisztázni kell, hogy a bejelentő milyen kapcsolatban van az eltűnt személylyel (például az eltűnthöz fűződő személyes viszonya, rokoni fokozata, egyéb kapcsolatainak tisztázása);
- az eltűnt személyes adatainak rögzítése (családi neve és utóneve; születési családi és utóneve, továbbá annak megváltozása esetén korábbi születési családi és utóneve; neme; születési helye és ideje; anyja születési családi és utóneve, továbbá annak megváltozása esetén korábbi születési családi és utóneve; okmányai; állampolgársága vagy hontalansága; lakcímadata, továbbá annak megváltozása esetén korábbi lakcímadata; értesítési címe);
- az eltűnt álneve, gúnyneve, foglalkozása, munkahelye, nyelvismerete;
- személyleírása (figyelembe véve az ALFONZ Személyleírási Rendszer alkalmazását);
- különös ismertetőjegyei: az eltűntön van-e valamilyen műtéti heg, jellegzetes sérülés, amennyiben igen, akkor melyik testrészen, van-e egyéb testi fogyatékossága;
- ruházatának, a nála lévő tárgyaknak a megnevezése, leírása (ajánlott a ruházat anyagának, színének, márkájának, méretének megnevezése);
- vitt-e magával készpénzt (ha igen, milyen összegben) vagy bankkártyát, gyógyszert (tisztázni kell, hogy milyen gyógyszert és miért vitt magával);
- az eltűnés körülményeinek részletezése (például mikor észlelték az eltűnést, mikor, hol, ki és milyen körülmények között látta utoljára, az eltűnés feltételezett vagy tényleges időpontja, az eltűnést megelőző hangulata, a bejelentő hogyan szerzett tudomást az eltűnésről);
- lehetséges tartózkodási helye(i);
- korábban említette-e úti célját, távozásának okát;
- hova és mikor kellett volna megérkeznie az eltűntnek;
- honnan tűnt el (lakásból, iskolából, munkahelyről stb.);

– az eltűnt személy életvitele;
– az eltűntnek volt-e korábban öngyilkossági kísérlete, van-e öngyilkos hajlama (korábban mikor, honnan tűnt el, mi volt az oka, hol találták meg, megtalálás körülményei);
– hagyott-e hátra búcsúlevelet;
– tett-e öngyilkosságra utaló kijelentést (milyen volt az érzelmi állapota, hangulata);
– az eltűnt tagja-e valamelyik közösségi oldalnak;
– az eltűntnek kik a barátai (nevek, címek, elérhetőségek, telefonszámok);
– az eltűntnek mi a hobbija, szabadidejét hol tölti (például milyen szórakozóhelyeket látogat);
– szokott-e utazni belföldön vagy külföldön (mikor utazott, kikkel, hová, új barátokat szerzett-e az utazás alatt);
– az eltűntnek kik a rokonai, szokott-e hozzájuk járni (nevek, címek, elérhetőségek, telefonszámok);
– az eltűnt személy kapcsolatainak (a barátok, a munkatársak, az iskolatársak, a haragosok) feltérképezése;
– az eltűnt hová jár iskolába (hányadik osztályos);
– az eltűntnek mi a munkahelye (cím, munkatársak és vezetők neve, elérhetőségei);
– az eltűnt áll-e gyámság, gondnokság alatt, az eltűnt tud-e gondoskodni magáról;
– egészségügyi adatok tisztázása: az eltűnt áll-e rendszeres orvosi kezelés alatt (ha igen, hol és ki a kezelőorvosa, háziorvosa; az eltűnt szed-e rendszeresen gyógyszereket, ha igen, akkor mit és milyen betegségre);
– beszélt-e a bejelentő a szomszédokkal, rokonokkal (valaki rendelkezik-e valamilyen információval);
– a bejelentő vagy valaki más kereste-e az eltűntet (ha igen, hol);
– az eltűnés óta valaki látta-e az eltűnt személyt (hol és mikor);
– az eltűntnek van-e anyagi problémája, tartozása (banki hitel, egyéb tartozás);
– az eltűntnek van-e elszámolási vitája valakivel, ebből kifolyólag kapott-e fenyegetéseket;
– milyen az eltűnt személy természete (könnyen vagy nehezen teremt kapcsolatot idegenekkel, zárkózott stb.);
– milyen szenvedélye van (például alkohol, drog, szerencsejáték, internet);
– milyen helyeket kedvel (például parkok, erdők, szórakozóhelyek);

– a bejelentő szerint mi lehet az eltűnés oka;
– tervezett-e külföldi munkát, kikkel és hol vehette fel a kapcsolatot az eltűnt, milyen munkára jelentkezett;
– merre távozhatott (az útvonalon a kamerafelvételek beszerzése);
– milyen elektronikai eszközökkel rendelkezik, amelyeket nem vitt magával (például laptop, telefon, egyéb adathordozó, amelyből információt nyerhetünk az eltűnés okáról, körülményeiről);
– az eltűntről friss fényképpel rendelkezik-e a bejelentő vagy a meghallgatott személy;
– az eltűnt rendelkezik-e gépjárművel (mi a forgalmi rendszáma), gépjárművel távozott-e, mennyi üzemanyag volt benne;
– rendelkezik-e fegyverrel.[86]

Minden bűnügy egyedi, így minden eltűnés is egyedinek tekinthető, ezért a meghallgatást végzőnek kell eldöntenie, hogy a fenti kérdések közül melyik releváns.

Fontosnak tartom eltűnés rögzítése során a lehető legpontosabban, legrészletesebben felvenni a jegyzőkönyvet, mivel lehet olyan eset, főleg a gyanús eltűnés esetén, amikor az elkövető eltűnéssel igyekszik leplezni cselekményét, vagy az emberölést öngyilkosságnak állítja be. Egy részletes bejelentésből és elsődleges adatgyűjtésből következtetni lehet arra, hogy gyanús eltűnéssel állunk szemben.[87]

2.7. A körözési eljáráshoz kapcsolódó biometrikus adatok nyilvántartása

A körözési eljáráshoz kapcsolódó biometrikus adatok nyilvántartása két részre oszlik: a körözési célú daktiloszkópiai nyilvántartásra és a körözési célú DNS-profil-nyilvántartásra.

A körözési célú daktiloszkópiai nyilvántartás célja egyrészt az eltűnés miatt körözött személy felkutatásának, holléte, illetve személyazonossága

[86] Nyitrai 2020c: 463–465.

[87] Kriminalisztikai értelemben megkülönböztetjük a gyanús eltűnést, amely „esetében jogos az a feltételezés, hogy az illető nem önszántából tűnt el, vagy komoly érdeke fűződik ahhoz, hogy a hatóságok, illetve egyes személyek eltűntnek tartsák. Például bűncselekmény áldozatává vált, félelmében rejtőzködik, a felelősség alól így akar kibújni; a környezete azért nem várja vissza, mert nagyon is jól tudják, hogy hol van stb. – vö. a fenti felsorolás a) és c) pontjával.” Lakatos 2005: 152.

megállapításának elősegítése, másrészt az ismeretlen személyazonosságú holttest vagy holttestrész azonosítása. További két nyilvántartásra tagozódik: az eltűnés miatt körözött személyek ujj- és tenyérnyomatának nyilvántartására, illetve az ismeretlen holttestek vagy holttestrészek ujj- és tenyérnyomatainak nyilvántartására.[88]

A körözési célú DNS-profil-nyilvántartás feladata kettős: az eltűnés miatt körözött személy felkutatásának, holléte, illetve személyazonossága megállapításának elősegítése, valamint az ismeretlen személyazonosságú holttest vagy holttestrész azonosítása. Három nyilvántartást foglal magába:

- az eltűnés miatt körözött személyek DNS-profiljainak nyilvántartását;
- az eltűnés miatt körözött személyek vér szerinti hozzátartozói DNS-profiljainak nyilvántartását;
- az ismeretlen holttestek vagy holttestrészek DNS-profiljainak nyilvántartását.[89]

2.8. A Robotzsaru rendszer

A Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer (a továbbiakban: Robotzsaru rendszer), amely a rendőrség alap informatikai rendszere, informatikai alkalmazások együttesének tekinthető. A rendőri szervek a feladatellátásuk során keletkező, illetve beszerzett valamennyi nyílt adatot, iratot, bűnjelet a Robotzsaru rendszerben kötelesek rögzíteni, amennyiben azok rögzítése technikailag lehetséges. A rendszer három részből tevődik össze:

- Dokumentumtár (elektronikus adatbázis, amely elektronikus formátumban tartalmazza a Robotzsaru rendszerben előállított, illetőleg rögzített iratokat az ügy selejtezéséig);
- Netzsaru rendszer (országos digitális, bűnügyi és rendészeti elektronikus adatbázis, amely strukturált adatbázis formájában magában foglalja a Robotzsaru NEO rendszer használata során rögzített ügyek, események releváns adatait az ügy selejtezéséig). Felületén keresztül kereső, kutató és egyedi ügyviteli tevékenységek végezhetők, azonban az adatokba való betekintés jogosultságfüggő;

[88] Körtv. 14/D–14/F §.
[89] Körtv. 14/K–14/L §.

– Robotzsaru NEO rendszer, amely a Robotzsaru-2000 integrált ügyviteli ügyfeldolgozó rendszer korszerű, továbbfejlesztett változata; olyan informatikai ügyviteli, ügyfeldolgozó és elektronikus iratkezelő alkalmazás, amely az iratkezelési szoftverekkel szemben támasztott követelményeknek megfelel, tanúsítvánnyal rendelkezik, továbbá 24 órában folyamatos üzemmódban rendelkezésre áll valamennyi rendőri szerv részére, és strukturált adatbázis formában tárolja a rendőri szervek által rögzített adatokat, iratokat.[90]

A Robotzsaru rendszer önmagában nem nyilvántartás, hanem a rendőrség alap informatikai rendszere, azonban a rendőrség köteles benne a feladata ellátása során keletkezett valamennyi iratot és adatot rögzíteni. A Robotzsaru előnye még, hogy lehetőséget biztosít más intézmények rendszerével történő együttműködésre (például körözési nyilvántartási rendszerrel, telefontársaságokkal – HAR).[91] A rendszerben óriási adatmennyiség keletkezik évről évre, mivel a büntetőeljárások/nyomozások során keletkezett iratok itt megtalálhatók. Egy bűnügy előadója (nyomozó) a rendszerben szűrő-kutató munkát tud folytatni, így személyre, bűnügyre vagy többféle objektumra (például telefonszámra, gépjárműrendszámra, elkövetés időpontjára stb.) tud keresni. Különféle keresőpaneleket találunk a rendszerben. Ha a szűrő-kutató munka oldaláról nézzük, a Robotzsaru rendszert a rögzített adatok tekintetében elektronikus adatbázisnak/nyilvántartásnak is tekinthetjük. A bűnügyekben – a büntetőeljárás irataiban – kutatás egyrészt lehetővé teszi, hogy a kihallgatás előtt felkészüljünk az ügyből és a személyből, ami elősegíti az eljárás sikeres lefolytatását, illetve a sorozat-bűncselekmények felderítésében és felismerésében is segítségül szolgálhat.

A digitális adatok választ adhatnak a kriminalisztikai alapkérdésekre, illetve a hét kriminalisztikai alapkérdés kiegészíthető a *milyen?* kérdéssel. A *milyen?* kérdés egyrészt utalhat arra, hogy milyen lehet az elkövető, milyen az elkövető személyisége, mint például a specifikus profilkészítésénél. Másrészt utalhat arra, hogy milyen elektronikus (digitális) adatok beszerzésére van szükség.

[90] 18/2011. (IX. 23.) ORFK utasítás a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól. Megjegyzendő, hogy az utasítást 2023. október 1-jével hatályon kívül helyezték, azonban a fogalmak miatt szükséges az idézése.

[91] Sütő 2016: 359.

Így a *milyen?* kérdés két fő irányra mutathat rá: az elkövető személyiségére és a beszerezni kívánt elektronikus (digitális) adatra. A *milyen?* kriminalisztikai alapkérdésre kapott válasz lehetővé teheti, hogy a hatóság újabb nyilvántartáshoz juthasson el, vagy egy újabb verziót tudjon felállítani, majd az elkövetőt intézkedés alá tudja vonni. A következő, *Az adatvagyon felhasználására vonatkozó esetfeldolgozás* című alfejezet szemlélteti a *milyen?* kérdés jelentőségét.

2.9. Az adatvagyon felhasználására vonatkozó esetfeldolgozás

A nemzeti adatvagyon körébe tartozó nyilvántartások felhasználása bűnüldözésre, pontosabban a nyomozás metodikájára és eredményességére is hatással lehet. A nyilvántartások, adattárak feltérképezése, az e-nyomozási ismeretek – digitális adatok beszerzése, nemzeti adatvagyon feltérképezése, a mesterséges intelligencia alkalmazása – hozzájárulhat a kriminalisztikai gondolkodás formálásához, ezáltal elősegítheti a kriminalisztikai alapkérdések megválaszolását és a kriminalisztikai ajánlások megfogalmazását.

Ha ismerjük a nyilvántartásokat, adatbázisokat, illetve azoknak a tartalmát, és használjuk a kriminalisztikai gondolkodás eseteit, akkor az elkövetők által hátrahagyott „digitális nyomok" információval szolgálhatnak.

Az alábbi fiktív adatokat tartalmazó eset az adatvagyon jelentőségét a kriminalisztikai gondolkodáson keresztül szemlélteti.

2.9.1. Esetfeldolgozás

A kérdéses (fiktív, nem létező adatokat tartalmazó) ügyben több szálon el lehet indulni, illetve számos verziót fel lehet állítani. Ebben a példában kizárólag a nyilvántartások (adatbázisok) oldaláról vizsgálom az ügyet. A cél, hogy szemléltessem, milyen jelentősége van a magunk után hagyott „digitális nyomoknak", a nyilvántartások közötti kapcsolatoknak, illetve annak, hogy a digitális adatok egy információlánc részeivé is válhatnak.

Példa: A Fővárosi Állat- és Növénykertből 2022. november 8-án reggel fél 10-kor egy bejelentés érkezik, hogy eltűnt egy parlagi sas, egy törpe selyemmajom, egy rákosi vipera és egy hucul fajta ló, pontosabban egy kiscsikó. Később,

10 órakor pedig, hogy egy orrszarvútetemet találtak, amelynek hiányzott a tülke, azt ismeretlen személy levágta.[92]

A rendelkezésre álló adatok alapján azt lehet tudni, hogy a gondozó november 7-én a délutáni órákban (3–4 óra körül) etette meg az állatokat, majd hazament körülbelül fél 5-kor, és november 8-án reggel 9 óra körül észlelte, hogy több állat hiányzik, és egy levágott szarvú orrszarvútetem fekszik az udvaron.

Az esti műszakban dolgozó biztonsági őr (nő) a szolgálatot 2022. november 7-én reggel fél hétkor vette fel, majd másnap, november 8-án reggel 7-kor adta le. Az állatkert az eset után többször hívta az őrt, aki telefonon nem volt elérhető, a telefon kikapcsolt állapotot jelzett.

A rendőrség 2022. november 8-án délelőtt 11 órakor megjelent az őr címén, azonban ott már több rendőr tartózkodott, mivel a biztonsági őr öngyilkos lett.

Búcsúlevelet hagyott, amelyben az állt, hogy nem bírta elviselni, feldolgozni, hogy megölték az orrszarvút, és több állatot elloptak az ő segítségével. A „Drága Kicsimnek" címzett búcsúleveléből kiderül, hogy zsarolás hatására működött együtt, de nem bírja a szégyent elviselni, és bűntudata van.

A biztonsági őr élettársa tanúkihallgatása során az alábbi információkat közölte:

> „Nem tudom, ki zsarolta meg, és azt sem, hogy ki vitte el a védett állatokat az állatkertből. Mostanában nagyon ideges volt a párom, az elmúlt napokban, többször mondta, hogy gondjai vannak, de mindig azt válaszolta, hogy megoldja, és nem akar róla beszélgetni, nem akar engem idegesíteni.
> Egyik nap valaki hívta telefonon délután, hogy itt van a ház előtt, jöjjön ki. Pár perc múlva én is kimentem, hogy miért van olyan sokáig, akkor két férfit láttam. A párom mondta, hogy menjek vissza, mert lemaradok a filmről, minden rendben van. Ez az esemény múlt héten pénteken volt délután. 2022. november 5-én fél 5 körül, jól emlékszem, mert akkor kezdődött a *Szerelem van a levegőben*. (Az említett hívás után a páromat már senki sem kereste telefonon.)
> Az egyik férfi a másikat Tifinek szólította. Amikor visszajött a párom, nagyon feszült volt, és csak annyit mondott, hogy nem akarja megcsinálni.
> A párom telefonszáma: 06-30-555-55-55
> Az utcában nincs térfigyelő kamera, de szerencsére Gera Béla bácsinak a szemközti szomszédban, a 21. számban van kamerája, de titkolja, szinte észrevehetetlen, és az ablakban van felszerelve, a parkoló kocsiját figyeli, mivel többször megrongálták."

[92] „Napjainkban a világpiacon az orrszarvúszarvúnak magasabb az értéke, mint az aranynak: a szarvakat kilogrammonként 25 000–40 000 USD áron hozzák forgalomba a feketepiacon. Az ok elsősorban az, hogy az ázsiai országokban továbbra is bíznak az egyes, állatokból készült termékek gyógyító hatásában." Idézi: Sziebig 2021: 19.

További releváns adatok:

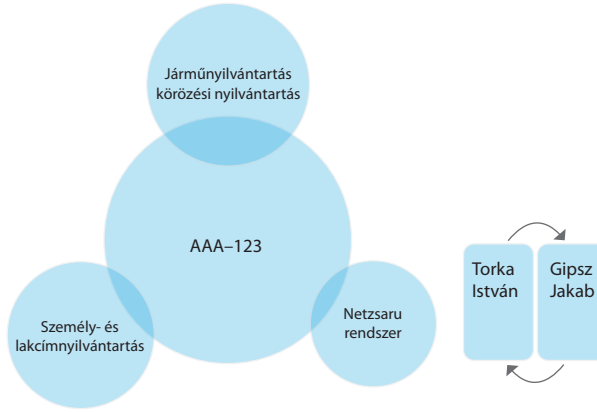
- A Gera Béla (szemközti szomszéd) által üzemeltetett kamerafelvételt lefoglalták. A kamerafelvételen 2022. november 5-én fél 5-kor egy AAA 123 rendszámú szürke Opel Insignia látható, amely a biztonsági őr háza előtt állt meg, a gépkocsi vezetőjéről jó minőségű felvétel készült, míg utasának arca nem látható.
- A Fővárosi Állat- és Növénykert kamerája egy furgont rögzített, illetve egy Opel Insignia típusú szürke gépkocsit. Azonban személygépkocsi rendszámának csak a töredéke látható: . . A 123.
- Az Opel Insignia gépkocsivezetőjéről jó minőségű felvétel készült, amelyen az is látható, hogy a gépkocsivezető az állatokat egy furgon csomagterébe pakolja. A furgonvezetőről nem készült kép, ő nem szállt ki a furgonból.

Összegzés *a releváns adatokról, amelyek ellenőrzendők a nyilvántartásokban:*

- AAA 123 rendszámú Opel Insignia;
- a 06-30-555-55-55 telefonszám;
- a Tifi gúnynév;
- a kamerafelvétel.

1. AAA 123 rendszámú Opel Insignia vonatkozásában használt nyilvántartások

- A *gépjármű-nyilvántartásban* történő lekérdezés célja, hogy megtudjuk, ki a tulajdonos és/vagy az üzembentartó. A kettő egymástól elválhat.
- Az AAA 123 Opel Insignia jármű tulajdonosa és üzembentartója: Torka István (sz.: Budapest, 1956. 01. 12., an.: Tota Anna, Alsóörs, 8226, Szabó Helena utca 32. szám). A gépkocsi hat éve van Torka István tulajdonában. A gépkocsi a *körözési nyilvántartásban* nem szerepelt.
- A *személyiadat- és lakcímnyilvántartásban* történő lekérdezés célja egy úgynevezett fordított keresés végrehajtása. Arra vagyunk kíváncsiak, hogy Alsóörs, 8226, Szabó Helena utca 32. szám alatti címre Torka Istvánon kívül ki van még bejelentve, illetve kinek a tartózkodási címe. A lekérdezés során kiderült, hogy Torka István elhalálozott, és rajta kívül senki sincs bejelentve a címre.
- A *Netzsaru rendszerben* a rendszámra keresés során kiderült (rendőri jelentés alapján), hogy Gipsz Jakab (sz.: Budapest, 1985. 12. 12., an.: Kita Margit) VIII. kerület Diószegi Sámuel utca 38–42. szám alatti lakost fokozott ellenőrzés keretében igazoltatták, és az AAA 123 Opel Insignia típusú gépkocsit vezette (18. ábra).



18. ábra: A jármű használójának azonosítása
Forrás: a szerző szerkesztése

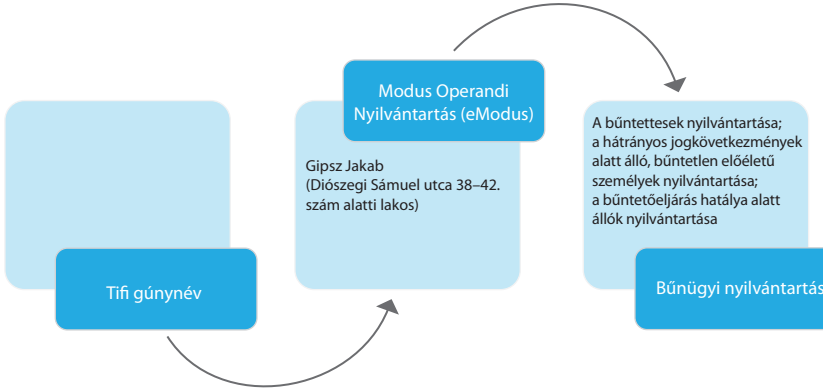
2. Telefontársaság megkeresése (nyilvántartása)

- A 06-30-555-55-55 telefonszámot 2022. november 5-én 16:20 perckor a 06-30-123-45-67-es telefonszámról hívták.
- A 06-30-123-45-67 telefonszám előfizetője: Malo Natasa (sz.: Budapest, 1986. 12. 15., an.: Erta Vilma) Budapest, 1015, Szabó János utca 15. szám alatti lakos.
- A *Google értékesítési oldalakon* szűrő-kutató munka folyt a telefonszám vonatkozásában, amely nem vezetett eredményre.
- Malo Natasa szerepel *közösségi oldalon,* élettársaként Gipsz Jakab (sz.: Budapest, 1985. 12. 12., an.: Kita Margit) VIII. kerület Diószegi Sámuel utca 38–42. szám alatti lakost tüntette fel (19. ábra).

19. ábra: A telefonszám használója
Forrás: a szerző szerkesztése

3. A Tifi gúnynév ellenőrzése

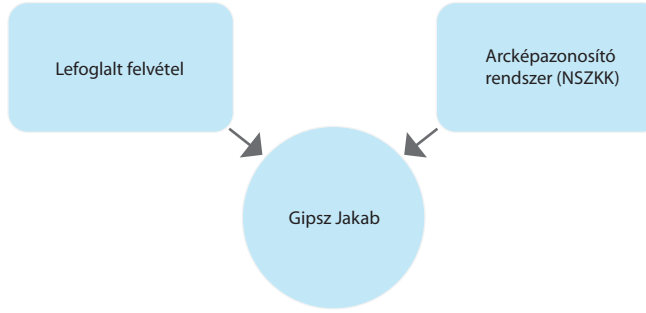
- az elektronikus *Modus Operandi Nyilvántartásban* (a továbbiakban: eModus) történt, amely kriminalisztikai jellemzőket tartalmaz, itt kezelik a személyek gúnynevét és tetoválását. Megállapították, hogy a nyilvántartásban szerepel a Tifi gúnynév Gipsz Jakab (sz.: Budapest, 1985. 12. 12., an.: Kita Margit, VIII. kerület Diószegi Sámuel utca 38–42. sz.) neve mellett, illetve kiderült, hogy természetkárosítás bűncselekménye miatt már folytattak vele szemben eljárást.
- Gipsz Jakabnak a *bűnügyi nyilvántartásban (a bűntettesek nyilvántartása; a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartása; a büntetőeljárás hatálya alatt állók nyilvántartása)* történő ellenőrzése során megállapították, hogy jelenleg is folyik vele szemben büntetőeljárás természetkárosítás bűncselekménye miatt (20. ábra).



20. ábra: Gúnynév ellenőrzése
Forrás: a szerző szerkesztése

4. A kamerafelvétel ellenőrzése

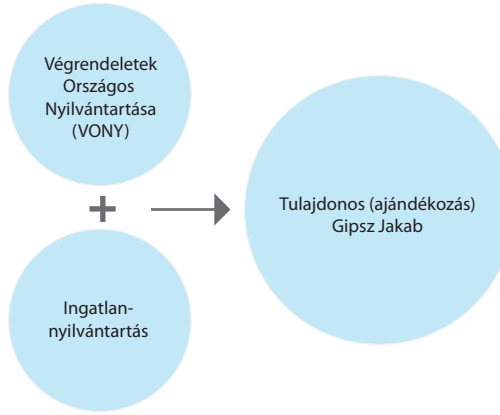
A Fővárosi Állat- és Növénykerttől és a Gera Bélától lefoglalt felvételek megküldése arcképelemzés céljából a Nemzeti Szakértői és Kutató Központ Arcképfelismerő Elemző Osztályának a felvételen látható személy személyazonosságának elősegítése érdekében. Az elemzés alapján a felvételeken szereplő személy megfelel Gipsz Jakab (sz.: Budapest, 1985. 12. 12., an.: Kita Margit) VIII. kerület Diószegi Sámuel utca 38–42. szám alatt lakosnak (21. ábra).



21. ábra: Arckép-azonosítás
Forrás: a szerző szerkesztése

A lakókörnyezetében végzett adatgyűjtés után megállapítható, hogy Torka Istvánnak nincs se családja, se gyereke. Nagyon ritkán járt hozzá egy fiatal férfi, aki mindig egy szürke Opel Insigniával érkezett, évente két-három alkalommal. A szomszédok elmondása szerint Torka bácsi egyszer azt mondta, hogy a házát erre a férfira fogja hagyni, mert sokat segített neki.

Célszerű ellenőrizni, hogy Torka István végrendelkezett-e. Ez ügyben megkereséssel lehet élni a *Végrendeletek Országos Nyilvántartása (VONY)* felé. Itt kiderült, hogy Torka István nem végrendelkezett. Továbbá az *ingatlan-nyilvántartásban* is ellenőrizhetjük, hogy Torka István ingatlanának tulajdoni lapján milyen információk vannak bejegyezve. Az ellenőrzések célja az Opel Insigniával közlekedő személy beazonosítása. A lekérdezés eredménye alapján az ingatlan tulajdonosa: Gipsz Jakab (sz.: Budapest, 1985. 12. 12., an.: Kita Margit) VIII. kerület Diószegi Sámuel utca 38–42. szám alatti lakos, jogcímként ajándékozás szerepel (22. ábra).



22. ábra: A nyilvántartások
Forrás: a szerző szerkesztése

A bizonyítási cselekmények közül elsőként a szemlét foganatosítottuk a Fővárosi Állat- és Növénykert területén. A rögzített nyomok és anyagmaradványok tekintetében azonban a *daktiloszkópiai nyilvántartás* és a *DNS-profil-nyilvántartás* nem szolgált releváns adattal.

Továbbá a nyomozás során jelentkezett egy tanú, aki végignézte az állatok elszállítását az állatkertből, és az adathordozó útján történő felismerésre bemutatás során felismerte Gipsz Jakab (sz.: Budapest, 1985. 12. 12., an.: Kita Margit) VIII. kerület Diószegi Sámuel utca 38–42. szám alatti lakost.

A rendelkezésre álló adatok alapján Gipsz Jakab – a bűncselekmény elkövetésével megalapozottan gyanúsítható személy – tényleges tartózkodási helye ismeretlen. A nyomozás során a személyi szabadságot érintő bírói engedélyes kényszerintézkedésekkel elérni kívánt célok biztosítása érdekében elfogása indokolttá vált.

A Gipsz Jakab által használt AAA 123 rendszámú gépkocsit ellenőrizték a *VÉDA Közúti Intelligens Kamerahálózat* rendszerében, azonban abban nem szerepelt.

A rendőrség titkos együttműködő személytől megtudta, hogy Gipsz Jakab az említett gépkocsival három éve közlekedik (használja), és Torka Istvántól kapta. Továbbá az együttműködő személy még annyit tudott elmondani, hogy Gipsz Jakab rendszeresen jár valahová a Balatonra vitorlázni, minden szabadidejét itt tölti, ha teheti, valamint a vitorlásnak van egy hálókabinja is. Még annyit

tudtunk meg, hogy Gipsz pár hónapja a csónakkikötő parkolóját működtető cég vezetőjével összeveszett, mert eleinte nem akartak neki kedvezményes behajtási engedélyt adni a kikötő területére, de később Gipsznek kedvezményesen meghosszabbították a behajtási engedélyét.

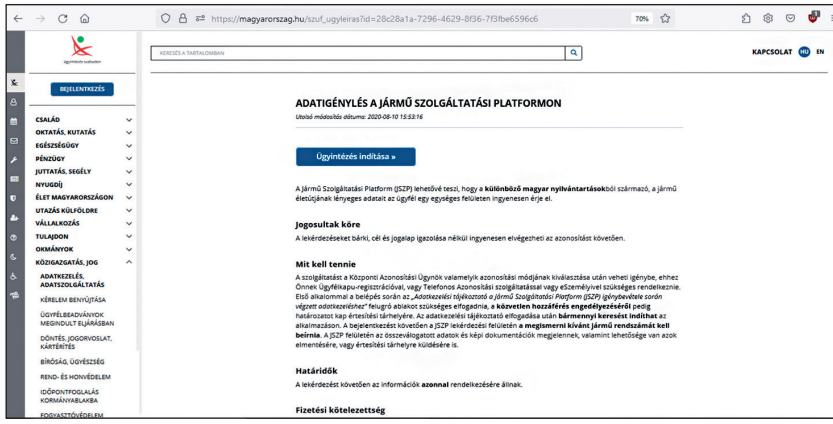
A Balatonon közel száz vitorláskikötő van, Balatonfüreden például kilenc.[93] Egy verzió keretében feltételezhető, hogy a vitorlásban bujkál, itt tartózkodik. Az információt le kell ellenőrizni. Jelen esetben még a gyanúsítható személyhez köthető egy AAA 123 rendszámú személygépkocsi. A személygépkocsiról annyit tudunk, hogy hat éve Torka István a tulajdonosa, de a kezdetektől Gipsz Jakab használja, amit a nyomozás adatai is alátámasztanak.

Itt van jelentősége ismét a kriminalisztikai gondolkodásnak, a fantáziának, illetve az adattárak, a különböző platformok ismeretének. Mivel a gépkocsi 2013-as évjáratú, így az elmúlt hat évben Torka Istvánnak mint tulajdonosnak (vagy Gipsz Jakabnak) több alkalommal kellett műszaki vizsgára vinnie. A műszaki vizsga érvényessége általában 2 év, az új kocsik kivételével. Jelen esetben egy 10 éves gépkocsit, illetve annak használóját, Gipsz Jakabot keressük. A műszaki vizsgák alkalmával fényképes dokumentáció készül a gépkocsiról kívülről és belülről egyaránt, amely árulkodó információkat tartalmazhat:

- meg kell nézni, hogy a szélvédőre milyen matricát helyeztek fel, mit raktak ki a műszerfalra (sokan ott hagyják a különböző belépési, parkolási kártyákat);
- a gépkocsiról kívülről készített felvételeken az oldalát is megnézhetjük, hátha reklámfelületként is használták;
- a gépkocsi belsejéről készült fotók is árulkodók lehetnek, mivel óhatatlanul hagyunk különböző nyílt rekeszekben, tárolókban vagy az utastérben dokumentumokat, vagy olyan tárgyakat, amelyek információval szolgálhatnak.

A fenti verziók ellenőrzésére lehetőség van a korábban tárgyalt *magyarorszag.hu* platform oldalán a „közigazgatás, jog", azon belül „adatkezelés, adatszolgáltatás" menüpont alatt, a *Jármű Szolgáltatási Platform*ban (a továbbiakban: JSZP). A JSZP lehetővé teszi, hogy a jármű életútjának a *különböző magyar nyilvántartásokból* származó lényeges adatait a nyomozó elérje (23. ábra).

[93] *Balatoni kikötők* weboldalán Vitorláskikötők menüpont.



23. ábra: Jármű Szolgáltatási Platform

Forrás: magyarorszag.hu weboldal, Adatigénylés a jármű szolgáltatási platformon ügyintézési felület

A JSZP-be az ügyfélkapun keresztül tudunk belépni. Ha beléptünk, akkor lehetőségünk nyílik az alábbi menüpontokban keresni:

- járműnyilvántartás adatai;
- származás-ellenőrzés és eredetiségvizsgálat;
- forgalomban tartás és forgalmazási korlátozás;
- műszaki állapotra vonatkozó adatok;
- futásteljesítmény adatok;
- biztosítás és kártörténet.

A JSZP-ben szereplő egyik fotón látható egy behajtási matrica, amelyre ránagyítva olvashatóvá válik a behajtási engedély egy kikötő területére (24. ábra).

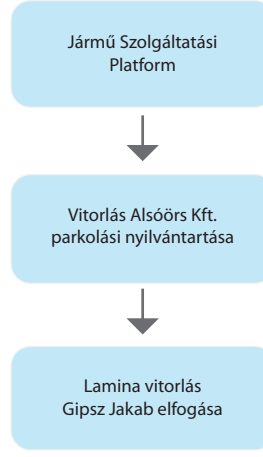
24. ábra: A szélvédőn elhelyezett behajtási engedély

Forrás: a szerző szerkesztése

A behajtási engedélyt a Vitorlás Alsóörs Kft. adta ki, és a 45. sorszám tartozik hozzá. A *cégnyilvántartásban* a Vitorlás Alsóörs Kft. székhelyét és telephelyét is lekérdezték. Innen kezdve célirányos adatgyűjtést végezhetünk annak a megállapítására, hogy a gyanúsítható személyhez tartozó gépkocsihoz adtak-e ki behajtási engedélyt.

A cég képviselőjétől a hatóság megtudta, hogy a nyilvántartásuk szerint Gipsz Jakabnak van behajtási engedélye a kikötő területére, és a Lamina elnevezésű vitorlás használója, amelynek tulajdonosa Torka István. Továbbá megtudtuk, hogy a cég képviselője feljelentést kíván tenni, mivel az utóbbi időben teljes mértékben eltűntek a környékükről a mocsári teknősök, amely faj Magyarország egyetlen őshonos teknősféléje. A cég munkatársai szerint valaki elvitte és illegálisan értékesíthette őket, mivel teknőstetemeket nem találtak.

Jelen adat tükrében a hatóság figyelést szervezett a kikötőben, és sikerült Gipsz Jakabot elfogni, intézkedés alá vonni.



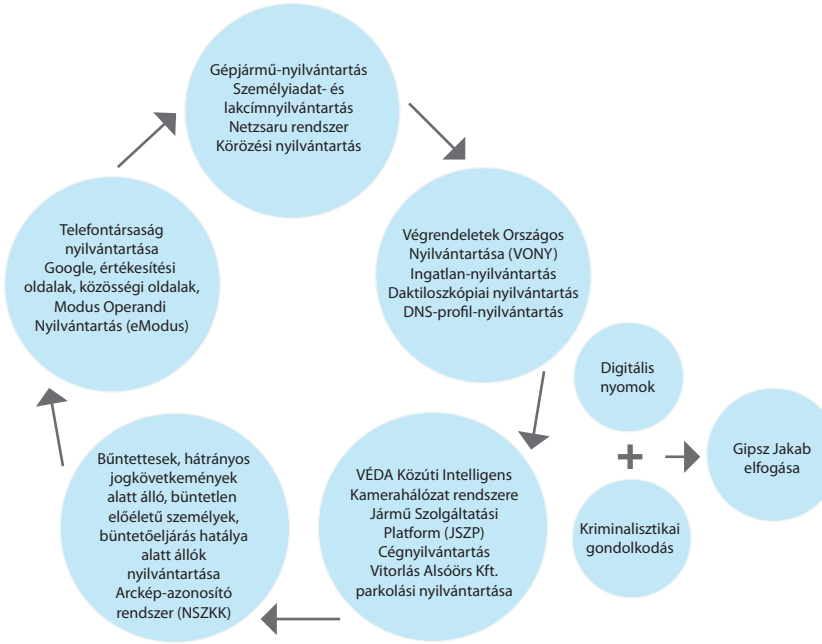
25. ábra: parkolási nyilvántartás
Forrás: a szerző szerkesztése

A JSZP lehetővé teszi, hogy a jármű életútjának a *különböző magyar nyilvántartásokból* származó lényeges adatait az ügyfél egy egységes felületen ingyenesen érje el. A lekérdezéseket az ügyfélkapus azonosítást követően bárki, cél és jogalap igazolása nélkül ingyenesen elvégezheti, ráadásul otthonról. Ha valaki gépkocsit szeretne vásárolni, az alábbiakat tudja ellenőrizni:

- a jármű forgalomban vagy körözés alatt áll-e;
- a kereskedő vagy magánszemély (természetes személy) állítását a gépkocsi előző tulajdonosainak számát illetően;
- a forgalomba helyezés dátumát, illetve azt, hogy valóban magyarországi gépkocsi, vagy külföldről hozták be;
- a biztosítási, kártörténeti eseményeket;
- valamint a műszaki vizsgán készült fotókat.

A bemutatott ügyben több közhiteles és nem hiteles nyilvántartást, keresőportált, webes felületet, azonosító rendszert alkalmaztak (26. ábra):

- Gépjármű-nyilvántartás;
- személyiadat- és lakcímnyilvántartás;
- Netzsaru rendszer;
- körözési nyilvántartás;
- telefontársaság nyilvántartása;
- Google;
- értékesítési oldalak;
- közösségi oldal;
- Modus Operandi Nyilvántartás (eModus);
- bűntettesek nyilvántartása;
- hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartása;
- büntetőeljárás hatálya alatt állók nyilvántartása;
- arckép-azonosító rendszer (NSZKK);
- Végrendeletek Országos Nyilvántartása (VONY);
- ingatlan-nyilvántartás;
- daktiloszkópiai nyilvántartás;
- DNS-profil-nyilvántartás;
- VÉDA Közúti Intelligens Kamerahálózat rendszere;
- Jármű Szolgáltatási Platform (JSZP);
- cégnyilvántartás;
- Vitorlás Alsóörs Kft. parkolási nyilvántartása.



26. ábra: Nyilvántartások használata
Forrás: a szerző szerkesztése

A nyilvántartásokban, webes felületeken, platformokon, azonosítási rendszerekben szereplő adatok az esetek többségében egymást kiegészítették, egy mozaik részét képezték, így információs láncsorozatot alakítottak ki, és az abban megállapított adatok alapján lehetett eljutni az elkövetőhöz.

A kérdéses ügyet több oldalról meg lehetett volna oldani, illetve számtalan nyomozási (bizonyítási) cselekményt kellett volna még foganatosítani, ám jelen példában kizárólag a digitális adatok, nyilvántartások és a kriminalisztikai gondolkodás létjogosultságát kívántam kiemelni és bemutatni.

3. Az adatok hálózatának jelentősége a kriminalisztikában

Digitális világunkban számos *elektronikus nyomot* vagy úgynevezett *digitális lábnyomot* hagyunk magunk után, amelyekből kapcsolati hálók hozhatók létre. A digitális lábnyom magában foglalja a felkeresett weboldalakat, az általunk küldött e-maileket, az igénybe vett online szolgáltatásokat, de azt is, amikor állami szervnél, intézetnél ügyeinket intézzük, és ezekhez megadjuk az adatainkat. A digitális lábnyomok két fajtáját különböztetjük meg: a passzívat és az aktívat. A *passzív digitális lábnyom* olyan adatnyom, amelyet akaratlanul is hagyunk az interneten, például amikor meglátogatunk egy webhelyet, és a webszerver naplózhatja az IP-címünket, amely azonosítja az internetszolgáltatót és a hozzávetőleges tartózkodási helyet. Az *aktív digitális lábnyom* olyan adatokat tartalmaz, amelyeket szándékosan küldünk el az online térben, ilyen például az e-mail küldése.[94]

A hálózatkutatás az élet számos szegmensének megértését segíti, eredményesen alkalmazzák például az egészségügyben az egészségügyi profil kialakításában, a deepfake, a fake news elemzésében, a közlekedés tervezésében vagy éppen a rendészeti munkában, például a terroristák felderítésében.

Az adat vonatkozásában egyre gyakrabban lehet hallani azt, hogy ez a 21. század olaja, a gazdaság egyik mozgatórugója. Így van ez a rendészet területén is, hiszen adat, információ nélkül nehezen tudjuk megismerni a múltbeli, a jelenben zajló vagy a jövőben elkövetni kívánt releváns eseményt. Az adat (információ) az e-nyomozási folyamatok alapját is képezi.

A rendőrségen a bűnügyi hálózatkutatási ökoszisztéma kialakításában megfelelő keretet biztosíthatnak a Nemzeti Adatvédelmi és Információszabadság Hatóság, a Nemzeti Adatvagyon Ügynökség, a Nemzeti Adatgazdasági Tudásközpont és a Digitális Magyarországi Ügynökség.[95] A nemzeti adatvagyon részét képező adathalmazok nemcsak a piaci szereplőknek nyújthatnak segítségét, hanem a rendőrségnek is, amennyiben a hatóság tagjai rendelkeznek megfelelő adatelemzési képességgel.

[94] Christensson 2014.

[95] Lásd részletesebben az *1.3. alfejezet*et.

A hálózatkutatásban rejlő lehetőségek feltárásával és az összefüggések vizsgálatával az innováció erősödhet, és egy „adatelkövető" információs láncsorozat, valamint egy elektronikusadat-alapú bűnügyi ökoszisztéma alakulhat ki.

Az információk gyűjtésének, elemzésének és felhasználásának a módja hatással van a kriminalisztikai ajánlások megfogalmazására, és ezáltal a bűncselekmények felderítésére és bizonyítására is. Az elektronikusan rögzített adatok megkönnyítik a hálózati adatelemzést, amelynek eredménytermékei számos intézkedés foganatosítását valósíthatják meg, mint például az érintett személyek tettenérését, elfogását, azonosítását és az általuk a jövőben megvalósítani kívánt események (bűncselekmények) meghiúsítását, illetve azok kimenetelének befolyásolását. Összegezve elmondható, hogy a hálózatkutatás eszköztára a nem egy adathalmazban található adatkatasztereket összeilleszteti és elemezheti, ezáltal segítheti a bűnüldöző szervek munkáját például a klasszikus bűncselekmények vagy a terrorista hálózatok felderítésekor.

3.1. A kriminalisztika hálózatelemzési területei

A hálózatkutatás alapvető eleme nem más, mint maga az adat. Az átláthatatlannak tűnő adatmennyiség vizsgálatát segíti a hálózatelemzés, amely sokszor felhívja a figyelmet arra is, hogy az elemzés hiányában mennyi információ maradt volna látenciában. Például a telefon- és az e-mail-adatok alapján össze lehet kötni a telefonálókat, megkaphatjuk az ismeretségek hálózatát, amely lehet szakmai, baráti és intim kapcsolatokat is felölelő hálózat.[96]

A hálózati gondolkodásmódnak jelentős szerepe van a bűnözők, bűnözői csoportok és a bűnszervezetek pénzügyi hálóinak a feltérképezésében, valamint a bűnelkövetők közötti kapcsolatábra elkészítésében. A bűnözői kapcsolatoknak és hálózatoknak az elemzése a bűnözői magatartás megértéséhez, megismeréséhez vezethet.[97]

A hálózatelemzési módszerek és eszközök használata hozzájárulhat

a) a bűnöző, valamint civil kapcsolatok, kapcsolatrendszer feltérképezéséhez;
b) a bűnös vagyonelemek feltérképezéséhez;

[96] Varga–Ruppert–Barabási 2019: 35.
[97] Van der Hulst 2009: 101.

c) a múltbeli, a jelenben zajló és a jövőbeli cselekmények megismeréséhez;
d) elkövetői tulajdonságok, magatartási formák megismeréséhez, ami nélkülözhetetlen a profilalkotásban is, annak a bázisát is adhatja.

3.1.1. A kapcsolatrendszerek feltérképezése

A nyomozás teljessége alapelvének teljesülését is elősegíti a hálózatkutatás, mivel ha sikerül a kapcsolatrendszert feltérképezni, akkor az elemzés során a vizsgált esemény vonatkozásában az összes elkövető és az összes jogsértő cselekmény feltárhatóvá válhat.

A gyanúsított kapcsolatrendszerének feltérképezésében sokszor a korábbi – lezárt – büntetőügyek segíthetnek, amelyek alátámaszthatják, illetve kizárhatják egy másik folyamatban lévő bűnügyben (büntetőeljárásban) például a gyanúsítottak azon állítását, hogy ők nem ismerik egymást, soha nem találkoztak. Ha a korábbi ügyeket elemezzük, akkor a kapcsolati háló elemzésén keresztül megtudhatjuk azt is, hogy valójában a két gyanúsított állítása az ismeretség tekintetében nem helytálló, mivel egy korábbi – lezárt – büntetőeljárásban már szerepeltek tettesként, és a jegyzőkönyvekből kiderül, hogy ismerik egymást. A Netzsaru adatbázis rendszerében kapcsolati hálóra is lehet keresni, ami alkalmas arra, hogy az elkövetők előélete, kapcsolati hálója megismerhetővé váljon.

A hálózatkutatás során az elkövető úgynevezett civil kapcsolatai is feltérképezhetők. Így feltárhatók azok a személyek is, akik nem vettek részt a bűncselekményben, de akaratuk, illetve tudtuk ellenére az elkövető kihasználhatja őket, így ők is segítséget nyújthatnak az elkövető vagy a bűnös vagyoni elemek elrejtésében.

3.1.2. A bűnös vagyonelemek feltérképezése

A hálózatkutatás fontos szerepet játszik a bűnös úton szerzett vagyon visszaszerzésében is. Figyelembe véve, hogy a vagyonvisszaszerzéssel kapcsolatos feladatokról szóló 32/2022. (X. 25.) ORFK utasítás alapján a büntetőeljárást folytató nyomozó hatóságnak a vagyont generáló bűncselekménnyel kapcsolatban indult nyomozás során – a vagyonvisszaszerzés, illetve az elkobzás vagy a vagyonelkobzás végrehajthatósága érdekében – vizsgálni kell a bűncselekményből származó vagyon elvonásának lehetőségét. A hálózatkutatási elemzések

a gyanúsított kapcsolatrendszerének megismerése mellett a bűnös vagyonelemek, illetve a leplezett vagyonelemek feltérképezésében is segítségül lehetnek. Azonban a vagyonelemek feltérképezésekor szem előtt kell tartani az elkövetőhöz és közvetlen környezetéhez köthető vagyontárgyakat; valamint az érintett személyek jövedelmi viszonyait, életmódját, pénzügyi befektetéseit és megtakarításait. Valamint fel kell tárni az elkövető kapcsolatrendszerét, hogy kik azok a személyek, akik a vagyona elrejtésében közreműködhetnek, illetve a leplezett vagyonelem megismerésében a hatóság segítségére lehetnek. A hálózatkutatásban a mesterséges intelligencia is segítségül fog szolgálni, ezáltal lehetővé válhat, hogy még jobban megértsük a körülöttünk zajló folyamatokat, illetve megismerjük az elkövetői hálózat jellemzőit.

3.1.3. A releváns cselekmények megismerése

A nyomozás kriminalisztikai nézőpontból a múltban és a jelenben zajló, valamint a jövőben elkövetni kívánt esemény megismerésére irányúló tevékenység. A nyomozás során beszerzett adatok elemzése és értékelése nyomozási cselekmények foganatosításához járulhat hozzá. Az eredmények megalapozhatják egy személy figyelését, ami szintén megerősíthet vagy kizárhat egy kapcsolati rendszerhez tartozó bűncselekményt elkövető személyt. A kapcsolati hálózati figyelések esetében lehetőség adódhat a kapcsolati ábrán szereplő személyek azonosítására, vagy segítségül szolgálhat az általuk használt gépjárművek, telefonszámok vagy tartózkodási helyek megállapításában is.

3.1.4. Adatszolgáltatás a profilalkotáshoz

Hazánkban a bűnüldöző szervnek számos esetben a specifikus profilalkotás nyújt támaszt, támogató módszerként az ismeretlen személyazonosságú elkövető beazonosításában, vagy már ismert személyazonosságú gyanúsított kihallgatásában, illetve öngyilkosságot elkövetni kívánó személy minél hamarabbi megtalálásában, hogy megelőzhető legyen a tervezett cselekmény. A beszerzett, rendelkezésre álló adatok alapján az elkövető tulajdonságai határozhatók meg, vagyis az, hogy milyen volt az elkövető.

A profilozó a kriminalisztikai alapkérdések közül nem a *ki?,* hanem a *milyen?* kérdésre keresi a választ. A *milyen?* kérdésre adott válasz segíti megválaszolni

a *ki?* kérdést, azonban a válasz megszerzése a nyomozó feladata. A specifikus profilelemzés vonatkozásában – különösen emberölés vagy szexuális bűncselekmények esetén – a nyomozó a kriminalisztikai alapkérdést kiegészítheti a *milyen?* kérdéssel is.[98]

Az elkészült profil olyan információ a nyomozó hatóság számára, hogy milyen körben kell keresni az elkövetőt, ki az, aki számításba jöhet. Itt is jelentősége van a big datának[99] és az intézetek, szervek adatbázisainak, nyilvántartásainak, a hálózatelemzési folyamatoknak, ahol a *milyen?* kérdésre adott válasz segíthet egy társadalmi hálókapcsolatban a személyek szűkítésében. A hálózatelemzési folyamat a már megválaszolt kriminalisztikai alapkérdésekre építkezik, illetve a megválaszolandó kriminalisztikai kérdésekre is megadhatja a választ. Az elkészült profilokat össze kell kapcsolni a hálózat embereivel, szereplőivel. Az összekapcsolás segítséget nyújthat a hálózatbomlasztási vagy a kihallgatási stratégiák kialakítása során.[100]

Szükséges a hálózatelemzési képesség kiépítése, amely három dolgot foglal magában:

- adatbázisok, nyilvántartások meglétét, azok feltérképezését;
- hálózatelemzési módszerek alkalmazását (megfelelő elemzési kérdések megfogalmazását);
- az elemzések eredményének értelmezését, nyomozási cselekmények foganatosítását, kriminalisztikai ajánlások megfogalmazását.

A hálózatelemzés egy sor információs áradatot indíthat el, ezáltal elősegítve a bűncselekményt elkövető személyek tettenérését, elfogását, azonosítását, így az általuk a jövőben megvalósítani kívánt események (bűncselekmények) meghiúsíthatók, illetve a kimenetelük befolyásolható.

A helyszín adataiból következtetést vonhatunk le az (ismeretlen) elkövető tulajdonságaira.[101] A bűncselekmény helyszíne az elkövető jellemzőit tartalmazza.[102] Az elkövető jellemzőinek ismerete pedig egyenes út a digitális profilalkotáshoz.

[98] Nyitrai 2015: 145.

[99] A big data: azt a hatalmas információmennyiséget és feldolgozását jelenti, amelyet a felhasználók és a hálózatba kötött digitális eszközeik generálnak, és amelyet a számítógépek elemeznek, valamint bárki számára elérhetők. Szűts 2017.

[100] Keszi–Lohner 2022: 83.

[101] Baumgartner–Ferrari–Palermo 2008: 563.

[102] Baumgartner–Ferrari–Salfati 2005: 2702.

3.1.5. Segítségnyújtás a bűnügyi digitális ökoszisztéma kialakításában

A rendőrségnek vagy általánosságban véve a rendészeti szerveknek az adatalapú gazdasági és közszolgálati ökoszisztéma élvezőjének kell lennie, ezért a hálózattudomány alkalmazását szükséges bevezetni a rendészet területein is. A globális cégek már rendelkeznek hálózatelemzési ismeretekkel, képességekkel, eszközökkel és módszerekkel. Ezekre az új képességekre mielőbb fel kell készíteni a rendőrséget is. A világcégek folyamatosan fejlesztik hálózatkutatási képességüket. A kriminalisztikai gondolkodás ismereteit ki kell egészíteni a hálózati gondolkodási ismeretekkel, és célszerű elsajátítani az újdonságokat.

A rendőrségnek ki kell alakítania a bűnügyi digitális ökoszisztéma rendszerét – beleértve a hálózatkutatási ökoszisztémát. A rendőrségnek muszáj megértenie a digitális ökoszisztéma működését, hogy kedvező szereplője legyen a digitális átalakulási folyamat rendszerének.

A digitális technológiának köszönhetően folyamatosan óriási méretű adathalmazok jönnek létre. Ha rendelkezünk a kellő adatelemzési képességgel, akkor ezek segítséget nyújthatnak a bűncselekmények felderítésében és a bizonyításban, illetve előrejelzések esetén a bűncselekmények megelőzésében is.

A rendőrségnek használnia kell a mesterséges intelligencián és adatelemzésen alapuló technológiákat, valamint a big data elemzéseket és közigazgatási adatbázisokban tárolt adatokat is meg kell ismernie, ki kell aknáznia. A hálózatkutatás a szétszórtan található adatkataszterek elemzésében is segítséget adhat.

3.2. A hálózatkutatást támogató információgyűjtési módok

Az információgyűjtés során jelentősége van a HUMINT-nak (Human Intelligence, az emberi erőforrással folytatott hírszerzés), az OSINT-nak (Open Source Intelligence – nyílt hozzáférésű hírszerzés), a SOCMINT-nak (Social Media Intelligence – közösségi médiában folytatott hírszerzés) és a TECHNIT-nek (Technical Intelligence, technikai hírszerzés).[103] Az információgyűjtés során egyre gyakrabban szokták emlegetni a FININT-t (Financial Intelligence – pénzügyi hírszerzés) mint hírszerzési lehetőséget a pénzügyi folyamatok megismerésére.

[103] Nándori 2019.

Ezek az információgyűjtési módok kriminalisztikai értelemben adatok halmazát hozhatják létre, amelyek egymást keresztezhetik is akár, lehetnek köztük kapcsolódási pontok. A hálózatkutatás a kapcsolódások és az új irányok, összefüggések feltárásában nyújthat segítséget.

3.2.1. Az OSINT

A nyílt forrású információgyűjtésnek nincs pontos fogalma, de az alábbi meghatározások kiemelik a legfontosabb ismérveket.

Vida Csaba szerint

> „az OSINT-tevékenység: az önálló nyílt adatszerző tevékenység valamely személy vagy szervezet által közzétett, nyilvánosan, legális eszközökkel megszerezhető vagy korlátozott körben terjesztett, de nem minősített adatoknak a hírszerzési igények kielégítésére, speciális módszertan alapján történő felkutatását, gyűjtését, szelektálását, értékelését és felhasználását jelenti".[104]

Bálint László szerint

> „az OSINT az amerikai titkosszolgálatok által kifejlesztett módszer, amely az internet terjedésével általánossá vált nemcsak a titkosszolgálatoknál, hanem az üzleti élettől a kormányzati tevékenységig széles spektrumon. Az interneten keresztül az elmúlt évtizedekben olyan mennyiségű adat halmozódott fel, hogy követése, kutatása már csak célirányos eszközökkel és módszerekkel lehetséges".[105]

Egy harmadik megközelítésben:

> „Az OSINT-tevékenység lényege tehát, hogy olyan tartalmakat kutassunk fel a hírközlő és továbbító hálózatok segítségével, amely tartalmakat nyílt forrásokból, legális eszközökkel gyűjtünk össze, rendszerezzük azokat és elemző-értékelő munkafolyamatokat végzünk rajtuk a további feldolgozhatóság érdekében."[106]

[104] Vida 2013: 101.
[105] Bálint 2018: 138.
[106] Molnár 2021: 83.

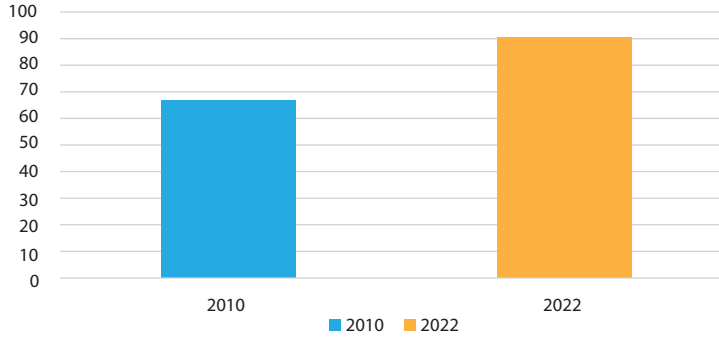
Az OSINT alkalmazása során találkozhatunk az álhírekkel, álvideókkal, amelyek téves információáradatot indíthatnak el, amennyiben nem észleljük őket időben.[107]

Napjainkban az OSINT legnagyobb forrását az internet, pontosabban az azon futó világháló (www: World Wide Web) jelenti.[108] Az interneten számos digitális adatot vagy lábnyomot is hagyhatunk, amelyek árulkodó információkat fognak szolgáltatni rólunk, szokásainkról, tevékenységünkről, hobbinkról. Internetes felületek a digitális nyomokból egy profilt is felállíthatnak rólunk, amely alapján célirányos reklámok fognak megjelenni internetezés közben. Az NMHH részére *Lakossági internethasználat* témakörben készült 2016-os online piackutatás adatai alapján a felhasználók 78%-a családdal, barátokkal, más, személyesen ismert személlyel való kapcsolattartásra használja az internetet, de magasnak tekinthető azon válaszolóknak az aránya is, akik kapcsolatot akarnak tartani olyan ismerősökkel, akikkel személyesen nem vagy nehezen tudnak találkozni.[109]

Az internet életünk részévé vált. A felhasználók sokszor szenzitív adatokat is megosztanak magukról például a közösségi oldalakon. Valaki meg akarja mutatni egy kép megosztásával az összes ismerősének, hogy adott pillanatban éppen külföldön a tengerparton nyaral a szeretteivel. De ha a közösségi oldalon nem gondoskodott arról, hogy csak az ismerősei lássák az adatait, akkor az elkövetők ezzel az információval visszaélhetnek. A külföldön nyaraló személy a fényképmegosztással közölte, pontosabban utalt rá, hogy nincs otthon, így ezt kihasználva akár a lakásába is betörhetnek, vagy az udvaron parkoló nagy értékű gépkocsiját eltulajdoníthatják.

2022-ben a magyar lakosság több mint 90,5%-a internetező volt, ami óriási ugrásnak tudható be a 2010-es arányhoz képest, amely csak 66,9% volt (27. ábra).[110]

[107] Lásd részletesebben a *7. fejezetet*.
[108] Csizner 2019: 20.
[109] Ariosz–NRC 2016: 40.
[110] Medve 2023.

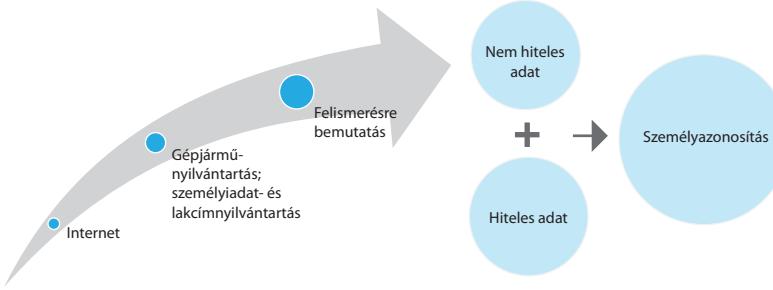


27. ábra: Internethasználat
Forrás: Medve 2023 alapján a szerző szerkesztése

A kibertér a valós, fizikai tér mellett a 2010-es évek végére második életterünkké vált.[111] Az elmúlt évtizedben jelentős növekedés figyelhető meg az internethasználat tekintetében. Az internetes felület azonban az elkövetők beazonosítását is segítheti, például ha az elkövető személyazonossága nem ismert, de tudjuk, hogy ki az élettársa/barátnője, akkor rajta keresztül sikerülhet a beazonosítás. Például a barátnő képet tölt fel a közösség oldalra, hogy hol vacsoráztak, merre mennek, és egy gépkocsi előtt készül a fotó, amelynek látszik a rendszáma. A rendszám a gépjármű-nyilvántartásból lekérhető, majd a tulajdonos/üzembentartó személy további nyilvántartásokban ellenőrizhető (például személy- és lakcímnyilvántartás, Netzsaru adatbázis, bűnügyi nyilvántartások). A gépjármű tulajdonosáról a nyilvántartásban szereplő képet egy felismerésre bemutatás keretében demonstrálhatjuk a sértettnek és/vagy a tanúnak, ami információs áradatot indíthat el. A későbbiekben a rendelkezésre álló adatok egy kutatás foganatosítását is megalapozhatják.

A másik példa lehetne az is, hogy erőszakos bűncselekmény (például rablás) esetén a sértett hallotta, hogy az egyik elkövető a másikat milyen becenéven szólította. Ezek a személyek leszűrhetők a közösségi oldalon, majd lekérdezhetők a személy- és lakcímnyilvántartásban, ahol fényképek is szerepelnek, amelyek prezentálhatók a sértettnek a felismerésre bemutatás szabályai szerint (28. ábra).

[111] Krasznay 2020b: 6.



28. ábra: A személyazonostás
Forrás: a szerző szerkesztése

A közösségi oldalak adatai nem tekinthetők hitelesnek, mivel bárki bármit feltölthet, ami nem biztos, hogy megfelel a valóságnak. Ezeket az adatokat egy hiteles nyilvántartásban kell ellenőrizni, például a személy- és lakcímnyilvántartásban, a gépjármű-nyilvántartásban stb., ami megalapozhatja egy bizonyítási cselekmény lefolytatását.

3.2.2. A HUMINT

A HUMINT (Human Intelligence – emberi erőforrással folytatott hírszerzés) Kis-Benedek József megfogalmazása szerint „a nemzetbiztonsági tevékenység azon eljárása, amelynek középpontjában az ember áll, akinek ismeretét, képességét a nemzetbiztonsági szolgálatok tervszerűen és szervezett formában használják fel”.[112] Az alkalmi adatszolgáltatótól a szervezetszerű titkos együttműködőkön át a külföldi hírszerző ügynökök alkalmazásáig terjed a humán források köre.[113] Egy másik meghatározás szerint az emberi erővel folytatott felderítés magába foglalja a figyelők és a felderítők által végzett tevékenységet is.[114]

A hálózatkutatást támogató információgyűjtési módok egyben rávilágítanak arra is, hogy ezek az információs források egymást mozaikként kiegészíthetik. Az egyik forrásban található mozaikdarab egy másik forrásban elhelyezkedő

[112] Kis-Benedek 2014: 155–156.
[113] Kis-Benedek 2014: 156.
[114] Füzesi 2004.

mozaiknak lesz a társa, majd a végén egymást kiegészítve kiadnak egy egységes képet. Az emberi kapcsolatok a világhálóhoz hasonlóan hálózatot alkotnak.[115]

A hálózatkutatás segítségül lehet akkor is, ha egy rendszer különböző szereplői, tényezői vagy éppen eseményei közötti összefüggéseket szeretnénk mérhető adatok alapján dokumentálni, valamint lehetőséget nyújthat direkt és indirekt, látható és „láthatatlan" összefüggések detektálására nagy mennyiségű, strukturálatlan adat esetén is.[116]

A HUMINT-tevékenység hagyományos jellemzője, hogy alkalmazása során lehetővé válik a mélységi információk konspirált felfedése, amiben fontos szerepet kaphat a kommunikáció és az észlelés.[117]

A rendőrség bűncselekmény elkövetésének megelőzése (bűncselekményre vonatkozó információk megszerzése) céljából az információk megszerzése érdekében a rendőrséggel titkosan együttműködő személyt vehet igénybe. A rendőrség anyagi ellenszolgáltatást nyújthat a vele együttműködő magánszemély részére annak tevékenységéért.[118] Az anyagi ellenszolgáltatás egy motiváló tényező az információszerzésre. Az információszerzés során számos költség is felmerülhet az adatszolgáltató irányából, amely ezt a költséget is fedezheti.

3.2.3. A TECHINT

A TECHINT (Technical Intelligence – technikai/technológiai hírszerzés) célja, hogy egy kérdéses technológiát a kifejlesztő államtól megszerezzenek és képesek legyenek előállítani,[119] ezáltal elősegítve saját technikai fölényüket úgy, hogy a célország technikai fölénye megtörik.[120] Az adat az eszközök technikai paramétereinek felderítésével keletkezik.[121]

Gál István László szerint

> „a technikai hírszerzés egy átfogó megnevezés, amely a hagyományos titkosszolgálati eszközök (például lehallgatás) alkalmazásától az elektronikus eszközökkel folytatott

[115] Nándori 2019: 100.
[116] Szócska et al. 2019.
[117] Dobák–Tóth 2021: 197.
[118] 1994. évi XXXIV. törvény indokolása a rendőrségről 66. §-hoz.
[119] Bányász 2018: 65.
[120] Béres 2014: 124.
[121] Kovács 2003: 40.

felderítésig és tudományos módszerekkel kidolgozott eljárásokig terjed. A technikai információszerzés fogalma a távközlési csatornákból és adatátviteli hálózatokból történő, továbbá a rejtjelző és irodatechnikai berendezések műszaki eszközökkel és módszerekkel való támadásával megvalósuló információszerzést foglalja magában."[122]

A távközlési csatornákból történő információszerzés elsősorban egyes külföldi kormányzati-távközlési csatornák támadásával valósul meg.[123]

A technikai hírszerzésen keresztül egy adott állam próbál versenyhelyzetben maradni, a technológia nyújtotta lehetőséget alkalmazni, ezáltal elősegítve a technikai fejlődését.

3.2.4. A SOCMINT

A SOCMINT (Social Media Intelligence – közösségi médiában folytatott hírszerzés, információgyűjtés) olyan információgyűjtő eszközök és módszerek összességének tekinthető, amelynek forrása a közösségi média, továbbá olyan adatok, amelyek az egyes felhasználók közösségi médiában folytatott tevékenységéhez kapcsolódnak.[124]

Egyes szerzők az OSINT-on belül tárgyalják a SOCMINT-ot, míg mások megkülönböztetik egymástól a két információgyűjtési módot. A megkülönböztetés okaként a közösségimédia-platformok sajátosságait emelik ki. Az érdemi információ megszerzéséhez a felhasználónévhez kötött online profil szükséges, és olyan fedőprofilt kell létrehozniuk, amely nem kelt gyanút.[125]

3.2.5. A FININT

A pénzügyi hírszerzés (FININT, Financial Intelligence) fontos szerepet tölt be a pénzügyi tranzakciók felderítésében, illetve az úgynevezett pénzügyi profilalkotásban. A pénzintézetektől kérhető információ segítheti a bűnös vagyonelem felderítését, amely során az érintett személyről az alábbi adatok szerezhetők be:

[122] Gál 2019: 42.
[123] Gál 2014.
[124] Dobák–Tóth 2021: 198.
[125] Erdész 2018: 33–34.

– rendelkezik-e *simple/simple pay* szolgáltatással, milyen profillal rendelkezik, milyen szolgáltatásokat vett igénybe, illetve milyen adatokat (elérhetőséget) adott meg;
– milyen internetbank- és mobilbank-szolgáltatásokat vett igénybe;
– történt-e telefonos bankszolgáltatás-használat, amennyiben igen, milyen szolgáltatást vett igénybe;
– rendelkezik-e számlával (befektetési, pénz-, deviza-, értékpapírszámlával, hitelkártyával, nyereménybetétkönyvvel stb.), amennyiben igen, úgy annak igénylésekor milyen címet adott meg elérhetőségként;
– mely gazdasági társaságok számlái felett jogosult rendelkezni;
– nem számlavezetőként, hanem meghatalmazottként jogosult-e más természetes személy vagy jogi személy bankszámlája felett rendelkezni;
– rendelkezik-e vagy rendelkezett-e széffel, illetve jogosult-e más személy széféhez hozzáférni;
– amennyiben nevezett személy rendelkezik a pénzintézetnél folyószámlával, úgy ahhoz kapcsolódó készpénzt helyettesítő fizetési eszköz használatának helyszínére és időpontjára vonatkozóan adat kérhető;
– nevezett személy bankkártyáról töltött-e fel telefonszámot, illetve rendelkezik-e sms-szolgáltatással, amennyiben igen, milyen számra történt a feltöltés, valamint milyen számra érkezik a szolgáltatás.[126]

A vagyonvisszaszerzéssel kapcsolatos feladatokról szóló 32/2022. (X. 25.) ORFK utasítás alapján a büntetőeljárás során azonosítani kell valamennyi, a bűncselekményből származó vagyon átvételével, tárolásával, elrejtésével, átalakításával, átruházásával, elidegenítésével vagy abban történő részvétellel, felhasználásával, azzal összefüggésben végzett pénzügyi vagy gazdasági tevékenységgel, ilyen igénybevételével, vagy arra irányuló rendelkezéssel bármilyen módon összefüggésbe hozható természetes vagy jogi személyt, jogi személyiséggel nem rendelkező szervezetet.

További segítségül szolgálhatnak az applikáción keresztül intézett pénzügyi tranzakciók, például banki szolgáltatások, vagy akár egy parkolási díj fizetése. A parkolási applikáción keresztül beazonosíthatóvá válhat az elkövető birtokában lévő személygépkocsi, a gépjármű-nyilvántartásban pedig a tulajdonos/üzembentartó. Az elkövető a bűnös vagyon elrejtése és leplezése céljából nem

[126] Nyitrai 2014: 221–222.

a saját nevére fogja íratni a gépkocsit, hanem a hozzá közel álló, megbízható személyre. Az applikáció használata így hozzájárulhat a bűncselekmény elkövetésével gyanúsítható személyhez és közvetlen környezetéhez köthető vagyonok megismeréshez, illetve az érintett személy kapcsolatrendszerének feltérképezéséhez. A cél, hogy a leplezett vagyonelem megismerhetővé váljon, és annak bűnös eredete, a leplezés ténye bizonyítható legyen.

A pénzügyi profilalkotásban a pénzügyi hírszerzési módoknak és az így megismert digitális adatoknak, majd azok elemzésének kiemelkedő szerepük van, mivel hozzásegíthetnek a bűnös úton szerzett vagyon, illetve annak elrejtésében közreműködők felderítéséhez.

Az információgyűjtés során említett HUMINT, OSINT, SOCMINT, TECHNIT és FININT adatszerző metódusoknak a fogalmánál, határaik tárgyalásánál mindig több kérdés merült fel, lásd például a fent tárgyalt SOCMINT és OSINT elhatárolását. Véleményem szerint ezek az információszerző metódusok kriminalisztikai értelemben tárgyalhatók e-nyomozás néven, amely magába foglalja ezeket a hírszerzési lehetőségeket. Az e-nyomozás részeit és alegységeit képezik, amelyekhez az eredményes nyomozás érdekében kriminalisztikai ajánlások és elvek is készíthetők.

4. Internet of Things

Számos érzékelő (szenzor) vesz körbe minket, amelyek érzékelik a környezetünket, detektálják a beállt – fizikai, kémiai, biológiai stb. – állapotváltozásokat, valamint az interneten keresztül kapcsolatba lépnek, kommunikálnak egymással, illetve a felhasználóval.[127] Napjainkban egyre nagyobb az *Internet of Things* (dolgok internete, a továbbiakban: IoT) szerepe, amelynek felhasználási köre elég széles körű, mivel átszövi az egész társadalmat, így a mezőgazdaságot, az ipart, a közlekedést, az oktatást, a közigazgatást, a bűnüldözést, illetve a bűncselekményt elkövető körök tevékenységét is.

Az IoT fogalma:

> „magyar fordításban a »dolgok internete« egy társadalmi-technológiai keretkoncepció, ami azt írja le, hogy termékek, tárgyak, eszközök online összekapcsolódnak, egymással kommunikálnak, feladatokat hajtanak végre, anélkül, hogy ehhez feltétlenül felhasználói kezelőfelület csatlakozna. Technikailag olyan természetes vagy ember által megalkotott objektumok sokaságát írjuk így le, amik IP-címmel rendelkeznek és képesek az internetes hálózaton keresztül adatot forgalmazni."[128]

Tehát az IoT egymással összekapcsolt tárgyak, eszközök, objektumok világméretű hálózata, amely egyedileg címezhető és saját IP-címmel rendelkezik.[129]

Az IoT-eszközök képesek kommunikálni egymással valamilyen hálózathoz való csatlakozással. A kapcsolódás megvalósulhat egyrészt engedélyhez kötött frekvencia használatára alapuló technológia segítségével (például 4G; 5G), másrészt engedély nélkül használható frekvencia (például SigFox) alkalmazásával, vagy a magánjellegű technológiák használatával (például WIFI; Bluetooth).[130]

Az *Ericson Mobility Report* szerint 2020 végére a mobil-előfizetések száma a világban elérte a 8 milliárdot, míg az 5G előfizetések száma a világban az év utolsó három hónapjára 70 millióról 130 millióra bővült.[131] Egy közelmúltbeli

[127] Haig 2018: 97–98.
[128] IVSZ 2014–2015: 11.
[129] Haig 2018: 97.
[130] Gellért 2022: 56.
[131] Sipos 2021a.

statisztikai felmérés alapján az internetes hozzáférés a magyar háztartásokban 2019-ben elérte a 86%-ot, amely 2014-hez képest 13%-os emelkedést jelent.[132]

4.1. Az IoT szabályozása

Egyes előrejelzések szerint 2025-re megközelítőleg 100 milliárd IoT-eszközt fogunk számon tartani, és óránként 2 millió szenzort telepítenek majd.[133] Az eszközszám emelkedésével várhatóan az IoT-eszközök elleni támadások száma is meg fog növekedni. A védelem szempontjából jelentős az Európai Parlament és Tanács 2013/40EU irányelve. Az ennek való megfelelés érdekében hazánkban a 2014. évi LXXII. törvény módosította a Büntető Törvénykönyvről szóló 2012. évi C. törvény 423. §-át, az „Információs rendszer vagy adat megsértése" tényállást.[134] A Btk. 459. § 15. pontja alapján „az információs rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége".

Ez a meghatározás magába foglalja a számítógépeket, az IoT-eszközöket, a hírközlési és telekommunikációs hálózatokat, rendszereket, valamint a különböző típusú SIM-kártyákat, továbbá a definíció nem tesz különbséget a jelek továbbítása között, ezért magába foglalja az elektronikus, az optikai és a különböző rádióhullámok, valamint műholdas sugárzás útján keletkezett információs rendszereket.[135] Az Európai Parlament és Tanács 2013/40/EU irányelvének eleget téve átvettük az adat fogalmát is:

> „információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."[136]

[132] Eurostat 2021.
[133] ELEKTROnet Online 2017.
[134] Gellért 2021: 18.
[135] Gellért 2021: 18.
[136] 2012. évi C. törvény 423. § (5).

4.2. Internet of Everything (IoE)

A technológiai elemzők a Cisco által alkotott Internet of Everything (a továbbiakban: IoE) kifejezést a Kevin Ashton-féle IoT-definíciónál többnek tekintik, annak a következő szakaszának tartják.[137]

A „minden internet" kifejezés jóval többet takar az IoT-nél:

- az IoT esetében egymással internetkapcsolatban álló eszközök az emberek beavatkozása nélkül érzékelik és osztják meg egymással az adatokat;
- az IoE nemcsak a gépek közötti kommunikációt foglalja magába (M2M); hanem az emberek és a gépek közöttit (P2M), valamint
- az emberek közötti olyan kommunikációt is, amikor valamilyen technológiát felhasználtak;
- az IoE-nek négy alappillére van: dolgok, ember, adat, feldolgozás.[138]

Az IoT és az IoE folyamatábráját és kapcsolódási pontjait az alábbi információs láncok jól szemléltetik:

IoT = hálózat + tárgyak;

IoE = hálózat + tárgyak + emberek + adat + feldolgozás.[139]

4.3. Az eSIM és az iSIM

Az IoT-eszközökbe az adatvitel legfontosabb eleme, a SIM-kártya (előfizetői azonosító modul) van beépítve az okoseszköz azonosítása céljából.[140] Mostanában egyre nagyobb teret kap kényelmi szempontként a környezetbarát eSIM-kártya használata, amely a bűnüldöző hatóságok adatkérési szempontjait is ki fogja bővíteni. Az eSIM-képes készülékekre egyszerűen letölteni az előfizető profilját a mobilba épített chipkártyára, amely tartalmazza az előfizetés jellemzőit. További előnye még, hogy egyszerűen és gyorsan lehet váltogatni az eSIM-profilokat az eszközök között; a PIN- és egyéb biztonsági kód az online

[137] Sipos 2021b: 12.
[138] Sipos 2021b: 14.
[139] Sipos 2021b: 14.
[140] Gellért 2022: 58.

fiókban bármikor megnézhető, valamint az eSIM-es telefonok duál SIM-esként is használhatók.[141] Ezek a lehetőségek (profilok) a nyomozó hatóság munkáját is támogatják az elkövető beazonosításában.

Azonban el kell mondanunk, hogy az IoT-eszközök tekintetében megjelent az előfizetőt azonosító áramkör új generációjának számító iSIM (integrated SIM), amely lehetővé teszi, hogy a SIM-kártya funkcióinak a készülék fő processzorába történő integrálódásával a kérdéses eszköz még kisebb legyen.[142] Az iSIM esetén egyes előrejelzések szerint 2025-re az emberiség 488 millió db fogyasztói piacra szánt eszköz használhat. Az iSIM előnyei az eSIM-mel szemben:

- az eSIM-nél külön processzor szükséges, míg az iSIM-nél a fő processzorba történik a funkciók integrálódása;
- az eSIM-ek külön chipen működnek, az iSIM esetében nincs szükség ilyenre, valamint a SIM-szolgáltatások számára elkülönített helyre sem;
- az iSIM operátori oldalról további fejlesztést nem igényel.[143]

Az okoseszközök és az 5G technológia használatával a digitalizáció még jobban erősödni fog, még nagyobb szerepe lesz a digitális társadalom megteremtésében. Az 5G hálózattal az adatátviteli sebesség nő, valamint az évtized végére lehetővé válik több milliárd eszköz összekapcsolása.[144] Tehát az 5G hatással lesz az IoT- és az IoE-eszközök elterjedésére, továbbá a meglévő, valamint újnak számító területek fejlődéséhez is hozzá fog járulni. Ezek az alábbiak:

- az önvezető autók valós idejű kapcsolattal lesznek ellátva;
- az egészségügyi alkalmazások fejlesztésével egyre gyakoribb lesz a „távgyógyítás”;
- az okos otthoni eszközökkel az IoT és az IoE megteremtése;
- holografikus kiterjesztett valóság elterjedése;
- kiterjesztettvalóság-alapú térkép, navigáció;
- 3 dimenziós holografikus kommunikáció;
- virtuális online vásárlások;
- az érzékelők és a szenzorok mezőgazdasági elterjedésére is hatással lesz.

141 *Vodafone* weboldal eSIM-tájékoztatója.
142 Sipos 2022.
143 Sipos 2022.
144 Haig 2018: 107.

A fenti csoportok már az IoE-eszközök és -módszerek táborát fogják gazdagítani, továbbá a kapcsolatok hálózatának kialakításával egy hármas felállással fogunk találkozni, amikor a technológia felhasználásával történő, gépek közötti, gépek és ember közötti, valamint az emberek közötti kommunikációról beszélünk.

A „dolgok/tárgyak internete" és a „minden internet" már egymással párhuzamosan van jelen az életünkben, és ez a jövőben is így lesz, ezért még jobban meg fogják határozni a mindennapjainkat, ezáltal a bűnüldöző szervek munkáját is. Az IoT és az IoE által előállított adattömeg feldolgozási folyamatában és felhasználásában a mesterséges intelligencia és a hálózattudományi kutatási módszerek alkalmazása óriási jelentőségű lesz.

Olyan informatikai eszközöket kezdünk el használni, amelyeknek pár évvel ezelőtt még nyomuk sem volt, és az otthonaink is okkossá válnak.[145] Az Iot-eszközök száma 2030-ra várhatóan 125 milliárdra fog növekedni.[146] Ezek az eszközök egymással fognak kommunikálni, és egy digitális ökoszisztémát, egy kapcsolódási hálózatot, térképet fognak alkotni. Ezeknek az eszközöknek a hálózata kisméretben az okosotthonok, míg egy nagyobb kiterjesztésben az okosvárosok formájában alakul ki. Az okosotthon hálózata kapcsolódhat egy másik okosotthon hálózatához, ezzel még összetettebb hálózat jön létre, illetve az okosotthon vagy az okosotthonok hálózata kapcsolódhat az okosváros hálózatához.

4.4. Mobiltelefon használata során keletkezett digitális adatok

Az IoT-rendszerek esetében a digitális társadalomban a digitális állampolgár mint ügyfél a privát eszközövél csatlakozhat egy hivatalos állami szerv gépéhez az interneten keresztül, és így kommunikációs folyamat jöhet létre a közigazgatási ügyek intézésére.[147] A csatlakozás a privát oldalról legyakrabban mobil eszközről (például telefonról, iPadról, okostévéről, okosóráról stb.), ritkábban asztali gépről történik. Ha az okostelefon webböngészőjén a *magyarorszag.hu* oldalon belépünk az ügyfélkapunkra, és ügyet intézünk, akkor e-közigazgatásról beszélünk, míg az m-közigazgatási megoldások három kategóriát különböztetnek meg: sms-alapú értesítések (például a szülők az iskolás gyermek igazolatlan

[145] Krasznay 2020c: 122.

[146] IHS Markit 2017.

[147] Általában ez az ügyintézési folyamat a *magyarorszag.hu* oldalon zajlik. Lásd részletesebben az *1. fejezetet.*

hiányzásáról kapnak értesítést), mobiltelefonos fizetés (például parkolási díj kifizetése) és mobilapplikációk (például ügyintézés OkmányAppról).[148]

Az e-közigazgatás részeként az m-közigazgatás sikere a mobilitásban és a vezeték nélküliségében rejlik. Az m-közigazgatási szolgáltatások tulajdonképpen az e-közigazgatás elérhető szolgáltatásainak mobil eszközökkel való alkalmazásait foglalja magába.[149]

A m-közigazgatást (okostelefon-alapú) jelenleg még kevesen tanulmányozzák. Előnyei:[150]

- sokkal egyszerűbb és kényelmesebb módja az állampolgár – a telefon használója – állammal és közigazgatási szervekkel való kapcsolattartásának;
- az okostelefonok többféle érzékelővel vannak felszerelve, például kamerával, fényképezővel, diktafonnal és GPS-ekkel, amelyek lehetőséget biztosítanak a használónak a valós idejű kommunikációra, valamint az információk és a környezet adatainak rögzítésére, ezáltal nem csak azok eléréséhez, megtekintéséhez elegendőek;
- a hagyományos e-közigazgatás inkább a nem mobil (számítógépen elérhető) szolgáltatásokra koncentrál;
- nagy előnye az m-közigazgatásnak, hogy bárhol, bármikor és bármely internetkapcsolattal rendelkező kommunikációs eszközről elérhető, illetve ez fordítva is igaz, hogy a közigazgatási szerv képes valós időben az állampolgár számára releváns hiteles információt szolgáltatni, például veszélyhelyzetben;
- internetkapcsolat esetén a használó bármikor bárhonnan kérvényt tud benyújtani vagy eljárást kezdeményezni, ezáltal rengeteg időt és pénzt takaríthat meg más kommunikációs csatornával szemben (nem kell közlekedési eszközt használnia stb.), ezáltal gyorsíthatják a kérelmek feldolgozásának sebességét.[151]

Egyetérthetünk Szabó Balázzsal, hogy az emberek az okostelefonjaikat egyre ritkábban használják a klasszikusnak számító hívás lebonyolítására, inkább e-mailekkel, közösségi oldalakon keresztül teremtenek kapcsolatot egymással,

[148] Beláz 2020: 37.
[149] Szabó 2020b: 138.
[150] Szabó 2020a: 130–136.
[151] Szabó 2020a: 130–136.

vagy applikáción keresztül intézik például banki ügyeiket.[152] Az okostelefonok lehetővé teszik, hogy a használóik ne csak egy embert szólítsanak meg egy időpontban vagy időtartamban, hanem számos embert, illetve közösséget, akár a fórumokon, vagy akár egy link megosztásán keresztül egy közösségi oldalon.

A mobilinternet-előfizetések száma az elmúlt években folyamatosan emelkedett, az emberek egyre gyakrabban használnak mobil eszközöket internetezés céljából. A kommunikációs technológiák rohamos fejlődése sürgeti a mobilalkalmazások (mobilapplikációk) fejlesztését, ezáltal hozzájárulva a gyors és hatékony ügyintézéshez.[153] Az applikációk segítséget nyújtanak a közigazgatási ügyeink intézésében is, erre kiváló példa az OkmányApp.

A GPS-alapú applikációk azt is lehetővé teszik, hogy a bűnüldöző hatóságok a gyanúsított „elektronikus mozgását" nyomon követhessék. Az Iot-eszközök száma rohamosan növekszik, mivel itt kriminalisztikai szempontból jelentősége van a mobil eszközöknek, amelyek közül jelenleg a leggyakoribbnak a mobiltelefon telekinthető. Egyrészt az IoT-eszközök számának növekedése, másrészt az 5G szaporítja az IoT-eszközök számát. A legtöbb eszköz előbb-utóbb eSIM-mel vagy iSIM-mel fog rendelkezni, hasonlóan a mobiltelefonhoz, így indokolt az IoT fejezetén belül egy különálló alfejezetként tárgyalni a mobiltelefon használata során keletkezett digitális adatokat, amelyek kriminalisztikai nézőpontból segítik a bűnüldöző szervek munkáját.

4.4.1. Az elektronikus hírközlési szolgáltató által nyújtott digitális adatok

A mobiltelefon használatával az elkövetők számos elektronikus adatot (digitális nyomot) hagyhatnak maguk után. Az adatok keletkezhetnek egyrészt a hívások alkalmával, másrészt az applikációk, az internet használatával.

Az elektronikus hírközlésről szóló törvény (a továbbiakban: Eht.) 159/A. § (1) bekezdése alapján az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltatás szolgáltatója megőrzi az elektronikus hírközlési szolgáltatás előfizető, illetve felhasználó általi igénybevételével kapcsolatos, az érintett elektronikus hírközlési szolgáltatás nyújtásával összefüggésben a szolgáltató által előállított vagy kezelt adatokat. Az adatkérésre külön törvény szerint jogosult a bíróság, az ügyészség, a nyomozó hatóság, illetve

[152] Szabó 2020a: 131.
[153] Beláz 2020: 32.

az előkészítő eljárást folytató szerv, valamint a nemzetbiztonsági szolgálat törvényben meghatározott feladatai ellátásának biztosítása céljából. A szolgáltató által kezelt előfizető azonosításához szükséges adatok:

1. az előfizető neve, lakóhelye, tartózkodási helye vagy székhelye;
2. az előfizető számlázási címe, pénzforgalmi számlaszáma;
3. az előfizető születési neve, születési helye és ideje, anyja születési neve;
4. az előfizető képviselőjének 1–4. pont szerinti adatai;
5. az előfizető cégjegyzékszáma vagy más nyilvántartási száma;
6. az előfizető személyazonosság igazolására alkalmas hatósági igazolványának típusa és száma;
7. az előfizető lakcímet igazoló hatósági igazolványának száma.[154]

A nyomozó hatóságok és a rendőrségről szóló törvényben meghatározott belső bűnmegelőzési és bűnfelderítési feladatokat ellátó, valamint terrorizmust elhárító szerv, valamint a nemzetbiztonsági szolgálatok a törvényben foglaltak szerint a közléseket megfigyelhetik, lehallgathatják, tárolhatják, vagy a küldeménybe, közlésbe azok megfigyelése érdekében más módokon beavatkozhatnak.[155]

Az Eht. 159/A. § (1) bekezdése alapján az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltatás szolgáltatója:

– az adatkérésre külön törvény szerint jogosult bíróság, ügyészség, nyomozó hatóság;
– az előkészítő eljárást folytató szerv, valamint nemzetbiztonsági szolgálat törvényben meghatározott feladatai ellátásának biztosítása céljából, a kérelmükre történő adatszolgáltatás érdekében megőrzi az elektronikus hírközlési szolgáltatás előfizető, illetve felhasználó általi igénybevételével kapcsolatos, az érintett elektronikus hírközlési szolgáltatás nyújtásával összefüggésben a szolgáltató által előállított vagy kezelt alábbi adatokat:

„*a)* helyhez kötött telefon- vagy mobil rádiótelefon szolgáltatás, internet-hozzáférési szolgáltatás, internetes telefon-, internetes levelezési szolgáltatás, illetve ezek kombinációja esetén az előfizető egyedi előfizetői szerződésben rögzített személyes adatai;

b) helyhez kötött telefon- vagy mobil rádiótelefon szolgáltatás, internet-hozzáférési szolgáltatás, internetes telefon-, internetes levelezési szolgáltatás, illetve ezek kombinációja esetén az előfizetői, felhasználói

[154] 2003. évi C. törvény az elektronikus hírközlésről 154. § (2).
[155] 2003. évi C. törvény 155. § (5).

végberendezés vagy előfizetői hozzáférési pont hívószáma vagy egyéb, az előfizető, felhasználó egyedi azonosításához szükséges – az előfizetői szerződésben rögzített, vagy az elektronikus hírközlési szolgáltató által egyéb módon az előfizetőhöz, felhasználóhoz rendelt – állandó műszaki-technikai azonosítók;

c) helyhez kötött telefonszolgáltatás, helyhez kötött internet-hozzáférési szolgáltatás, illetve ezek kombinációja esetén az előfizetői, felhasználói végberendezés vagy előfizetői hozzáférési pont létesítési címe és típusa;

d) a kommunikációban részt vevő előfizetők, felhasználók hívószámai, egyedi műszaki-technikai azonosítói, felhasználói azonosítói, az igénybe vett elektronikus hírközlési szolgáltatás típusa, a kommunikáció dátuma, kezdő és záró időpontja;

e) helyhez kötött telefon- vagy mobil rádiótelefon szolgáltatás, illetve ezek kombinációja igénybevételénél alkalmazott hívásátirányítás és hívástovábbítás esetén a hívásfelépítésben részt vevő köztes előfizetői vagy felhasználói hívószámok;

f) mobil rádiótelefon szolgáltatás esetén a szolgáltatás igénybevételekor használt, a kommunikációban részt vevő felek készülékazonosítója (International Mobile Equipment Identity – nemzetközi mobil eszköz azonosító, továbbiakban: IMEI), valamint mobil-előfizetői azonosítója (IMSI);

g) mobil rádiótelefon szolgáltatás esetén a szolgáltatást nyújtó hálózat- és cellaazonosítója a közlés megkezdésekor, valamint az adott szolgáltatás nyújtásának időpontjában az adott cellaazonosítóhoz tartozó cella tényleges földrajzi helyének meghatározását lehetővé tevő adatok;

h) internetes elektronikus levelezési, internetes telefonszolgáltatás, illetve ezek kombinációja esetén a szándékolt címzett irányában megkezdett kommunikációra vonatkozóan a d) pont szerinti adatok;

i) internet-hozzáférési, internetes elektronikus levelezési, internetes telefonszolgáltatás, illetve ezek kombinációja esetén az elektronikus hírközlési szolgáltatás típusa és a szolgáltatás előfizető vagy felhasználó általi igénybevételének dátuma, kezdő és záró időpontja, az igénybevételnél használt IP-cím, felhasználói azonosító, hívószám;

j) internet-hozzáférési, internetes elektronikus levelezési, internetes telefonszolgáltatás, illetve ezek kombinációja során az előfizetők, felhasználók egyedi műszaki-technikai azonosítóinak az elektronikus hírközlési szolgáltató általi bármely átalakításának követéséhez szükséges adatok (IP-cím, portszám);

k) előre fizetett anonim hívókártyás mobil rádiótelefon szolgáltatás esetében a szolgáltatás első igénybevételének dátuma és időpontja, valamint a cellaazonosító, amelyről az aktiválás megtörtént."[156]

A felderítés és a bizonyítás során a mobiltársaságoktól kérhető adatok kulcsfontosságúak lehetnek. Azonban a megkereső szervnek figyelembe kell vennie, hogy a fent említett *a)–c)* pontok szerinti adatokat az előfizetői szerződés megszűnését követő, a *d)–k)* pontjaiban meghatározott adatokat azok keletkezését követő egy évig, míg a sikertelen hívások során előállított adatok esetében azok keletkezését követő fél évig köteles megőrizni az elektronikus hírközlési szolgáltató.

Az elkövető földrajzi helyzetének meghatározásában jelentős szerepe van a közlés –telefonbeszélgetés – megkezdésekor keletkezett cellaazonosítónak, azonban az elkövető földrajzi helyzetének meghatározásában a forgalmi adatokon kívül a helymeghatározási adatoknak is jelentőségük van. Az elektronikus hírközlési szolgáltató az ismeretlen helyen tartózkodó személy hollétének megállapítása – ennek keretében kapcsolatrendszerének, feltételezhető tartózkodási helyének megismerése – céljából a körözési eljárást lefolytató szerv megkeresésére köteles megállapítani és részére továbbítani a felhasználóval és az előfizetővel kapcsolatos hívásforgalmi, helymeghatározási és előfizetői adatokat.[157]

Meg kell jegyezni, hogy az elektronikus hírközlési szolgáltató nemcsak a nyomozó hatóságnak szolgáltathat – a törvényi feltételek megléte esetén – adatot, hanem a szabálysértési hatóság kérelmére a segélyhívó számok rendeltetéstől eltérő igénybevétele szabálysértés elkövetőjének azonosítása céljából is köteles átadni a segélyhívószámra kezdeményezett hívó telefonszám vonatkozásában:

„*a)* az előfizető családi nevére és utónevére, születési helyére és idejére, anyja születési családi és utónevére, lakcímére és értesítési címére, vagy

b) a nem természetes személy előfizető esetén annak cégnevére, székhelyére, telephelyére, képviselőjének családi nevére és utónevére vonatkozó adatokat."[158]

[156] 2003. évi C. törvény 159/A. § (1).
[157] 2003. évi C. törvény 156. § (17).
[158] 2003. évi C. törvény 157. § (11).

Továbbá a rendőrség kezeli az általa fogadott segélyhívások esetén a hívó fél által közölt adatokat és a hívó fél által használt telefonállomás azonosított adatait a segélyhívás fogadásától számított egy évig.[159]

Releváns adatot rejthetnek magukban a szolgáltatást igénybe vevő előfizető adatai, a mobil rádió telefonszolgáltatás igénybevételekor használt készülék egyedi azonosítója (IMEI), valamint nemzetközi mobil-előfizetői azonosító (International Mobile Subscriber Identity, a továbbiakban: IMSI), illetve előfizetői azonosító kártya (a Subscriber Identity Module, a továbbiakban: SIM).

Az IMEI-kifejezés az *International Mobile Equipment Identity* rövidítése és a szolgáltatók ebből az adatból kiindulva azonosítják a hálózatra regisztrált eszközöket.[160] Az IMEI a mobiltelefonok azonosítására használt olyan egyedi számsor, amelynek segítségével az egyes készülékek adott időben és helyen egyértelműen beazonosíthatóvá válnak.[161] Az IMEI olyan egyedinek tekinthető, mint a gépkocsinál a rendszám. Az IMEI 15 vagy 16 számjegyű azonosító számból áll, amely a következőket tartalmazza:

– az első nyolc szám az eredet és a modell számát jelenti,
– míg a többi számjegyet az eszköz gyártója határozza meg.[162]

Az IMEI-szám általában megtalálható az akkumulátor alatt, de ha a telefonba beírjuk a *#06# kódot, akkor a készülék is kijelzi az azonosítót.[163] Ha a készüléket eltulajdonítanák (ellopnák), akkor a mobilszolgáltató az IMEI-számmal letilthatja a készüléket. Ez azt jelenti, hogy a telefon „új tulajdonosa" nem tudja használni a készüléket, mivel az blokkolható a hálózatról.[164] Az IMEI-számot a telefonkészülék ellenőrzés céljából minden egyes bekapcsolásakor automatikusan elküldi a hálózatnak.[165]

A hazai jogszabályok alapján a telefonkészülékek IMEI-száma egyedi, nincs két ugyanolyan IMEI-számú készülék. Azonban ezeket az eszközöket is lehet klónozni illegálisan, ami azt jelenti, hogy több készüléknek lesz ugyanaz az IMEI-száma. Még az is előfordulhat, hogy egyes ázsiai országokban a gyártás során több készüléknek lesz ugyanaz az IMEI-száma, ami problémát jelenthet például

159 1994. évi XXXIV: törvény a Rendőrségről 81/A. §.
160 Patrik 2022.
161 *Vodafone ÁSZF 3. számú melléklet* [é. n.]: 7.
162 *Mi az IMEI-szám és az IMEI bármely eszköz keresése* 2019.
163 *Telefonguru* weboldalon IMEI-szócikk.
164 Balázs 2021.
165 *Szotarjelentese* weboldalon IMEI jelentése.

lopás esetén a készülék letiltásakor, vagy annak megállapításakor, hogy milyen SIM-kártyát helyeztek be a készülékbe, pontosabban a sok SIM-kártya közül melyik lehet a releváns. Kínában 2003-ban és 2004-ben 50 millió készüléket gyártottak le ugyanolyan IMEI-számmal, s például a 2005-ös londoni terrortámadás során használt telefonoknak is pont ugyanolyan IMEI-számuk volt, ezért az elkövetőket a telefon alapján nem lehetett lenyomozni.[166]

A telefonkészülék eltulajdonítása (lopása) esetén az IMEI-számnak mint egyedi azonosítónak az ismerete nélkülözhetetlen az eltulajdonított dolog körözésének az elrendelésében. A körözött dolgok nyilvántartásában rögzítik a mobileszköz IMEI-számát, így egy rendőri intézkedés vagy ellenőrzés (például egy kutatás) keretében a telefonok ellenőrizhetők a körözési nyilvántartási rendszerben, így az előállított személynek a készülékét is ellenőrizhetik.

Az IMEI tartalmazza az úgynevezett SIM-kártya adatait. A SIM-kártya az Eht. 188. § 121. pontja alapján

> „az előfizető mobil rádiótelefon-hálózaton belüli azonosítását szolgáló adatokat, illetve a mobil rádiótelefon-szolgáltatás igénybevételéhez szükséges információkat tartalmazó kártya vagy beépített modul. A beépített modul tartalma távolról beállítható és módosítható is lehet (eSIM)."

Az eSIM mellett megjelent a legújabb hálózati kártya, az iSIM, amelyet az okostelefon processzorába fognak beágyazni.[167] Ezáltal a mobilszolgáltatás integrálhatóvá válhat számos eszközbe, kiterjesztve az IoT-eszközökre is.[168] A SIM-kártyán tárolják az IMSI-számot egyedi azonosítóként, amely a mobilelőfizetők, valamint a felhasználók azonosítására szolgál, és a mobiltársaságok ennek a számnak a segítségével azonosítják az előfizetőket és felhasználókat.[169]

A jövőben kényelmi és környezetvédelmi szempontból is egyre nagyobb teret fog kapni az eSIM-kártya használata, amely a bűnüldöző hatóságok adatkérési szempontjait is ki fogja bővíteni. Az eSIM képes a készülékekre egyszerűen letölteni az előfizető profilját a mobilba épített chipkártyára, amely tartalmazza az előfizetés jellemzőit. További előnye még, hogy egyszerűen és gyorsan lehet váltogatni az eSIM-profilokat az eszközök között; a PIN- és egyéb biztonsági kód az online fiókban bármikor megnézhető, valamint az eSIM-es telefonok duál

166 SZTEinfo–Móczár 2020.
167 Richárd 2022.
168 Vodafone 2022.
169 *Vodafone ÁSZF 3. számú melléklet* [é. n.]: 7.

SIM-esként is használhatók.[170] Ezek a lehetőségek (profilok) a nyomozó hatóság munkáját is támogatni fogják az elkövető beazonosításában.

A nyomozás során az elkövetőhöz köthető telefonszámok beszerzési lehetőségei:

- tanú és a terhelt kihallgatása során (a kihallgatás alkalmával nyilatkoztatni kell a telefonos elérhetőségére);[171]
- telefonkészülék IMEI-számából visszafejtve;
- Robotzsaru rendszerből, azon belül a Netzsaru rendszerből;
- közösségi oldalak, fórumok, hirdetési oldalak segítségével;
- adatgyűjtés keretében.

A felsorolást még lehetne folytatni, de le kell szögezni, hogy a beszerzési mód mindig az adott ügytől és típustól függ, illetve a rendelkezésre álló adatoktól, mivel minden ügy egyedi. Ha figyelembe vesszük, hogy minden ügy egyedi, és az Eht. szakaszaiból indulunk, akkor összegezve az alábbi kérdések fogalmazhatók meg:

- a hívószámhoz milyen IMSI-szám, illetve egy meghatározott időszakban (időtartamban) milyen IMEI-szám vagy előfizetői adatok tartoznak;
- a hívószámhoz tartozó számegyenleg vagy tartozás lekérdezése, vagy ha feltöltős a hívószám, akkor a feltöltés adatai (például mikor, hol történt a feltöltés, mi a tranzakció azonosítója);
- a hívószám alapján mik az értékesítőhely adatai;
- SIM-kártya vagy IMSI alapján mik az előfizetői adatok, az IMSI-számhoz milyen hívószám tartozik;
- SIM és a hívószám alapján PIN (Personal Identification Number – SIM-azonosító kód) és PUK (PIN Unlock Key, SIM-azonosító kód feloldó kulcs) lekérése;
- mobilszámhoz tartozó híváslista, figyelemmel az Eht. adatmegőrzésére egy időintervallumot kell megjelölni;
- a kérdéses (kommunikációban részt vevő) telefonszám melyik másik telefonszám híváslistájában szerepel (ennek a sorozat-bűncselekmények felderítésekor van nagy jelentősége, amikor a hívásokat külföldi telefonszámról kezdeményezik);

[170] *Vodafone* weboldal eSIM-tájékoztatója.

[171] 2017. évi XC. törvény a büntetőeljárásról 178. § (2) *g);* 184. § (2) *g).*

– az előfizetői adatok birtokában megkérdezhetők az előfizetőhöz tartozó hívószámok és szerződési adatok (az így kapott adatokat ajánlott összevetni a hiteles nyilvántartásokkal, mint például a személy- és lakcímnyilvántartással, vagy a Robotzsaru rendszerrel, mivel előfordulhat, hogy a szolgáltatónál olyan tartózkodási helyet adott meg, amely nem szerepel a hiteles nyilvántartásban). A kérdéses hívószámot, illetve ha kaptunk e-mail-címet, azt is célszerű az interneten is végigfuttatni, mert lehet, hogy egy fórumban vagy oldalon egy hirdetést adott fel az érintett személy, s ezen keresztül újabb adatokhoz juthatunk;
– az adott IMEI-számú készülékbe a meghatározott időtartamban milyen hívószámot, SIM-kártyát helyeztek, vagy milyen eSIM- vagy iSIM-adatokkal rendelkezik. Az eSIM-hez tartozó profil megküldése által kiderülhet, hogy az eSIM-hez tartozó QR-kódot milyen e-mail-címre küldték meg;
– az IMEI-szám alapján a készülék vásárlásával kapcsolatos adatok is kiderülhetnek (például milyen hívószámmal értékesítették, milyen ahhoz tartozó előfizetői adat lelhető fel). Ehhez fontos, hogy hálózati forgalmazás történjen;
– az IMEI-számhoz vagy hívószámhoz kapcsolódó letiltási események is relevánsak lehetnek;
– IP esetén az ahhoz tartozó hívószámok;
– vezetékes hívószám előfizetői adatai, híváslistája;
– az érintett a mobilszolgáltatónál milyen szolgáltatást vett igénybe;
– cellainformációk bekérése, a bűncselekmény helyszínén található bázisállomásokra milyen hívószámok jelentkeztek fel a kérdéses időintervallumban. Azonban figyelembe kell venni, hogy a közlés megkezdésekor keletkezik a cellainformáció, amely a kommunikáció elindításakor keletkezett adatokat fogja tartalmazni, ez az alibivizsgálatnál nagyon fontos szempont;
– a felhasználóval és az előfizetővel kapcsolatos, a forgalmi adatokon kívüli helymeghatározási adatok (bázisállomás azonosítójának, címének vagy geokoordinátájának) beszerzése.[172]

[172] *Vodafone ÁSZF 3. számú melléklet* [é. n.].

Az Eht. 188. § 59. pontja alapján a helymeghatározási adat:

> „a nyilvános mobilhálózatokon a hálózati infrastruktúrából vagy mobil készülékekből származó mindazon feldolgozott adat, amely meghatározza a végfelhasználó mobil végberendezésének földrajzi helyzetét, illetve nyilvános helyhez kötött hálózatokon a hálózati végpont nyilvántartásban rögzített címét."
> „[B]ázisállomásnak hívják azokat az antennákat vagy adótornyokat, amelyek továbbítják az elektronikus hírközlési szolgáltatás nyújtásához elengedhetetlen elektromágneses hullámokat. A bázisállomások működésük során elektromágneses, azaz rádiófrekvenciás hullámokat bocsátanak ki, melyek a szabad térben terjednek, és közvetlen összeköttetést biztosítanak a nálunk lévő mobiltelefon és az összeköttetést biztosító bázisállomás antennája között."[173]

A fenti kérdésekre kapott válaszok elemzésével és értékelésével közelebb kerülhetünk a múltbeli releváns esemény megismeréséhez, a jelenben zajló cselekmény megszakításához, vagy a jövőben tervezett elkövetni kívánt cselekmény felderítéséhez.

4.4.2. A mobiladatok gyakorlati jelentősége egy konkrét eset tükrében

A büntetőeljárásokban eléggé gyakori a híváslisták és a hívásforgalmi adatok tekintetében az úgynevezett „cellaadatok" bekérése és elemzése. Jól szemlélteti ezt az N. J. ellen indult büntetőügyben meghozott Bhar.III.1.530/2019/23. számú ítélet.

A vád szerint N. J. vádlott feleségét N-né K. J. sértettet M., H. út … szám alatti munkahelyének környezetében megölte, majd a sértett testét és táskáját, benne a mobiltelefonjával a Škoda Roomster személygépkocsi csomagtartójába tette.

A vádlott, miután a fia elaludt, a Škoda Roomster típusú gépkocsijával betolatott a ház udvarára, a füstölő bejárata felé. A sértett testét a csomagtartóból kiemelte, a gépjárműtárolón át a húsfeldolgozó helyiségbe vitte és feldarabolta. N. J. vádlott még az éjszaka folyamán a holttest darabjait részben égésgyorsító, aromás hígító segítségével elégette, részben tartva attól, hogy a sértett testének még a birtokában lévő darabjait nála megtalálják, azokat D. határába, a lakásától néhány kilométerre található Zs-rétre vitte.

[173] *Vodafone ÁSZF 3. számú melléklet* [é. n.].

A vádlott és a sértett cellapozíciójának párhuzamosságára vonatkozóan az alábbi adatok keletkeztek:

- X hívások időpontjában a vádlott mobiltelefonjával együtt a Telekom MOVAR1R-3 jelű mobilcella lefedettségi területén tartózkodott, amelyben a sértett munkahelye, a M., H. út ... szám található.
- Az igazságügyi távközlési szakértői vélemény szerint N. J. vádlott 20/… hívószámú mobiltelefonja 18 óra 39 perc 8 másodperckor a Magyar Telekom által üzemeltetett mobilhálózat M., F. K. utca … szám alatti bázisállomás MOVAR1R_1 jelű cellájára, 19 óra 37 perc 53 másodperckor, 20 óra 7 perc 58 másodperckor, 20 óra 36 perc 36 másodperckor, 20 óra 37 perc 24 másodperckor, 20 óra 39 perc 43 másodperckor, 20 óra 39 perc 57 másodperckor és 20 óra 46 perc 27 másodperckor a Magyar Telekom által üzemeltetett mobilhálózat M., F. K. utca … szám alatti bázisállomás MOVAR1R_3 jelű cellájára jelentkezett fel, ami a szakértői vélemény szerint azt jelenti, hogy az ekkor kezdeményezett, illetve érkezett hívások kezdetének időpontjában a mobiltelefon és – mivel adat arra nem merült fel, hogy a vádlott a telefonját másnak adta volna oda – a vádlott is e cellák területén volt. A szakvélemény alapján megállapítható az is, hogy N-né K. J. munkahelye az M., H. utca … számú ház is e cella területén van. Ekként tehát megállapítható, hogy a vádlott N-né K. J. eltűnésekor a felesége közelében tartózkodott.
- A vádlott hazaért a D., H. út … szám alá. A vádlott híváskezdeményezése előtt 46 másodperccel a sértett gépkocsiban lévő mobiltelefonjára is hívás érkezett. A hívások időpontjában a vádlott mobiltelefonja a Telekom HEDER13, míg a sértett mobiltelefonja a Telenor 16203 jelű mobilcellájára jelentkezett fel. A vádlott háza a két mobilszolgáltató mobilcelláinak közös lefedettségi területén található. Pár perccel később a sértett mobiltelefonjára újabb hívás érkezett, a mobiltelefon cellapozíciója megegyezett a korábbi hívásával. Ezt követően a sértett mobiltelefonja elérhetetlenné vált.
- A sértett mobiltelefonjának utolsó hívásakor rögzített Telenor 16203 jelű mobilcella területén volt, amely közös lefedettségű a vádlott mobiltelefonjának Telekom HEDER13 jelű mobilcellájával, s e két mobilcella közös lefedettségű területén található a vádlott D., H. u. … szám alatti lakóhelye.[174]

[174] Tatabányai Törvényszék 17.B.419/2017/39. számú ítélete.

Összegezve:

- A hívások időpontjában a vádlott mobiltelefonjával együtt a mobilcella lefedettségi területén tartózkodott, amelyben a sértett munkahelye található (cellainformációk – informatikai szakértő véleménye).
- A vádlott híváskezdeményezése előtt 46 másodperccel a sértett mobiltelefonjára is hívás érkezett. A hívások időpontjában a vádlott mobiltelefonja a sértett mobiltelefonja mobilcellájára jelentkezett fel. A vádlott háza a két mobilszolgáltató mobilcelláinak közös lefedettségi területén található, a sértett a hívást nem fogadta (cellainformációk – informatikai szakértő véleménye).[175]

Az elkövetők általában a SIM-kártyát cserélik, és ugyanazt az IMEI-számú készüléket használják. Az új SIM-kártya számát, illetve ebből adódóan az IMSI-számot és a telefonszámot a nyomozó hatóság a mobiltársaság megkeresése útján azonnal megtudhatja. Jól szemlélteti ezt a Fővárosi Törvényszék 25.B.539/2013/374. számú ítélete:

> „II. rendű vádlott a sértettel történő kapcsolatfelvételre és kapcsolattartásra ugyanazt a mobiltelefon-készüléket (IMEI ...) használta, amelyet (más hívószámú SIM-kártyákkal) ugyanilyen célra a jelen vádirat más vádpontjaiban írt bűncselekmények elkövetéséhez is felhasznált."

Az új hívószám vonatkozásában híváslista kérhető, illetve újabb sértettek deríthetők fel. Súlyos bűncselekmény esetén, ha a törvényi feltételek rendelkezésre állnak, bírói engedélyhez kötött leplezett eszköz lehallgatása is alkalmazható.

A fentiekből megállapítható, hogy a vádlott és a sértett mobiltelefonjának cellája közös lefedettségi területen volt található, és a helyzetük között párhuzamot lehetett megállapítani.

A cellainformációkból a terhelt(ek) vonatkozásában sokszor az alábbiakra lehet következtetni:

- az elkövetési helyszínen való jelenlét;
- hogyan mozog(tak) a helyszínen;
- az úgynevezett „munka" SIM-kártya saját telefonkészülékben való működtetése (például a bíróság „a cellainformációk általános részének bemutatásánál kifejtette, hogy mely esetben történt meg az, hogy

[175] Kúria Bhar.III.1.530/2019/23. számú ítélete.

a II. rendű vádlott neve II. r. vádlott az egyik, elkövetésekhez felhasznált »munka« SIM-kártyát a saját hívószámához használt telefonkészülékben üzemeltette");[176]

- a saját SIM-kártya „munka" telefonkészülékben való működtetése (például volt olyan eset, amikor a bíróság „a cellainformációk általános részének bemutatásánál kifejtette, hogy mely esetben történt olyan, hogy III. rendű vádlott neve III. r. vádlott a saját mobiltelefonszámához tartozó SIM-kártyát az egyik, elkövetésekhez felhasznált »munka« telefonkészülékben üzemeltette");[177]
- az egyes elkövetésekhez használt munkatelefonoknak és a saját telefonjának az állandó együttes mozgása;
- a kelő/fekvő pozíció megállapítása (például „az úgynevezett »kelő-fekvő«, tehát a reggeli legelső és az esti legutolsó cellák mindig ott jelentkeztek, tehát a telefon használója ez idő alatt is pont abban a szűk körzetben ébredt fel és aludt el. […] A vizsgált időszakokban mindkét SIM-kártya esetében ugyanazok a leggyakrabban használt földrajzi cellák [tehát leggyakrabban ugyanazon átjátszótornyokra jelentkeznek fel], ami kifejezetten igaz a telefonhasználó életvitelszerű tartózkodási helyét meghatározó úgynevezett »kelő-fekvő« celláknak [adott napokon a legkorábbi reggeli, illetőleg a legkésőbbi esti, tehát nagy valószínűséggel még/már a használó lakóhelyéről indított, vagy ott fogadott hívásokhoz tartozó] cellainformációk esetében is. A leggyakrabban igénybe vett átjátszótorony mindkét hívószám esetében azonos, de a többi ahhoz közel eső tornyon is jelentős az aktivitás");[178]
- a cellapozíció segítség lehet a valótlan tartalmú vallomás kiszűrésében is (az Egri Törvényszék Bf.273/2019/27. számú ítélete alapján vádlottak terhére értékelt bizonyítékok bizonyító erejét egy további tanú, személyl nyilatkozata sem tudná lerontani, hiszen a vádlottak bűnössége részben olyan objektív bizonyítékon is nyugszik, mint a vádlottak által használt mobiltelefonok cellainformációja, amely alapján megállapították, hogy az I. rendű vádlott a valótlan tartalmú jegyzőkönyvben szereplő

[176] Fővárosi Törvényszék 25.B.539/2013/374. számú ítélete.
[177] Fővárosi Törvényszék 25.B.539/2013/374. számú ítélete.
[178] Fővárosi Törvényszék 25.B.539/2013/374. számú ítélete.

időtartamban a jegyzőkönyv helyszínéül feltüntetett kótaji címtől eltérő helyen tartózkodott);[179]
– a híváslista – időbeli, illetve földrajzi helymeghatározással egybekötött – elemzésével lehetővé válhat a múltbeli releváns esemény megismerése és rekonstruálása.[180]

A mobilkommuikációs eszközök lefoglalása egyre több kérdést vet fel, főleg az IoT-rendszerekbe ágyazott eszközök tekintetében. Ha azt feltételezzük, hogy az eszközön biztonsági elemek vagy a titkosítás akadályoznák a *post mortem* (kikapcsolt állapotú) szakértés hatékonyságát, akkor szükséges az eszközt működésben – bekapcsolva – tartani, a hálózattól elszigetelten, biztosítva a tápellátást.[181]

A mobiltelefonokból a technológia fejlődésével egyre több adat nyerhető ki. Néhány releváns kinyerhető adat például: telefonkönyv; kimenő és bejövő híváslista; bejegyzések; naptár; fénykép-, hang- és videófelvételek; internethasználattal kapcsolatos adatok (böngészési előzmények, levelezés, letöltött fájlok és dokumentumok); GPS-adatok; vásárlási és pénzügyi adatok.[182]

4.4.3. A készletező adatgyűjtéssel – kommunikációs profillal – létrejött alapjog korlátozása

Az Alkotmánybíróság a 15/2022. (VII. 14.) AB határozatával (a továbbiakban: Abh.) megállapította, hogy az Országgyűlés mulasztásban megnyilvánuló alaptörvény-ellenességet idézett elő azáltal, hogy *az elektronikus hírközlésről szóló 2003. évi C. törvény* (a továbbiakban: Eht.) 157. § (2), (3) és (10) bekezdése, valamint a 159/A. §-a szerinti szabályozás nem áll összhangban az Alaptörvény VI. cikk (1) bekezdésében foglalt magánszféra tiszteletben tartásához való jogból, valamint a (3) bekezdésében rögzített személyes adatok védelméhez való jogból fakadó alkotmányos követelményekkel. Az Alkotmánybíróság ezért felhívta az Országgyűlést, hogy jogalkotói feladatának tegyen eleget.

Az Alkotmánybíróság álláspontja szerint a vizsgált szabályozásban készletező adatkezelés valósul meg, az adatgyűjtés egy alkotmányjogilag értékelhető

[179] Egri Törvényszék Bf.273/2019/27. számú ítélete.
[180] A Pécsi Ítélőtábla Bf.II.262/2011/10. számú ítélete.
[181] Simon–Gyaraki 2020: 137.
[182] Máté–Sándor 2019: 17–18.

célhoz a törvényszöveg alapján kellőképpen nem kötődő, a felhasználás körét túl tágan meghatározó adatszolgáltatás érdekében történik.[183] Egy úgynevezett kommunikációs profil állítható elő (a kapcsolattartására vonatkozó adatokra figyelemmel), amely szoros összefüggésben áll az érintett személyek magánszférájával, illetve emberi méltóságával, és ez következtetések levonását teheti lehetővé azon személyek magánélete vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében.[184]

Az Alkotmánybíróság továbbá utalt arra, hogy alkotmányos követelmény, hogy a „kérelmező jogosultként vagy az adatszolgáltatási kérelem előzetes, érdemi felülvizsgálójaként az eljárásban részt vegyen bíróság vagy független, a bírósági eljárás folyamatában nem érdekelt közigazgatási szerv".[185]

A telekommunikációs adatok a rendőrség bűnüldözési munkájában fontos szerepet játszanak, mivel az eredményes nyomozásban pótolhatatlanok. Az NMHH „Az elektronikus hírközlési piac fogyasztóinak vizsgálata" témakörben 2020-ban végeztetett egy háztartási felmérést, amely alapján a háztartások 94%-a rendelkezik mobiltelefon-előfizetéssel, és egy háztartás átlagosan 2,2 SIM-kártyát használ, pontosabban a háztartások 64%-ában van egynél több SIM-kártya.[186]

Az Alkotmánybíróság határozatában megállapítottak figyelembevételével az Országgyűlés által megalkotott jogszabály a rendészeti szervek bűnüldöző munkájára is hatással lesz.

[183] Abh. 27. pontja.
[184] Abh. 27. pontja.
[185] Abh. 41. pontja.
[186] Ariosz 2020: 33.

5. Az okosváros és az okosrendőrség

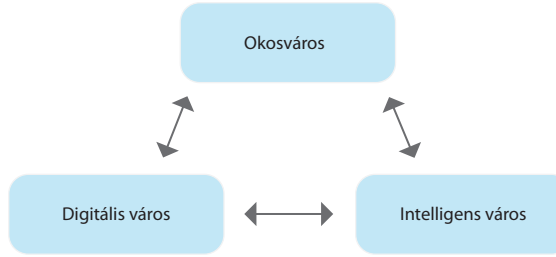
5.1. Az okosváros

Az *okosváros* fogalma pár évtizede jelent meg a köztudatban, amely koncepció célja eredendően a gyors kommunikáció, információáramlás és a fenntartható növekedés volt.[187] Az okosváros ismérvei megközelíthetők kutatói oldalról, valamint a jogalkotó által megfogalmazott definíció alapján. Az okosváros (smart city) elterjedt városfejlesztési fogalomnak számít napjainkban, és nagy népszerűségnek örvend.[188] Egyes nézőpontok szerint az okosváros alatt az infokommunikációs technológiák (IKT) teljes körű kiépítése és széles elterjedése értendő, fontosnak tekintik az IKT-rendszer kiépítését, amely alapvetően a számítógépes, illetve az informatikai technológiai hálózatra épít.[189]

Szendi és szerzőtársai szerint „az okos város komplex fogalom. Olyan város, amely innovatív stratégiát és megoldásokat alkalmaz annak érdekében, hogy javítsa a lakosság életminőségét, miközben hatékonyan használja a lakosság kreativitását és tudásbázisát."[190] A Brit Szabványügyi Hivatal (BSI) okosváros-definícióját az alábbiakban adja meg: „[a]z okos város olyan település, ahol megvalósul a fizikai, digitális és humán rendszerek hatékony integrációja az épített környezetben, hogy fenntartható, prosperáló és inkluzív jövőt biztosítson lakóinak."[191]

Számos megközelítéssel találkozhatunk a hazai és a nemzetközi irodalomban is, továbbá számtalan kérdés felmerül, hogy mitől lesz „okos" egy város, mi a célja. Az okosváros középpontjában az ember foglalt helyet, mivel a technológiának kell biztosítania a lehetőséget arra, hogy a városok hatékonyabban működjenek, élhetőbbek, innovatívabbak legyenek, és képesek legyenek helyt állni a polgárokért vívott versenyben.[192]

[187] *Mitől okos egy okos város* 2023.
[188] Árvai 2022: 16.
[189] Muhi B. – Vemić Đurković 2021: 114.
[190] Szendi–Nagy – Sebestyénné Szép 2020: 252.
[191] Ritó 2019: 235.
[192] Gyimesi – Somlyódyné Pfeil 2021: 59.



29. ábra: Az okosváros
Forrás: a szerző szerkesztése

A smart city kifejezésnek nincs egységesen elfogadott alkalmazása, különböző elnevezésekkel találkozhatunk, ezek közül a legelterjedtebbek az alábbiak:

- digitális város (digital city): az infrastruktúra kiépülését és az infokommunikációs szolgáltatások elérhetőségét foglalja magában;
- intelligens város (intelligent city): az információs és kommunikációs technológiai háttéren alapuló elektronikus szolgáltatások széles körét tartalmazza (e-kormányzat, e-tanulás, e-egészségügy);
- okosváros (smart city): az adatok gyűjtésére, feldolgozására épít, internet-alapú alkalmazások sokaságát jeleníti meg, amelyek egyre inkább integrált formában hasznosulnak.[193]

A digitális, intelligens és okosváros elnevezések egyben fokozatok is, amelyek egymást követő stratégiai fejlesztési fázisoknak is tekinthetők, és a magasabb fokozat képességei az alatta levő fokozat képességeit is magukban foglalják (29. ábra).[194]

A fogalmak ICT-megoldások alkalmazására építenek és a fenntartható városfejlesztéshez köthetők. Hazánk az okosváros fejlesztését tekinti követendő stratégiának.[195] Magyarország kormánya 2017. március 20-án a *Magyar Közlöny*ben megjelent 56/2017. (III. 20.) kormányrendeletben fogalmazta meg az okosváros fogalmát, eszerint az „okos város: olyan település, amelyik az integrált településfejlesztési stratégiáját okos város módszertan alapján készíti és végzi”, míg az okosváros módszertana:

[193] Sallai 2019: 54.
[194] Sallai 2019: 54.
[195] Rab–Szemerey 2018: 89.

„települések vagy települések csoportjának olyan településfejlesztési módszertana, amely a természeti és épített környezetét, digitális infrastruktúráját, valamint a települési szolgáltatások minőségét és gazdasági hatékonyságát korszerű és innovatív információtechnológiák alkalmazásával, fenntartható módon, a lakosság fokozott bevonásával fejleszti."[196]

Azonban az okosváros és az okosváros-módszertan fogalmai helyébe 2021 szeptemberében az alábbi rendelkezés lépett:

„okos város: olyan település vagy önkormányzatok közös tervezésében részt vevő település, amely integrált településfejlesztési stratégiáját okos város módszertan alapján készíti el és hajtja végre; […] okos város módszertan: települések vagy települések csoportjának olyan településfejlesztési módszertana, amely azok társadalmi, természeti és épített környezetét, digitális infrastruktúráját, valamint az állami ügyintézési szolgáltatás, közszolgáltatás, közműszolgáltatás, önkormányzati szolgáltatások és magánszolgáltatások elérhetővé tétele települési szolgáltatások körét, minőségét és hatékonyságát korszerű technológiák és módszerek alkalmazásával, fenntartható módon, a lakosság, a helyi társadalmi és gazdasági partnerek fokozott bevonásával fejleszti."[197]

A magyar okosváros-stratégiáknak kapcsolódniuk kell a kormány által elfogadott Digitális Nemzeti Fejlesztési Programhoz (DNFP), az Európai Digitális Menetrendhez (Digital Agenda for Europe), és egyetértésben kell lenniük a Nemzeti Infokommunikációs Stratégia (NIS) 2014–2020 célkitűzéseivel.[198]

Az okosváros stratégiáját a Lechner Tudásközpont Területi, Építészeti és Informatikai Nonprofit Korlátolt Felelősségű Társaság (a továbbiakban: Lechner Tudásközpont) által biztosított okosváros-módszertan alapján készítik el. A Lechner Tudásközpont 2017-ben kiadta a módszertani útmutatót, amelyet 2018-ban továbbfejlesztettek.

Az okosváros hat komponense, alrendszere:

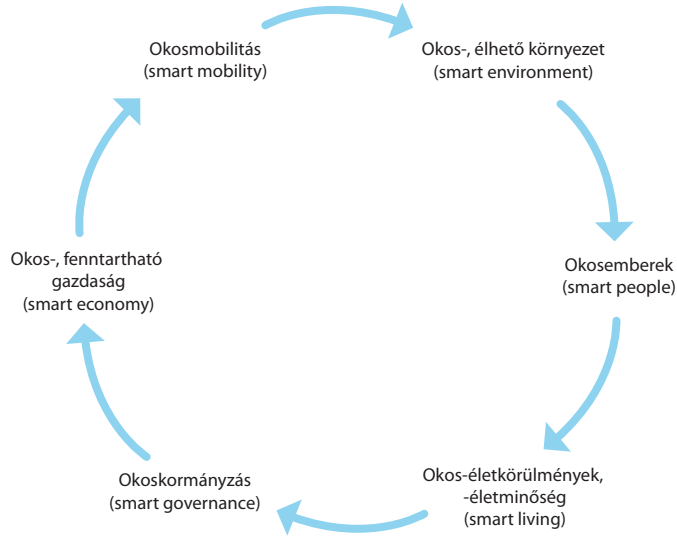
– okosmobilitás (smart mobility): szállítás, fuvarozás, multimodális elérhetőség, műszaki infrastruktúra;
– okos-, élhető környezet (smart environment): okosépületek, távlatos erőforrás-gazdálkodás, klímabarát város;

[196] 56/2017. (III. 20.) Korm. rendelet egyes kormányrendeleteknek az „okos város", „okos város módszertan" fogalom meghatározásával összefüggő módosításáról.

[197] 314/2012. (XI. 8.) Korm. rendelet a településfejlesztési koncepcióról, az integrált településfejlesztési stratégiáról és a településrendezési eszközökről, valamint egyes településrendezési sajátos jogintézményekről.

[198] Kovács 2018: 44.

– okosemberek (smart people): befogadás, integráció, iskolázottság, képzettség, kreativitás;
– okos-életkörülmények, -életminőség (smart living): jólét, biztonság, egészségi állapot;
– okoskormányzás (smart governance): online folyamatok, infrastruktúra, oktatási és kulturális, művelődési intézmények, egészségügy, közművek, hulladékgazdálkodás;
– okos-, fenntartható gazdaság (smart economy): e-gazdaság, innováció, termelékenység, hatékonyság, helyi és globális összeköttetések (30. ábra).[199]



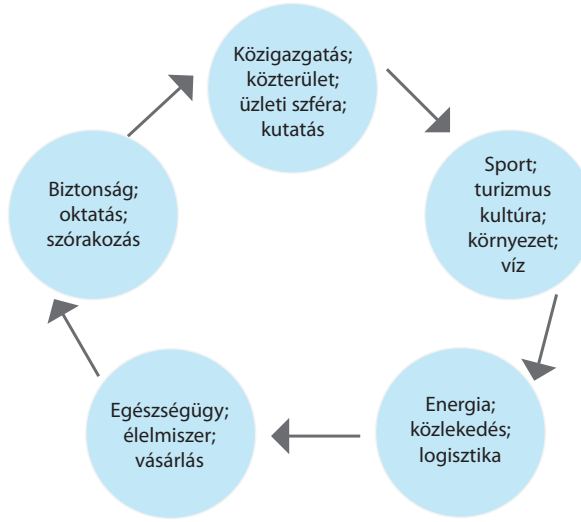
30. ábra: Az okosváros komponensei
Forrás: a szerző szerkesztése

A kormány megalkotta az okosváros-szolgáltatások összehangolt bevezetését és működését támogató szervezeti és tudásplatform létrehozásáról és működtetésétől szóló kormányhatározatot,[200] továbbá az okosváros-technológia helyszínéül

[199] Dobos et al. 2015: 28–36.
[200] 1024/2017. (I. 24.) Korm. határozat.

egy pilotprojekt keretében tesztalanynak Monor várost jelölte ki.[201] A kormány elrendelte „az Okos Város munkacsoport, illetve Okos Város és Okos Térség közigazgatási mintaprojekt létrehozását, valamint az Okos Város megoldások megjelenítését a kormánytisztviselői és köztisztviselői képzésekben".[202]

Az életünk számos területén jelent meg és elérhető az okosváros-alkalmazások sokasága, ezek a perifériák (területek) a közigazgatás; a közterület; az üzleti szféra; a kutatás; a sport; a turizmus; a kultúra; a környezet, a víz; a biztonság; az energia; a közlekedés; a logisztika; az oktatás; az egészségügy; az élelmiszer; a szórakozás és a vásárlás (31. ábra).[203]



31. ábra: Az okosváros-alkalmazások

Forrás: a szerző szerkesztése

[201] 2040/2017. (XII. 27.) Korm. határozat Monor település „okos város" funkcionalitással összefüggő fejlesztéseinek támogatásáról; 1165/2018. (III. 27.) Korm. határozat az „okos város" funkcionalitás magyarországi elterjedését szolgáló központi szolgáltatásplatform létrehozásával kapcsolatos intézkedésekről.

[202] 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről.

[203] Sallai 2018: 18–19.

Az okos területi alkalmazással az állampolgárok digitális adatokat hagynak maguk után, akár a közszolgáltatások használata során is, amikor ügyeiket az interneten intézik.

A korszerű települési ökoszisztéma szerves részét képezi a központi kormányzati közszolgáltatások (például e-közigazgatás, közműszolgáltatások) és magánszolgáltatások sokasága (például közlekedéstervezés és -szervezés, kulturális szolgáltatások, okosépület). Ezeken kívül egy település „okos" jellegét nem csak a település (önkormányzat) által nyújtott szolgáltatások határozzák meg.[204] Hazánkban is kialakult a digitális ökoszisztéma, amely nemcsak a felhasználók, hanem az eszközök milliót is összeköti, amelyek hálózatként kapcsolódnak egymáshoz, továbbá sok szolgáltatás válik elérhetővé a felhasználók számára.[205]

Az okosváros és az okosrendőrség számtalan ponton tud csatlakozni, azonban a kutatás szempontjából a közös fő kapcsolatot a digitális közigazgatás valósítja meg az elektronikus szolgáltatáson keresztül. Az okosváros lakói ügyeiket elektronikusan intézik, ehhez azonban szükséges a korszerű és hatékony digitális közigazgatás, egy elektronikus szolgáltatási háló. Az okosváros nyújtotta alkalmazások használatával számos digitális adatot hagyhatunk magunk után. Ugyanígy az elkövetők is sok digitális nyomot hagyhatnak maguk után, amelyek a raszter, illetve az e-nyomozás keretében kapcsolódási gócpontként hatékonyan segíthetik a bűnüldöző szervek munkáját. Az okosváros ökoszisztémájában megjelenő szolgáltatások olajának tekinthető a nemzeti adatvagyon, amely a digitális állampolgárság létrejöttében is domináns szerepet játszik. Az okosváros és az okosrendőrség kapcsolódási pontjait, mint egy információláncot, jól szemlélteti az *1.* és a *2. fejezet*.

5.2. Az okosrendőrség

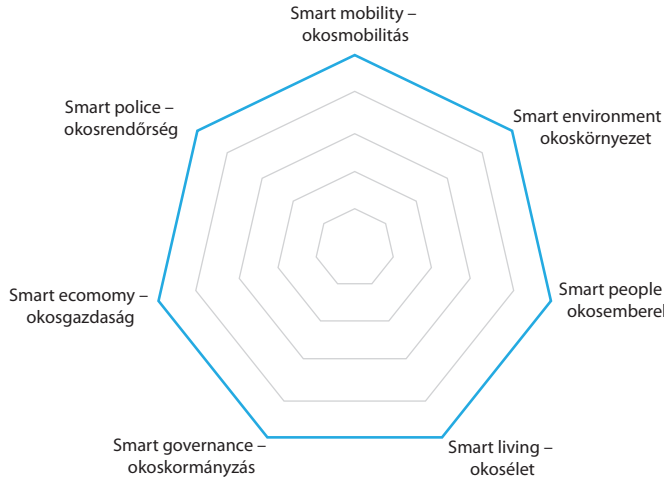
A digitális ökoszisztémának jelentős szerepe van a bűnüldözés és a közbiztonság terén, mivel az elektronikus eszközök és szolgáltatások elérhetősége, illetve a fejlett informatikai háttér elősegíti a bűnmegelőzéshez kapcsolódó tevékenységek

[204] 459/2021. (VIII. 4.) Korm. rendelet végső előterjesztői indokolása a településfejlesztési koncepcióról, az integrált településfejlesztési stratégiáról és a településrendezési eszközökről, valamint egyes településrendezési sajátos jogintézményekről szóló 314/2012. (XI. 8.) Korm. rendelet módosításáról.

[205] *Nemzeti Infokommunikációs Stratégia 2014–2020* 2014: 16.

hatékonyságát és egyben eredményességét, valamint csökkenti a bűnüldöző szervek reakcióidejét, illetve gyorsítja az igazságszolgáltatás működését.[206]

Az okosváros alapjának kellene lennie az okosrendőrségnek, mivel az okosváros biztonságát, működését és fejlődését is akadályozhatja annak hiánya (32. ábra).



32. ábra: Smart city

Forrás: a szerző szerkesztése

Az állampolgároknak elektronikusan, akár otthonról is el kell érniük a rendőrséget. Ezt szolgálja a rendőrség ügyintézési portálja.

5.2.1. A rendőrségi ügyintézési portál

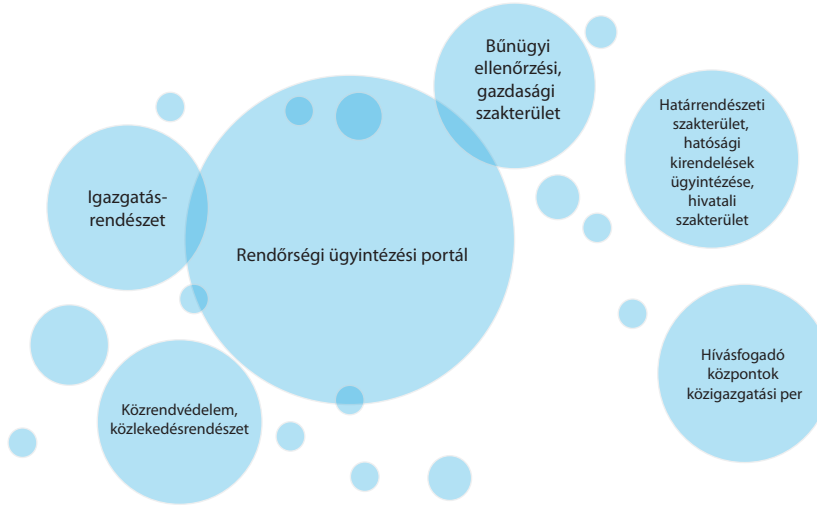
A 21. század technikai fejlődését követi a rendőrség is, folyamatos fejlesztésekkel lehetővé teszi az eljárások gyorsítását és az adminisztrációs terhek csökkentését. A magyar rendőrség ügyintézési portálja otthonról is elérhető az ugyintezes.police.hu oldalról. A portálon egyszerűen el lehet indítani a legtöbb rendőrségi ügyet, vagy a folyamatban lévőket az interneten lehet befejezni. A felmerülő

[206] *Nemzeti Infokommunikációs Stratégia 2014–2020* 2014: 16.

költség pedig bankkártya használatával is rendezhető.[207] A rendőrség az elektronikus ügyintézést az ügyintézési portál felületén elérhető online kitölthető űrlapok (inNOVA űrlapok) segítségével teszi lehetővé.

A rendőrség ügyintézési portálján több ügyintézési típus (szakterület) választható (33. ábra):

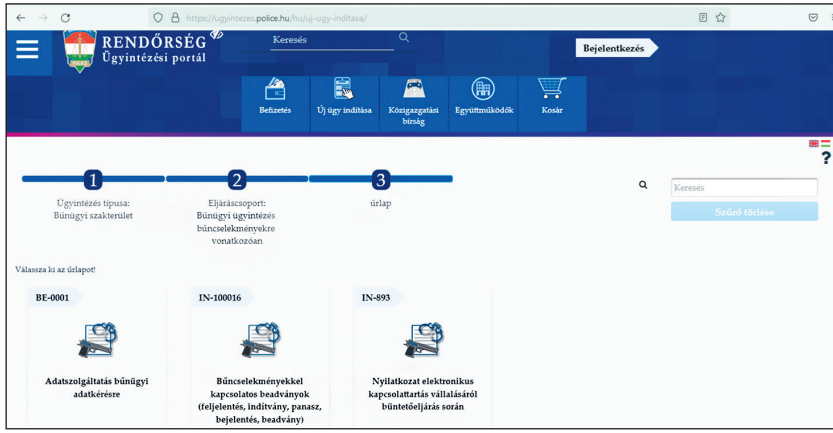
- bűnügyi szakterület;
- ellenőrzési szakterület;
- gazdasági szakterület;
- határrendészeti szakterület;
- hatósági kirendelések ügyintézése;
- hivatali szakterület;
- hívásfogadó központok;
- igazgatásrendészet;
- közigazgatási per (bírósági felülvizsgálat);
- közlekedésrendészet;
- közrendvédelem.



33. ábra: Rendőrségi ügyintézési portál

Forrás: a szerző szerkesztése

[207] *Police.hu* weboldal Ügyintézési portálja.



34. ábra: Rendőrségi ügyintézési portál

Forrás: Police.hu weboldal, Ügyintézési portálon, új ügy indítása

A szakterületeken belül többféle űrlap található, ezek egyikének kitöltésével elindítható az eljárás. A bűnügyi szakterületi ikonra lépve például a bűncselekményekkel kapcsolatos beadványok (feljelentés, indítvány, panasz, bejelentés) közül választhatunk (34. ábra).

A beadványra lépve a rendszer az ügyfélkapun keresztül azonosítja az állampolgárt, majd ezt követően leírhatja például a feljelentés szövegét, és elküldheti a kiválasztott hatóságnak.

Az állampolgárok az ügyfélkapu folyamatos fejlesztésével egyre több ügyet tudnak online intézni, ami növeli az elektronikusan rögzített digitális nyomok számát. Az ügyfél-regisztrációs szerv az ügyfél hozzájárulása nélkül a rendőrség hatáskörébe tartozó bűncselekmények megelőzése, illetve megszakítása, továbbá személyvédelmi és létesítménybiztosítási feladatai ellátása céljából megadhatja az ügyfél általa kezelt adatait.[208]

A rendőrség ügyintézési portálja jelentősen megkönnyítheti egyes esetekben az állampolgárok ügyintézését, azonban figyelembe kell venni, hogy sok esetben az elektronikus ügyintézés nem tudja kiváltani a személyes megjelenést a hatóságnál (a rendőrségnél).

[208] 2015. évi CCXXII. törvény 32. § (7).

A technikai fejlődés a rendőrség munkáját is jelentősen segíti például az igazoltatásnál, amely során a jogszabályban meghatározott esetben arcfelismerés, arcképelemzés történhet. A Rendőrségről szóló 1994. évi XXXIV. törvény 29. § (4) bekezdése szerint

> „a személyazonosság igazolásának megtagadása esetén az igazoltatott a személyazonosság megállapítása céljából feltartóztatható, a személyazonosság megállapításának sikertelensége esetén – ha a személyazonosság megállapítása más módon nem biztosítható vagy hitelt érdemlően nem bizonyítható – a személyazonosság megállapítása céljából az igazoltatottról fényképfelvétel készíthető".

Az így

> „készített fényképfelvételt az erre a célra rendszeresített eszköz alkalmazásával az arcképelemzési nyilvántartásról és az arcképelemző rendszerről szóló törvényben szabályozott automatizált összehasonlítás igénybevételével, az ott meghatározott szabályoknak megfelelően – személyazonosság megállapítása céljából – a helyszínen ellenőrizni lehet."[209]

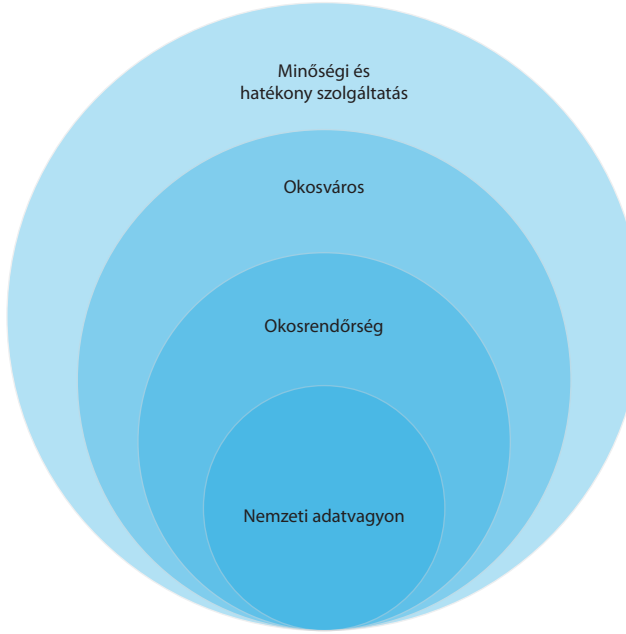
Az okosrendőrség vonatkozásában is szükség van az e-nyomozási ökoszisztéma kialakítására a még gyorsabb információáramlás érdekében. Az e-nyomozási ökoszisztémához köthető kriminalisztikai adatokat, nyilvántartásokat, modern eszközöket az *1.* és a *2. fejezet*ben tárgyaltam részletesebben.

Az okosrendőrségnek az okosváros felépítése elengedhetetlen részének, elemének kell lennie: egy olyan állami szervezetnek, amely feladatainak ellátása során korszerű és innovatív információtechnológiákat alkalmaz, képes a digitalizáció, a hálózatkutatási elemzések és a mesterséges intelligencia nyújtotta lehetőségeket felhasználni, azaz alappillérként kell funkcionálnia. Az okosrendőrség egyik alapforrását pedig a nemzeti adatvagyonnak kellene képeznie (35. ábra).

Egy okosváros-stratégia vagy -módszertan kialakításában nélkülözhetetlen szerepet kell képviselnie az okosrendőrségnek, mivel hiánya megingatja az okosváros működését, arra nézve negatív következménnyel járhat.[210]

[209] 1994. évi XXXIV. törvény a Rendőrségről 29.§ (4) (4a).

[210] Berki–Nyitrai 2021.



35. ábra: Okosváros – okosrendőrség
Forrás: a szerző szerkesztése

5.3. A mesterséges intelligencia létjogosultsága

A mesterséges intelligencia rövidítésére hazánkban az (MI) betűszót használják, míg az angol kifejezés az Artificial Intelligence (AI).[211] A mesterséges intelligencia a biztonságtudomány forenzikus területén alkalmazható az elkövetői csoport és profil megrajzolására; felderítésre, kapcsolati háló feltérképezésére; kép, hang, szöveg, mintázatok felismerésére; nyomkövetés; haladási útvonal predikciójára egyaránt, illetve kiemelendő felhasználási területe az arcfelismerés.[212]

[211] Mandić 2022: 34.
[212] Kollár 2019: 50.

Az MI meghatározására többféle álláspontal lehet találkozni. Dobó és Gyaraki szerint

> „az (MI) a gépek emberhez hasonló képességeit jelenti, mint például az érvelés, a tanulás, a tervezés és a kreativitás lehetőségét. Az MI lehetővé teszi a technika számára, hogy érzékelje környezetét, foglalkozzon azzal, amit észlel, problémákat oldjon meg, és konkrét cél elérése érdekében tervezze meg lépéseit."[213]

Az Európai Bizottság megfogalmazása alapján „a mesterséges intelligencia intelligens viselkedésre utaló rendszereket takar, amelyek konkrét célok eléréséhez elemzik a környezetüket és – bizonyos mértékű autonómiával – intézkedéseket hajtanak végre".[214] A Bizottság a mesterséges intelligencián alapuló rendszereket két csoportra osztja:

- kizárólag szoftveralapú rendszerekre, amelyek a virtuális világban működnek (például hangasszisztensek, képelemző szoftverek, keresőprogramok, hang- és arcfelismerő rendszerek);
- a hardvereszközökbe is beépíthető mesterséges intelligenciára (például fejlett robotok, autonóm járművek, drónok és a dolgok internetéhez kapcsolódó alkalmazások).[215]

Napjainkban a rendőrség már napi szinten alkalmazza a mesterséges intelligenciát, azok közül is az arcképfelismerő szoftverek a legelterjedtebbek. A rendőrségen belül használnak még napi szinten videóelemzési szoftvereket, amelyek mesterséges intelligenciával támogatottak, azonban sok esetben fordulnak megkereséssel a Nemzeti Szakértői és Kutató Központ Arcképfelismerő Elemző Osztályához.

A mesterséges intelligenciát alkalmazzák az egészségügyben és a közigazgatásban, illetve más területen is, de a rendőrség szempontjából ez a két bázis adja a legtöbb adatot. A közigazgatás területén a kiosk oszlopok gyorsítják a digitalizációt, míg az egészségügyben az EESZT teszi ezt lehetővé. A mesterséges intelligencia segít a világ legnagyobb kihívásainak megoldásban. Ezek során rengeteg digitális adat, illetve nyom keletkezik, amelyeket szintén tud hasznosítani a rendőrség az e-nyomozás keretében, amely a bűnügyi digitális ökoszisztéma létrejöttét segíti elő.

[213] Dobó–Gyaraki 2021: 67.
[214] Európai Bizottság 2018: 1.
[215] Európai Bizottság 2018: 1.

A mesterséges intelligencia fejlesztése hatalmas mennyiségű adatot igényel, amely a rendőrség számára egyrészt meríthető a közigazgatásból és az egészségügyből, illetve a saját adatbázisából is. A Magyarországon keletkezett (rendészeti) adatok óriási mennyiségére utal, hogy 2019-ben összesen 107,6 millió iratot tartottak nyilván a NAV elektronikus iratnyilvántartást végző alkalmazásai, ami az előző év azonos időszakához képest 5,6%-os növekedést jelent.[216] A NAV-nál óriási mennyiségű, jelenleg 7,5 petabyte-nyi adat keletkezik, és ez évről évre nő. Ennek kezelésében a mesterséges intelligencia használata jelenti a jövőt, mivel segítségével hihetetlen gyorsasággal lehet majd kiszűrni a gyanús üzleti számokat.[217] A rendőrség tekintetében a Robotzsaru NEO adatbázis jelenleg több mint 55 terabyte-nyi adatot tartalmaz.[218]

Az MI-ökoszisztéma kialakulásával számos technológiai előny jelenik meg:

- a polgárok részére (jobb egészségügyi ellátás, jobb közszolgáltatás);
- a vállalkozók részére (szolgáltatások új generációját fejlesztik ki);
- a közérdekű szolgáltatások részére (a bűnüldöző hatóságokat megfelelő eszközzel látják el az emberek védelme érdekében, így például segíthetnek az online terrorista propaganda azonosításában, a gyanús tranzakciók felderítésében, tiltott anyagok vagy termékek azonosításában).[219]

A mesterséges intelligencia alkalmazásával a hatékonyság, az adatfeldolgozás és -értékelés gyorsasága növelhető, valamint létrejöhet a *real time* üzemmódban történő reagálás a felhasználók számára úgy, hogy az emberi tevékenységet kiváltja.[220] Tekintettel arra, hogy a mesterséges intelligencia jelentős hatást gyakorolhat a nyomozás kimenetelére és annak eredményességére, szükséges, hogy kiépüljön az abba vetett bizalom a hatóság tagjainak részéről.

A mesterséges intelligencia az egyik legújabb tudományterületnek is tekinthető, amely gyors ütemben alakítja át a világunkat, megváltoztatja a mindennapokat, azonban az emberek és az intelligens gépek közötti kapcsolat kihívást jelent számos területen az államok működése és a jogi szabályozás szempontjából az Európai Unió és a tagállamok szintjén egyaránt.[221]

[216] *NAV évkönyv 2019* 2020.
[217] Károly 2020.
[218] Az Országos Rendőr-főkapitányság (ORFK) Hivatalának válasza a megkeresésre.
[219] Európai Bizottság 2020a.
[220] Nagy 2021: 226.
[221] Ritó 2021: 45.

6. Modern technikai eszközök és programok a kriminalisztikában

A modern technikai eszközök használata több oldalról segítheti a bűnüldöző szervek munkáját:

- hozzásegíthet a múltbeli releváns esemény megismeréséhez;
- megkönnyítheti a bűnös tevékenység felismerését;
- elősegítheti az adatelemző és -értékelő munkafolyamatot.

6.1. Az infrakamera és a hőkamera

Az infrakamera fekete-fehérben rögzíti a tárgyakról visszavert infravörös sugarak által kirajzolt képet.[222] Azok a tárgyak, amelyek látható fényben világosak, az IR-képen sötétek, amelyeknek sötétnek kellene lenniük az infraképen, azok pedig világosan fognak fényleni.[223] Itt szükség van inframegvilágítókra. Azonban a technikai fejlődésnek köszönhetően napjainkban a megfigyelésre szánt kamerák jelentős része rendelkezik inframegvilágítással, amely az éjjellátáshoz szükséges.[224]

A hőkamera esetében inframegvilágítóra nincs szükség, mivel a hőkamerák a tárgyak által kibocsátott termikus sugárzást detektálják, pontosabban a testek által kibocsájtott hőt érzékelik, illetve minél melegebb egy adott tárgy, annál több hősugarat bocsájthat ki magából.[225]

A hőkamera alkalmazásának kriminalisztikai lehetőségei:

- a kriminalisztika területén hőmérséklet-változással járó nyomok kimutatása céljából is alkalmazzák tárgyak használatának az ellenőrzésére (például hőkamerás felvétel készíthető az inkriminált helyen található két székről, és ahol az elkövető ült, ott erősebb lesz a hősugarak kibocsátása);

[222] Balláné Füszter 2020.
[223] Balláné Füszter 2019: 83.
[224] *Infra kamera…* [é. n.].
[225] Balláné Füszter 2017.

– személykutatásban, például eltűnt (veszélyeztetett) személyek[226] keresésében, azáltal, hogy a fellelhetőségük helyéről információval szolgálhat, akár éjszaka, akár ködös, esős időben rossz látási viszonyok között is;
– a személyazonosításban: a hőkamera az arc felszínéről érkező hősugárzást érzékeli, illetve méri, és az eszközhöz csatlakoztatott számítógép a beérkező adatokat színes képekké konvertálja, majd hőtérkép formájában megjelenik a monitoron, s mindez kontaktmentesen történik;[227]
– az államhatár őrizetében a stabil és mobil hőkamerák, illetve kézi hőkamerák alkalmazhatók,[228] a hőkamerák határrendészeti célok esetén például a migrációban részt vevő személyek felderítésére is alkalmazhatók;[229]
– a katasztrófavédelmi egységeknél a hőkamera alkalmazásával idő nyerhető. A tűzeseteket követően a területek átvizsgálásában, valamint az ott megbújó parazsak felkutatásában egy hőkamerával felszerelt drón segítség lehet, hiszen hatékonyabb és gyorsabb, mintha a végrehajtó személyi állomány közreműködésével történne az átvizsgálás;[230]
– a vagyont érintő kényszerintézkedéseknél, például a (ház)kutatás során a rejtekhelyek felderítésében is segítségül szolgálhat a falba épített csövek, tárgyak, üregek, vájatok stb. helyének a meghatározásával;
– a bűncselekmény helyszínén vagy egy parkolóban gépkocsiban bujkáló személy esetén is segítségül szolgálhat a hőkamera a gépkocsi használatának ellenőrzésére.

Hollandiában Utrecht városában használják a ThermiCam nevű speciális hőkamerát, amelynek az a feladata, hogy az útkereszteződésekben segítsen megkülönböztetni a motoros járműveket és a bicikliseket. Így egy biciklis jelenlétét az útkereszteződést vezérlő közlekedési lámpának külön tudja jelezni, amely ennek megfelelően tudja vezérelni a zöld jelzést.[231]

[226] Veszélyeztetett eltűnt: „az eltűnt valamely okból (tipikusan a koránál, az állapotánál fogva) nem képes az őt fenyegető veszélyt felismerni és/vagy elhárítani.” Lakatos 2005: 153.
[227] Balla 2019: 120–123.
[228] Kui 2016: 115.
[229] Papp 2020: 336–337.
[230] Kiss–Major 2021: 296.
[231] Vida 2020: 43.

6.2. A 3D lézerszkennerek

A 3D lézerszkennerek olyan eszközök, amelyek a tárgyakat, térrészleteket vagy objektumok egyes részeinek formai jellemzőit digitalizálják, és 3D-s adatállomány formájában rögzítik azok geometriai jellemzőit úgy, hogy nem érintik meg azokat.[232] Ez azért fontos, mert a szemle alkalmával elkerülhető a kontamináció, így nem szennyeződnek vagy semmisülnek meg a nyomok vagy az anyagmaradványok.[233]

A lézerszkenner működésére jellemző, hogy pár másodperc alatt több millió lézersugarat bocsát ki, amelyek segítségével megméri a műszer és a térbeli objektum pontjai közti távolságot, az így létrejött adathalmazból/térbeli pontfelhőből pedig egy szoftver segítségével kinyerhetők a vizsgált objektum geometriai adatai.[234]

A térszkenner használható az alábbi célokra: háromdimenziós bejárható modell létrehozására; metszetek készítésére; pontos és részletes dokumentálásra; rekonstrukcióra; helyszín biztonságos felmérésére; tetszőleges mérések elvégzésére; valamint geometriailag szabálytalan depóniák térfogatszámítására. A kézi szkenner alkalmazásának területei lehetnek például: a tárgyak (ruházat, elkövetés eszköze stb.) méretpontos rögzítése és dokumentálása; holttestek rögzítése, dokumentálása a halottszemle és a boncolás alkalmával.[235]

A szkennerek közül kiemelendő a 3D térszkenner (például Leica RTC 360; Leica BLK360, Spheron VR; Leica P20), valamint kézi szkenner (például Faro Freestyle 3D; Artec Spider 3D). A rendőrség is használja, illetve használni kívánja a tér- és kézi szkennereket. Például a Készenléti Rendőrség bűnügyi technikai célú eszközöket szeretne elérni közbeszerzés formájában.[236] A közbeszerzés esetén sajnos elmondható, hogy mire megérkezik a kívánt/megrendelt termék, a piacon már megjelenik egy újabb technikai eszköz, amely szintén segíthetné a rendőrség munkáját. Ez is mutatja, milyen rohamosan fejlődnek a technikai eszközök: elképzelhető, hogy a megrendelést követő napon már egy fejlettebb, nagyobb tudású technikai termék jelenik meg a piacon.

[232] Balláné Füszter 2019: 83.

[233] „Kontamináció: a nyomok és anyagmaradványok nemkívánatos beszennyezését, ill. összekeveredését jelenti, amely bekövetkezhet külső, objektív tényezők által, valamint emberi (célirányos vagy mulasztásos) tevékenységek következményeként is.” Boda 2019: 334.

[234] Balláné Füszter 2019: 83.

[235] Pásztor 2016: 66.

[236] Közbeszerzési Hatóság 2021.

A bűncselekmény helyszínének szemléjén napjainkban kiemelkedő szerepet kap a térszkenner (például a Leica P20 típusú), amely néhány perc alatt képes megmérni több millió pont 3D koordinátáját, körülbelül 150 méteres távolságig, továbbá az eszköz közel 360 fokban képes körbeforogni és színes, virtuális háromdimenziós felvételt készíteni.[237] A szemlén a technikusok munkáját segíti a kézi szkenner (például Artec 3D), amelynek az az előnye, hogy a hagyományosnak tekinthető megmintázási eljárásokkal szemben a háromdimenziós felvételt úgy készíti el, hogy az elváltozáshoz, helyszíni nyomhoz nem kell hozzáérni, csak közel tartani hozzá az eszközt, illetve az is előny, hogy a mérés akárhányszor meg is ismételhető.[238]

A lézerszkenner előnye a hagyományos fényképfelvételekkel szemben, hogy minden részletet méretarányosan rögzít – még az irrelevánsnak tűnőket is. Ez azért fontos, mert a későbbiekben a hatóságnak szüksége lehet olyan információra, amely a helyszíni szemle alkalmával még nem tűnt fontosnak, de ismerete az ügy felderítésének folyamatában jelentős lehet.[239]

6.3. A 3D nyomtató

A 3D nyomtatás olyan gyártófolyamat, amely során egy számítógép által létrehozott digitális fájl alapján szilárd tárgyak, termékek állíthatók elő.[240] Számos területen több mint harminc éve létezik a 3D nyomtatási technológia, amelynek létrejöttekor a cél a gyors és költséghatékony prototípusgyártás volt.[241]

A 3D nyomtatás az ipar és az élet számos területén jelen van mint dinamikusan növekvő technológia. Alkalmazásának fontosabb területei például: ipari és üzleti szektor; autógyártás; repülőgépgyártás, kormányzati, katonai, oktatási, orvosi szektor; fogyasztói és építészeti szektor.[242] Az egészségügy területén sok helyen például a szájsebészeti vagy az ízületi implantátumok egyedi gyártására már rutinszerűen alkalmazzák a 3D nyomtatás technológiáját.[243] A 3D szkennelés és a 3D nyomtatás összekapcsolása egy egységes rendszer megalkotását teszi

237 Rucska 2017: 40.
238 Rucska 2018.
239 Rucska 2018.
240 Robin [é. n].
241 Horváth–Maróti 2018: 74.
242 Gajdács–Szűcs 2020: 103–104.
243 Kocsis 2019: 100.

lehetővé, mivel egyrészt egy átfogó megoldást kínál a bűnjelek digitális archiválására, másrészt lehetővé válhat pontos másodpéldányoknak a létrehozása is.[244] A 3D felvételek nemcsak a monitoron jelennek meg, hanem a 3D nyomtatóval meg is „mintázhatók".[245]

A 3D nyomtatás új lehetőséget kínál mind a bűnüldözés, mind a bűnözés terén. A technológia fejlődésével új elkövetési módok jelennek meg, s ez kihívás elé állítja a hatóságokat. A bűnüldözés terén az elemző-értékelő munkafolyamatot erősítheti, egyben a múltbeli releváns esemény megismerésében is eszközként szolgálhat.

6.4. A talajradar és a fémkereső

A talajradar segítségével a föld alatti tárgyak meghatározhatók, s képes a nem fémből készült tárgyak felkutatására, amely roncsolásmentesen, geofizikai módszerrel valósul meg.[246]

A talajradar által kibocsátott jelek folyamatosan visszaverődnek, és a műszer jelzi használójának a talaj szerkezetétől eltérő tárgyak, anyagok (anomáliák) által visszavert eltérő hullámokat.[247] A talajradar az objektumok felett elmenve néhány centiméteres pontossággal meghatározza a földben található tárgyak helyét és mélységét.[248] Bűncselekményből származó elásott tárgyak vagy egy holttest keresése során az eszközt alkalmazhatja a nyomozó hatóság is. Azonban a felderítés hatékonysága és eredményessége függ a talaj jellemzőitől: a talajtípustól, a konzisztenciától, a nedvességtartalomtól.[249]

A talajradar segítségével rejtekhelyek is felkutathatók – ezt példázza az az eset is, amikor az elkövető a heroint a kertben ásta el. Az eszköz használatával a nyomozók közel 5 kilogramm kábítószergyanús anyagot – az előzmények ismeretében feltehetően heroint – találtak elásva, az anyag vizsgálatára szakértőt rendeltek ki.[250]

[244] Papp 2017.
[245] Rucska 2018.
[246] Kutassy 2021: 104.
[247] Mama–Gárdonyi 2016: 71.
[248] Kutassy 2021: 104.
[249] Kovács–Ember 2021: 13.
[250] Készenléti Rendőrség Nemzeti Nyomozó Iroda 2020.

A fémkereső a föld felszínén vagy az alatt minimálisan elhelyezkedő fémtárgyak megtalálására szolgál, így például alkalmazható bűncselekmény esetén lőfegyver vagy annak alkatrészei, lövedékek felkutatására, amelyek lehetnek akár a bűncselekmény helyszínén vagy azon az útvonalon, esetleg környezetben, ahol az elkövető mozgott, illetve menekült. A fémkereső a hatóságok munkáját is segítheti, azonban az elkövetők is használják, hogy régészeti leleteket találjanak és azokat értékesítsék. A fémkereső műszerek technikai fejlődése és elterjedése okán az ezredfordulótól kezdve különösen nemzetközi és egyben nemzeti problémává vált a régészeti lelőhelyek, a kulturális örökség értékeinek fosztogatása, aminek következtében az eltulajdonított leletek vagy közvetlenül magángyűjtőkhöz, vagy az illegális műkincspiac hálózatába kerültek.[251] A fémkeresőt sok esetben nem a jogszabályban meghatározott feltételeknek megfelelően használják, amit az alábbi eset jól szemléltet.

> „A Kaposvári Járási és Nyomozó Ügyészség folytatólagosan, kisebb értékre, régészeti leletre elkövetett lopás bűntette miatt emelt vádat egy kaposvári férfival szemben, aki két és fél évig járta fémdetektorral a somogyi kistelepülések szántóföldjeit, ahol több száz régi pénzérmét és egyéb használati tárgyakat is talált.
> A vádlott az ajándékba kapott fémkeresővel engedély nélkül kutatott régészeti leletek után több kistelepülés, például a Hetes, Orci, Somodor, Zimány és Magyaratád melletti szántóföldeken. Kutatásai rendszerint sikerrel jártak, ugyanis több száz, régészeti leletnek minősülő tárgyat talált. Pénzérmeket, köztük az ókorból I. és II. Constantinus, Commodus császárok korából, a sisciai verdéből származó érméket, az Árpádházi uralkodók korából II. András dénárt, vagy a későbbi, középkorból származó Hunyadi Mátyás, II. Lajos, illetve II. Mátyás nevével fémjelzett dénárokat is. A szántóföldek felszínén őskorból származó magkövekre és pattintékokra is rálelt, valamint különféle ékszerekre, állatfigurákra.
> A régészeti leletek a magyar állam tulajdonát képezik, a vádlott azonban a megtalált tárgyakat hazavitte, és rendszeresen egy internetes eladási portálon árulta. Ez lett a veszte, mivel az örökségvédelmi hatóság munkatársai a hirdetések alapján tettek feljelentést, így indulhatott meg a nyomozás."[252]

6.5. A drón

A pilóta nélküli légi jármű (angolul: Unmanned Aerial Vehicle, UAV; a továbbiakban: drón) fogalmát a légi közlekedésről szóló 1995. évi XCVII. törvény 71. § 35. pontja határozza meg, amely alapján drónnak minősül „bármely olyan légi jármű,

[251] Hudák 2022: 78.
[252] Magyarország Ügyészsége 2018.

amely a fedélzetén tartózkodó pilóta nélkül üzemel vagy amelyet ilyen üzemmódra terveztek, és amely önálló vagy távirányítással történő üzemelésre képes".

A drón alkalmazásának lehetőségei a technológia fejlődésével bővülnek, mivel egyre fejlettebb, kompatibilisebb eszközöket gyártanak, illetve egyre több olyan érzékelő, szenzor jelenik meg, amely drónra szerelhető. A drón a rendészeti munkát széles körben segítheti az alábbiakban:

- tömegrendezvények (például sportesemények, tüntetések) alkalmával a rendőri erők számára támogatást nyújthat a beavatkozásoknál, kiürítési feladatok tervezésében és irányításában, a jelenlévők tájékoztatásában, törvénysértő cselekményt végrehajtó személyek felismerésében, a kiemelést megelőzően pedig a figyelem elterelésében, valamint a helyszínt elhagyó személyek követésében;[253]
- az arcelemző programok segítségével eltűnt vagy körözött személyek felkutatása is lehetővé válhat akár a városi környezetben, tömegrendezvényeken;[254]
- ha az eltűnt személy tartózkodási helye szélsőséges sziklás-hegyes vonalakon van, ami az ember által nehezen megközelíthető, a drónnal lehetővé válhat a keresés. A drónra több érzékelő helyezhető, egyrészt például hőkamera a személy megtalálása céljából, másrészt mikrofonnal is felszerelhető, amely a kommunikációt teszi lehetővé. Ha például egy földrengésnél, árvíznél több személy megközelíthetetlen, akkor a drón segítheti az ellátásukat élelemmel, gyógyszerrel, valamint információ nyerhető a személyek állapotáról is;
- a szökött elítélt vagy kényszerintézkedés alatt álló személy felkutatásában;
- a drónon elhelyezhető fémtartalmat detektáló aknakereső műszer és hőkamera, amely használható akna felderítéséhez, illetve hatástalanításához;[255]
- helyszínek feltérképezésében (bűncselekmények helyszínei, de akár katasztrófa sújtotta területeken is);
- a bűncselekmény helyszínén a szemle alkalmával az esetleges megközelítési, menekülési útvonalak megállapításában;[256]

[253] Németh–Pápics 2020: 7–8.
[254] Németh–Pápics 2020: 8.
[255] Kovács–Ember 2021: 17, 19.
[256] Vigh 2018: 101.

– friss ásások (emberölés esetén „sírok”) felkutatására. Valamikor egy egyszerű felvételen már látható, hogy a kérdéses területen valamit elástak, mivel következtetni lehet a növényzet hiányosságából vagy a földfelület színéből. Azonban speciális hőkamerát is lehet használni, amely a kérdéses területet jobban jelzi;
– a katasztrófavédelemi feladatok megoldását több oldalról is támogathatja: a kutató-mentő feladatok végrehajtásában; kár- vagy állapotfelmérési, illetve tűzfelderítési feladatok végrehajtása során; megközelíthetetlen területek átvizsgálásakor; helyszíni mintavételezésre; vegyi, biológiai, illetve nukleáris szennyezéssel járó balesetek esetén a környezetbe kiszabaduló veszélyes gázok, folyadékok koncentrációjának és terjedésének folyamatos nyomon követésére; árvízvédelmi létesítmények, töltések, gátak vagy sérült közlekedési infrastruktúra állapotának felmérésére;[257]
– a drón által készített felvétel a büntetőeljárás (nyomozás) során tervezett feladatokban is segítségül lehet: kihallgatásra való felkészülés előtt emléknyomok felidézésében; a bizonyítási kísérletre való felkészüléskor a helyszín rekonstrukciójában; a helyszíni kihallgatást megelőző előzetes kihallgatás során nyilatkozott információk ellenőrzésében; nagy kiterjedésű helyszínek fotózásában, kutatást vagy elfogást megelőzően az objektum feltérképezésében;
– a kutatás vagy elfogás tervezésekor a TakarNetben (földnyilvántartásban) szereplő objektum adatai összevethetők a videófelvételekkel, vagy a műholdas térképeken megállapítottak összehasonlíthatók a helyszínen vagy tágabb környezetében készített felvételekkel;[258]
– a magyar rendőrség egyre gyakrabban alkalmazza a drónt a szabálysértők kiszűrésében, a közlekedési szabályok betartásának ellenőrzésében. Az ilyen jellegű akció célja egyrészt a közúti közlekedési balesetek megelőzése, másrészt a kiemelt közlekedési szabályszegések visszaszorítása.[259]

Az eszköz pilótát nem igényel, így meghibásodás, lezuhanás esetén nem kell a pilóta személyi sérülésével számolni. Továbbá fontos előnye, hogy az irányító távközlési kommunikáció meghibásodása esetén a drón a GPS-koordinátákat

[257] Németh–Pápics 2019: 4–5.
[258] Nyitrai 2020b: 101–102.
[259] Zala Megyei Rendőr-főkapitányság 2022.

használva képes a kiindulási helyre visszatérni.[260] A dróninfrastruktúra kialakításánál a lehetséges kibertámadásokat szem előtt kell tartani.[261]

A drónt nemcsak a rendészet területén lehet alkalmazni, hanem az élet számos más területén is, például a mezőgazdaságban, a kereskedelemben vagy az egészségügyben.

6.6. Az UFED

A Universal Forensic Extraction Device (a továbbiakban: UFED) elnevezésű eszköz kifejlesztésének célja a nagy mennyiségű, modern mobil eszközökön tárolt adatok hatékony kinyerése. Az ellenőrzés alá vont telefonkészülék adatbázisából lehetővé teszi a rögzített adatok azonnali kinyerését, ami lépéselőnyt jelent a hatóságnak mind az egyszerű megítélésű ügyeknél, mind a súlyos bűncselekményeknél.

Az eszköz még a törölt állományokról is képes információkkal szolgálni, mert ezek bizonyos esetekben visszaállíthatók.[262]

A kimentett adatokkal elemzési művelet végezhető, ezt biztosítja egyrészt maga a technológia, az UFED Reader, illetve az adatok importálhatók, ami más szoftverekkel való feldolgozást is lehetővé tesz.[263] A kinyert adatok elemzésével és értékelésével lehetővé válhat eljárási cselekmények végrehajtása, valamint verziók felállítása.

Az informatikai rendszerekkel végzett helyszíni munka sok eszközt, felszerelést igényel, ez az eszközpark tartalmazhatja a mobil adatmentő eszközt, amilyen például a Cellebrite UFED Touch.[264]

Az UFED-et körülbelül 100 országban használják a rendészeti szervek, valamint több ezer nyomozásban szolgált segítségül. Előnye, hogy különféle eszközökkel kompatibilis.[265]

[260] Vigh 2018: 90–91.
[261] Krasznay–Ináncsi 2021: 68.
[262] Benedek 2018: 151.
[263] Bischoff–Tánczi 2019: 55.
[264] Herédi 2020: 1841.
[265] Ufed, az adatkitermelő eszköz… 2022.

6.7. A röntgensugaras vizsgáló, CT-vizsgálat

A csomagvizsgáló röntgent több helyen alkalmazzák a rendészeti szervek személyek poggyászainak átvizsgálására. Például a Nemzeti Adó- és Vámhivatal a reptereken használ ilyen berendezést, ami nagymértékben gyorsítja a csomagok ellenőrzését, így nem kell mindegyiket egyesével kinyitni, ezáltal az áthaladás is gyorsabb lesz, ami csökkenti a várakozási időt.[266] A röntgenvizsgálattal lehetőség nyílik a csempészet visszaszorítására is, valamint egészségügyi szempontból is előnyös a készülék alkalmazása, mivel a határátlépők csomagjait nem kell átforgatni.[267]

Azonban vannak olyan esetek, amikor nem kisméretű tárgyakat kell átvizsgálni, hanem rakományt egy kikötőben vagy egy repülőtéren – erre szolgál a röntgensugaras rakományátvilágító berendezés. A berendezés célja a biztonsági ellenőrzések fokozottabb és egyben hatékonyabb végrehajtása.[268]

Előfordulhat olyan eset, hogy a határon átkelő személyek például a kábítószert nem a csomagjaikban kívánják átcsempészni, Magyarország területére behozni, hanem a testükben. Így a csomagvizsgálat nem fog eredményre vezetni. Ilyenkor az úgynevezett CT-vizsgálatra van szükség. Az alábbi eset jól szemlélteti, hogy az elkövetők mennyire leleményesek, hogyan próbáljak elkerülni a büntetőeljárást, de nem minden esetben sikerül nekik.

> „Több mint nyolcmillió forint értékű kokaint talált a Nemzeti Adó- és Vámhivatal (NAV) a Liszt Ferenc Nemzetközi Repülőtéren egy nő testében. A hivatal csütörtökön az MTI-hez eljuttatott közleményében azt írta, a nő Sao Paulóból, Zürichen keresztül érkezett a budapesti repülőtérre, ahol a pénzügyőrök igazoltatták, és átvizsgálták a csomagjait, valamint ruházatát. A pénzügyőrök a vizsgálat során nem találtak kábítószer gyanús anyagot, de a nő viselkedése arra utalt, hogy a testében kábítószert rejthetett el, ezért a Semmelweis Egyetemre vitték CT-vizsgálatra. A közlemény szerint a CT körülbelül 10-11 darab idegen testet mutatott a nő testüregének alsó részében, ahonnan végül 13 darab, összesen mintegy 410 gramm, gumiövszerbe csomagolt kokain került elő. A NAV munkatársai a nő ellen kábítószer birtoklás megalapozott gyanúja miatt feljelentést tettek a Repülőtéri Rendőr Igazgatóság nyomozóinál."[269]

[266] Felkészültek a nyári utasforgalom növekedésre Röszkénél 2021.
[267] *Boxert és viperát is találtak…* 2021.
[268] Dankó 2019: 77.
[269] Több mint nyolcmillió forint értékű… 2019.

Az eset is az mutatja, hogy a technikai eszközöknek milyen jelentőségük van a felderítés alkalmával.

6.8. A spektrométer

A kézi Raman-spketrométer segít az anyagok beazonosításában. Ennek jelentősége van elfogás, szemle, kutatás vagy egyéb nyomozati cselekmény foganatosításánál, mivel másodpercek alatt lehet azonosítani az ismeretlen vegyületet, ami lehet kábítószer vagy akár robbanóanyag is. És nem kell képzett vegyésznek lenni a használatához.[270]

Különböző szerves komponensek mennyiségi és minőségi analízisére alkalmas a Raman-spektroszkópia.[271] A vizsgálat előnye, hogy nem igényel laboratóriumi minta-előkészítést, továbbá alkalmas szilárd, folyékony és gáznemű anyagok vizsgálatára is.[272]

6.9. A BriefCam

A mesterséges intelligencia és a mélytanulás által vezérelt videointelligencia-szoftver észleli és kivonja a videóban lévő objektumokat, és azonosítja, majd osztályozza ezeket. A BriefCam előnyei:

- több órányi videót képes áttekinteni percek vagy másodpercek alatt;
- egyidejűleg képes megjeleníteni a különböző időpontokban történt eseményeket;
- képes felismerni a megadott mintát a hatalmas mennyiségű adatból;
- képes a gépjárműrendszer felismerésére és nyomon követésére;
- arcfelismerés vagy hasonlóság felismerése nyomán azonosítani és követni tudja a személyt;
- fel tudja mérni az emberek közötti távolságot, figyelmeztetni tudja a veszélyeztetett személyt. Ez a felismerés a pandémia idején volt jelentős, de bűnügyi szempontból a követés felismerésére is lehetőséget ad;

[270] Anton Paar [é. n.].
[271] Salamon 2020: 192.
[272] Balláné Füszter 2019: 298.

– képes mérni az egyén-egyén közötti távolságot, illetve az egyén és a helyek közötti távolságot;
– felismeri a térben tartózkodó személyek számát.[273]

A bűnüldöző hatóság tagjai órákat tölthetnek el azzal, hogy megtalálják az őket érdeklő részleteket egy videófelvételen, azonban a BriefCam úgynevezett Video Synopsis technológiája képes felismerni a nagy mennyiségű videófelvételen a keresett objektumokat (például személyt vagy járművet), így pár másodpercbe sűríti a releváns eseményeket.[274]

6.10. Gangikonspi

Ez egy olyan program, amely egyrészt a telekommunikáció, másrészt egyéb elektronikus adatok elemzését segíti elő.

> „[A] szoftver egymásra épülő, kompatibilis és egymással összehangolt elemekből álló speciális, komplex, egységes célrendszer. A szoftver a titkos információgyűjtések során bonyolult összefüggéseket célirányosan elemez, melyet a magyar rendőrség részére a magyar adat- és jogszabálykörnyezetre hangolva hoztak létre, és amelynek nem lehet reális alternatívája egy, a piacon fellelhető úgynevezett »dobozos« szoftver."[275]

A használata gyorsan elsajátítható, és a nyomozó is elvégezheti az egyszerűbb értékeléseket, továbbá a rendszer alkalmas komplex bűnelemzésre is.[276] A program képes arra, hogy az egyes nyomozások (bizonyítási eljárások) részfeladatait, például adatok elemzését órák alatt lebonyolítsa, elkerülve a több hónapos munkát, így lehetőséget biztosítva arra, hogy a nyomozási cselekményt gyorsabban és hatékonyan lehessen végrehajtani. Költséghatékony, illetve további felderítési lehetőségek nyílnak meg ezáltal.[277]

[273] *Technology Overview*... [é. n.].
[274] *AI a videórendszerekben*... 2021.
[275] Közbeszerzési Hatóság Elnökének HNT-00269/03/2019. hirdetmény nélküli tárgyalásos eljárásról hozott 2019. december 19-i döntése a Gangikonspi szoftver támogatási szolgáltatása tárgyában.
[276] Gárdonyi–Hautzinger 2021: 1732.
[277] Bischoff–Tánczi 2019: 65.

Eredetileg a híváslisták elemzése volt a célja a Gangikonspi programoknak, de már egyéb kommunikációs forrásból származó adatoknak az elemzésére, valamint a pénzügyi tranzakciók, a NUSZ (Nemzeti Útdíjfizetési Szolgáltató Zrt. által működtetett ellenőrző pontokon rögzített áthaladások) és a VÉDA (Közúti Intelligens Kamerahálózat) adatainak összekapcsolására, valamint az elemzésére is képesek.[278]

6.11. Az arckép-azonosító rendszer

Az ismeretlen bűnelkövetők korszerű technológián alapuló, minél rövidebb időn belül történő azonosításához, az okmánybiztonság adminisztratív védelméhez, valamint a bűnmegelőzéshez fűződő társadalmi érdek indokolttá tette a személyazonosítási módszerek kiegészítését és a biometrikus arckép-azonosítás törvényi szintű szabályozását.[279] Az arcképelemzési nyilvántartásról és az arcképelemző rendszerről szóló 2015. évi CLXXXVIII. törvény szabályozza az arcképelemző rendszert, amely az arcképprofilok létrehozására, valamint összehasonlító elemzésére képes, a személyazonosítást elősegítő informatikai alkalmazás.

Az arcfelismerő rendszereket két fő csoportra lehet osztani, egyrészt a képalapú, másrészt a videóalapú felismerésre.[280]

A bűncselekmények megelőzése, megakadályozása, felderítése és megszakítása, valamint az elkövetők elfogása és felelősségre vonása céljából a nyomozó hatóság, az ügyészség és a bíróság a rendelkezésükre álló vagy általuk rögzített arcképmás felhasználásával az arcképelemző tevékenységet végző szerv arcképelemző tevékenységét jogosult igénybe venni a terhelt személyazonosságának megállapítása, valamint ellenőrzése érdekében.[281] Az arcképelemző tevékenységet végző szervként a Nemzeti Szakértői és Kutató Központot jelölték ki.

[278] Németh 2021: 157. 18, 19. lj. idézi ezeket a forrásokat: „[sz.n.] A HLS felhasználói útmutatója. 2016.; Kiss Jenő: Gangikospi [sic!] 18.15 telekommunikációs adatok elemzését segítő program, Használati Kézikönyv 2011-2016. [é. n.].”

[279] 2015. évi CLXXXVIII. törvény indokolása az arcképelemzési nyilvántartásról és az arcképelemző rendszerről.

[280] Gárdonyi 2021: 1135.

[281] 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről 9. § (1).

Az arcképelemzési eljárás során

> „az azonosításra váró képeket a vezető szignálja ki két arcképelemzőre, akik egymástól független irodában végzik párhuzamos kiértékelő tevékenységüket. A képet és a hozzá kapcsolódó leírást kizárólag az elemzésben érintettek ismerhetik meg. A munkatársak beemelik a képet a szoftverbe, és abból profilt képeznek."[282]

Az arcképelemzésnél jelentősége van a szoftvernek és a humán forrásnak, pontosabban az arcképelemzést végző személynek is, a gép/szoftver és az ember munkája együttesen fogja adni az arcképelemzés eredményét. A program egy bonyolult algoritmus alapján elemzi azt a közel 23 millió fotót, amely több adatbázisban szerepel, és közülük választja ki azokat, amelyek számításai szerint különféle morfológiai szempontok szerint nagyfokú vagy részleges hasonlóságot mutatnak a keresés alatt álló emberrel.[283] Ha az elemzők nem tudnak egyértelmű választ adni, olyan listát állítanak össze, amelyben több lehetséges személy szerepel, figyelembe véve, hogy sok esetben már ez is segítségül szolgálhat a megkeresést küldő szervnek.[284]

Az NSZKK már számos esetben segítette a bűnüldöző szervek munkáját az arcképelemző tevékenységgel, azonban ehhez elengedhetetlenül szükséges, hogy folyamatosan figyelje a technológia nyújtotta új lehetőségeket. Az arcképelemzésben az alapot a szoftver adja, ezért szükséges figyelemmel kísérni a technológiai újdonságokat, és mindig a legújabb elemző szoftverek beszerzésére és használatára kell törekedni.

6.12. Multispektrális UV/VIS és IR megjelenítő eszköz (Forensic Tablet)

A bűncselekmény helyszínén kimutathatók például emberi szem által nem érzékelt látens nyomok, vagy láthatóvá válhatnak anyagmaradványok. Ilyenek az alábbiak:

- egy bankjegyen vagy egyéb felületen található ujjnyom;
- rossz állapotban lévő szövegek olvashatóvá tétele (például erősen szennyezett papír szövegének vagy áthúzott, lesatírozott eredeti szöveg láthatóvá tétele);

[282] Ferentzi 2017.
[283] Ferentzi 2017.
[284] Ferentzi 2017.

– okmányok, bankjegyek biztonsági elemének láthatóvá tétele, amely lehetővé teszi a hamis vagy hamisított bankjegyek kiszűrését;
– sperma, nyál, vizelet, izzadtság, egyéb emberi testnedv.[285]

Az eszköz nélkülözhetetlen segítséget nyújthat bűnügyi (helyszíni) szemlék alkalmával, használatával eleget lehet tenni a nyomozás gyorsasága elvének.

6.13. Az artificial nose (elektronikus orr)

> „Az elektronikus orr (electronic nose, E-nose, artificial nose) különböző (egymástól eltérő) karakterisztikájú és szelektivitású (kémiai, gáz) érzékelőkből, jelfeldolgozó és adatgyűjtő rendszerből és valamilyen alakzatfelismerő algoritmusból áll. Működése azon alapul, egy adott szagot nagyszámú különböző vegyület határoz meg. A kémiai érzékelősor egy ennek megfelelő válaszjel sorozatot szolgáltat, mindegyik szenzor a saját szelektivitási tényezőivel súlyozva, melyet a kérdéses szagot jellemző vegyületek kombinációja határoz meg."[286]

Az egyes szenzorok szelektivitása, illetve a válaszjelek specifikussága gyenge, de a válaszjelek együttese jelentős információtartalmat képvisel, amely által lehetővé válhat az egyes szagok megkülönböztetése.[287]

Az ember leheletében több mint 3000 illékony szerves vegyület (VOC) található, amelyek kapcsolódnak a szervezetben lejátszódó belső biokémiai folyamataihoz.[288] Az elektronikus orr (E-orr) fontos szerepet játszhat a különböző légúti betegségek szűrésében és elemzésében.[289]

– Az elektronikus orr használhatóságát kutatják az egészségügyben is a cukorbetegség és a légúti betegségek, daganatok és fertőzések tekintetében. A légzéselemzés gyors és olcsó lehetőséget biztosít korai diagnózisok felállítására például a tüdőrák területén.[290]

[285] *Mobile Multispectral Forensic Tablet…* [é. n.].
[286] Pődör 2010.
[287] Pődör 2010.
[288] Behera 2019.
[289] Behera 2019.
[290] Freddi–Sangaletti 2022.

– Az elektromos orrot használják az élelmiszeriparban is az élelmiszer-vizsgálatok során, az élelmiszer-előállítás és -forgalmazás területén (például a polcon tarthatósági idő becslése), kimutathatók a romlásra utaló aromaanyagok, valamint előre jelezhető a szüretidő (például paradicsom érettségi státuszának vizsgálata). Az elektronikus orrok tényezői sarkallják a kutatókat újabb és újabb alkalmazási területek felderítésére. A befolyásoló tényezők például a készülék nagy érzékenysége, roncsolás- és vegyszermentes működése, alacsony üzemeltetési költsége.[291]
– Gyakorlati szempontból figyelemre méltó, hogy az ember orra a többféle illatösszetevőket a komponensek elkülönítése helyett tulajdonképpen elegyként kezeli, míg ezzel szemben az elektronikus orr szenzorok sorából épül fel, amelyek képesek a megfelelő mintafelismerés alapján egyszerű és összetett szagokat is azonosítani.[292]

Az E-orr a rendőrség munkáját is segíthetné, például marihuánaültetvények felderítésénél, különböző tárgyak rejtekhelyének a megtalálásában, robbanóanyagok keresésében vagy radioaktív helyszínek felismerésében is. Az E-orr akár a drónra szerelve, annak kiegészítőjeként is használható, így nagy területű helyszínek átvizsgálásában is segítség lehet, valamint az olyan területek esetén, ahol veszélyes gázok, gőzök, egyéb anyagok vannak jelen, hiszen a velük való közvetlen érintkezés is elkerülhető a felderítés során, ami a szakemberek egészségügyi kockázatát csökkenti. A mesterséges intelligencia segítség lesz az illatanyag, illetve szag különböző komponenseinek a felismerésében, detektálásában.

[291] Farkas–Dalmadi 2013: 172.
[292] Farkas–Dalmadi 2013: 172.

7. A deepfake és a fake news jelenség, valamint az igazságügyi (forenzikus) nyelvészet

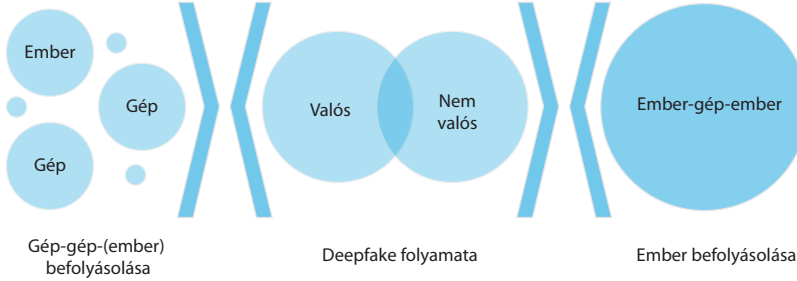
7.1. A deepfake technológia

Deepfake-ről akkor beszélhetünk, amikor a deep learning találkozik a fake news-zal.[293] Összemossa a valóságot és fikciót, ezért is veszélyes az új technológia.[294] A deepfake alkalmazása révén egy ember arca, hangja, sőt még a mozgása is újrateremthetővé válhat, így például a deepfake-et felhasználhatják arcok kicserélésére, az arc újraanimálására, különböző részletek eltávolítására, kitalált arcok létrehozására.[295] Akár valós képek segítségével is létrehozhatnak kitalált, nem valós arcokat. Például amikor az egyik embernek az orrát, a másik embernek a homlokát stb. használják fel, és így hoznak létre valós arcelemekből nem valós egész arcot. A deepfake álvideók lényege abban rejlik, hogy bárkinek a szájába adhatunk bármilyen tartalmat, illetve bárki bármilyen szituációba bele is helyezhető.[296]

> „A deepfake kifejezés egy Reddit-felhasználótól származik 2017-ből, maga a fogalom a deep-learning és a fake kifejezés »összeolvasásából« született. A deep-learning (»mély tanulás«) utal arra, hogy az effajta videókat a mesterséges intelligencia segítségével hozzák létre azáltal, hogy egy gépi tanulási módszerrel működő algoritmusnak információkat adnak."[297]

A deepfake megvalósítása, létrehozása két időben történhet: egyrészt nem valós időben, másrészt akár valós időben (real time-ban) audiovizuális tartalmak közvetítésével (36. ábra).[298]

[293] *Hét dolog...* 2018.
[294] Delfino 2019: 892–893.
[295] Marinov 2019.
[296] Rudolf 2019.
[297] Bruckner 2020.
[298] Bányász et al. 2019: 114.



36. ábra: A deepfake folyamata
Forrás: a szerző szerkesztése

Jelenleg már ott tartunk, hogy élő műsorban, azaz valós időben készítenek deepfake videót, egy videóklipben a műsorvezető arcát teszik egy előadó arcára, megdöbbentő hasonlóságot tükrözve, laikusok számára nem is látható a különbség. Ez a technológia a szórakoztató műsornak készült, a technikai ismereteket felhasználva, minden hátsó szándék nélkül.[299] Ez a deepfake pozitív oldalát jelenti, mivel a cél nem az, hogy az „érintett közönség" áldozat legyen.

Azonban egyre gyakrabban alkalmazzák őket dezinformációs kampányokban, csalás céljából, valamint közszereplők és hírességek lejáratására.[300] A figyelemre méltó hírességek lejáratására példa Tom Cruise esete, amikor a színészt megszemélyesítő hamis videót tettek közzé, ami mintegy 3,6 millió követőt vonzott.[301]

Amikor valós időben kell reagálni az eseményekre, az a deepfake legnehezebb formája – függetlenül attól, hogy mi az elérni kívánt cél –, hiszen itt azonnal kell válaszolni. Hang vagy kép formájában kell meggyőzni vagy éppen szuggerálni a partnert, a másik felet.

A valós idejű deepfake videókkal új csalási elkövetési mód is megjelenhet, ami bűncselekmény-sorozatot valósíthat meg. A legveszélyeztetettebb az idős korosztály: ha megszerzik például a sértett unokájának a fotóját (mondjuk egy közösségi oldalon az elérhető profilból), és annak az arcát átültetik egy másik személyre, aki online elérhető, még jobban fogja erősíteni azt a hitet az idős személyben, hogy az unokájával beszél a laptopon keresztül. De az álvideó

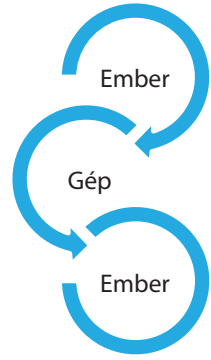
[299] Tangermann 2022.
[300] Cover 2022.
[301] Cover 2022.

az idős személytől függetlenül más személyt is megtéveszthet, hiszen egy bűncselekmény esetén bármelyik hozzátartozót sokkhatásként érheti, ha online látja a szeretteit, mivel a csaló a hozzátartozó hangján tud megszólalni, és a képmását is fel tudja használni. Egy kihallgatás esetén a sértett biztosra fogja állítani, hogy a hozzátartozójával kommunikált online, mivel a befolyásolás, megtévesztés hatásos volt. Valójában ez nem felel meg a valóságnak, csak az arcképpel éltek vissza egy deepfake videóban.

Még számtalan olyan esetet lehetne bemutatni, amely az elkövetés módját befolyásolni fogja a jövőben. Az elkövetők vissza fognak élni a szuggesztió negatív hatásával: a deepfake videóknak nem a szórakoztató jellegét fogják kihasználni, hanem ezeket az álfelvételeket a bűncselekmény megvalósításához fogják alkalmazni, akár valós időben is. Ha a deepfake nem valós időben történik, akkor a befolyásolás vagy a szuggesztió elérése érdekében több idő áll rendelkezésre, ugyanakkor a megtévesztett félnek is több ideje van a nem valós elemek felismerésére.

Ha a deepfake-eket csoportosítani szeretnénk a megvalósulást kivitelező résztvevők és az érintettek (befolyásoltak) oldaláról, akkor két fő csoportot célszerű megkülönböztetni.

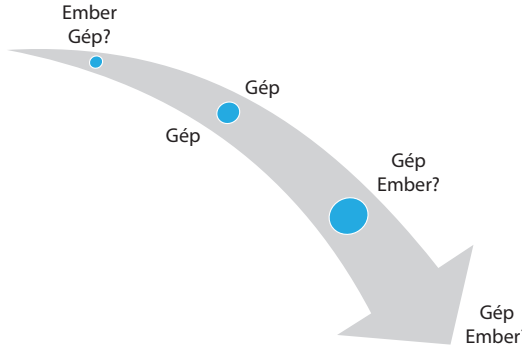
Az elsőben párhuzamos a humán tényező és a technológia (mesterséges intelligencia) használata. Az ember a gép (technológia, mesterséges intelligencia) segítségével hozza létre a deepfake-et, így megtévesztve egy másik embert. Ebben az esetben a deepfake-kel az a cél, hogy az ember a gép beiktatásával egy másik személyt befolyásoljon (37. ábra).



37. ábra: Ember-gép-ember kapcsolata a deepfake működtetésében
Forrás: a szerző szerkesztése

A másodikban pedig a gép és gép közötti kommunikáció létrejöttébe csatlakozik be a deepfake jelenség. Ebben az esetben gép a gépnek küld megtévesztő információt, amely egy valótlan adatokra épülő láncsorozatot indíthat el. Pontosabban ebben az esetben gép vezeti félre a kommunikációban részt vevő másik gépet. A gépek kommunikálnak egymással a rendelkezésre álló adatok (például bejövő képek, videó, egyéb információk stb.) alapján, elemzéseket és értékeléseket hajtanak végre. Itt is a mesterséges intelligencia működik közre kártékonyan a deepfake megvalósításában. Ha – akár egy kártékony vírus alapján – hamis, torz információ kerül be a rendszerbe, a hálózatba vagy a tanulási programba, az akár egy közlekedési struktúrát is megbéníthat, vagy legrosszabb esetben emberek életét is veszélyeztetheti. Az IoT és az IoE elterjedésével, amikor több milliárd eszköz csatlakozik a hálózatba 5G segítségével, és gépek kommunikálnak gépekkel, egy deepfake számos negatív folyamatot vagy cselekedetet indíthat el. A gépek közötti deepfake megjelenése mögött az ember áll, de az IoT és az IoE elterjedésével, a technológia fejlődésével elképzelhető, hogy lesz olyan eset, amikor ebből a folyamatból az ember ki fog esni, és a gépek fogják generálni a hamis videókat vagy az álhíreket (38. ábra).

A mesterséges intelligenciának nemcsak a deepfake elkészítésében van jelentősége, hanem annak felismerésében is, amikor egy gép a mesterséges intelligencia segítségével harcol a deepfake jelenségek kiszűréséért, felismeréséért és elterjedésének megakadályozásáért.



38. ábra: Ember-gép-gép-ember kapcsolatának folyamata a deepfake működésében
Forrás: a szerző szerkesztése

Említettem a legkritikusabb példát, amikor a deepfake az emberek életét is veszélyeztetheti. Ha például távműtét esetén az orvos és a beteg nem egy helyen tartózkodik, hanem a világ két különböző pontján, és ilyenkor az orvos deepfake adatokat (például képeket) kap, akkor sikertelen lehet a műtét. Ezért elengedhetetlen a kiberbiztonsági kockázatok vizsgálata és biztonsági lépések megtétele a deepfake jelenség elkerülése, illetve minimalizálása érdekében.[302]

Egy kutatás szerint 2019 szeptemberében 15 000 deepfake videó volt az interneten. Ami megdöbbentő, hogy ezek 96%-a pornográf tartalmú volt, és a feltérképezett arcok 99%-a női híresség, pornósztárok arcaiból volt generálva.[303] Beszélhetünk az úgynevezett bosszúpornó jelenségéről (revenge porn) és az algoritmusok által manipulált felvételek nyilvánosságra hozataláról, így „deepfake pornográfiának nevezzük azokat a szexuális tartalmakat, amelyeket algoritmusok segítségével, valós felvételek montázsolásával készítenek el".[304]

Hazánkban sem a bosszúpornó, sem a deepfake pornográfia nem jelenik meg önálló tényállásként a büntető törvénykönyvben. Azonban a Btk. 226/B. szakasza, amely a becsület csorbítására alkalmas hamis kép- vagy hangfelvételek készítését és nyilvánosságra hozatalát is büntetni rendeli, megoldást jelenthet egyes deepfake felvételekkel kapcsolatos ügyek esetében.[305] A becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatalának bűncselekménye valósul meg, ha valaki a közösségi oldalon nagy nyilvánosság előtt azzal a célból oszt meg tartalmat, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt hozzáférhetővé tegyen.

A deepfake jelenséggel a személyes adattal visszaélés bűncselekmény is megvalósítható. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 3b. alpontja különleges személyes adatnak tekinti a biometrikus adatot, amely

> „egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat".

[302] Jelen tanulmány a kibervédelmi lehetőségeket nem vizsgálja, mivel ez külön kutatási terület.
[303] Sample 2020.
[304] Sorbán 2020: 84.
[305] Sorbán 2020: 84.

Így ha valakinek az arcképét a beleegyezése hiányában a pornográf felvételben szereplő személy testéhez szerkesztik, és ezt haszonszerzési célból vagy jelentős érdeksérelmet okozva valósítják meg, akkor a személyes adattal visszaélés bűncselekménye valósul meg.[306]

Felmerülhetnek még a zsarolás vagy a becsület csorbítására alkalmas hamis kép- vagy hangfelvétel készítése és nyilvánosságra hozatala bűncselekményei, valamint a zaklatás tényállásának megvalósulása, ha a manipulált felvételt rendszeresen a sértettnek küldik.[307]

A deepfake videókat a technológia fejlődésével egyre nehezebb felismerni. Árulkodó jelek voltak korábban, hogy az alany nem pislog rendszeresen – azonban a gyengeségre való reagálásként elkezdték ezt problémát is kiküszöbölni, kijavítani.[308]

Lilian Edwards professzor szerint: „[a] probléma nem annyira a hamis valóság, mint inkább az a tény, hogy a valós valóság hihetően tagadhatóvá válik".[309] Ez a kijelentés véleményem szerint alátámasztja, hogy kettős problémával állhatunk szemben, amikor azt az esetet vesszük figyelembe, hogy nem jó szándékkal készítették a deepfake videót:

- egyrészt a hamis videók negatívan befolyásolhatnak eseményeket, ezáltal akár bűncselekmény is megvalósulhat;
- másrészt a valóságot kérdőjelezhetik meg, ami számos problémához vezethet, például az elkövető, hogy időt nyerjen, szándékosan azt nyilatkozza, hogy a lefoglalt bemutatott felvétel egy deepfake videó. A kijelentést azonban ellenőrizni kell, ami időkiesést, illetve többletmunkát is jelenhet.

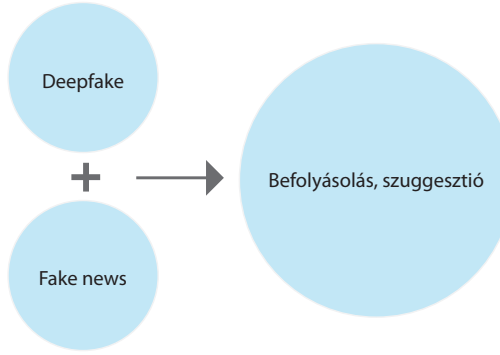
A deepfake a szemre és a fülre is hat, ebben különbözik a photoshopolt képektől.[310] E kettős hatás miatt is veszélyes egy álvideó, mert befolyásolhat, és legrosszabb esetben szuggesztív hatással is járhat, ezáltal jogellenes cselekmények (bűncselekmények) megvalósulását is előmozdíthatja.

306 Ambrus 2021: 126.
307 Ambrus 2021: 126–127.
308 Sample 2020.
309 Sample 2020.
310 Veszelszki 2021: 98.

7.2. A fake news

A valótlan hírek létrehozásával hatékonyan és olcsón lehet befolyásolni a társadalmat, ami akár nyereséges is lehet.[311] Mindennap különféle hírekkel találkozunk az interneten, közösségi oldalakon, vagy akár a munkahelyi levelezésekben is, ami hatással, befolyással lehet ránk. Ezeket a híreket megoszthatjuk a másokkal vagy a kollégákkal anélkül, hogy meg tudtunk volna győződni a valóságtartalmukról.[312] A megtévesztő tartalom legtöbbször írásban jelenik meg, de a technológia fejlődésével már hamis képet és videókat lehet létrehozni az írott szöveghez társítva, tehát az álhírek szoros kapcsolatban vannak az álvideókkal.

A deepfake az álhírek terjedésében is szerepet vállalhat, például ha egy gazdasági társaság vezetőjének arcképével és hangjával visszaélve adnak nyilatkozatot, az akár a tőzsdei folyamatokat is negatív irányba befolyásolhatja. A deepfake-kel közvetített hamis hírt a befolyásolás nehézfegyverének is szokták nevezni. A fake news és deepfake együttes megjelenésével növelhető a befolyásolás vagy a szuggesztió ereje. Az álhírek terjesztése egyfajta kognitív befolyásolási technika, s elsődleges platformjai a különféle a közösségi hálózatok (39. ábra).[313]



39. ábra: A befolyásolás elemei
Forrás: a szerző szerkesztése

311 Klein 2018: 244.
312 Ürmösné Simon – Nyitrai 2021: 87.
313 Haig 2022: 124, 128.

Az álhír szándékosan hamis, nem tartalmaz tényeket és félrevezetheti az olvasókat.[314] Egy másik meghatározás szerint olyan hamis információ, amelyet pénzügyi haszonszerzés céljából hoztak létre.[315] Véleményem szerint az álhír vagy fake news (hoax) kategóriába nemcsak a hamis, valótlan információ tartozik, hanem a valós tény elferdítése, hamis színben való feltüntetése is, amikor a valós tényeket összekeverik valótlan elemekkel, figyelembe véve, hogy a valós és a valótlan elemek keveredése olyan mértékű eredményt vált ki, mint a valótlan közlés.

A fake news mint valótlan, elferdített, kiszínezett tény állítása több bűncselekmény alapjául szolgálhat, így az alábbiak gyanúját is megalapozhatja:

- közveszéllyel fenyegetés (aki a köznyugalom megzavarására alkalmas olyan valótlan tényt állít, híresztel, vagy azt a látszatot kelti, hogy közveszéllyel járó esemény bekövetkezése fenyeget);
- rágalmazás (aki valakiről más előtt a becsület csorbítására alkalmas tényt állít, híresztel, vagy ilyen tényre közvetlenül utaló kifejezést használ);
- csalás (aki jogtalan haszonszerzés végett mást tévedésbe ejt, és ezzel kárt okoz). Napjainkban nagyon gyakori, hogy az interneten keresztül hamis állításokat tesznek a jogtalan haszonszerzés érdekében, itt a rendelkezésre álló adatok alapján vizsgálni kell a sorozatba illeszthetőséget is;
- rémhírterjesztés (aki különleges jogrend idején nagy nyilvánosság előtt olyan valótlan tényt vagy valós tényt oly módon elferdítve állít vagy híresztel, amely alkalmas arra, hogy a védekezés eredményességét akadályozza vagy meghiúsítsa).

Az álhírekkel kapcsolatosan egyre több ítélet születik. A bírósági ítéleti tényállás szerint

> „a nyíregyházi férfi 2020. november 25-én »A választás szabadsága« címmel egy írást jelentetett meg a saját internetes oldalán, melyben értelmetlen intézkedésnek nevezte a nyugdíjasok számára biztosított vásárlási idősávot. A vádlott ezen interneten megjelent írásában a kötelezően elrendelt maszkviselés vonatkozásában azt írta, hogy a szájmaszkok az egészségre ártalmas és értelmetlen védekezési eszközök. Ezzel valótlan tényeket állított, és ez a magatartása alkalmas volt arra, hogy a bevezetett védelmi intézkedések eredményességét akadályozza. Mivel az írás az interneten – a vádlott saját oldalán – jelent meg, az nagy nyilvánosság előtt elkövetettnek minősül, továbbá különleges jogrend idején jelent meg, amellyel a rémhírterjesztés bűntettét valósította meg."[316]

[314] Allcott–Gentzkow 2017.
[315] Craig 2017.
[316] Nyíregyházi Törvényszék Sajtóosztály 2022.

A fake news elleni küzdelem egyrészt fontos az internetfelhasználók információhoz való joga tekintetében, másrészt a pandémiás helyzetben a valósághű tájékoztatás és valós információkhoz való hozzájutás is egyaránt fontossá, sőt létfontosságúvá válhat.[317] A jogalkotó a rémhírterjesztés bűncselekményének módosításával megváltoztatta a korábbi norma hatókörét, érzékeltetve ezzel a szólásszabadság határait különleges jogrend idején.[318]

Az Európai Bizottság 2020-as a digitális gazdaság és társadalom fejlettségét mérő mutatója (DESI) szerint a magyar internethasználók 86%-a használ közösségi hálózatokat, ami az EU-ban a legmagasabb értéknek mondható.[319] Egyre jobban elterjedt az internet a különféle generációk körében is, folyamatos növekedés figyelhető meg.[320]

A Nemzeti Média- és Hírközlési Hatóság (a továbbiakban: NMHH) lakossági felhasználói szokásokat felmérő kutatásának adatai alapján az internetezők fele találkozott már álhírrel. A 2019-ben készült, legalább a heti egyszer internetezők körében végzett kérdőíves kutatás eredményei alapján az álhírekkel különösen a közösségi oldalakon találkozhatnak az internetezők.[321]

Az álhírek vagy álvideók negatív irányba befolyásolhatják a kihallgatást/vallomástételt, mivel a kihallgatott (befolyásolt személy) azt hiheti, hogy igazat mond, de a közölt tények valótlanok. Jelen esetben a vallomástevő igazat akar mondani, azonban nem azért mond valótlan információt a múltbeli releváns eseményről, mert rosszul emlékszik, hanem azért, mert befolyásolás vagy szuggesztió hatása alatt volt, és téves, nem a valóságnak megfelelő következtetést vont le. Tehát ilyen nyilatkozat esetében a kihallgatott nem hazudott, mivel nem valótlant akart mondani, nem akarta félrevezetni hatóságot, hanem a nyilatkozata azért nem felel meg a valóságnak, mert tévedésben van. Az ilyen vallomás objektíve hamisnak, de szubjektíve igaznak mondható (40. ábra).

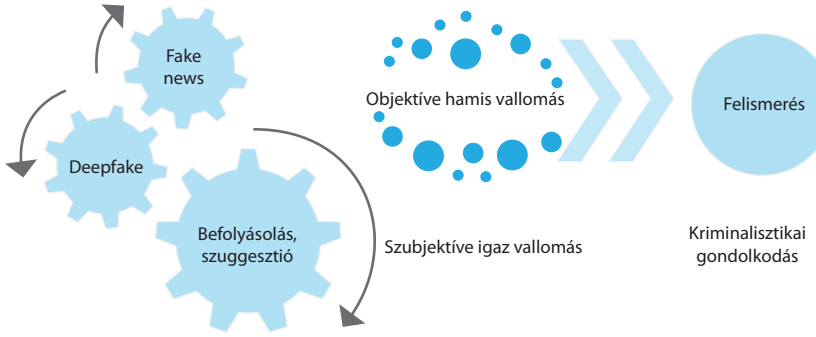
317 Monori 2021.

318 Monori 2021.

319 Európai Bizottság 2020b: 11.

320 Az egyes generációk elnevezésére gyakran használják az alábbiakat: „az 1945 előtt születettek az úgynevezett Silent generációba tartoznak, a Baby boom-korszak az 1946 és 1964 között született embereké, míg az X-generációhoz az 1965 és 1980 között születettek tartoznak. Az Y-generációba az 1981 és 1996 között, a Z-generációba pedig az 1997 és 2012 között születetteket sorolják." Ariosz 2020: 5.

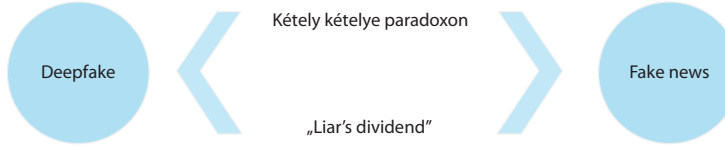
321 NMHH-piackutatás… 2020.



40. ábra: A felismerés folyamata
Forrás: a szerző szerkesztése

Az álvideók és az álhírek felismerésében segítségül szolgálhat a kriminalisztikai gondolkodás elengedhetetlen eleme, a kételkedés, amikor azt kell vizsgálni, hogy valóságos ellenérvvel lehet-e cáfolni a megállapított adatokat.

A deepfake és a fake news kiválthatja a *kétely kételye paradoxon*t és a *liar's dividend* jelenséget (41. ábra).



41. ábra: Az információs bizonytalanság
Forrás: a szerző szerkesztése

De az is probléma lehet, ha ok nélkül folyamatosan kételkedünk, gyanakszunk. Veszelszki Ágnes felhívja a figyelmet a kétely kételye paradoxon fogalmára. Ebben az esetben már mindenben elkezdünk kételkedni, és már azt sem hiszszük el, ami valós információnak tekinthető, ami hiteles forrásból származik.[322] Veszelszki a deepfake és a fake news kapcsán kitér arra is, amit angolul liar's dividendnek mondanak. Lehet olyan személy, aki egy hiteles forrásból származó

[322] Orbán 2022.

információra, tartalomra is azt mondja, hogy hamis.[323] A deepfake és a fake news létrejötte információs bizonytalanságot okozhat.[324]

A liar's dividend olyan jelenség, amikor valaki megúszhatja a hazugságot azzal, hogy valamiről azt állítja fake news/álhír. Ha a média megpróbálja leleplezni ezt a hazugságot, akkor ez még rosszabbul is elsülhet, mivel csak még hitelesebbnek tűnik a hazugság.[325]

7.3. Az igazságügyi (forenzikus) nyelvész

Egy fake news tartalom készítésekor az elkövető akaratlanul úgynevezett nyelvi ujjnyomot is hagyhat maga után, ezért a felderítésben és a bizonyításban az igazságügyi (forenzikus) nyelvésznek jelentős szerepe van.

Az alkalmazott nyelvészeti eljárások összefoglaló elnevezése az igazságügyi (forenzikus) nyelvészet, amely az igazságszolgáltatás sikerességét segítő elő.[326] A nyelvi ujjnyomok többsége digitálisan, az internet világában keletkezik, de ettől függetlenül papíralapon is létrejöhet. Az emberek egyre gyakrabban használják digitális információs csatornákat, a közösségi médiát, a különböző platformokat az interneten – beszédes adat, hogy az egyik legnagyobb internetszolgáltató cég 9,1 Terabit (TBit) másodpercenkénti adatforgalmi csúcsról számolt be.[327]

A befolyásoló eszközök kelléktárában kiemelendők a deepfake felvételek, illetve a fake news (hoax), amelyekkel nagy kárt tudnak okozni azáltal, hogy a kérdéses személyről készült képet, hangot vagy a kettő kombinációját a mesterséges intelligencia segítségével egy videóba vagy képbe illesztik bele.[328]

Egy fenyegető, zsaroló vagy álhírt tartalmazó levélnél, cikknél, vagy egy emberölésnél hátrahagyott búcsúlevél esetén fontos kérdés, hogy ki írta, illetve készítette, pontosabban, ki az, aki megfogalmazta az inkriminált szöveget, esetleg kinek a hangja hallható az adott felvételen, lehallgatási hanganyagban (közleményben). Ennek a kérdésnek a megválaszolása az eljárás során különleges szakértelmet igényel. Ha a bizonyítandó tény megállapításához vagy megítéléséhez

[323] Orbán 2022.
[324] GVU Center [é. n.].
[325] Micstusmi 2020.
[326] Ránki 2019: 76.
[327] Wiggen 2020: 2.
[328] Nyitrai–Rucska 2020.

különleges szakértelem szükséges, akkor szakértőt kell alkalmazni. A felmerült kérdések megválaszolásában számos esetben a nyelvész szakértői vélemények nyújthatnak segítséget, ezáltal lehetőség nyílik arra, hogy szűkíteni lehessen a gyanúsítotti kört, verziókat lehessen felállítani és ellenőrizni, valamint nyomozati cselekményeket végrehajtani.

Egy nyomozótól nem várható el az a nyelvi kompetencia, ami alkalmassá tenné arra, hogy fölmérje egy szövegnek a köznyelvitől eltérő sajátosságait. A nyomozó feladata a tartalmi elemzés (megjegyzendő, hogy a tartalomelemzés is része lehet a nyelvész szakértői munkának, amelybe bevonható pszichológus és pszichiáter egyaránt).[329]

Ránki Sára a hazai forenzikus nyelvészet szakterületeit az alábbiak szerint csoportosítja: kriminalisztikai szövegnyelvészet (például szerzőségvizsgálat, tartalomelemzés), törvényszéki fonetika (hangazonosítás, hangadatbázis építése), nyelvi profilalkotás, bűnügyi lexikográfia (bűnügyi szótárak, kategóriaszótárak készítése), börtönnyelvi vizsgálatok, tárgyalótermi diskurzuselemzés, gyűlöletbeszéd-elemzés stb.[330]

A felderítés szempontjából jelentős a nyelvi profilalkotás, amely nyelvészeti módszerekkel egy szöveg (írott vagy hangzó) ismeretlen (vagy álneves) szerzőjének profilját kívánja meghatározni.[331] Ez a profilalkotás nem azonos a grafológiával, mivel a szakértő szöveget, és nem írásképet vizsgál, ennek keretében egy szerzőnek nem a személyiségjellemzőit határozza meg, hanem a szociodemográfiai jellemzőit: például a nemét, korát, nyelvjárását, azt, hogy milyen anyanyelvű, egynyelvű vagy kétnyelvű-e, az iskolai végzettségét vagy a foglalkozását stb.[332]

A nyelvész szakértő a nyelvi profilalkotás módszerével segíti a rendészeti szervek munkáját.[333]

Az alábbiakban bemutatott esetek a nyelvész szakértői vélemények létjogosultságát emelik ki, bemutatva, hogy a szakértő megállapításai a bűnügyben szereplő személyek kilétének és személyazonosságának megállapításához, illetve a felderítéshez és a bizonyításhoz is hozzájárulhatnak.

329 Ránki 2011.
330 Ránki 2021: 2156.
331 Ránki 2021: 2156.
332 Ránki 2021: 2157.
333 Ránki 2015: 65.

Bűnszervezet tagjaként elkövetett embercsempészés bűntette felderítése során is igénybe vett a hatóság hang- és nyelvész szakértőt az ügyben szereplő személyek kilétének és személyazonosságának megállapítása céljából. Az ügyben az elsőfokú bíróság

> „valamennyi vádlott tekintetében hivatkozott a hang- és nyelvész szakértő szakvéleményében írt ténymegállapításokra, azokat bizonyítékként figyelembe vette, és ennek alapján logikus és okszerű indokát adta annak, hogy miért a vádlottak hangja hallható a bűncselekmények elkövetése idején az egyes telefonbeszélgetések hanganyagában".[334]

A nyelvészeti szakvélemény kiegészítheti a hangszakértő véleményének esetleges hiányosságait, mint ahogyan a fent tárgyalt ügyben is történt.

Terrorcselekmény elkövetésével fenyegetés bűntette; lőszerrel visszaélés bűntette miatt indult büntetőeljárás nyomozati szakaszában nyelvész szakértőt vontak be. A bíróság a tárgyaláson a nyelvész szakértői véleményeket a bizonyítás tárgyává tette. A nyelvész szakértő az inkriminált (robbantásos merényleteket kilátásba helyező) e-mail vonatkozásában az alábbiak szerint foglalt állást:

> „A levél első sorai a fogalmazó-szerző társadalmi státusának, körülményeinek definiálását, a levélírás motivációinak feltárását hivatottak közölni. A tartalom és a forma teljes összhangot mutat, így hitelesnek tűnik. Amit a közlemény készítője magáról elárul, arra enged következtetni, hogy korábban a kormányban bízó, mára azonban saját és környezete sorsának rosszabbra fordulásától elkeseredő, a jövőt kilátástalannak ítélő személy lehet az e-mailező. A szakértő jelentőséget tulajdonított egyrészt a megszólításnak, mely nem személyeskedő, nem csupán egy embert felelőssé tevő, nem durva hangnemű; másrészt az időzítésnek, miszerint nem zárható ki, hogy az október 23-ai események hatással voltak rá, de igyekszik tudatosan elhatárolni magát a szélsőséges utcai zavargásoktól, az abban résztvevő csoportoktól. A fogalmazást tekintve a szakértő úgy foglalt állást, hogy színvonala jó, hangneme kulturált, tisztelettudó, a stílus választékosnak tűnik, korrektnek mondható. Azt határozottan megállapíthatónak találta, hogy a levél megírásának fő indoka a szerző életkörülményeiben bekövetkezett negatív irányú változás lehetett."[335]

Az igazságügyi nyelvész szakértő a következő fenyegető e-mail vonatkozásában kijelentette, hogy az a korábbi szakértői véleményben szereplő fogalmazószerzőtől származik.

[334] Fővárosi Ítélőtábla Kbf.99/2008/13. Bűnszervezet tagjaként elkövetett embercsempészés bűntette és más bűncselekmények.

[335] Fővárosi Bíróság B.1103/2009/16. Terrorcselekmény elkövetésével fenyegetés bűntette; lőszerrel visszaélés bűntette.

„Megjegyezte a szakértő, hogy ezen megállapítása még akkor is helytálló, ha az utóbbi fogalmazás kevésbé személyes hangvételű, markánsabban elítélő, és agresszívabban támadó véleményt fogalmaz meg. Mégis hasonló okok késztetik a levélírásra, egyezik a követelt összeg nagysága, és ez esetben is a teletext játssza a kommunikációs közvetítői eszköz szerepét. A tartalmi és formai hasonlóságon túl az azonos fogalmazó-szerző tényét egyértelművé teszi a nagy számban előforduló egyező szavak és kifejezések használata, mint a »sorsolással választott«, »nyom nélkül eltűnik« stb. A fogalmazó-szerző »nyelvi profilja« tekintetében részben megerősödni, részben módosulni látszottak a korábbi véleményben tett megállapítások a korát, iskolai végzettségét, szakképzettségét illetően, de megjegyezte a szakvélemény, hogy bármilyen magas intellektusúnak tételezi is az e-mailek íróját, nagy a valószínűsége annak, hogy semmiféle konspirált csoport megszervezésére, sorsolással kiválasztott húsz helyszínen való terrorcselekmény elkövetésére nem lenne képes, de feltehetően nem is ez a szándéka: maga a rendőrséggel szembeni »macska-egér játék« okozhat számára szellemi izgalmat. Megjegyezte a szakértő, hogy túl gyengék a deklarált indítékai egy ilyen nagyságrendű zsarolás kivitelezéséhez, bármennyire is körültekintően részletezőek, mégis »gyermetegek« az esetleges végrehajtás módozatai, és – aki ennyire tisztában van a rendvédelem feladatával, lehetőségeivel, az – nem gondolhatja komolyan, hogy teljesítik a követelését.

Rámutat a bíróság, hogy az igazságügyi nyelvész szakértői vélemények olyan időben készültek, amikor V vádlottat gyanúsítottként még nem hallgatták ki, így vallomása a szakértők előtt nem volt ismert. V vádlott pedig úgy tett a bűnösségére is kiterjedő beismerő vallomást, hogy a szakértői véleményeket nem ismerhette. A szakértői vélemények, és a vádlott gyanúsítottként tett vallomása azonban kétségtelenül összhangot mutat, ami nyilvánvaló, hiszen a vádlott abban tett beismerő vallomást, amit elektronikus fenyegető levélben leírt, majd a kormány felé elküldött, és a szakértők is ezen levelek alapján alkottak véleményt, melyben olyan következtetésekre jutottak, amelyet a vádlott csupán a gyanúsítotti beismerő vallomásában tárt fel teljességgel. E vonatkozásban lényeges megállapítás, hogy a levél megírásának fő indoka a levélíró életkörülményeiben beállt negatív irányú változás volt, hogy a kilátásba helyezett agresszív cselekmények illetve ezek előkészületei csak a fantáziájában léteznek, hogy bármilyen magas intellektusú is, semmiféle konspirált csoport megszervezésére nem lenne képes, de nem is ez a szándéka; aki ennyire tisztában van a rendvédelem lehetőségeivel, az nem gondolhatja komolyan, hogy teljesítik a követelését. Ezek a megállapítások tükröződnek vissza a vádlottnak a nyomozás során gyanúsítottként tett beismerő vallomásában foglaltakkal."[336]

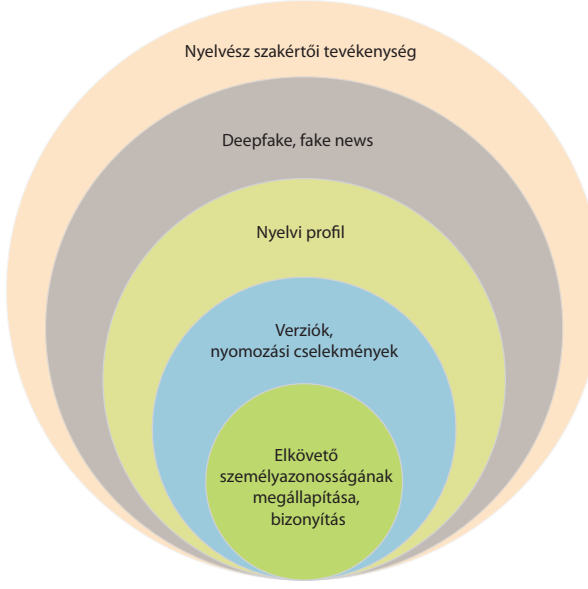
Ezekben az ügyekben különböző bűncselekmények valósultak meg, azonban a bűncselekmény felderítésében a nyelvi szakértő véleménye segítségül szolgálhatott. A nyelvi szakértő a már beazonosított személy esetén is kirendelhető, annak alátámasztására, hogy valóban az érintett személytől származik az inkriminált dokumentum vagy hanganyag. Az ismertetett ügyekben egy közös vonás

[336] Fővárosi Bíróság B.1103/2009/16. Terrorcselekmény elkövetésével fenyegetés bűntette; lőszerrel visszaélés bűntette.

van: a nyelvi profil, a nyelvi ujjlenyomatok, amelyeknek a vizsgálata különleges szakértelmet kíván, ezért ahhoz a nyelvész szakértő bevonása szükséges.

A nyelvész szakértő alkalmazása fontos lehet az álhírek miatt indult eljárásokban is. A nyelvi profil létrehozásával a nyomozati szakaszban olyan nyomozási verzió állítható fel, amely az ismeretlen személyek azonosításához, felderítéséhez és bizonyításához is hozzájárulhat. Ezt a folyamatot szemlélteti a 42. ábra.

A verzió számos intézkedés foganatosítását eredményezheti, figyelembe véve a raszternyomozást, azaz az adatbázisokban (nyilvántartásokban) zajló szűrő-kutató munkát. A profil alapján megállapított adatok egy láncsorozatot indíthatnak el, amely a nyomozati cselekmények foganatosítását elősegítheti, és eljuthatunk az elkövetőhöz. A nyelvész szakértői vélemények önmagukban nyilvánvalóan nem alkalmasak a vádlott büntetőjogi felelősségének megállapítására. Ugyanakkor egymással kiegészítve, az okirati bizonyítékokkal, tanúvallomásokkal összevetve a bíróság kétséget kizárhatóan megállapíthatja a vádlott büntetőjogi felelősségét.



42. ábra: Nyelvi profil az álhírek felderítésében
Forrás: a szerző szerkesztése

A kriminalisztikai nyelvészet keretében a bűncselekmények nyelvi bizonyítékainak elemzése történik, amely során a hatóság arra keresi a választ, hogy ki írta az ominózus szöveget.[337] A kriminalisztikai nyelvészet feladata, hogy elemezze a bűncselekmények nyelvi bizonyítékait.[338] A forenzikus nyelvészetre folyamatos fejlődés jellemző, amely egyrészt a digitalizációnak is betudható, és a jövőben a mesterséges intelligencia használatával minden bizonnyal még nagyobb előrelépés várható ezen a szakterületen.

7.4. A közösségi média és a bűnüldözés

A közösségi médiának egyre nagyobb szerepe van a bűnüldözés során, figyelembe véve, hogy az emberek rengeteg időt töltenek az interneten, a különféle közösségi portálokon akár szabadidejükben, akár munkavégzés közben. A fiatalok a hagyományos médiával szemben előnyben részesítik az internetet, továbbá az online közösségi média az ismeretségi hálózati szerepen túllépve információk, eszmék, alkotások forgalmazója lett, és magába foglalja a klasszikus média funkcióit, ráadásul hihetetlen gyorsaság jellemző rá.[339]

A klasszikus média jellemzői az alábbiak voltak:

- használói anonimak és elszigeteltek;
- a tartalom a megjelenés után nem módosítható;
- tipikusan pénzbe kerül a megjelenés;
- hosszabb idő telik el a hír megjelenése és közzététele között;
- egy fajta (például írott szöveg vagy hang) kommunikációs módot alkalmaz;
- hivatásos személyek, intézmények generálják, felügyelik a tartalmat.[340]

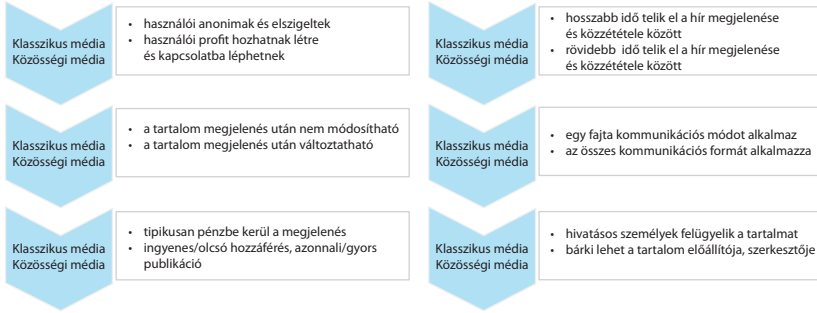
Ezzel ellentétben a közösségi média jellemzői:

- használói profilt hozhatnak létre maguknak és kapcsolatba léphetnek egymással;
- a tartalom a megjelenés után változtatható;
- ingyenes/olcsó hozzáférés;

[337] Hugyecz 2011.
[338] Ürmösné Simon 2019.
[339] Ariosz–NRC 2016: 38.
[340] Ariosz–NRC 2016: 38.

– azonnali/gyors publikáció;
– az összes kommunikációs formát alkalmazza (multimédia);
– bárki lehet a tartalom előállítója, szerkesztője.[341]

A 43. ábra szemlélteti a különbségeket.

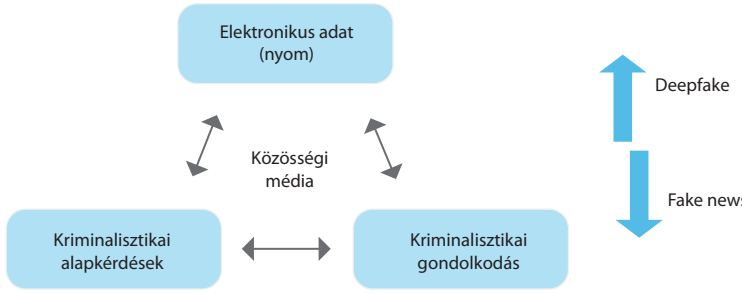


43. ábra: A klasszikus és a közösségi média különbségei
Forrás: a szerző szerkesztése

A közösségi média fogalmát illetően több száz meghatározás létezik, amelyekben a megalkotók saját tudományterületeik jellemzőit fogalmazták meg.[342] Bányász Péter szerint „a közösségi média olyan internetes oldalak és alkalmazások összessége, amelyeknél a szolgáltató csupán a keretet biztosítja, a tartalmat a felhasználók állítják elő".[343]

Bányász a fenti meghatározást alapul véve a közösségi média alkotóelemei közé sorolja többek között a blogokat, mikroblogokat, közösségi hálózatokat, fórumokat, kép- és videómegosztó oldalakat/alkalmazásokat, illetve az olyan közösségi szerkesztésű oldalakat is, amelyek a hírszolgáltatásra, közösségi tevékenységek szerkesztésére irányulnak.[344] Azonban a közösségimédia-platformok felgyorsították az álhírek (fake news) terjedését, és megsokszorozták őket.[345]

341 Ariosz–NRC 2016: 38.
342 Bányász 2020: 85.
343 Bányász 2020: 85.
344 Bányász 2020: 86.
345 Hulkó 2021.



44. ábra: Elektronikus adatok a közösségi médiában
Forrás: a szerző szerkesztése

Ha a fenti meghatározásból indulunk ki, és figyelembe vesszük a kriminalisztikai alapkérdéseket, valamint a kriminalisztikai gondolkodás mentén indulunk el, akkor az elkövető számos elektronikus nyomot, releváns adatot hagyhat maga után a közösségi média használata során. Itt kulcsfontosságú lehet a látogatott az internetes oldal és a felhasználó – aki lehet akár az elkövető, a sértett, a tanú vagy harmadik személy – által feltöltött tartalom. A blogokban vagy fórumokban a sértettek is információt cserélhetnek, amely során elmondják, hogy kit, hogyan, milyen módon ejtettek tévedésbe. Az is előfordulhat, hogy egy blogbejegyzésben vagy egy fórumban szándékosan dezinformációt fognak elhinteni a közösség táborában, amely lehet, hogy megmarad egy fake news szintjén, de az is lehet, hogy deepfake-et fognak benne elhelyezni (44. ábra).

Ha a hatóság csatlakozik a fórumhoz – amelyhez például az egyik tanú információja alapján jutott el –, akkor korábban látenciában maradt sértetteket tud felderíteni, és a tőlük beszerzett nyilatkozatok alapján közelebb kerülhet az elkövetőhöz, így eleget tehet a nyomozás teljessége elvének. De a fórumokhoz, egyéb oldalakhoz az elkövetők is csatlakozhatnak, és ott konspiráltan információt cserélhetnek, leplezve bűnös tevékenységüket, amelynek keretében a jövőben elkövetni kívánt bűncselekményt is megszervezhetik. Az oldalak folyamatosan kiegészülhetnek információval vagy törlődhetnek is, ezért célszerű az adatgyűjtés (nyomozás) során a folyamatos mentés.

A közösségi média felületei alkalmasak arra, hogy az elkövető az eltulajdonított (lopott) értékeket internetes felületen értékesítse. A körözési nyilvántartási rendszerrel és a körözési eljárással kapcsolatos rendőrségi feladatokról szóló 54/2013. (XII. 21.) ORFK utasítás 25. *b)* pontja alapján a dologkörözés

elrendelését követően szükségességi és célszerűségi indokok figyelembevételével végre kell hajtani a beszerzett adatok és információk alapján a számba vehető értékesítési helyek, vonalak, valamint a rendelkezésre álló online hirdetési és közösségi (social media) felületek ellenőrzését. A hatóság tagjának a közösségi (social media) felületeken is ellenőrzést kell végrehajtani, utalva arra, hogy a digitális tér számtalan lehetőséget rejt az elkövetőnek arra, hogy a bűnös úton szerzett dolgot értékesítse.

A közösségi médiában keletkezett ellenőrizhetetlen adatok sokak számára az egyetlen hírforrási lehetőséget, információforrást jelentik.[346] A közösségi média kedvezőtlenül befolyásolja a bűncselekmények számát, mivel azok a platformok, amelyeket az online térben a szórakozásra, ismerkedésre, társkeresésre hoztak létre, melegágyai a bűncselekményeknek.[347]

A fiatalok könnyen válhatnak bűncselekmények áldozatává vagy elkövetőjévé, amikor a közösségi oldalakat használják, úgy, hogy közben lehet, nem is érzékelik a valós problémát.[348] A deepfake és a fake news tartalmú oldalak negatív hatással lehetnek rájuk, illetve veszélyeztethetik a kiskorú testi, értelmi, erkölcsi vagy érzelmi fejlődését.

[346] Forgács 2018: 527.
[347] Gyaraki 2021: 67.
[348] Szabó–Horváth–Nagy 2017: 99.

8. A kérdőívek elemzése

A „Digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában, a deepfake és a fake news jelenség” témakörben kérdőíves kutatást végeztem.

A kérdőív három nagy témakörre fókuszált a kvantitatív adatfelvétel során. A kérdőív első kérdéscsoportjában az adattárak használatára vonatkozó kérdéseket, míg a második részben a modern technikai (elektronikai) eszközök és programok használatára vonatkozó kérdéseket tettem fel. Az utolsó kérdéscsoport a kép- és/vagy videómanipulációval kapcsolatos kérdéseket foglalta magában.

A kutatás (célja) hipotézisei:

- a válaszadók jelentős része már alkalmazza munkája során a bűnügyi nyilvántartásokat, a Robotzsaru NEO rendszert, a gépjármű-nyilvántartást, a személy- és lakcímnyilvántartást és a körözési nyilvántartást, azonban a rendészeti (például rendőrségi) munkában az adatbázisok, nyilvántartások minél szélesebb körű ismeretét szükségesnek tartják;
- az adattárak és modern technikai eszközökkel kapcsolatos képzésre igény van a levelezős (többségében hivatásos) hallgatók körében, továbbá a raszternyomozásról, interoperabilitási e-nyomozásról, valamint az OSINT-ról (nyílt forrású információgyűjtésről) a válaszadók többsége nem hallott;
- a más hatóság által vezetett nyilvántartásokról, másrészt az új nyomozati módszerekről és az új technikai eszközökről informálisan tájékozódnak a válaszadók;
- a válaszadók (hallgatók) a kép- és/vagy videómanipulációval kapcsolatos ismeretei fejlesztésre szorulnak, és igény merül fel a képzésre, valamint szükségesnek tartják egy módszertani útmutató/segédlet kidolgozását az arcképcserés videók (deepfake) nyomozásához.

8.1. A célcsoport behatárolása és a kérdőív bemutatása

A kérdőívet a Microsoft Forms Office alkalmazásba rögzítettem, és a link megküldésével juttattam el a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar levelező munkarendben tanuló bűnügyi és rendészeti BA szak I–III. évfolyama, valamint a kriminalisztikai mesterszak I–II. évfolyama hallgatóihoz. A kutatási alanyok (hallgatók) évfolyam-előadás keretében töltötték ki a kérdőívet.

Az online kérdőív kitöltése pár percet vett igénybe, és teljes mértekben önkéntes és névtelen volt. A felmérésben személyes, beazonosításra alkalmas adatokat nem gyűjtöttem. A Microsoft Forms Office alkalmazás lehetővé tette a kérdőív kitöltésének anonimitását és hitelességét.

Az adatfelvételre 2022. április–június hónapban került sor. A kérdések elkészítésénél törekedtem a semlegességre, hogy a válaszokat ne befolyásoljam, és az alanyok őszintén osszák meg azokat. A válaszokban megjelennek szakmai tapasztalataik és véleményük is.

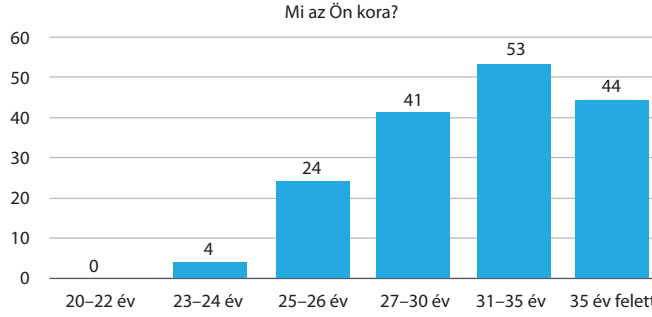
A kérdőív 27 kérdésből állt. A felmérést négy fő kérdéscsoportra bontottam:

– Az első kérdéscsoport (1–7. kérdések) a kitöltőre vonatkozik (neme, életkora, legmagasabb iskolai végzettsége, lakóhelye, beosztása, munkatapasztalata, melyik szakra jár).
– A második rész (8–18. kérdések) az adattárak használatára vonatkozik (munkája során milyen adattárakat és milyen gyakorisággal használ, adatgyűjtési módszerek ismerete, Nemzeti Adatvagyon Ügynökségre, képzésen való részvételre, adatbázisok jelentőségére vonatkozó kérdések stb.).
– A harmadik rész (19–21. kérdések) a modern technikai (elektronikai) eszközök és programok használatára vonatkozó kérdéscsoport.
– Az utolsó rész (22–27. kérdések) a kép- és/vagy videómanipulációval kapcsolatos kérdéseket tartalmazza.

8.2. A kérdőívre adott válaszok bemutatása és elemzése

Az 1. kérdés a kitöltő nemére vonatkozott, amelyre összesen 166 fő válaszolt. Ebből 121 fő férfi, míg 45 fő nő (45. ábra).

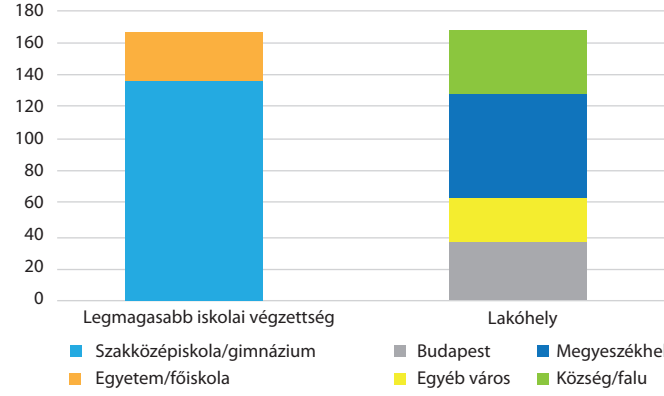
45. ábra: A válaszadók nemek szerinti bontása
Forrás: Microsoft Forms Office



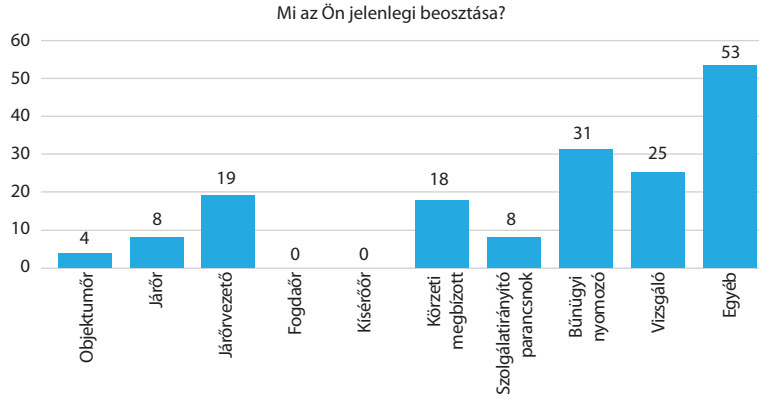
46. ábra: A válaszadók kor szerinti csoportosítása
Forrás: Microsoft Forms Office

A 2. kérdés a kitöltő életkorára vonatkozott, amelyre összesen 166 fő adott választ. Az összesítés alapján megállapítható, hogy a kitöltők többsége 25 év fölötti személy (46. ábra).

A 3. kérdés a legmagasabb iskolai végzettségre vonatkozott, amelyre összesen 166 fő adott választ. Ebből 136 fő szakközépiskolai/gimnáziumi végzettséggel, míg 30 fő főiskolai/egyetemi diplomával rendelkezett. A 4. kérdésre adott válaszokból kiderül, hogy a válaszadók jelentős része városban lakik (47. ábra).



47. ábra: A válaszadók iskolai végzettsége és lakóhely szerinti eloszlása
Forrás: a szerző szerkesztése

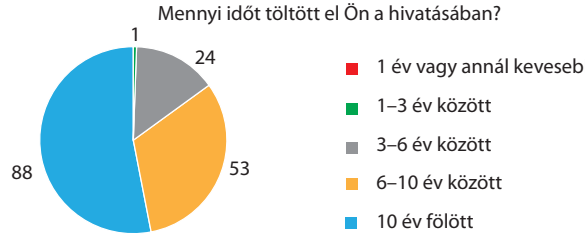


48. ábra: A válaszadók beosztás szerinti bontása

Forrás: Microsoft Forms Office

Az 5. kérdés a kitöltő jelenlegi beosztására vonatkozott, amelyre összesen 166 fő adott választ. Ha a szolgálati ágakat nézzük, akkor a közrendvédelmi területen[349] 57 fő dolgozik, a bűnügyi területen[350] 56 fő, míg egyéb beosztásban 53 fő (48. ábra).

A 6. kérdés a hivatásban eltöltött időre vonatkozott. A többség, 88 fő 10 év fölötti tapasztalatot jelölt meg, azonban elmondható, hogy minimális, legalább 3 éves munkatapasztalattal minden válaszadó rendelkezett (49. ábra).

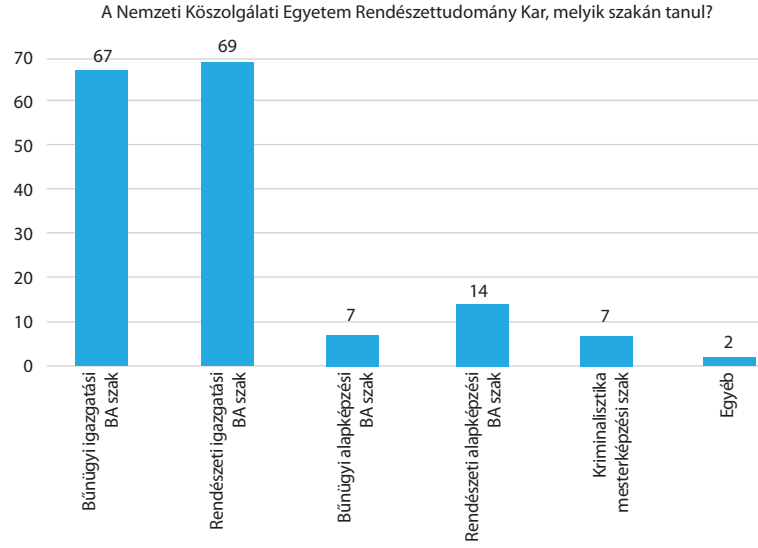


49. ábra: A válaszadók hivatásban töltött ideje

Forrás: Microsoft Forms Office

[349] A közrendvédelmi területhez sorolom az elemzés szempontjából az objektumőr, járőr, járőrvezető, fogdaőr, kísérőőr, körzeti megbízott, szolgálatirányító parancsnok beosztást.

[350] A bűnügyi területhez sorolom az elemzés szempontjából a bűnügyi nyomozó és a vizsgáló beosztást.



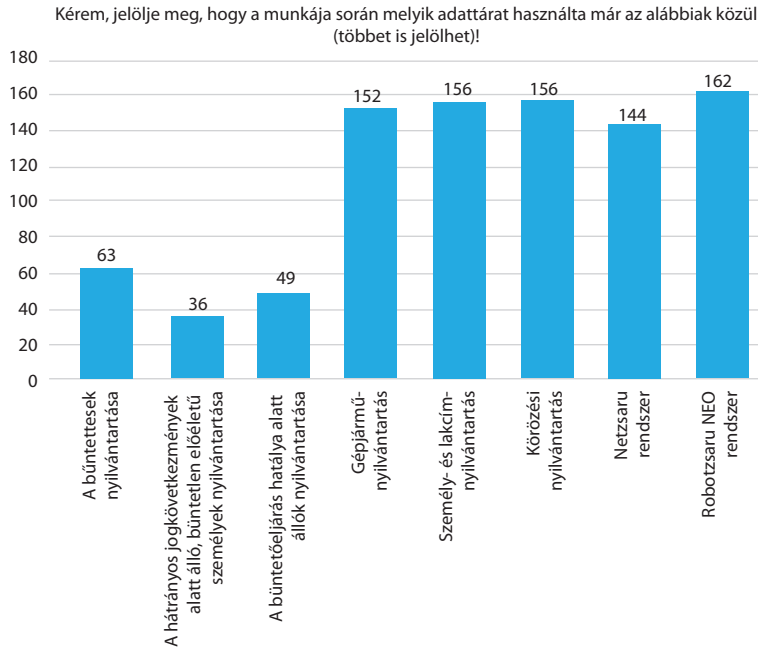
50. ábra: A válaszadók szak szerinti csoportosítása
Forrás: Microsoft Forms Office

A 7. kérdésre 166 fő adott választ. A kérdés arra irányult, hogy a kitöltő melyik szakon tanul. A válaszadók többsége a bűnügyi és a rendészeti területet jelölte meg (50. ábra).

A 8. kérdés arra irányult, hogy a kitöltő munkája során a megadott adattárak közül melyiket használta. A válaszokból kiderül, hogy az alanyok többsége a megadott adatbázisokat már használta:

- a bűnügyi nyilvántartásokat[351] 146 fő;
- a gépjármű-nyilvántartást 152 fő;
- a személy- és lakcímnyilvántartást 156 fő;
- a körözési nyilvántartást 156 fő;
- a Netzsaru rendszert 144 fő;
- a Robotzsaru NEO rendszert 162 fő (54. ábra).

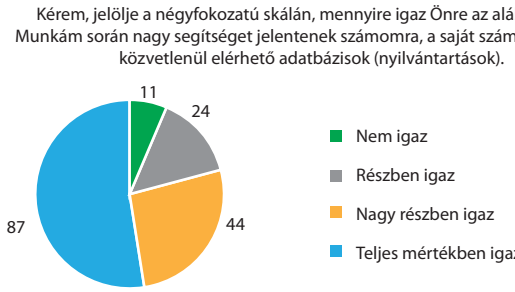
[351] A bűnügyi nyilvántartások közé tartozik: a bűntettesek nyilvántartása; a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartása; a büntetőeljárás hatálya alatt állók nyilvántartása és a külföldre utazási korlátozás hatálya alatt állók nyilvántartása!



51. ábra: Az adattárak használata a válaszadók körében
Forrás: Microsoft Forms Office

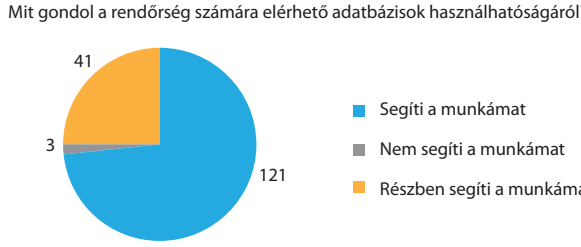
A 9. kérdés arra irányult, hogy a válaszadó a fenti adattárakat milyen gyakran használja. Ennél a kérdésnél 77 fő a fenti nyilvántartásokra úgy tekint, hogy azok alapnyilvántartások, és a munkához nélkülözhetetlenek, míg 57 fő azt nyilatkozta, hogy naponta használja őket. Ez a két számadat is alátámasztja azt a feltételezésemet, hogy a válaszadók az említett nyilvántartásokat rendszeresen alkalmazzák.

Ezt erősíti a 15. és 18. kérdés is. A 15. kérdésnél egy négyfokozatú skálán kellett megjelölni, hogy mennyire igaz az adatközlőre az az állítás, miszerint munkája során nagy segítséget jelentenek számára a saját számítógépéről közvetlenül elérhető adatbázisok (nyilvántartások). A 166 főből 44 fő nyilatkozta azt, hogy „nagyrészt igaz", míg 87 fő azt, hogy „teljes mértékben igaz" (52. ábra).



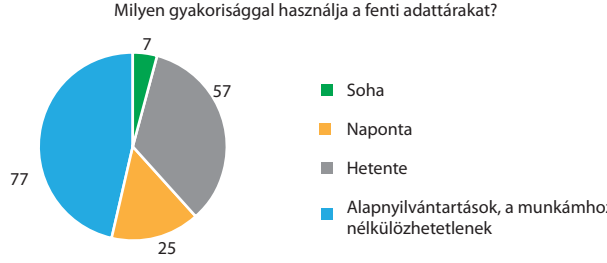
52. ábra: Az adattárak használata a válaszadók körében
Forrás: Microsoft Forms Office

A 18. kérdés arra irányult, hogy mit gondol a rendőrség számára elérhető adatbázisok használhatóságáról. A 165 válaszadóból 162 fő nyilatkozta azt, hogy azok segítik vagy részben segítik a munkáját, ez az arány a válaszadók 98%-át jelenti (53. ábra).



53. ábra: Az adatbázisok használhatósága a válaszadók szerint
Forrás: Microsoft Forms Office

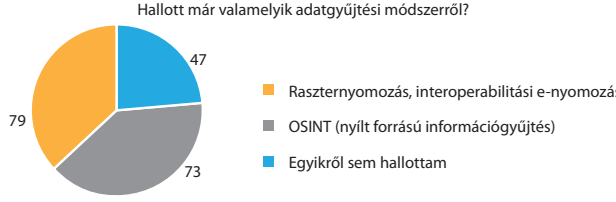
Ez is azt mutatja, hogy szükséges az említett nyilvántartások még részletesebb oktatása, az azokban foglalt adatok ismerete, azok kapcsolódási pontjainak feltárása. Ehhez pedig véleményem szerint további adatnyilvántartások feltérképezése és oktatása szükséges, illetve elengedhetetlen a kriminalisztikai ajánlások megfogalmazása, amelyek az adatok hatékony feldolgozását segíthetik elő, illetve egy információs áradat elindítói lehetnek (54. ábra).



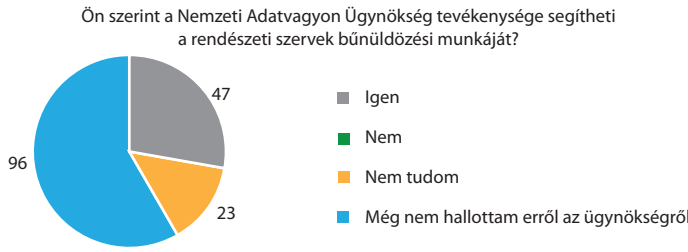
54. ábra: Az adattárak használatának gyakorisága a válaszadók körében
Forrás: Microsoft Forms Office

A 10. kérdésre adott válaszban fel kellett sorolni azokat a nyilvántartásokat, adattárakat, amelyeket eddig a munkája során használt – a fent említetteken kívül (beleértve a megkeresés útján elérhető nyilvántartásokat és a közvetlenül elérhető nyilvántartásokat is). Itt a válaszadók száma már lecsökkent 76 főre, csak 45% nyilatkozott. Ez is arra utalhat, hogy általában csak az alapnyilvántartásokat használják a munkájuk során, amelyeket közvetlenül, portálszerűen elérnek az irodából. A válaszadók legtöbbször az alábbiakat jelölték meg: telefonszolgáltatók, NEAK, cégnyilvántartás, banki megkeresések, TakarNet, Facebook, OSINT.

A 11. kérdés arra vonatkozott, hogy a kitöltő hallott-e már a raszternyomozásról, az interoperabilitási e-nyomozásról vagy az OSINT-ról (nyílt forrású információgyűjtésről). A raszternyomozásról, az interoperabilitási e-nyomozásról 47 fő, az OSINT-ról 79 fő hallott, míg 73 fő azt nyilatkozta, hogy egyikről sem hallott. A kérdésre adott utolsó válasz alátámasztja azt a feltételezésemet, hogy a hallgatók egy része nem hallott az említett adatgyűjtési módszerekről (55. ábra).



55. ábra: Az adatgyűjtési módszerek ismerete
Forrás: Microsoft Forms Office

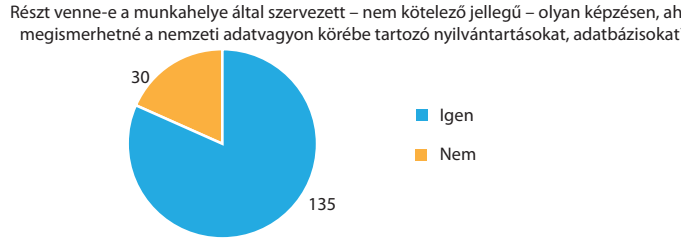


56. ábra: A Nemzeti Adatvagyon Ügynökség tevékenységének megítélése a válaszadók körében
Forrás: Microsoft Forms Office

A 12. kérdésben arra voltam kíváncsi, hogy mit gondolnak, a Nemzeti Adatvagyon Ügynökség tevékenysége segítheti-e a rendészeti szervek bűnüldözési munkáját. A válaszadók többsége, 96 fő (58%) azt nyilatkozta, hogy még nem hallott erről az ügynökségről (56. ábra). A NAVÜ-ről részletesen írok az *1.3.1. fejezetben.*

A 13. és 14. kérdéseket célszerű együtt tárgyalni és elemezni. Ezek az adatbázisokra vonatkozó képzésre és annak hasznosságára irányultak.

A 13. kérdésben 165 fő válaszadóból 135 fő (82%) azt nyilatkozta, hogy részt venne a munkahelye által szervezett – nem kötelező jellegű – olyan képzésen, ahol megismerhetné a nemzeti adatvagyon körébe tartozó nyilvántartásokat, adatbázisokat. Ez a válasz is megerősíti azt a feltételezésemet, hogy a válaszadók hajlandók képezni magukat. Ez alapján nemcsak az iskolarendszerű képzésben tartom fontosnak a nyilvántartásokról szóló naprakész információk oktatását, hanem a gyakorlati szakemberek továbbképzésében is. Olyan képzéseket kellene szervezni a rendészeti egységeknél, amelyek az e-nyomozás, a nyilvántartások jelentőségét mutatnák be, mindezt úgy, hogy az elméleti ismereteket ötvözik a gyakorlattal (57. ábra).

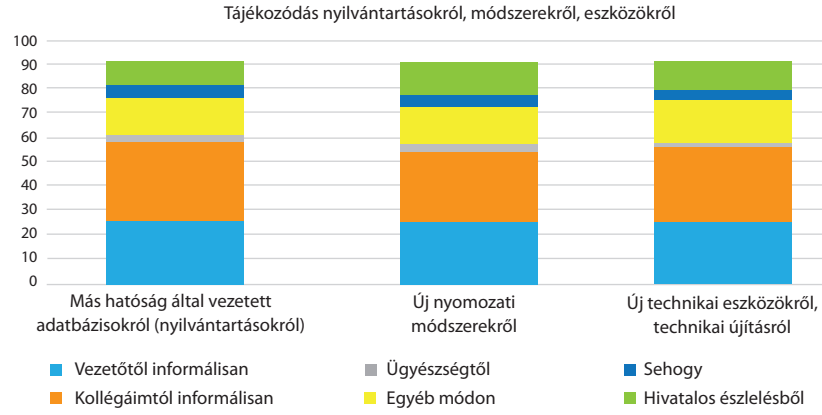


57. ábra: A válaszadók képzésen való részvételi szándéka
Forrás: Microsoft Forms Office

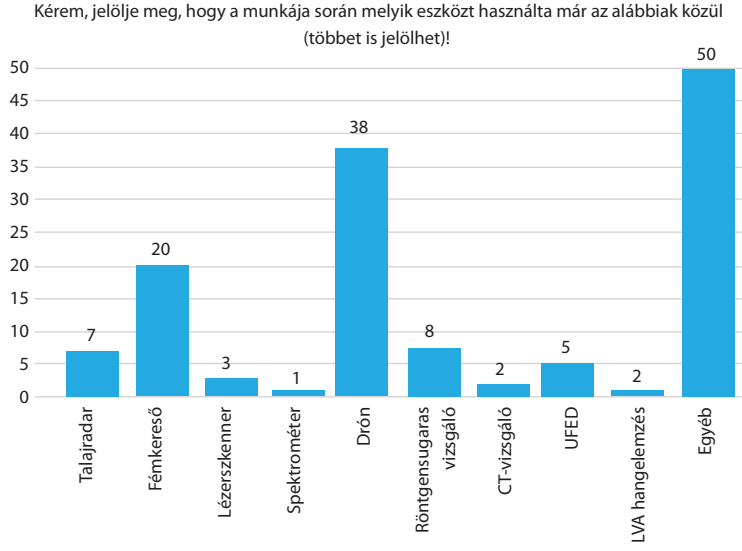
A 14. kérdésnél a 166 fő válaszadóból 144 fő (86%) úgy gondolja, hogy a rendészeti (például rendőrségi) munkában az adatbázisok, nyilvántartások minél szélesebb körű ismerete elengedhetetlenül szükséges, mivel a jövőben a digitalizáció térnyerésének köszönhetően ezek segítségével hatékonyabban lehetne dolgozni (58. ábra).

58. ábra: Az adatbázisok ismeretének hasznossága a válaszadók szerint
Forrás: Microsoft Forms Office

A 16–17. és a 21. kérdéseket célszerű együtt tárgyalni. Ezek arra irányultak, hogy megtudjuk, milyen módon tájékozódnak a válaszadók a más hatóság által vezetett nyilvántartásokról, az új nyomozati módszerekről és az új technikai eszközökről. Mindhárom kérdés esetében a legtöbb válasz az volt, hogy a kollégáktól informálisan, majd az, hogy a vezetőtől informálisan. Ez arra utalhat, hogy a kérdéses témakörben szükséges hivatalosan képzéseket szervezni (59. ábra). Ez hivatalosan megvalósítható lehetne a Belügyminisztérium Rendészeti Vezetőkiválasztási, Vezetőképzési és Továbbképzési Főosztály Rendészeti Továbbképzési Rendszerében. Itt a képzési rendszerben szereplő tagok a szabadon választható képzések keretében jelentkezhetnének a kérdéses témakörre. Azonban a modul létrehozásakor az összes tagot célszerű hivatalosan e-mailen keresztül is tájékoztatni a képzés lehetőségéről.



59. ábra: A válaszadók tájékozódási forrásai az adatbázisokról és a nyomozati módszerekről
Forrás: Microsoft Forms Office



60. ábra: A válaszadók által a munka során már használt eszközök
Forrás: Microsoft Forms Office

A 19. kérdés arra vonatkozott, hogy milyen modern technikai (elektronikai) eszközök, elemző programok segítik (segíthetnék) a válaszadók munkáját. Az esetek többségében a Gangikonspi alkalmazást jelölték meg. A 20. kérdésben a megadott/nevesített eszközök közül az adatközlők többsége a drónt és a fémkeresőt jelölte meg, mert ezeket már használtak a munkájuk során (60. ábra).

Az utolsó öt kérdés a fake news és a deepfake jelenségével volt kapcsolatos. A kérdések az alábbiakra irányultak:

- hallott-e már a deepfake-ről;
- látott-e deepfake videót;
- találkozott-e már munkája során kép- és/vagy videómanipulációval;
- szerinte hol lehet leginkább kép- és/vagy videómanipulációval, illetve fake news-zal találkozni;
- részt venne-e a munkahelye által szervezett – nem kötelező jellegű – olyan képzésen, ahol megismerhetné azokat a kriminalisztikai ajánlásokat, amelyek a fake news-zal, deepfake-kel megvalósítható bűncselekmények felderítésével kapcsolatosak.

A kérdésekre kapott válaszokat az alábbiak szerint lehet összegezni:

- a válaszadók csak 54%-a hallott, 46%-a még nem hallott a deepfake-ről;
- 57%-uk még nem látott deepfake videót, csak 43%-uk;
- 28%-uk már találkozott munkája során kép- és/vagy videómanipulációval;
- a válaszadók többsége szerint kép- és/vagy videómanipulációval, illetve fake news-zal leginkább az elektronikus médiában és a politikai hirdetésekben lehet találkozni.

Az utolsó két kérdésnek kiemelt jelentősége van, mivel a válaszadók 90%-a részt venne a munkahelye által szervezett – nem kötelező jellegű – olyan képzésen, ahol megismerhetné azokat a kriminalisztikai ajánlásokat, amelyek a fake news-zal és a deepfake-kel megvalósítható bűncselekmények felderítésével kapcsolatosak. Továbbá az alanyok/hallgatók 96%-a szerint szükség lenne egy módszertani útmutató/segédlet kidolgozására az arcképcserés videók nyomozásához.

Ez is azt mutatja, hogy szükséges a deepfake-kel kapcsolatos ismeretek oktatása, mivel sokan nem is ismerik a jelenséget. De volt olyan válaszadó, aki a munkája során már találkozott kép- és/vagy videómanipulációval. Továbbá a kérdésre adott válaszok megerősítik azt a feltételezést, hogy a deepfake-kel kapcsolatos ismeretek fejlesztésre szorulnak, és igény merül fel a képzésre.

8.3. A kérdőívek elemzéséből levonható következtetések

Az alábbi adatok alapján a válaszadók az első három feltételezésemet alátámasztották:

- A feltevésben szereplő nyilvántartásokat a 166 fő válaszadóból 77 fő alapnyilvántartásnak tekinti, és a munkájához elengedhetetlennek tartja, míg 57 fő azt nyilatkozta, hogy napi szinten használja azokat.
- Arra a kérdésre, hogy az adatközlőre mennyire igaz az az állítás, hogy munkája során nagy segítséget jelentenek számára a saját számítógépéről közvetlenül elérhető adatbázisok (nyilvántartások), 166 főből 44 fő nyilatkozta azt, hogy „nagyrészt igaz", míg 87 fő, hogy „teljes mértékben igaz".
- Arra a kérdésre, hogy mit gondol a rendőrség számára elérhető adatbázisok használhatóságáról, 165 válaszadóból 162 fő nyilatkozta azt, hogy segítik vagy részben segítik a munkáját, ami a válaszadók 98%-át jelenti.
- 165 fő válaszadóból 135 fő (82%) azt nyilatkozta, hogy részt venne a munkahelye által szervezett – nem kötelező jellegű – olyan képzésen, ahol megismerhetné a nemzeti adatvagyon körébe tartozó nyilvántartásokat, adatbázisokat.
- A 166 fő válaszadóból 144 fő (86%) úgy gondolja, hogy a rendészeti (például rendőrségi) munkában az adatbázisok, nyilvántartások minél szélesebb körű ismerete elengedhetetlenül szükséges, mivel a jövőben a digitalizáció térnyerésének köszönhetően ennek segítségével hatékonyabban lehetne dolgozni.
- A megkérdezettek közül 47 fő nyilatkozta, hogy hallott a raszternyomozásról, az interoperabilitási e-nyomozásról, míg 79 az OSINT-ról (nyílt információgyűjtésről), azonban 73 fő azt nyilatkozta, hogy egyikről sem hallott.
- Azokra a kérdésekre, hogy a más hatóság által vezetett nyilvántartásokról, az új nyomozati módszerekről és az új technikai eszközökről milyen módon tájékozódik, a legtöbb válaszadó azt nyilatkozta, hogy azokról a munkatársaitól, illetve a vezetőtől informálisan értesül.

Arra a kérdésre, hogy sorolja fel azokat a nyilvántartásokat, adattárakat, amelyeket eddig a munkája során használt – a kérdőívben említetteken kívül (beleértve a megkeresés útján elérhető nyilvántartásokat és a közvetlenül elérhető nyilvántartásokat is) a válaszadók száma már lecsökkent 76 főre, ami csak 45%-os

válaszadói arány a korábbihoz képest. Ez is arra utalhat, hogy általában csak az alapnyilvántartásokat használják a munkájuk során, amelyeket közvetlenül, portálszerűen érnek el az irodából.

Az alábbi válaszok alapján az utolsó feltételezésem is megerősítést nyert:

- a válaszadók csak 54%-a hallott, míg 46%-a még nem hallott a deepfake-ről;
- 57%-uk még nem látott deepfake videót, csak 43%-uk;
- 28%-uk már találkozott munkája során kép- és/vagy videómanipulációval;
- a válaszadók 90%-a részt venne a munkahelye által szervezett – nem kötelező jellegű – olyan képzésen, ahol megismerhetné azokat a kriminalisztikai ajánlásokat, amelyek a fake news-zal és a deepfake-kel megvalósítható bűncselekmények felderítésével kapcsolatosak;
- az alanyok/hallgatók 96%-a szerint szükség lenne egy módszertani útmutató/segédlet kidolgozására az arcképcserés videók (deepfake) nyomozásához.

A fenti válaszok a képzések szükségességét is alátámasztják, továbbá megerősítik azt a feltételezésemet, hogy a válaszadók hajlandók képezni magukat.

A Nemzeti Közszolgálati Egyetem Rendészettudományi Karán a nyilvántartások egy részét – például a bűnügyi nyilvántartásokat – oktatjuk, azonban szükség lenne

- a digitalizáció gyorsasága, a mesterséges intelligencia által kínált lehetőségek oktatására;
- a több ezer már meglévő nyilvántartás/adatbázis,[352] illetve további adatnyilvántartások feltérképezésére és oktatására, valamint elengedhetetlen a kriminalisztikai ajánlások megfogalmazása, amelyek az adatok hatékony feldolgozását segíthetik elő, illetve információs áradat elindítói lehetnek;
- az elkövetők által hátrahagyott digitális nyomok felkutatásának, megismerésének, elemzésének és értékelésének oktatására;

[352] „Nagyjából 100-120 olyan nagy állami nyilvántartás van, amely a zömét adja a magyar nemzeti adatvagyonnak, de ha minden apró nyilvántartást is számba veszünk, akkor tízezret meghaladja ez a nyilvántartási rendszer, és nagyon vegyes." Idézi: Infostart/Inforádió – Király 2020.

– a modern technikai eszközök, elemzőprogramok megismertetésére;
– a bűncselekmények nyomozására vonatkozó legújabb ismeretek, legkorszerűbb vizsgálati módszerek és taktikai ajánlások megismerésére és elsajátítására.

Célszerű lenne önálló tantárgy keretében oktatni a raszternyomozási, az interoperabilitási e-nyomozási és OSINT-tal (nyílt forrású információgyűjtés) kapcsolatos ismereteket.

Nemcsak az iskolarendszerű képzésben tartom fontosnak a naprakész információk oktatását a nyilvántartások és a digitális adatok vonatkozásában, hanem a gyakorlati szakemberek továbbképzésében is. Olyan képzéseket kellene szervezni a rendészeti egységeknél, amelyek az e-nyomozás és a nyilvántartások jelentőségét mutatnák be olyan módon, hogy az elméleti ismereteket ötvözik a gyakorlattal. Erre kiválóan alkalmas lenne a Belügyminisztérium Rendészeti Vezetőkiválasztási, Vezetőképzési és Továbbképzési Főosztály Rendészeti Továbbképzési Rendszere.

A Rendészeti Továbbképzési Rendszer honlapján az alábbiak olvashatók: „Célunk olyan továbbképzési rendszer, illetve továbbképzési kultúra kialakítása, amely nem csak intézményesíti a továbbképzést, hanem értéket közvetít és hagyományt teremt." E célkitűzést figyelembe véve célszerűnek tartanám a belső továbbképzési program keretein belül „e-nyomozás" címmel egy képzési programot indítani, amelyre a jelentkezés önkéntes lenne. A képzés magában foglalná a raszternyomozáson keresztül az e-nyomozást, az OSINT, valamint a digitális adatok felhasználásának lehetőségeit, figyelemmel a nyilvántartásokra, illetve a fake news és deepfake jelenségekre, illetve a forenzikus igazságügyi nyelvészetre.

A képzés lehetőséget adna a gyakorlati szakemberek számára információcserére, illetve a jó gyakorlatok megismerésére és elsajátítására is. A képzésen célszerű lenne nemcsak a nyomozó hatóságnak képviseltetnie magát oktatóként és hallgatóként, hanem az ügyészségnek is. Ez lehetőséget teremtene a közös módszertani útmutatók kidolgozására, vagy a meglévő szakmai anyagok átdolgozására.

9. A kutatási eredmények összefoglalása

A tanulmány első nyolc fejezete átfogja a kutatási téma három irányvonalát a digitális adatok (1–8. fejezet) és a modern technikai eszközök (4–6. és 8. fejezet) jelentősége a kriminalisztikában témakört, valamint a deepfake és a fake news jelenségek (7–8. fejezet) területét.

Az 1. fejezetben tárgyaltam a digitális közigazgatást kriminalisztikai nézőpontból, amely magába foglalta az elektronikus ügyintézést, a nemzeti adatvagyont és adatgazdálkodást, a Nemzeti Adatvagyon Ügynökséget és a Nemzeti Adatvagyon Tanácsot, a digitális állampolgárságot és az e-nyomozási ökoszisztémát.

Az elektronikus közigazgatási szolgáltatások, illetve az állami érdekkörbe tartozó egyéb elektronikus (például egészségügyi, oktatási, könyvtári, kulturális örökséghez kapcsolódó vagy az állami adat- és információs vagyon megosztását célzó) szolgáltatások igénybevétele során nap mint nap hatalmas mennyiségű adat keletkezik, amelyek a nemzeti adatvagyon részét képezik. Ezeknek az adatoknak a keletkezését nagymértékben elősegítik az elektronikus ügyintézési szolgáltatások.

Az elektronikus ügyintézési szolgáltatás mesterséges intelligenciával támogatott, amely három csoportra bontható:

- a mesterséges intelligenciával támogatott hangképzés szolgáltatás (célja az elektronikusan rendelkezésre álló szövegek gépi úton hangalapú beszéddé alakítása);
- a mesterséges intelligenciával támogatott hangleiratozás szolgáltatás (célja az élő beszéd, valamint az archív-mentett médiaanyagokban a digitálisan rögzített beszéd írásos szöveggé alakítása);
- a mesterséges intelligenciával támogatott kommunikációs asszisztens (olyan szoftvermegoldás, amely képes az emberek között megvalósuló párbeszédhez rendkívül hasonló beszélgetés lefolytatására és interaktív kommunikációra valós személy közreműködésével kollaboratív módon, illetve valós személy beavatkozása nélkül, automatizáltan és gépi öntanuló folyamat révén képes a fejlődésre).

Javaslatként fogalmaztam meg, hogy a mesterséges intelligenciával támogatott hangleiratozás szolgáltatás keretében létrejött hangfájl rögzítését és feldolgozását lehetővé kellene tenni, mivel ez a bűnüldöző szerveknek újabb lehetőséget adna a bűncselekményt elkövető személyek beazonosítására. A bírói engedélyhez

kötött leplezett eszköz keretében alkalmazott lehallgatás esetén – amennyiben a lehallgatott személy személyazonossága nem ismert –, ha a hangleiratozás során a hangfájlt rögzítenék, akkor az összehasonlítható lehetne a lehallgatási közlemény hanganyagával. Így a célszemély beazonosíthatóvá válhatna, amennyiben a célszemély korábban hangleiratozó szolgáltatást vett igénybe.

Az Országgyűlés felismerte, hogy a korszerű digitális államkormányzás és gazdaság megvalósítása szintén a mesterséges intelligencián és adatelemzésen alapuló technológiák elterjedésével történhet meg, ezért létrehozta a Nemzeti Adatvagyon Ügynökséget, amelynek képesnek kell lennie a nemzeti adatvagyon széles körű hasznosítására. Azonban az ügynökség az adatvagyont és annak hasznosíthatóságát elsősorban nem kriminalisztikai (rendészeti) oldalról vizsgálja. A jövőben fontos a rendészeti szerveknek együttműködés keretében az ügynökséggel közös kutatásokat folytatni, hogy ezáltal elősegítse a bűnügyi e-nyomozási ökoszisztéma kialakulását.

A digitalizációt, a digitális állampolgárságot, valamint az e-közigazgatási folyamatokat (az elektronikus szolgáltatást) elősegíti az önkiszolgáló mesterséges intelligenciával támogatott ügyintézési pont, az úgynevezett kiosk-eszköz, amely segítségével az állampolgári ügyintézési folyamatok automatizálódnak, továbbá az elektronikus ügyintézés lehetősége azok számára is elérhető a Mesterséges Intelligencia Asszisztens szolgáltatáson keresztül, akik nem rendelkeznek megfelelő saját technikai eszközzel. Az önkiszolgáló mesterséges intelligenciával támogatott ügyintézési pontok kriminalisztikai jelentőségűek, mivel hozzájárulhatnak akár az elkövetők beazonosításhoz, vagy az általuk használt telefonszámok megismeréséhez is, mivel számos digitális adat visszafejthető.

Az elektronikus szolgáltatások igénybevétele során az ügyfél többféleképpen azonosíthatja magát. Ha az ügyfél a videotechnológián keresztül történő azonosítást választja, akkor a személyazonosság igazolására alkalmas hatósági igazolványa bemutatásával és videojellel készített arcképének a nyilvántartásban tárolt arcképével való összevetésével azonosítja magát. Az arckép-azonosítás – a mesterséges intelligencia segítségével – nemcsak a közigazgatási ügyek intézését teheti egyszerűbbé, hanem hozzájárul az automatikus határátlépési pont kialakításhoz is, amely a határforgalom gyorsítását és egyszerűsítését fogja elősegíteni, az ott szolgálatot teljesítő állomány tevékeny közreműködése nélkül.[353] A biometrikus azonosítás a mesterséges intelligenciával párosulva számos

[353] A mesterséges intelligencia területén megvalósult fejlesztések, a Belügyminisztérium tájékoztatása. Lásd részletesebben: Hajzer 2021.

lehetőséget fog megnyitni, amelyeket ki kell használniuk nemcsak az állampolgároknak az e-közigazgatási ügyintézési folyamatoknál, hanem a hatóságnak is a felderítés és a bizonyítás során.

A *magyarorszag.hu* webes felületen azonosítás nélküli publikus szolgáltatások is elérhetők, úgymint az általános jellegű információk, ügyleírások, azonban a felületen több mint 300 elektronikus szolgáltatás érhető el.[354] A *magyarorszag.hu* internetes oldalról nagyjából 3700 hivatali szervet lehet elérni, amelyen keresztül 80 ezer kérelem érkezik havonta.[355] Ez az óriási kérelemmennyiség szintén adathalmazok sokaságát hozza létre, amely egy bűnügyben digitális lábnyomként szolgálhat.

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 32. § (7) bekezdése alapján az ügyfél-regisztrációs szerv az ügyfél hozzájárulása nélkül a következő szervek részére adhatja meg a kliens általa kezelt adatait:

> „*a)* a bíróságnak az előtte folyamatban lévő eljárásban részt vevő személyekre vonatkozó tényállítások helytállóságának, továbbá a bemutatott okirat adattartalma valódiságának ellenőrzése, valamint büntetőeljárás lefolytatása vagy büntetés és intézkedés végrehajtása céljából,
> *b)* a nyomozó hatóságnak bűncselekmények megelőzése, felderítése, büntetőeljárás lefolytatása vagy büntetés és intézkedés végrehajtása céljából,
> *c)* az ügyészségnek az ügyészségről szóló törvényben meghatározott közérdekvédelmi és törvényességi felügyeleti feladatainak ellátása, valamint a bűncselekmények megelőzése, felderítése, büntetőeljárás lefolytatása vagy büntetés és intézkedés végrehajtása céljából,
> *d)* a nemzetbiztonsági szolgálatnak a törvényben meghatározott felderítési, nemzetbiztonsági védelmi és elhárítási, információszerzési, továbbá nemzetbiztonsági, iparbiztonsági, belső biztonsági és bűnmegelőzési ellenőrzési célból,
> *e)* a rendőrségről szóló törvényben meghatározott terrorizmust elhárító szervnek a rendőrségről szóló törvény alapján hatáskörébe tartozó bűncselekmények megelőzése, illetve megszakítása, továbbá személyvédelmi és létesítménybiztosítási feladatai ellátása céljából."

A *magyarorszag.hu* felületen elérhető szolgáltatások háttérnyilvántartásaiban szereplő adatok közvetlen elérése a terrorizmus elleni küzdelemben, bűnmegelőzési, bűnfelderítési célú feladatok végrehajtásában, a bűncselekményből származó vagyon visszaszerzésében, valamint az idegenrendészeti és menekültügyi feladatok ellátásában is segítségül szolgálhatna.

[354] Orbán 2019: 117.

[355] Molnár–Sasvári–Tarpai 2021: 6–7.

Ezért javaslatként fogalmaztam meg, hogy célszerű lenne kiépíteni a rendészeti szerveknél portálszerűen egy automatikus adatszolgáltatási rendszert, hogy a szolgáltatások háttérnyilvántartásaihoz, az azokban található nemzeti adatvagyonhoz a bűnüldöző szervek közvetlenül hozzáférjenek, hasonlóan a személy- és lakcímnyilvántartáshoz vagy a gépjármű-nyilvántartáshoz, amelyeket már évek óta elérnek. Ha a nyomozó hatóság az ügyészség engedélyével kérhet adatszolgáltatást a Be. alapján, akkor az ügyészség engedélye is kellene a rendszerben. Hasonlóan működik a rendőrség által használt Robotzsaru rendszer is: amikor például a Vodafone automatikus adatszolgáltatási rendszerén (AAR) keresztül történik az adatszolgáltatás (AAR–RZS interfészen keresztül), akkor technikailag az ügyész mint engedélyező is része ennek a folyamatnak. Az adatszolgáltatás (lekérdezés) jogszabályi háttere már kidolgozott, amit az említett példák is alátámasztanak, azonban szükséges az informatikai háttér megteremtése.

Kriminalisztikai értelemben több konkrét példa szerepelt a fejezetekben, amikor szükséges és indokolt az adatkérés, amely számos intézkedést generálhat. Továbbá az adatszolgáltatás hozzájárulhat a bűnmegelőzéshez, mivel a gyors adatszolgáltatásnak és a releváns információknak köszönhetően sikerülhet egyrészt a múltbeli esemény megismerése, másrészt a jelenben zajló vagy a jövőben tervezett bűncselekmények megakadályozása.

A 2. fejezetben az úgynevezett kriminalisztikai nyilvántartásokat tárgyaltam, amelyek magukban foglalják a bűnügyi nyilvántartási rendszert, azon belül az alapnyilvántartásokat mint a nemzeti adatvagyon részét, amelyeket rendszeresen használnak a nyomozó hatóság tagjai. Az egyes nyilvántartások, például a bűnügyi nyilvántartások adataihoz vagy a Netzsaru rendszer elektronikus adatbázisához – jogosultsági szinttől függően – a bűnüldöző szervek munkatársai közvetlenül hozzáférhetnek. A nyomozó hatóságnak a nyomozás során be kell szereznie a gyanúsított bűnügyi előéletére vonatkozó adatokat, ebben nyújt segítséget a bűnügyi nyilvántartási rendszer. Feladat hárul a bűnügyi nyilvántartások tekintetében a bíróságra is, mivel be kell szereznie

> „a vádlott bűnügyi előéletére vonatkozó adatokat és a szabálysértési nyilvántartási rendszer vádlottra vonatkozó adatait, valamint hivatalból beszerezheti a jogszabállyal rendszeresített egyéb közhiteles nyilvántartásnak a vádlottra, illetve a vád tárgyára vonatkozó adatait. A bíróság gondoskodik a vádlottra vonatkozó, az eljárásban figyelembe vehető tagállami ítélet megfeleltetéséről vagy külföldi ítélet érvényének az elismeréséről."[356]

[356] 2017. évi XC. törvény a büntetőeljárásról 498. § (3).

Továbbá

> „a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény alapján a bűnügyi nyilvántartás a bűntettesek nyilvántartása mellett tartalmazza a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartását is. Ez utóbbi nyilvántartásba egyebek mellett azon személyek korábbi elítéléseivel kapcsolatos adatok kerülnek, akiknek az adatait a bűntettesek nyilvántartásából a mentesítés folytán törölték (2009. évi XLVII. tv. 15. §). Ez a nyilvántartás teremti meg tehát a bűnismétlés, illetve a visszaesés büntetőjogi értékelésének alapját, lehetőséget biztosítva az előzményi elítélésekből fakadó hátrányos jogkövetkezmények alkalmazására az esetekben is, amikor az elítélt a büntetett előélethez fűződő hátrányos jogkövetkezmények alól már mentesült. Ha azonban az elítélttel kapcsolatos adatokat a mentesítést követően a hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartásából is törlésre kerültek, hátrányos jogkövetkezmény ezen elítélés miatt a terhelttel szemben a Btk. 97. § (2) bekezdés 1. mondatának II. fordulata alapján már nem alkalmazható, azaz a törölt elítélés, az elkövető személyében rejlő társadalomra veszélyességet növelő súlyosító körülményként, de például az üzletszerű minősítés alapját képező tényként sem értékelhető."[357]

A kriminalisztikai nyilvántartásoknak (a bűnügyi nyilvántartási rendszernek, a bűnügyi és rendészeti biometrikus adatok nyilvántartásának, az eModus-nak és a körözési nyilvántartási rendszereknek), valamint a digitális közigazgatás nyilvántartásainak (a *magyarorszag.hu* platform alapján) elengedhetetlen szerepe van a büntetőeljárások (nyomozások) során. Az „elektronikus nyomok" segítségével megválaszolhatjuk a kriminalisztikai alapkérdéseket, illetve a hét kriminalisztikai alapkérdés kiegészíthető a *milyen?* kérdéssel. A *milyen?* kérdés egyrészt utalhat arra, hogy milyen lehet az elkövető, milyen az elkövető személyisége, milyen digitális nyomokat hagy maga után. Másrészt iránymutatást adhat, hogy milyen elektronikus (digitális) adat beszerzésére van szükség. *Az adatvagyon felhasználására vonatkozó esetfeldolgozás* című 2.9. alfejezet szemlélteti a *milyen?* kérdés jelentőségét.

A digitális közigazgatás kriminalisztikai megközelítésből című 1. fejezet és *A kriminalisztikai nyilvántartások* című 2. fejezet kriminalisztikai nézőpontból egy egységet alkotnak, mivel az elektronikus (digitális) adatok hálószerűen összekapcsolódnak, pontosabban a bűnügyi e-nyomozási ökoszisztéma alapját képezik.

[357] Fővárosi Ítélőtábla Bf.31/2021/22. Testi sértés bűntettének kísérlete és más bűncselekmény.

A két fejezetben tárgyalt nyilvántartások a nemzeti adatvagyon részét képezik, amelyek több ponton kapcsolódnak. Ha egy bűnügyön (büntetőeljárásban) dolgoznánk, és ismernénk, hogy milyen digitális adatokat lehet beszerezni, akkor nagy valószínűséggel a nyomozás nem jutna holtpontra, mert a digitális adatok hozzájárulnának az eredményességhez. Ezt igazolja *Az adatvagyon felhasználására vonatkozó esetfeldolgozás* című alfejezet. A bemutatott ügyben több közhiteles és nem hiteles nyilvántartást, keresőportált, webes felületet, azonosító rendszert alkalmaztak: gépjármű-nyilvántartást; személyiadat- és lakcímnyilvántartást; Netzsaru rendszert; körözési nyilvántartást; telefontársaság nyilvántartását; Google-t; értékesítési oldalakat; közösségi oldalt; Modus Operandi Nyilvántartást (eModus); bűntettesek nyilvántartását; hátrányos jogkövetkezmények alatt álló, büntetlen előéletű személyek nyilvántartását; büntetőeljárás hatálya alatt állók nyilvántartását; arckép-azonosító rendszert (NSZKK); Végrendeletek Országos Nyilvántartását (VONY); ingatlan-nyilvántartást; daktiloszkópiai nyilvántartást; DNS-profil-nyilvántartást; VÉDA Közúti Intelligens Kamerahálózat rendszerét; Jármű Szolgáltatási Platformot (JSZP); cégnyilvántartást; Vitorlás Alsóörs Kft. parkolási nyilvántartását.

A nyilvántartásokban, webes felületeken, platformokon, azonosítási rendszerekben szereplő adatok az esetek többségében egymást kiegészítették, egy mozaik részét képezték, és információs láncsorozatot alakítottak ki, az abban megállapított adatok alapján lehetett eljutni az elkövetőhöz. A kérdéses ügyet több oldalról meg lehetett volna oldani, illetve számtalan nyomozási (bizonyítási) cselekményt kellett volna még foganatosítani, azonban a vizsgálat kizárólag a digitális adatok, nyilvántartások, a kriminalisztikai gondolkodás létjogosultságát kívánta kiemelni és bemutatni.

A 3. fejezetben az adatok hálózatának jelentőségét és a kriminalisztikai hálózatelemzési területeket tárgyaltam. A hálózati gondolkodás kiegészíti a kriminalisztikai gondolkodást, mivel hozzájárul, hogy a rendészeti szerv az adatalapú folyamatok részese legyen, és kialakuljon a bűnügyi digitális ökoszisztéma. Ebben segítségül lesz a jövőbeni adatvezérelt szolgáltató állam. Az adatvezérelt szolgáltató állam létrejöttével elkerülhetetlen lesz a kriminalisztikai (digitális) profilalkotás. A digitális profilalkotás a hálózatkutatással összhangban új tudást fog adni a nyomozónak, mivel az adatok elemzésével új összefüggések, kapcsolati hálók és trendek válnak azonosíthatóvá, ami hatékonyabb intézkedéseket fog kialakítani, valamint lehetővé válhat egy újfajta adatalapú döntéshozatal.

A digitális profilalkotás számtalan jogszabály létrejöttét fogja generálni. Azonban ezeknek a jogszabályoknak nem szabad alaptörvény-ellenességet

előidézniük, mivel a szabályozásnak összhangban kell állnia az Alaptörvénybe foglalt magánszféra tiszteletben tartásához való joggal, valamint a személyes adatok védelméhez való jog alkotmányos elvárásaival. Az adatok puszta készletező megőrzése is a személyes adatok védelméhez való alapjog korlátozását jelentheti, mert potenciálisan magában rejti a profilalkotás és ezáltal egy súlyos alapjogi sérelem lehetőségét.

A rendőrségnek a mesterséges intelligencián és adatelemzésen alapuló technológiákat érdemes használnia, valamint a big data elemzéseket és a közigazgatási adatbázisokban tárolt adatokat is célszerű megismernie, ki kell aknáznia. Az átláthatatlannak tűnő adatmennyiség vizsgálatát segíti a hálózatelemzés, amely sokszor felhívja a figyelmet arra is, hogy az elemzés hiányában mennyi információ maradt volna látenciában. Például a telefon- és az e-mail-adatok alapján össze lehet kötni a telefonálókat, megkaphatjuk az ismeretségek hálózatát, amely lehet szakmai, baráti és intim kapcsolatokat is felölelő hálózat.[358]

A hálózatelemzési módszerek és eszközök használata hozzájárulhat

- a bűnöző, bűnözői, valamint civil kapcsolatok, kapcsolatrendszer feltérképezéséhez;
- a bűnös vagyonelemek feltérképezéséhez;
- a múltbeli, a jelenben zajló és a jövőbeli cselekmények megismeréséhez;
- elkövetői tulajdonságok, magatartási formák megismeréséhez, ami nélkülözhetetlen a profilalkotásban is, annak a bázisát is adhatja.

A hálózatkutatásban rejlő lehetőségek feltárásával és az összefüggések vizsgálatával az innováció erősödhet és „adat-elkövető" információs láncsorozat, valamint elektronikusadat-alapú bűnügyi ökoszisztéma alakulhat ki. A hálózati gondolkodásmódnak jelentős szerepe van a bűnözők, bűnözői csoportok és a bűnszervezetek pénzügyi hálóinak a feltérképezésében, valamint a bűnelkövetők közötti kapcsolatábra elkészítésében. A bűnözői kapcsolatok és hálózataik elemzése a bűnözői magatartás megismeréséhez, megértéséhez vezethet.[359]

A hálózatkutatást támogató információgyűjtési módok, a HUMINT (Human Intelligence – az emberi erőforrással folytatott hírszerzés), az OSINT (Open Source Intelligence – nyílt hozzáférésű hírszerzés), a SOCMINT (Social Media Intelligence – közösségi médiában folytatott hírszerzés) és a TECHNIT (Technical Intelligence – technikai hírszerzés) segítségével lehetőség adódhat digitális

[358] Varga–Ruppert–Barabási 2019: 35.
[359] Van der Hulst 2009: 101.

adatok (elkövetőhöz köthető digitális nyomok) beszerzésére. A beszerzett adatok függvényében hálózatelemzés végezhető.

Szociológiai szempontból nézve hazánkban jelenleg 6 különböző generáció él egymás mellett, amelyeket átsző a digitális társadalom:

- építők generációja (1946 előtt születettek);
- babyboomer generáció (1946 és 1964 között születettek),
- X generáció (1965 és 1979 közöttiek),
- Y generáció (1980 és 1994 közöttiek),
- Z generáció (1995 és 2009 közöttiek),
- alfa generáció (2010 után születettek).

Ahogy haladunk előre, látható, hogy az utolsó generáció életének már elválaszthatatlan részét képezik a digitális eszközök, kialakult egy úgynevezett hálózati társadalom.[360]

A rendőrségnek vagy általánosságban véve a rendészeti szerveknek az adatalapú gazdasági és közszolgálati ökoszisztéma élvezőjének kell lennie, ezért a hálózattudomány alkalmazását érdemes bevezetni a rendészet területein is. A kriminalisztikai gondolkodás ismereteit ki kell egészíteni hálózati gondolkodási ismeretekkel, és célszerű elsajátítani az újdonságokat.

A 4. fejezetben az *Internet of Things* jelenségét tárgyaltam, amely négy alfejezetet foglalt magába: az IoT szabályozását, az Internet of Everythinget, az eSIM-et és az iSIM-et, illetve a mobilkészülék használata során keletkezett digitális adatokat. A „dolgok/tárgyak internete" és a „minden internet" már egymással párhuzamosan van jelen az életünkben, és a jövőben még jobban meg fogja határozni a mindennapjainkat és a bűnüldöző szervek munkáját is. Ezért az IoT és az IoE során keletkezett adattömeg feldolgozási folyamatában és felhasználásában a mesterséges intelligencia és a hálózattudományi kutatási módszerek alkalmazása is fontos lesz.

Az Iot-eszközök száma várhatóan 2030-ra 125 milliárdra fog növekedni.[361] Ezek az eszközök egymással fognak kommunikálni, digitális ökoszisztémát, kapcsolódási hálózatot, térképet fognak alkotni. Ezeknek az eszközöknek a hálózata kisebb méretben okosotthonokként, míg nagyobb kiterjesztésben okosvárosként jelentkezik. Az okosotthon hálózata kapcsolódhat egy másik otthon hálózatához,

[360] Krasznay 2020c: 122–123.
[361] IHS Markit 2017.

ezzel még összetettebb hálózat jön létre, illetve az okosotthon vagy az okosotthonok hálózata kapcsolódhat az okosváros hálózatához.

A mobil eszközök közül kriminalisztikai szempontból a mobiltelefonoknak kiemelt jelentőségük van, s mivel a jövőben a legtöbbet eSIM-mel vagy iSIM-mel hozzák majd forgalomba, indokolt volt az IoT fejezetén belül különálló alfejezetként tárgyalni a mobiltelefon használata során keletkező digitális adatokat, amelyek kriminalisztikai nézőpontból segítik a bűnüldöző szervek munkáját.

A mobiladatok kriminalisztikai jelentőségét egy konkrét eset tükrében tárgyaltam, azonban kiemeltem egy külön alfejezetben, hogy a készletező adatgyűjtéssel – kommunikációs profillal – létrejöhet az alapjog korlátozása.

A *Mobiltelefon használata során keletkezett digitális adatok* című fejezet oktatási segédanyagként is szolgálhat, illetve a gyakorló bűnüldöző szervek munkatársainak is szakmai segítséget jelenthet a mindennapi nyomozati munka során.

Az 5. fejezetben az okosváros és az okosrendőrség fontosságát tárgyaltam. A digitális ökoszisztémának jelentős szerepe van a bűnüldözés és a közbiztonság terén, mivel az elektronikus eszközök és szolgáltatások elérhetősége, illetve a fejlett informatikai háttér elősegíti a bűnmegelőzéshez kapcsolódó tevékenységek hatékonyságát, egyben eredményességét, valamint csökkenti a bűnüldöző szervek reakcióidejét, illetve gyorsítja az igazságszolgáltatás működését.[362]

Az okosváros alrendszerének vagy alapelemének kellene lennie az okosrendőrségnek, mivel az okosváros biztonságát, működését és fejlődését is akadályozhatja az okosrendőrség hiánya. Az okosrendőrség egy olyan állami szervezet, amely feladatainak ellátása során korszerű és innovatív információtechnológiákat alkalmaz, képes a digitalizáció, a hálózatkutatási elemzések és a mesterséges intelligencia nyújtotta lehetőségeket felhasználni, és alappillérként funkcionál. Az okosrendőrség egyik alapforrását pedig a nemzeti adatvagyonnak kellene képeznie.

Az okosváros és az okosrendőrség számtalan ponton tud csatlakozni, azonban a kutatás szempontjából a közös fő kapcsolatot a digitális közigazgatás valósítja meg az elektronikus szolgáltatáson keresztül. Az okosváros lakói ügyeiket elektronikusan intézik, ehhez azonban szükséges a korszerű és hatékony digitális közigazgatás, valamint egy elektronikus szolgáltatási háló. Az okosváros nyújtotta alkalmazások használatával számos digitális adatot hagyhatunk magunk után. Ugyanakkor az elkövetők is rengeteg digitális nyomot hagyhatnak maguk után, ami a raszter-, illetve az e-nyomozás keretében kapcsolódási

[362] *Nemzeti Infokommunikációs Stratégia 2014–2020* 2014: 16.

gócpontként hatékonyan segítheti a bűnüldöző szervek munkáját. Az okosváros ökoszisztémájában megjelenő szolgáltatások olaja a nemzeti adatvagyon, amely a digitális állampolgárság létrejöttében is domináns szerepet játszik. Az okosváros és az okosrendőrség kapcsolódási pontjait információláncként jól szemlélteti az 5.1-es és 5.2-es fejezet.

Az okosrendőrségnek élnie kell a mesterséges intelligencia nyújtotta lehetőségekkel, mivel annak az alkalmazásával a hatékonyság növelhető. A mesterséges intelligencia alkalmazásával az adatfeldolgozás és -értékelés gyorsasága növelhető, létrejöhet a real time reagálás a felhasználók számára, emberi közreműködés nélkül.[363] Tekintettel arra, hogy a mesterséges intelligencia jelentős hatást gyakorolhat a nyomozás kimenetelére és annak eredményességére, szükséges, hogy kiépüljön az abba vetett bizalom a hatóság tagjainak részéről.

A 6. fejezetben a modern technikai eszközöket kriminalisztikai nézőpontból vizsgáltam. Ennek keretében bemutattam és elemeztem az alábbi eszközöket és programokat: infrakamera és hőkamera, 3D lézerszkennerek, 3D nyomtató, talajradar és fémkereső, drón, UFED, röntgensugaras vizsgáló, CT-vizsgálat, spektrométer, BriefCam, Gangikonspi, arckép-azonosító rendszer, multispektrális UV/VIS és IR megjelenítő eszköz (Forensic Tablet) és artificial nose (elektronikus orr). A modern technikai eszközök használata több oldalról járulhat hozzá a bűnüldöző szervek munkájához: közreműködhet a múltbeli releváns esemény megismerésében; megkönnyítheti a bűnös tevékenység felismerését, valamint elősegítheti az adatelemző és értékelő munkafolyamatot.

A 7. fejezet a deepfake és a fake news jelenséggel, valamint az igazságügyi (forenzikus) nyelvészettel foglalkozott. A fejezeten belül pedig külön alfejezetben tárgyaltam a közösségi média és a bűnüldözés kapcsolatát. Az álhírek és a deepfake videók megjelenésére aggodalommal tekintettek a felhasználók és a szakemberek.[364] A deepfake jelenség tekintetében még nincs közvetlen büntetőjogi szabályozás (tényállás).

A fake news és deepfake jelenség felderítése kihívás elé állítja a nyomozó hatóság tagjait. Egyrészt lehet, hogy egy deepfake vagy fake news jelenség közvetetten egy elkövetési magatartás részét képezi. Másrészt az álhírek és álvideók félrevezethetik a hatóságot, és hamis/valótlan tartalmú információáradatot indíthatnak el, amely hatással lesz egyes bizonyítási cselekmények végrehajtására

[363] Nagy 2021: 226.
[364] Molnár–Rab 2021.

és azok eredményének ellenőrzésére is. Az elkövetők szándékosan hamis videókat, felvételeket juttathatnak el a hatóságnak, illetve akár a sértettek is manipulálhatják a felvételeket, aminek több oka is lehet, például a harag, a boszszú, a megtorlás. A felvételek elemzése időt fog elvenni a hatóságtól, ezáltal sérülhet a nyomozás gyorsaságának az elve is, ha nem veszik észre, hogy egy deepfake felvétellel állnak szemben. Ebben a jövőben segítségre lehet a mesterséges intelligencia alkalmazása, amelynek használatával időben kiszűrhetővé válhatnak a hamis felvételek.

A fake news kiszűrésében a nyelvi profil nyújthat segítséget, amelyhez szükséges lehet egy nyelvi adatbázis létrehozása is, hasonlóan a daktiloszkópiai nyilvántartáshoz, amely ujj- és tenyérnyomtöredékeket, valamint ujj- és tenyérnyomatokat tartalmazó nyilvántartás. Az álhírekkel az elkövető nyelvi ujjnyomot hagyhat maga után, de az álvideókkal is, amennyiben valamilyen szöveg elhangzik, ezért szükséges lehet az igazságügyi (forenzikus) nyelvész igénybevételére is.

Továbbá a fake news és a deepfake jelenségek hatással lehetnek az infokommunikációs szolgáltatásokra, a közösségi média által nyújtott platformokra, valamint az információs és a kommunikációs technológiai háttéren alapuló elektronikus szolgáltatásokra is, ezáltal veszélyeztetve az okosváros működését.

A közösségi média különböző internetes felületein is számos elektronikus nyomot hagyhatnak az elkövetők azáltal, hogy egymással digitálisan kommunikálnak, közösségi oldalakat látogatnak és profilokat hoznak létre. Számos digitális adat visszafejthető, ami az elkövetőre vonatkozóan árulkodó lehet, még a deepfake vagy fake news jelenségek esetén is.

Javaslatok:

- a deepfake és fake news esetében egy nyelvi (elkövetői) adatbázis létrehozása a daktiloszkópiai nyilvántartáshoz hasonlóan, amely elősegítené a nyelvi profil elkészítését;
- a forenzikus (igazságügyi) nyelvész feladatáról és tevékenységéről szóló szakmai előadás a nyomozó hatóság gyakorló tagjai számára;
- konkrét ügyek ismertetésével és elemzésével felhívni a figyelmet a szakértői tevékenység jelentőségére;
- bűnmegelőzési kisfilmek készítése a fiatalkorúak és az időskorúak számára a deepfake és a fake news jelenségekről.

A 8. fejezetben a Digitális adatok, modern technikai eszközök jelentősége a kriminalisztikában és a deepfake, fake news jelenség témakörben végzett kérdőíves kutatás eredményét elemeztem és tárgyaltam.

A kutatás során az alábbi megállapításokra jutottam:

- a válaszadók hajlandók képezni magukat a témával kapcsolatban;
- a válaszadók jelentős része már alkalmazza munkája során a bűnügyi nyilvántartásokat, a Robotzsaru NEO rendszert, valamint a gépjármű-nyilvántartást, a személy- és lakcímnyilvántartást és a körözési nyilvántartást;
- az adattárakkal és modern technikai eszközökkel kapcsolatos képzésekre igény van a levelezős hallgatók körében, továbbá a raszternyomozásról, interoperabilitási e-nyomozásról, valamint az OSINT-ról (nyílt forrású információgyűjtésről) a válaszadók többsége nem hallott;
- egyrészt a más hatóság által vezetett nyilvántartásokról, másrészt az új nyomozati módszerekről és az új technikai eszközökről informálisan tájékozódnak a válaszadók;
- a válaszadók (hallgatók) a kép- és/vagy videómanipulációval kapcsolatos ismeretei fejlesztésre szorulnak, és igény merült fel a képzésre, valamint szükségesnek tartanák egy módszertani útmutató/segédlet kidolgozását az arcképcserés videók (deepfake) nyomozásához.

A Nemzeti Közszolgálati Egyetem Rendészettudományi Karán a nyilvántartások egy részét, például a bűnügyi nyilvántartásokat, illetve egyes adatgyűjtési módszereket, például a raszternyomozást és az OSINT-ot oktatjuk, azonban szükség lenne

- a digitalizáció gyorsasága, a mesterséges intelligencia által kínált lehetőségeknek az oktatására;
- a több ezer már meglévő nyilvántartás/adatbázis, illetve további adatnyilvántartások feltérképezésére és oktatására, valamint elengedhetetlen a kriminalisztikai ajánlások megfogalmazása, amelyek az adatok hatékony feldolgozását segíthetik elő, illetve egy információs áradat elindítói lehetnek;
- az elkövetők által hátrahagyott digitális nyomok felkutatásának, megismerésének, elemzésének és értékelésének oktatására;
- a modern technikai eszközök, elemzőprogramok megismerésére;
- a bűncselekmények nyomozására vonatkozó legújabb ismeretek, legkorszerűbb vizsgálati módszerek és taktikai ajánlások megismerésére és elsajátítására.

Ezért célszerű lenne önálló tantárgy keretében oktatni a raszternyomozási, az interoperabilitási e-nyomozási és OSINT-tal (nyílt forrású információgyűjtés) kapcsolatos, valamint a digitalizációs ismereteket a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar nappali és levelező munkarendben tanuló bűnügyi és rendészeti BA szak III. évfolyam, valamint a kriminalisztikai mesterszak II. évfolyam hallgatóinak. A tantárgyi programot a szakok képzési céljának megfelelően kellene kidolgozni. A vizsgált adatgyűjtési módszerek egyes tantárgyaknak már a részét képezik, de a digitális nyomozás témakörét lefedő tantárgy jóval nagyobb szeletet foglalna magába a digitalizációból, mivel tartalmazná

- a nemzeti adatvagyon feldolgozását;
- a digitális közigazgatás nyújtotta lehetőségeket;
- konkrét esetek feldolgozását, esettanulmányokat;
- a digitális lábnyomokkal párhuzamosan a modern technikai eszközök ismertetését kriminalisztikai nézőpontból;
- a bűnügyi nyomozási ökoszisztéma folyamatait;
- a digitalizációval és a technológiai fejlődéssel kapcsolatos kutatások eredményeit kriminalisztikai nézőpontból;
- valamint ami a legfontosabb, az NKE Államtudományi és Nemzeti Tanulmányok Kar, a Hadtudományi és Honvédtisztképző Kar, a Víztudomány Kar, valamint a Kutatóközpontok, Intézetek kutatási eredményeinek ismertetését kriminalisztikai nézőpontból. Az NKE karainak és kutatóközpontjának tudományos kapcsolódási pontjait feltárná, és ezáltal azoknak az eredményei is egy ökoszisztéma és a közös gondolkodás részévé válhatnának.

A tantárgy sokoldalúsága is utal arra, hogy a digitalizáció, a tudományos technikai fejlődés rohamos előremenetele egy önálló tanszéket is igényelne, amelynek fő oktatási és kutatási területe a digitálizáció kriminalisztikai megközelítése lenne.

Irodalomjegyzék

AI a videórendszerekben – kuriózumból hétköznapi megoldások (2021). *ITBusiness,* 19(3), 30–31. Online: https://epa.oszk.hu/04200/04265/00003/pdf/EPA04265_itbusiness_2021_03.pdf

Allcott, Hunt – Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* 31(2), 211–236. Online: https://doi.org/10.1257/jep.31.2.211

Ambrus István (2021): *Digitalizáció és büntetőjog.* Budapest: Wolters Kluwer Hungary.

Anton Paar [é. n.]: *Kézi Raman-spektrométer: Cora 100. Kézi Raman-spektrométer az anyagok egyszerű azonosításához.* Online: www.anton-paar.com/hu-hu/termekek/reszletek/kezi-raman-spektrometer-cora-100/

Ariosz Kft. (2020): *Az elektronikus hírközlési piac fogyasztóinak vizsgálata. Háztartási felmérés – 2020.* Nemzeti Média- és Hírközlési Hatóság. Online: https://nmhh.hu/dokumentum/218695/haztartasi_felmeres_2020.pdf

Ariosz Kft. – NRC Kft. (2016): *Lakossági internethasználat. Online piackutatás 2016. Kutatási jelentés az NMHH részére.* Online: https://nmhh.hu/dokumentum/187704/lakossagi_internethasznalat_2016.pdf

Árvai Anett (2022): Az okos város fogalom megjelenése a magyar közép- és nagyvárosok fejlesztési dokumentumaiban. *Földrajzi Közlemények,* 146(1), 16–32. Online: https://doi.org/10.32643/f k.146.1.2

Az e-közigazgatásban is hasít a mesterséges intelligencia (x). *Portfolio,* 2022. szeptember 29. Online: https://www.portfolio.hu/premium/20220929/az-e-kozigazgatasban-is-hasit-a-mesterseges-intelligencia-569439

Balázs (2021): Mi az az IMEI szám, miért fontos és hogy találjuk meg a telefonunkon? *Startlap.hu,* 2021. március 27. Online: www.startlap.hu/vasarlas/imei-szam-telefon-biztonsag/

Balla József (2019): *A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ-, illetve közbiztonság alakulására.* Budapest: Dialóg Campus Kiadó. Online: http://hdl.handle.net/20.500.12944/12779

Balláné Füszter Erzsébet (2017): Új technikai eszközök és módszerek a rendvédelmi munkában. In Boda József – Felkai László – Patyi András (szerk.): *Ünnepi kötet a 70 éves Janza Frigyes tiszteletére. Liber amicorum in honorem Friderici Janza septuagenarii.* Budapest: Dialóg Campus Kiadó, 65–74.

Balláné Füszter Erzsébet (2019): *Kriminál technika.* Budapest: Dialóg Campus Kiadó.

Balláné Füszter Erzsébet (2020): New Technical Devices and Methods in Crime Scene Investigation. *Journal of Eastern-European Criminal Law,* (1), 29–36.

Bálint László (2018): A Terrorelhárítási Információs és Bűnügyi Elemző Központ. In Resperger István (szerk.): *Nemzetbiztonsági alapismeretek.* Budapest: Dialóg Campus Kiadó, 129–141.

Bányász Péter (2018): *Közösségi média és közszolgálat.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet.

Bányász Péter (2020): Közösségi média a közigazgatásban. In Sasvári Péter (szerk.): *Az informatikai rendszerek a közszolgálatban II.* Budapest: Dialóg Campus Kiadó, 85–101. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15910/733_Informatikai_rendszerek_kozszolgalatban_II.pdf

Bányász Péter et al. (2019): Lélektani műveletek a közösségi médiában. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus Kiadó, 111–133.

Baráth Noémi Emőke (2022): Kutatói aranybánya? A Modus Operandi Nyilvántartás kutathatósága. *Belügyi Szemle,* 70(1), 17–30. Online: https://doi.org/10.38146/BSZ.2022.1.1

Baumgartner, K. – Ferrari, S. – Palermo, G. (2008): Constructing Bayesian Networks for Criminal Profiling from Limited Data. *Knowledge-Based Systems,* 21(7), 563–572. Online: https://doi.org/10.1016/j.knosys.2008.03.019

Baumgartner, K. C. – Ferrari, S. – Salfati, C. G. (2005): Bayesian Network Modeling of Offender Behavior for Criminal Profiling. *Proceedings of the 44th IEEE Conference on Decision and Control,* 2702–2709. Online: https://doi.org/10.1109/CDC.2005.1582571

Behera, Bhagaban et al. (2019): Electronic Nose: a Non-invasive Technology for Breath Analysis of Diabetes and Lung Cancer Patients. *Journal of Breath Research,* 13(2), 1–40. Online: https://doi.org/10.1088/1752-7163/aafc77

Beláz Annamária (2020): Appok a közigazgatásban. In Sasvári Péter (szerk.): *Informatikai rendszerek a közszolgálatban II.* Budapest: Dialóg Campus Kiadó, 29–49.

Benedek Zoltán (2018): Digitális adatok a helyszínen. *Belügyi Szemle,* 66(7–8), 147–160. Online: https://doi.org/10.38146/BSZ.2018.7-8.10

Béres János (2014): A hírszerzés feladatrendszere. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete*. Budapest: Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 117–128.

Berki Antal – Nyitrai Endre (2021): Mesterséges intelligencia gyakorlati alkalmazásának lehetőségei – okos város, okos rendőrség. *Rendőrségi Tanulmányok,* 4(3), 4–47.

Bischoff Georgina – Tánczi Tibor (2019): Innovatív adatbázisok létrehozásának lehetősége és gyakorlati haszna az illegális migrációhoz kapcsolódó büntetőeljárásokban. *Rendőrségi Tanulmányok,* 2(1), 29–68. Online: https://epa.oszk.hu/04000/04093/00005/pdf/EPA04093_rendorsegi_tanulmanyok_2019_1_029-068.pdf

Boda József főszerk. (2019): *Rendészettudományi szaklexikon.* Budapest: Dialóg Campus Kiadó. Online: http://hdl.handle.net/20.500.12944/14690

Boxert és viperát is találtak már a NAV ellenőrei a csomagröntgen segítségével (2021). *Szegedma,* 2021. augusztus 13. Online: https://szegedma.hu/2021/08/boxert-es-viperat-is-talaltak-mar-a -nav-ellenorei-a-csomagrontgen-segitsegevel

Bruckner Máté (2020): Ami ellen semmit nem tudsz tenni: deepfake-jelenségek a kampányokban. *Atv.hu,* 2020. január 14. Online: www.atv.hu/belfold/20200113-ami-ellen-semmit-nem-tudsz-tenni-deepfake-jelensegek-a-kampanyokban

Budavári Önkormányzat közterületet megfigyelő automatikus és intelligens kamerák helyszínei (2021). Online: https://budavar.hu/wp-content/uploads/2021/01/int_kam_2018.pdf

Christensson, Per (2014): Digital Footprint. *Techterms.com,* 2014. május 26. Online: https://techterms.com/definition/digital_footprint

Cover, Rob (2022): Celebrity Deepfakes Are All Over TikTok. Here's Why They're Becoming Common – and How You Can Spot Them. *The Conversation,* 2022. július 18. Online: https://theconversation.com/celebrity-deepfakes-are-all-over-tiktok-heres-why-theyre-becoming-common-and-how-you-can-spot-them-187079

Czékmann Zsolt – Cseh Gergely (2019): Elektronikus közszolgáltatások Magyarországon. In Czékmann Zsolt (szerk.): *Infokommunikációs jog.* Budapest: Dialóg Campus Kiadó, 73–88. Online: http://hdl.handle.net/20.500.12944/14474

Czékmann Zsolt – Cseh Gergely (2021): Az e-ügyintézés hazai szabályozása az EU jogalkotásának tükrében. *In Medias Res,* 10(2), 221–234.

Csáki-Hatalovics Gyula Balázs – Czékmann Zsolt (2019): Az elektronikus közigazgatás fogalma. In Czékmann Zsolt (szerk.): *Infokommunikációs jog.* Budapest: Dialóg Campus Kiadó, 15–23. Online: http://hdl.handle.net/20.500.12944/14474

Csizner Zoltán (2019): Az OSINT határai. *Nemzetbiztonsági Szemle,* 7(2), 19–31. Online: https://doi.org/10.32561/nsz.2019.2.2

Dankó Roland (2019): Hatékony konténer ellenőrzés a határátkelőhelyeken, a C-BORD projekt bemutatása. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata, 70–86. Online: https://doi.org/10.37372/mrttvpt.2019.1.4

Delfino, Rebecca A. (2019): Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act. *Fordham Law Review,* 88(3), 887–938.

Digitális Megújulás Cselekvési Terv 2010–2014. Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásért (2010). [H. n.]: Nemzeti Fejlesztési Minisztérium. Online: https://2010-2014.kormany.hu/download/7/0d/30000/Digitalis_Megujulas_Cselekvesi_Tervull.pdf

Dobák Imre – Tóth Tamás (2021): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle,* 69(2), 195–212. Online: https://doi.org/10.38146/BSZ.2021.2.2

Dobó Judit – Gyaraki Réka (2021): A mesterséges intelligencia egyes felhasználási lehetőségei a rendvédelmi területeken. *Magyar Rendészet,* 21(4), 67–81. Online: https://doi.org/10.32577/mr.2021.4.3

Dobos Klára et al. (2015): *Smart City Tudásplatform. Metodikai javaslat.* Budapest: Lechner Nonprofit Kft. Online: http://okosvaros.lechnerkozpont.hu/sites/default/files/2018-10/smart-city-tudasplatform-metodikai-javaslat.pdf

Dósa Imre – Polyák Gábor (2003): *Informatikai jogi kézikönyv.* Budapest: KJK-Kerszöv.

EESZT (2021): *Tájékoztató a személyes adatok Elektronikus Egészségügyi Szolgáltatási Térben megvalósuló kezeléséről az egészségügyi intézményben történő ellátás során.* Online: https://e-egeszsegugy.gov.hu/documents/26398/557047/EESZT_GDPR_erintett_tajekoztatasa_eu_intezmenyben_2021.pdf/2c05f1b9-9977-c9aa-923b-aafdebe15327

ELEKTROnet Online (2017): 2025-re már közel 100 milliárd IoT eszközt tartunk majd számon. *Elektronet,* 2017. június 28. Online: www.elektro-net.hu/uzlet/7996-2025-re-mar-kozel-100-milliard-iot-eszkozt-tartunk-majd-szamon?highlight=WyI1ZyJd

Erdész Viktor (2018): A SOCMINT helye, szerepe az összadatforrású hírszerzésben. *Felderítő Szemle,* 17(4), 27–41.

Európai Bizottság (2018): *A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. A közös európai adattér kialakítása felé.* Brüsszel, 2018. 04. 25. COM(2018) 237 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018DC0237

Európai Bizottság (2020a): *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése.* Brüsszel, 2020. 02. 19. COM(2020) 65 final. Online: https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_hu.pdf

Európai Bizottság (2020b): *A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI), 2020. Magyarország.* Online: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020

Eurostat (2021): *Statistics Explained. Archive: A digitális gazdaságra és társadalomra vonatkozó statisztikák – háztartások és magánszemélyek* Online: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:A_digit%C3%A1lis_gazdas%C3%A1gra_%C3%A9s_t%C3%A1rsadalomra_vonatkoz%C3%B3_statisztik%C3%A1k_%E2%80%93_h%C3%A1ztart%C3%A1sok_%C3%A9s_mag%C3%A1nszem%C3%A9lyek

Farkas Valér – Dalmadi István (2013): Elektronikus orr – az élelmiszervizsgálat sok célra használható új eszköze. *Élelmiszervizsgálati Közlemények,* 59(4), 171–183.

Fehér könyv a nemzeti adatpolitikáról (2016). Budapest: Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete. Online: www.magyary.hu/wp-content/uploads/2019/09/Adatpolitikai_feher_konyv_201608.pdf

Felkészültek a nyári utasforgalom növekedésre Röszkénél (2021). *Szegedma,* 2021. június 29. Online: https://szegedma.hu/2021/06/felkeszultek-a-nyari-utasforgalom-novekedesre-roszkenel

Ferentzi Tünde (2017): Arcról olvasnak. *Zsaru Magazin,* 2017. november 22. Online: www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/arcrol-olvasnak

Finszter Géza (2006): A bűnügyi nyilvántartás helyzete és fejlesztésének lehetőségei. In Irk Ferenc (szerk.): *Kriminológiai Tanulmányok 43*. Budapest: OKRI, 2006, 39–63.

Forgács Imre (2018): Szabályozható-e a közösségi média? *Jogtudományi Közlöny,* 73(12), 526–533.

Freddi, Sonia – Sangaletti, Luigi (2022): Trends in the Development of Electronic Noses Based on Carbon Nanotubes Chemiresistors for Breathomics. *Nanomaterials,* 17(12), 1–26. Online: https://doi.org/10.3390/nano12172992

Füzesi Ottó (2004): *A felderítés elméleti és gyakorlati kérdéseinek vizsgálata, különös tekintettel, az emberi erővel folytatott felderítésre.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar, Műveleti támogató tanszék. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/11979/ertekezes.pdf?sequence=1

Gajdács László – Szűcs Viktor (2020): A 3D-nyomtatás gyártástechnológiái, felhasználási területei, illetve az ebben rejlő potenciál. *Repüléstudományi Közlemények,* 32(1), 101–110. Online: https://doi.org/10.32560/rk.2020.1.7

Gál István László (2014): Az OSINT (Open Source Intelligence) mint a kémkedés lehetséges elkövetési magatartás. *Jura,* 20(1), 51–55.

Gál István László (2019): A kémkedés a magyar büntetőjogban. *Nemzetbiztonsági Szemle,* (7)2, 38–49. Online: http://doi.org/10.32561/nsz.2019.2.4

Gárdonyi Gergely (2021): Az állóképes arcképazonosítás Magyarországon. *Belügyi Szemle,* 69(7), 1133–1148. Online: https://doi.org/10.38146/BSZ.2021.7.3

Gárdonyi Gergely – Hautzinger Zoltán (2021): A kriminalisztikai kutatások fejlesztésének lehetősége. *Belügyi Szemle,* 69(10), 1725–1740. Online: https://doi.org/10.38146/BSZ.2021.10.3

Gellért Miklós (2021): IoT és kiberbűncselekmények szabályozása. *Biztonságtudományi Szemle,* 3(1), 15–23. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/100/110

Gellért Miklós (2022): Az IoT tartós barangolás szabályozásának eltérő megközelítéseinek áttekintése. *Biztonságtudományi Szemle,* 4(3), 55–63. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/230/206

GVU Center [é. n.]: *The Liar's Dividend: The Impact of Deepfakes and Fake News on Politician Support and Trust in Media.* Online: https://gvu.gatech.edu/research/projects/liars-dividend-impact-deepfakes-and-fake-news-politician-support-and-trust-media

Gyaraki Réka (2021): A közösségi média hatása a kiberbűncselekmények elkövetésére. *Magyar Rendészet,* 21(2), 67–82. Online: http://doi.org/10.32577/mr.2021.2.4

Gyimesi Áron – Somlyódyné Pfeil Edit (2021): Az adat és a kormányzás jelentősége az okos város stratégiai alapú értékteremtési folyamatában – Magyar nagyvárosok összehasonlítása egy szintetizáló ökoszisztéma modell keretében. *Tér és Társadalom,* 35(3), 59–86. Online: https://doi.org/10.17649/TET.35.3.3339

Haig Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.

Haig Zsolt (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle,* 15(2), 115–130. Online: https://doi.org/10.32563/hsz.2022.2.7

Hajzer Károly (2021): Fejlesztési irányok – mesterséges intelligencia a közigazgatás szolgálatában. Az MI alkalmazások terén elért eredmények az e-közigazgatás építőelemeiben, fejlesztés alatt álló MI alapú szolgáltatások, rendszerek. *Rendvédelem,* 10(1), 24–36.

Herédi István (2020): Az elektronikus adatokat érintő eljárási cselekmények végrehajtása. In Ruzsonyi Péter (szerk.): *Közbiztonság.* Budapest: Ludovika Egyetemi Kiadó, 1839–1852.

Hét dolog, ami nagyot változtat jövőre az életünkön (2018). Online: https://www.biztositas-info.hu/magazin/het-dolog-ami-nagyot-valtoztat-jovore-az-eletunkon/20181210-1700

Horváth Orsolya – Maróti Péter (2018): 3D nyomtatott fegyverek – vélt vagy valós veszélyek? *Pécsi Határőr Tudományos Közlemények,* 20, 73–78. Online: www.pecshor.hu/periodika/XX/horvath_maroti.pdf

Hudák Krisztina Eszter (2022): *Régészeti leletek illegális feltárásának és kereskedelmének megakadályozása.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola. Online: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Hudak_Krisztina_ertekezes.pdf

Hugyecz Enikő Henriett (2011): Ki a szerző? – Avagy hogyan profiloznak a laikusok? *E-nyelvmagazin.hu,* 2011. augusztus 31. Online https://e-nyelvmagazin.hu/2011/08/31/ki-a-szerzo-%E2%80%93-avagy-hogyan-profiloznak-a-laikusok/

Hulkó Gábor (2021): Fake news és social media: szabályozás és közigazgatási intézkedések Szlovákiában. *In Medias Res,* 10(2), 297–311. Online: https://inmediasresfolyoirat.hu/imr/article/view/235

IHS Markit (2017): *The Internet of Things: a Movement, Not a Market.* Online: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (IVSZ) (2014–2015): *Előzetes Megvalósíthatósági Tanulmány „Az Internet of Things koordinált fejlesztése és alkalmazásának elterjesztése Magyarországon" tárgykörben.* Online: https://ivsz.hu/wp-content/uploads/2016/04/az-internet-of-things-koordinalt-fejlesztese-es-alkalmazasanak-elterjesztese-magyarorszagon-.pdf

Infostart/Inforádió – Király István Dániel (2020): Gál András Levente: vissza kell szerezni a személyes adatvagyonunk feletti rendelkezési jogot. *Infostart,* 2020. december 9. Online: https://infostart.hu/interju/2020/12/09/gal-andras-levente-vissza-kell-szerezni-a-szemelyes-adatvagyonunk-feletti-rendelkezesi-jogot

Infra kamera, hogy éjjel is felismerhető legyen a kép [é. n.]. Online: www.alarmdirect.hu/infra-kamera-hogy-ejjel-felismerheto-legyen-kep/

Ipsits Csaba – Oszlánszki Sándor (2020): Koordinált nyomozás – A (vagyon elleni) sorozat-bűncselekmények felderítése. In Ruzsonyi Péter (szerk.): *Közbiztonság.* Budapest: Ludovika Egyetemi Kiadó, 713–731.

Juhász Gyöngyike (2022): A kriminalisztikai célú adatgyűjtés, az elektronikus Modus Operandi Nyilvántartás jövője és kutatási lehetőségei. *Belügyi Szemle,* 70(1), 59–67. Online: https://doi.org/10.38146/ BSZ.2022.1.4

Károly Gábor (2020): Annyi adat van a NAV-nál, ami 225 évnyi HD-filmmel ér fel. *Index,* 2020. december 17. Online: https://index.hu/gazdasag/2020/12/17/nav_adatvagyon_sors _laszlo/

Kárpáti Orsolya (2018): Nyilvántartások a közigazgatásban; nyilvántartásokkal szemben támasztott követelmények a XXI. században. *Új Magyar Közigazgatás,* 11(1), 8–15.

Keszi Tamás – Lohner Klaudia (2022): A hálózatelemzés elmélete és rendőrségi gyakorlata. *Belügyi Szemle,* (70)1, 69–86. Online: http://doi.org/10.38146/BSZ.2022.1.5

Készenléti Rendőrség Nemzeti Nyomozó Iroda (2020): Heroin a hátsó kertben elásva. *Police.hu,* 2020. június 22. Online: www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/heroin-a-hatso-kertben-elasva

Király Katalin (2018): Az okmányirodai igazgatáshoz kapcsolódó feladatok. In Kovács Éva et al.: *Egyedi ügyek és élethelyzetek.* Budapest: Nemzeti Közszolgálati Egyetem, 95–143. Online: http://hdl.handle.net/20.500.12944/7216

Kiss Béla – Major Gábor (2021): Légből kapott segítség a Covid-19 ellen. In Szilvássy László – Békési Bertold (szerk.): *Repüléstudományi tanulmányok. Repüléstudományi szemelvények.* Budapest: Ludovika Egyetemi Kiadó, 281–311. Online: http://hdl.handle.net/20.500.12944/17767

Kis-Benedek József (2014): Az emberi erőkkel folytatott információszerzés. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest: Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 153–163. Online: http://hdl.handle.net/20.500.12944/8567

Klein Tamás (2018): Az álhírek hatásmechanizmusa. In Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog.* Budapest: Wolters Kluwer Hungary, 244.

Kocsis Bence (2019): Az additív és szubsztraktív technológia katonai vonatkozású alkalmazási lehetőségeinek összehasonlító vizsgálata. *Műszaki Katonai Közlöny,* 29(2), 95–104. Online: https://doi.org/10.32562/mkk.2019.2.8

Kollár Csaba (2019): A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában. In Rajnai Zoltán (szerk.): *Kiberbiztonság – Cybersecurity 2.* Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 47–61.

Kormányzati Tájékoztatási Központ (2022): *Megalakul a Digitális Magyarország Ügynökség.* 2022. május 30. Online: https://kormany.hu/hirek/a-kormanyzati-tajekoztatasi-kozpont-kozlemenye-2022-05-30

Kovács Kálmán (2018): Az okos város modelljei. In Sallai Gyula (szerk.): *Az okos város (Smart City).* Budapest: Dialóg Campus Kiadó, 35–48.

Kovács László (2003): *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem. Online: http://hdl.handle.net/20.500.12944/11964

Kovács Zoltán – Ember István (2021): Aknafelderítés légi eszközökkel. *Műszaki Katonai Közlöny,* 31(4), 5–20. Online: https://doi.org/10.32562/mkk.2021.4.1

Közbeszerzési Hatóság (2021): *Bűnügyi technikai célú eszközök beszerzése II.* Online: www.kozbeszerzes.hu/ertesito/2021/0/targy/portal_402/megtekint/portal_26286_2021/

Krasznay Csaba (2022a): Adatok és automatizáció a kiberbiztonság szemszögéből. *Századvég,* (1), 29–46.

Krasznay Csaba (2022b): Kiberbiztonsági képzések a Nemzeti Közszolgálati Egyetemen. In Koltay András – Gellér Balázs (szerk.): *Jó kormányzás és büntetőjog. Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára.* Budapest: Ludovika Egyetemi Kiadó, 407–424.

Krasznay Csaba – Ináncsi Mátyás (2021): Az UAV-ok kiberbiztonsági elemzésének és tanúsításának lehetőségei. *Felderítő Szemle,* 20(3), 63–79.

Kui László (2016): A hőkép-alkotás története és gyakorlati alkalmazása. *Határrendészeti Tanulmányok,* 13(1), 107–117. Online: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/2016-1-szam-1.original.pdf

Kutassy Emese (2021): *Geodéziai alapismeretek II.* Budapest: Ludovika Egyetemi Kiadó. Online: http://hdl.handle.net/20.500.12944/16543

Lakatos János (2005): A körözés. In Lakatos János (szerk.): *Kriminál taktika II.* Budapest: Rejtjel Kiadó.

Magyarország Kormánya (2021): Ügyintézés szabadon – EFOTT-on! A Belügyminisztérium és NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. is várja az idei fesztiválozókat. *Kormany.hu,* 2021. augusztus 13. Online. https://kormany.hu/hirek/ugyintezes-szabadon-efott-on-a-belugyminiszterium-es-nisz-nemzeti-infokommunikacios-szolgaltato-zrt-is-varja-az-idei-fesztivalozokat

Magyarország Kormánya (2023): Megvalósítási szakaszba léphet a Digitális Állampolgárság Program. Kormany.hu, 2023. december 22. Online: https://kormany.hu / hirek/megvalositasi-szakaszba-lephet-a -digitalis-allampolgarsag-program

Magyarország Ügyészsége (2018): *Ókori és középkori kincseket is rejtett a szántóföld.* Online: http://ugyeszseg.hu/okori-es-kozepkori-kincseket-is-rejtett-a-szantofold/

Mama Sándor – Gárdonyi Gergely (2016): A talajradar használatának gyakorlati tapasztalatai a hazai bűnügyi helyszínelésben. *Belügyi Szemle,* 64(7–8), 70–76. Online: https://doi.org/10.38146/BSZ.2016.7-8.7

Mandić Dorottya (2022): A mesterséges intelligencia alkalmazása az okosotthonokban. *Biztonságtudományi Szemle,* 4(1), 33–41.

Marinov Iván (2019): Mi az a deepfake, és hogyan ismerhetjük fel az így készült videókat? *Urban Legends,* 2019. december 19. Online: www.urbanlegends.hu/2019/12/reuters-hogyan-ismerjuk-fel-a-deepfake-videokat/

Máté István Zsolt – Sándor Gábor (2019): *A mobilkommunikációs eszközök vizsgálatának általános eljárásaira vonatkozó módszertani leírás.* [H. n.]: Nemzeti Szakértői és Kutató Központ. Online: https://nszkk.gov.hu/content/modszertani-leirasok/5-2019-korlevel/melleklet-5-2019-korlevel_signed.pdf

Medve, Flora (2023): Internet Penetration Rate in Hungary from 2010 to 2022. *Statista.com,* 2023. január 3. Online: www.statista.com/statistics/1123184/hungary-internet-penetration-rate/

Micstusmi (2020): Liar's Dividend. *Urban Dictionary,* 2020. szeptember 8. Online: https://www.urbandictionary.com/define.php?term=Liar%E2%80%99s%20Dividend

Mitől okos egy okos város (2023). Online: https://eletokosan.hu/mitol-okos-egy-okos-varos

Mobile Multispectral Forensic Tablet. Designed for Crime Scene Investigation & Evidence Searching [é. n.]. Online: https://forenscope.com/en/product/mobile-multispectral-forensic-tablet

Mi az IMEI-szám és az IMEI bármely eszköz keresése (2019). Online: https://hu.gadget-info.com/32501-what-is-imei-number-and-how-to-find-imei-of-any-device

Miniszterelnöki Kabinetiroda (2002): *Nemzeti Digitális Stratégia 2022–2030.* Online: https://kormany.hu/dokumentumtar/nemzeti-digitalizacios-strategia-2022-2030

Molnár Anita – Rab Árpád (2021): A deepfake technológia és az amerikai elnökválasztás. *Ludovika.hu, ITKI blog,* 2021. január 18. Online: www.ludovika.hu/blogok/itkiblog/2021/01/18/a-deepfake-technologia-es-az-amerikai-elnokvalasztas/

Molnár László – Sasvári Péter – Tarpai Zoltán Tamás (2021): *Közigazgatási informatikai alkalmazások.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet. Online: http://hdl.handle.net/20.500.12944/16238

Molnár Tamás József (2021): Az internetes biztonság és az OSINT összefüggései. *Nemzetbiztonsági Szemle,* 9(2), 81–94. Online: https://doi.org/10.32561/nsz.2021.2.6

Monori Zsuzsanna Éva (2021): A szólásszabadság korlátozása a büntetőjog eszközeivel II. – A rémhírterjesztés bűncselekményének elemei. *MTMI,* 2021. június 3. Online: https://mtmi.hu/cikk/a-szolasszabadsag-korlatozasa-a-buntetojog-eszkozeivel-ii-a-remhirterjesztes-buncselekmenyenek-elemei

Muhi B. Béla – Vemić Đurković, Jelena (2021): Okos város megoldások mint városmarketing és városmárkázás eszközök – Újvidék esettanulmánya. *Turisztikai és Vidékfejlesztési Tanulmányok,* 6(3), 109–123.

Mű-Hely Zrt. (2021): *A Budavári Önkormányzat képviselő-testületének 16/2000. (VIII. 15.) Kt. rendeletével jóváhagyott, többszörösen módosított Budapest I. kerületi építtési szabályzat (kész) szabályozási terv.* Online: https://budavar.hu/wp-content/uploads/2021/01/szab9-16.pdf

Nagy Zoltán András (2021): Mesterséges intelligencia lehetőségei az adó- és vámügyi eljárásokban. In Czene-Polgár Viktória et al. (szerk): *„Tradíció, tudomány, minőség." 30 éves a Vám- és Pénzügyőri Tanszék. Tanulmánykötet.* Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata, 226–234. Online: http://doi.org/10.37372/mrttvpt.2021.2.15

Nándori Nikoletta Petra (2019): HUMINT – Gondolatok az emberi tényező szerepéről a 21. századi titkosszolgálati munkában. *Nemzetbiztonsági Szemle,* 7(4), 96–100. Online: https://doi.org/10.32561/nsz.2019.4.8

NAV évkönyv 2019. Tények, információk a Nemzeti Adó- és Vámhivatal szervezetéről és 2019-es tevékenységéről (2020). Budapest: NAV. Online: https://nav.gov.hu/kiadvanyok/evkonyvek/nav-evkonyv-2019

Németh Ágota (2021): A bűnügyi elemző-értékelő munka napjainkban. In Harmati Barbara et al. (szerk.): *Honestas, Humanitas, Humilitas. Ünnepi kötet Kerezsi Klára tiszteletére.* Budapest: L'Harmattan Kiadó, 152–160. Online: http://real.mtak.hu/135138/1/Honestas_beliv_press.pdf

Németh András – Pápics Patrik (2019): Mini UAV-rajok alkalmazásának lehetőségei, különös tekintettel a katonai célú igénybevételre II. rész. *Haditechnika,* 53(6), 2–6. Online: https://doi.org/10.23713/HT.53.6.01

Németh András – Pápics Patrik (2020): Mini UAV-rajok alkalmazásának lehetőségei, különös tekintettel a katonai célú igénybevételre III. rész. *Haditechnika,* 54(1), 6–10. Online: http://doi.org/10.23713/HT.54.1.02

Nemzeti Infokommunikációs Stratégia 2014–2020 (2014). Online: https://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf

NISZ (2020): *Mesterséges intelligenciával támogatott ügyintézési pont (Kiosk) kiterjesztése kormányhivatalokra, illetve más küldő ügyintézési helyszínekre.* Online: www.nisz.hu/hu/projektek/mesters%C3%A9ges-intelligenci%C3%A1val-t%C3%A1mogatott-%C3%BCgyint%C3%A9z%C3%A9si-pont-kiosk-kiterjeszt%C3%A9se

NMHH-piackutatás: a közösségi oldalakon találkozhatunk leginkább álhírekkel (2020). Online: https://nmhh.hu/cikk/213077/NMHHpiackutatas_a_kozossegi_oldalakon_talalkozhatunk_leginkabb_alhirekkel

Nyíregyházi Törvényszék Sajtóosztály (2022): *Nyíregyházi Törvényszék – Megrovásra enyhítette a törvényszék a rémhírterjesztés bűntette miatt elítélt férfi büntetését.* Online: https://birosag.hu/aktualis-kozlemenyek/nyiregyhazi-torvenyszek-megrovasra-enyhitette-torvenyszek-remhirterjesztes

Nyitrai Endre (2014): Civilnyilvántartások a nyomozásban. *Pécsi Határőr Tudományos Közlemények,* 15, 217–224.

Nyitrai Endre (2015): Bűnelemzés a nyomozásban. *Pécsi Határőr Tudományos Közlemények,* 16, 141–147.

Nyitrai Endre (2020a): A bűncselekményből eredő vagyon visszaszerzése. *Ügyészek Lapja,* 27(2–3), 39–53.

Nyitrai Endre (2020b): A drónok alkalmazásának lehetőségei a rendőrségi feladatok ellátása során. *Rendőrségi Tanulmányok,* 3(1), 94–119.

Nyitrai Endre (2020c): Közrendvédelem. Körözési tevékenység. In Ruzsonyi Péter (szerk.): *Közbiztonság.* Budapest: Ludovika Egyetemi Kiadó, 461–481.

Nyitrai Endre (2022): A magyar nemzeti adatvagyon jelentősége a bűnüldöző szervek munkája során. *Információs Társadalom,* 22(1), 67–80. Online: https://dx.doi.org/10.22503/inftars.XXII.2022.1.4

Nyitrai, Endre – Rucska, András (2020): Spread of 'Fake News' in the Present Days. *Часопис Національногоуніверситету „Острозька академія." Серія „Право",* 22(2), 1–8. Online: https://lj.oa.edu.ua/articles/2020/n2/20enntpd.pdf

Ollé János et al. (2013): *Digitális állampolgárság az információs társadalomban.* Budapest: ELTE Eötvös Kiadó. Online: www.eltereader.hu/media/2014/01/Digitalis_allampolgarsag_READER.pdf

Orbán Anna (2019): A közigazgatási portálok. In Czékmann Zsolt (szerk.): *Infokommunikációs jog.* Budapest: Dialóg Campus Kiadó, 109–124. Online: http://hdl.handle.net/20.500.12944/14474

Orbán Anna Mária (2021): *E-közigazgatási szolgáltatások hatékonyságának növelése az infokommunikációs technológiákkal.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola. Online: http://hdl.handle.net/20.500.12944/17786

Orbán Boglárka (2022): A kétely kételyébe sodorhat minket a deepfake. *Lakmusz,* 2022. július 6. Online: www.lakmusz.hu/a-ketely-ketelyebe-sodorhat-minket-a-deepfake/2022.11.16.

Papp Dávid (2020): Közterületi és őrszolgálat. In Ruzsonyi Péter (szerk.): *Közbiztonság.* Budapest: Ludovika Egyetemi Kiadó, 327–363.

Papp Olivér (2017): 3D nyomtatási technológiák alkalmazása a kriminalisztikában. *CNC Media,* 2017. július 11. Online: www.cnc.hu/2017/07/3d-nyomtatasi-technologiak-alkalmazasa-a-kriminalisztikaban/

Pásztor László (2016): A 3D térszkenner működése, tapasztalatok, lehetséges további felhasználási területek. *Belügyi Szemle,* 64(7–8), 61–69. Online: http://doi.org/10.38146/BSZ.2016.7-8.6

Patrik (2022): Ellopták a telefonod? Itt találod az IMEI számot! *Smartclinic.hu,* 2022. június 29. Online: https://smartclinic.hu/hu/blog/elloptak-telefonod-itt-talalod-imei-szamot/

Pócsi Anikó szerk. (2020): *Ügykezelői alapvizsga.* Fogalomtár. Budapest: Nemzeti Közszolgálati Egyetem, 159–170. Online: http://hdl.handle.net/20.500.12944/15022

Pődör Bálint (2010): *Érzékelők. 17. előadás: Kémiai érzékelők II. Elektronikus orr.* Óbudai Egyetem KVK Mikroelektronikai és Technológiai Intézet. Online: http://mti.kvk.uni-obuda.hu/adat/tananyag/sensor/erzekelok_17.pdf

Rab Judit – Szemerey Samu (2018): *Az okos város fejlesztési modell módszertani alapjai.* Budapest: Lechner Tudásközpont. Online: http://okosvaros.lechnerkozpont.hu/hu/dokumentumok

Ránki Sára (2011): A kriminalisztikai szövegnyelvészet hazai kutatástörténete 1960-tól 1990-ig. *E-nyelvmagazin.hu,* 2011. augusztus 31. Online: https://e-nyelvmagazin.hu/2011/08/31/a-kriminalisztikai-szovegnyelveszet-hazai-kutatastortenete-1960-tol-1990-ig/

Ránki Sára (2015): Nyelvi profilozás az interneten. In Sziklay Júlia (szerk.): *Kulcs a net világához! A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról.* [H. n]: [k. n.], 64–69. Online: https://naih.hu/files/Kulcs_anv_v2.pdf

Ránki Sára (2019): Bevezetés az igazságügyi nyelvészetbe. *Belügyi Szemle,* 67(3), 76–90. Online: https://doi.org/10.38146/BSZ.2019.3.5

Ránki Sára (2021): Nyelvi profilalkotás. *Belügyi Szemle,* 69(12), 2155–2166. Online: https://doi.org/10.38146/BSZ.2021.12.6

Richárd (2022): Bemutatták az iSIM-et, vagyis az okostelefonba integrált hálózati kártyát. *NapiDroid,* 2022. január 20. Online: https://napidroid.hu/bemutattak-az-isim-et-vagyis-az-okostelefonba-integralt-halozati-kartyat/

Ritó Evelin (2019): A „smart city" fogalma és háttere. *Publicationes Universitatis Miskolcinensis. Sectio Juridica et Politica,* (37)1, 227–238.

Ritó Evelin (2021): Mesterséges intelligencia az Európai Unió stratégiai és szabályozási dokumentumainak tükrében. *Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok,* 2(1), 33–47. Online: https://doi.org/10.47272/KIKPhD.2021.1.3

Robin [é. n.]: *The Ultimate Guide: Everything Need To Know About 3D Printing Services.* Online: www.rocheindustry.com/3d-printing-ultimate-guide/; magyarul: Minden, amit a 3D-nyomtatásról tudni kell. *CNC Media,* 2020. május 11. Online: www.cnc.hu/2020/05/minden-amit-a-3d-nyomtatasrol-tudni-kell/

Rucska András (2017): A helyszín képi rögzítése hagyományos és háromdimenziós eljárással a kriminalisztikai szabályok szerint. *Ügyészek Lapja,* 24(5), 35–42.

Rucska András (2018): Felderítés és bizonyítás új kriminál technikai eszközök segítségével. *Ügyészek Lapja,* 25(6), 55–66.

Rudolf Dániel (2019): Kamuvideók, életek, amiket tönkretesz a deepfake. *Dívány,* 2019. szeptember 22. Online: https://divany.hu/vilagom/2019/09/22/deepfake/

Salamon Endre (2020): Szerves mikroszennyezők kimutatása a környezetből. In Knisz Judit (szerk.): *Szerves mikroszennyezők a vizekben.* Budapest: Ludovika Egyetemi Kiadó, 181–216.

Sallai Gyula (2018): Az okos város koncepciója. In Sallai Gyula (szerk.): *Az okos város (Smart City).* Budapest: Dialóg Campus Kiadó, 13–34.

Sallai Gyula (2019): *Az okosváros-koncepció és az internettechnológia.* Budapest: Dialóg Campus Kiadó.

Sample, Ian (2020): What Are Deepfakes – And How Can You Spot Them? *The Guardian,* 2020. január 13. Online: www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

Samu Nagy Dániel (2020): Nyilvántartások korszerűsítése. *Infojegyzet,* 65. 2020. október 16. Online: www.parlament.hu/documents/10181/4464848/Infojegyzet_2020_65_nyilvantartasok_korszerusitese.pdf/02484308-6dee-5f57-1933-c6048a4788f9?t=1602828447258

Simon Béla – Gyaraki Réka (2020): Kiberbűncselekmények felderítése és nyomozása. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban.* Budapest: Dialóg Campus Kiadó, 121–150.

Sipos Mihály (2021a): Az IoT és az 5G – megállíthatatlan páros. *Elektronet,* 30(2), 8–11.

Sipos Mihály (2021b): Az IoT után IoE – de mi a különbség? *Elektronet,* 30(2), 12–14.

Sipos Mihály (2022): Bemutatták az iSIM technológiát. *Elektronet,* 30(2), 16. Online: www.elektro-net.hu/konstruktor/9705-bemutattak-az-isim-technologiat?highlight=WyJpb3QiLCInaW90JyIsImF6IiwiJ2F6IiwiNWciXQ==

Silverman, Craig (2017): *What Do We Mean When We Say Fake News?* Online: https://us2.cam paign-archive.com/?u=657b595bbd3c63e045787f019&id=e0b2b9eaf0&e=30348b6327

Sorbán Kinga (2020): A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle,* 68(10), 81–104. Online: https://doi.org/10.38146/BSZ.2020.10.4

Sütő Ákos (2016): Robotzsaru (NEO) Integrált ügyviteli és ügyfeldolgozó rendszer információvédelmi lehetőségei. *Hadtudományi Szemle,* 9(2), 353–366.

Szabó Balázs (2020a): Jó gyakorlatok a mobilapplikációk okmányügyi mint szakigazgatási célú felhasználására a V4-es országokban és az EU-ban. *Publicationes Universitatis Miskolcinensis. Sectio Juridica et Politica,* (38)2, 130–147.

Szabó Balázs (2020b): Mobil applikációk a közigazgatásban. *Miskolci Jogi Szemle,* 15(2. klnsz.), 134–141.

Szabó Csaba – Horváth Alexandra – Nagy Bence (2017): A közösségi média biztonságpolitikai kérdései. A közösségi tartalmak rendészeti vonatkozásainak vizsgálata. *Rendvédelem,* 6(1), 85–120. Online: http://epa.niif.hu/03300/03353/00011/pdf/EPA03353_rendvedelem_2017_1_085-120.pdf

Szendi Dóra – Nagy Zoltán – Sebestyénné Szép Tekla (2020): Mérhető-e az okos városok teljesítménye? – Esettanulmány a 2004 után csatlakozott EU-tagállamok fővárosairól. *Területi Statisztika,* 60(2), 249–271. Online: https://doi.org/10.15196/TS600207

Sziebig Orsolya Johanna (2021): *Vadvilág végveszélyben. A vadvilággal kapcsolatos büntetendő cselekmények nemzetközi és uniós jogi vonatkozásai.* Szeged: Iurisperitus Kiadó.

Szócska Miklós et al. (2019): A hálózatkutatás alkalmazhatósága a közszolgáltatások fejlesztésében. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus Kiadó, 9–26. Online: https://nkerepo.uni-nke.h/xmlui/bitstream/handle/123456789/14555/712_Halozatok_a_kozszolgalat-ban_WEB.pdf?sequence=1

SZTEinfo – Móczár Dóra (2020): Egy új kor küszöbén: a technológia szerepe a mindennapjainkban és a bűnüldözésben. *SZTEhírek,* 2020. március 3. Online: https://u-szeged.hu/sztehirek/2020-marcius/egy-uj-kor-kuszoben

Szűts Zoltán (2017): Híradatbázisok és médiatartalmak elemzése big data használatával. *Jel-Kép. Kommunikáció, Közvélemény, Média,* 6(1), 23–46. Online: https://doi.org/10.20520/JEL-KEP.2017.1.23

Tangermann, Victor (2022): Simon Cowell Shocked by Deepfake Copy of Himself. *Futurism, The Byte,* 2022. június 9. Online: https://futurism.com/the-byte/simon-cowell-deepfake

Tarpai Zoltán (2020): A hazai közigazgatási informatikai rendszerek fejlesztésének intézményei. In Sasvári Péter (szerk.): *Informatikai rendszerek a közszolgálatban II.* Budapest: Dialóg Campus Kiadó, 133–147.

Technology Overview. A Unique Fusion of Deep Learning and Computer Vision Technologies [é. n.]. Online: www.briefcam.com/technology/overview/

Több mint nyolcmillió forint értékű kokaint nyelt le egy nő – Ferihegyen csípték el + Videó (2019). *Kisalfold.hu,* 2019. április 25. Online: www.kisalfold.hu/kek-hirek/2019/04/tobb-mint-nyolcmillio-forint-erteku-kokaint-nyelt-le-egy-no-ferihegyen-csiptek-el-video

Ufed, az adatkitermelő eszköz, amely kulcsfontosságú olyan esetekben, mint a diana quer (2022). Online: https://phonenumber247.com/#menu-1

Ürmösné Simon Gabriella (2019): Miben segítik a nyelvi ujjnyomok a nyomozást? *Magyar Rendészet,* 19(1), 65–75. Online: http://doi.org/10.32577/mr.2019.1.4

Ürmösné Simon, Gabriella – Nyitrai, Endre (2021): The Phenomena of Epidemic Crime, Deepfakes, Fake News, and the Role of Forensic Linguistics. *Információs Társadalom,* 21(4), 86–101. Online: https://dx.doi.org/10.22503/inftars.XXI.2021.4.5

Van der Hulst, Renée C. (2009): Introduction to Social Network Analysis (SNA) as an Investigative Tool. *Trends in Organized Crime,* 12, 101–121. Online: https://doi.org/10.1007/s12117-008-9057-6

Varga Melinda – Ruppert Péter – Barabási Albert-László (2019): Komplex hálózatok szerkezetének elemzése és modellezése. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus Kiadó, 27–110.

Veszelszki Ágnes (2021): deepFAKEnews: Az információmanipuláció új módszerei. In Balázs László (szerk.): *Digitális kommunikáció és tudatosság.* Budapest: Hungarovox Kiadó, 93–105.

Vida Csaba (2013): Nyílt forrású adatszerzés (OSINT). In Kobolka István (szerk.): *Nemzetbiztonsági Alapismeretek.* Budapest: Nemzeti Közszolgálati Egyetem. 101–109

Vida Rolland (2020): *Szenzorhálózatokra épülő közszolgáltatások.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet. Online: http://hdl.handle.net/20.500.12944/16345

Vigh András (2018): A drónok rendészeti alkalmazási lehetőségei. *Belügyi Szemle,* 66(10), 88–107. Online: https://doi.org/10.38146/BSZ.2018.10.6

Vodafone (2022): A világon elsőként mutatták be az okostelefonba integrált SIM (iSIM) technológiáját. *NEWtechnology,* 2022. január 22. Online: https://newtechnology.hu/a-vilagon-elsokent-mutattak-be-az-okostelefonba-integralt-sim-isim-technologiajat/

Wiggen, Johannes (2020): The Impact of COVID-19 on Cyber Crime and State-Sponsored Cyber Activities. *Konrad Adenauer Stiftung, Tacts and Findings,* (391), 1–11. Online: www.kas.de/en/analysen-und-argumente/detail/-/content/die-auswirkungen-von-covid-19-auf-cyberkriminalitaet-und-staatliche-cyberaktivitaeten#

Zala Megyei Rendőr-főkapitányság (2022): *Drón segítségével szűrték ki a szabálysértőket. A zalai rendőrök a közlekedési szabályok betartását ellenőrizték a levegőből.* Online: www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/kozlekedesrendeszet/dron-segitsegevel-szurtek-ki-a-3

Jogszabályok

1024/2017. (I. 24.) Korm. határozat az „okos város” szolgáltatások összehangolt bevezetését és működését támogató szervezeti és tudásplatform létrehozásáról és működtetésétől, valamint a teljes rendszer működésének monitoringjáról

1165/2018. (III. 27.) Korm. határozat az „okos város” funkcionalitás magyarországi elterjedését szolgáló központi szolgáltatásplatform létrehozásával kapcsolatos intézkedésekről

12/2021. (IV. 30.) ORFK utasítás az elektronikus Modus Operandi Nyilvántartás működtetésével kapcsolatos feladatokról

1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről

18/2011. (IX. 23.) ORFK utasítás a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól

1994. évi XXXIV. törvény a Rendőrségről

1994. évi XXXIV. törvény indokolása a rendőrségről

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

1998. évi XII. törvény a külföldre utazásról

2003. évi C. törvény az elektronikus hírközlésről

2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról

2009. évi XLVII. törvény indokolása a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról

2012. évi C. törvény a Büntető Törvénykönyvről

2013. évi LXXXVIII. törvény a körözési nyilvántartási rendszerről és a személyek, dolgok felkutatásáról és azonosításáról

2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről

2015. évi CLXXXVIII. törvény indokolása az arcképelemzési nyilvántartásról és az arcképelemző rendszerről

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
2017. évi XC. törvény a büntetőeljárásról
2021. évi XCI. törvény a nemzeti adatvagyonról
2021. évi XCI. törvény végső előterjesztői indokolása a nemzeti adatvagyonról
2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól
2040/2017. (XII. 27.) Korm. határozat Monor település „okos város" funkcionalitással összefüggő fejlesztéseinek támogatásáról
307/2022. (VIII. 11.) Korm. rendelet a Digitális Magyarország Ügynökség Zártkörűen Működő Részvénytársaság kijelöléséről és egyes feladatainak meghatározásáról, valamint a nemzeti informatikai és e-közigazgatási tevékenység összehangolt biztosításával összefüggő részletszabályokról
314/2012. (XI. 8.) Korm. rendelet a településfejlesztési koncepcióról, az integrált településfejlesztési stratégiáról és a településrendezési eszközökről, valamint egyes településrendezési sajátos jogintézményekről
32/2022. (X. 25.) ORFK utasítás a vagyonvisszaszerzéssel kapcsolatos feladatokról
451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
459/2021. (VIII. 4.) Korm. rendelet végső előterjesztői indokolása a településfejlesztési koncepcióról, az integrált településfejlesztési stratégiáról és a településrendezési eszközökről, valamint egyes településrendezési sajátos jogintézményekről szóló 314/2012. (XI. 8.) Korm. rendelet módosításáról
56/2017. (III. 20.) Korm. rendelet egyes kormányrendeleteknek az „okos város", „okos város módszertan" fogalom meghatározásával összefüggő módosításáról
38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról
A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet melléklete
Az Európai Parlament és a Tanács 2013/40/Eu Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
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)

Felhasznált jogesetek jegyzéke

15/2022. (VII. 14.) AB határozat
BH2018. 303.
Bhar.III.1.530/2019/23.
Egri Törvényszék Bf.273/2019/27. számú ítélete
Fővárosi Bíróság B.1103/2009/16.
Fővárosi Ítélőtábla Bf.31/2021/22.
Fővárosi Ítélőtábla Kbf.99/2008/13.
Fővárosi Törvényszék 25.B. 539/2013/374. számú ítélete
Közbeszerzési Hatóság Elnöke HNT-00269/03/2019. hirdetmény nélküli tárgyalásos eljárásról hozott 2019. december 19-i döntése „Gangikonspi szoftver támogatási szolgáltatása" tárgyban. Online: www.kozbeszerzes.hu/media/hntdontes/2021/11/29/hnt-00269-2019.pdf
Kúria Bhar.III.1.530/2019/23. számú ítélete
Tatabányai Törvényszék 17.B.419/2017/39. számú ítélete
Pécsi Ítélőtábla Bf.II.262/2011/10. számú ítélete

Internetes hivatkozások

Balatoni kikötők weboldalán Vitorláskikötők menüpont. Online: www.balatonikikotok.hu/#vitorlskikoetk.
Budavári Önkormányzat weboldalán a Kerületi Építési Szabályzat. Online: https://budavar.hu/epitesi-informaciok/keruleti-epitesi-szabalyzat-1/
Digitális állampolgárság kutatás weboldala. Online: http://digitalisallampolgarsag.hu/
Digitális Magyarország Ügynök, Megvalósítási szakaszba léphet a Digitális Állampolgárság Program. Online: https://www.dmu.gov.hu/cikkek/megvalositasi-szakaszba -lephet -a-digitalis-allampolgarsag-program
*EESZT Lakossági Portál*on e-Profil. Online: www.eeszt.gov.hu/hu/eprofil
*EESZT Lakossági Portál*on e-Kórtörténet. Online: www.eeszt.gov.hu/hu/e-kortortenet
E-kreta.hu weboldalán e-ügyintézés. Online*:* https://eugyintezes.e-kreta.hu/kerelmek/BAI
Földhivatal Online weboldal. Online: https://info.foldhivatal.hu/tknet/kezdolap6_p.uk_kezdo?sid=0404202212021102040014679145546E6B34486B445A7272522 F3168466C4E386241424348706F6D303D

Magyarorszag.hu weboldal Adatigénylés a jármű szolgáltatási platformon ügyintézési felülete. Online: https://magyarorszag.hu/szuf_ugyleiras?id=28c28a1a -7296 -4629-8f36-7f3fbe6596c6
Magyarorszag.hu weboldal Család kategóriája. Online: https://magyarorszag.hu/szuf_szolg_lista?kategoria=CS
Magyarorszag.hu weboldal Kérelem benyújtása űrlapja. Online: https://magyarorszag.hu/szuf_iForm#urlap,744088ac-76a4-4b47-8b11-696ad1b0cb03
Magyarorszag.hu weboldal Kutatás kategóriája. Online: https://magyarorszag.hu/szuf_szolg_lista?kategoria=OT.KU
Police.hu weboldalon térfigyelő kamerák kimutatása. Online: https://www.police.hu/sites/default/files/HMRFK%20202210_%20t%C3%A9rfigyel%20kamer%C3%A1k%20kimutat%C3%A1sa.pdf
Police.hu weboldal Ügyintézési portálja. Online: https://ugyintezes.police.hu/hu/home
Police.hu weboldalon Ügyintézési portálon új ügy indítása. Online: https://ugyintezes.police.hu/hu/uj-ugy-inditasa/
Szotarjelentese weboldalon IMEI jelentése. Online: www.szotarjelentese.com/IMEI
Telefonguru weboldalon IMEI szócikk. Online: www.telefonguru.hu/wiki/imei
Vodafone weboldal eSIM-tájékoztatója. Online: www.vodafone.hu/esim
Vodafone Magyarország Zrt. Adatkezelési Tájékoztatója. Általános Szerződési Feltételek 3. számú melléklet [é. n.]. Online: www.vodafone.hu/static/documents/20143/330611/Vodafone-adatkezelesi-tajekoztato.pdf

A digitalizáció és a mesterséges intelligencia új fejezetet nyitott a tudomány területén, így a kriminalisztikában is. Nap mint nap folyamatosan digitális nyomokat (elektronikus adatokat) hagyunk magunk után. A bűnüldözés szempontjából ezek egyrészt azért fontosak, mert az ismeretlen személyazonosságú személy (elkövető) azonosításában segítséget jelenthetnek, másrészt a bűncselekmények megelőzéséhez, felderítéséhez, bizonyításához is szükségesek. A modern, innovatív eszközök és programok pedig az óriási adatmennyiség feldolgozását, pontosabban kriminalisztikai nézőpontból a nyomozási cselekmények végrehajtását segíthetik elő.

Figyelembe kell venni azonban, hogy az innovatív technológiákat a bűnözők is használják, így a *fake news, deepfake* videók is el fognak terjedni, illetve meg fognak jelenni új digitális elkövetési módok.

További fontos szempont, hogy fantázia (képzelőerő) vagy ötletelés nélkül a nyomozások során sem lehet előrejutni, ebben lesz segítségünkre a mesterséges intelligencia mint virtuális asszisztens.