Einnováció

HM Elektronikai, Logisztikai és Vagyonkezelő Zrt. IV. évfolyam 3-4. szám

Felelős kiadó

Dr. Trembeczki László András — vezérigazgató

Szerkesztőbizottság

Elnök	Dr. Trembeczki László András PhD	c. egyetemi docens
Főszerkesztő	Dr. Kobolka István PhD	egyetemi docens
Főszerkesztő-helyettes	Kiss Ferenc	
Olvasószerkesztő	Kiss Dezső	

Tagok

Baráth István	c. egyetemi docens
Dr. Felházi Sándor PhD	
Ladányi Éva	c. egyetemi docens
Prof. Dr. Sallai János	egyetemi tanár
Dr. Szilvágyi Tibor PhD	
Tömböl László	tudományos szakértő
Prof. Dr. Munk Sándor	MTA doktora
Dr. Fejes Zsolt PhD	
Prof. Dr. habil. Szakály Sándor	egyetemi tanár, az MTA doktora
Prof. Dr. Dobák Imre	egyetemi tanár
Angyal Júlia	tudományos segédmunkatárs

Elérhetőségek

Postacím	1101 Budapest, Salgótarjáni út 20.	HM EI Zrt. Kompetencia Központ
Telefon	Dr. Kobolka István	+36 30 979 6128
Email cím	kobolka.istvan@hmei.hu einnovacio@hmei.hu	

A kötetben foglalt tudományos cikkek, tanulmányok semmilyen szempontból nem minősülnek a HM EI Zrt. hivatalos álláspontjának, azok kizárólag a szerzők tudományos igénnyel összeállított személyes szakmai véleményét tükrözik, azokért szerzői jogi felelősséggel tartoznak. A kiadvány lektorálását a szerkesztőbizottság végzi.

Nyomdai munka: HM Zrínyi Nonprofit Kft.
2026
Felelős vezető: Pásztor Zoltán igazgató

ISSN 2939-7677

Varga Attila:[1]

Geoinformatikai referenciaadatokon alapuló GNSS-független lokalizáció lehetőségei pilóta nélküli légi járműveken

Absztrakt:

A globális műholdas navigációs rendszerek (GNSS – Global Navigation Satellite System) napjainkra a légi navigáció, és különösen a pilóta nélküli repülő eszközök lokalizációjának alapvető rendszereivé váltak. A gyenge műholdas rádiójelek, a környezeti korlátok, valamint a szándékos zavarás miatt katonai szempontból a GNSS azonban már nem biztosít kellően robusztus navigációt, ezért egyre nagyobb figyelmet kapnak a GNSS-független megoldások. Jelen cikk célja rendszerszintű áttekintést nyújtani a GNSS-független navigációs technológiákról, ezek lehetőségeiről és korlátairól, elsősorban a geoinformatika szemszögéből, kiemelten kezelve a térbeli referenciaadatokon alapuló módszereket.

Ez a technológiai áttekintés érinti az inerciális navigációt, a domborzatalapú, a radar- és LiDAR-alapú helymeghatározást, röviden foglalkozik a rádiós, a mágneses és a gravitációs mezőn alapuló lokalizációval, valamint kitér az újonnan megjelent kvantumszenzoros megoldásokra is. A térbeli referenciaadatokat[2] *használó, egymástól látszólag független navigációs technológiák valójában ugyanazon az általános elven alapulnak, vagyis a fedélzeti szenzoros megfigyeléssel nyert adatokat a környezet valamilyen georeferált reprezentációjával vetik össze. Ez a reprezentáció lehet egy domborzatmodell, egy georeferált légifelvétel, 3D pontfelhő, gravitációs, vagy egyéb fizikai jellemzőket tartalmazó térbeli adat.*

A cikkben kiemelt hangsúlyt kap a napjainkban egyre elterjedtebben alkalmazott, vizuális megfigyelésen alapuló helymeghatározás. Az ehhez használt kamera olcsó, kis tömegű és nagy információtartalmú szenzoradatot (képet) állít elő. A képfeldolgozáson alapuló vizuális odometria vagy az egyidejű helymeghatározás és térképezés külső georeferencia nélkül is biztosítja a mozgás- és a helyzetbecslést, de önmagában csak lokális koordinátarendszerben történő helymeghatározást tesz lehetővé. A fedélzeti szenzoradatoknak a georeferenciát tartalmazó referenciaadattal történő összevetése már abszolút földrajzi helymeghatározást tesz lehetővé.

---

[1] A szerző okleveles gépészmérnök és geoinformatikai szakmérnök, a HM EI Zrt. Elektronikai és Informatikai Igazgatóság Informatikai Alkalmazásfejlesztési Divíziójának munkatársa.

[2] *Térbeli referenciaadat* vagy *geoinformatikai referenciaadat* alatt a cikkben olyan, a környezet valamely geometriai, fizikai vagy szemantikai jellemzőjét reprezentáló adatot értjük, amelynek a térbeli helyzete a földrajzi vagy a vetületi koordinátarendszerben meghatározott.

A cikk fő következtetése, hogy nincs univerzális, a GNSS-t helyettesítő vagy kiváltó lokalizációs eljárás. A bemutatott technológiák mindegyike rendelkezik a környezet és a szenzor sajátosságaiból eredő valamilyen korláttal, hibával. Ezen hátrányok többféle szenzor alkalmazásával és a szenzoradatok fúziójával mérsékelhetők. A robusztus navigáció egyik ígéretes fejlődési irányának a többféle navigációs információforrás adaptív fúziója tűnik, ami tovább erősítheti a pilóta nélküli repülőgépek autonóm képességeit is. Ebben az adaptív navigációban a georeferált geoinformatikai referenciaadatok az abszolút földrajzi referencia GNSS-től független fontos forrását jelenthetik.

Kulcsszavak: GNSS-független navigáció, pilóta nélküli repülőgép, vizuális navigáció, térbeli referenciaadat, szenzorfúzió, autonóm navigáció

Abstract:

Global Navigation Satellite Systems (GNSS) have become fundamental to air navigation, particularly for unmanned aerial vehicles. However, because of the weak power of satellite radio signals, environmental constraints, and intentional jamming, GNSS can no longer be regarded as sufficiently reliable for military navigation. Consequently, solutions for positioning in GNSS-denied environments are attracting increasing attention. The purpose of this article is to provide a system-level overview of navigation technologies for GNSS-denied environments, examining their capabilities and limitations primarily from a geoinformatics perspective, with a special focus on methods based on georeferenced reference data.

The technological review covers inertial navigation, terrain-based, radar-based, and LiDAR-based localization; briefly discusses radio-based navigation, magnetic- and gravity-field-based navigation; and also considers newly emerging quantum sensor technologies. Despite their apparent differences, localization methods based on reference data share a common underlying principle: data obtained from onboard sensor observations are compared with a georeferenced representation of the environment. This representation may take the form of a digital elevation model, a georeferenced aerial photograph, a 3D point cloud, or a gravitational field model.

The article places particular emphasis on vision-based localization, which is becoming increasingly widespread. Cameras are inexpensive, lightweight, and information-rich sensors. Visual odometry based on image processing, or simultaneous localization and mapping (SLAM), enables motion and position estimation even without external georeferencing; however, without an external geospatial reference, localization remains confined to a local coordinate frame. Comparing onboard image sensor data with georeferenced reference data enables absolute localization within a geographic reference frame.

The main conclusion of this paper is that no single navigation method can serve as a universal replacement for GNSS. Each of the navigation technologies presented has specific limitations arising from environmental characteristics and intrinsic sensor properties. These drawbacks can be mitigated by employing multiple sensors and fusing their outputs. A particularly promising direction for the development of robust navigation appears to be the adaptive fusion of multiple sources of navigation information, which could further enhance the autonomous capabilities of unmanned aircraft. Within such adaptive navigation frameworks, geospatial reference data can provide an important source of absolute geographic reference in GNSS-denied environments.

Keywords: GNSS-denied environment; unmanned aerial vehicle (UAV); visual navigation; geospatial reference data; absolute localization; sensor fusion; autonomous navigation

1. Bevezetés

A katonai képességek egyik nélkülözhetetlen eleme a navigáció, amely a szárazföldi, a légi és a tengeri műveletekben egyaránt meghatározó szerepet tölt be. A megbízható navigáció biztosítása kulcsfontosságú a műveletek sikeres végrehajtásában.

A navigáció általános definíció szerint egy járműnek vagy eszköznek a kiindulási helyzetéből egy meghatározott célpontba való eljuttatásához szükséges folyamatok összessége. Ennek három alapvető részfolyamata van: a helymeghatározás (lokalizáció), a szükséges útvonal meghatározása, valamint a pályakövetés és szükség esetén a korrekció. Ez a három részfeladat nem egymás után lezajló egyszeri folyamatot alkot, hanem egy ismétlődő visszacsatolt ciklus része: folyamatos lokalizáció, a helyzet összevetése a céllal és az útvonallal, szükség esetén korrekció. Ha tartósan kiesik a lokalizáció, akkor megszakadhat a navigációs folyamat.

Jelen tanulmány nem a navigáció teljes folyamatával, hanem annak csak egyik részfolyamatával, a lokalizációval foglalkozik. A lokalizáció a jármű helyzetének valamilyen vonatkoztatási rendszerben értelmezett, vagy valamilyen referenciához viszonyított pozíciójának a meghatározását jelenti. A lokalizáció tágabb értelemben nemcsak a koordinátákat jelenti, hanem ebbe a jármű vagy az eszköz orientációját is beleértjük. Jelen cikkben ettől eltekintünk, az áttekintendő lokalizációs technológiák rendszerezése szempontjából az orientáció itt nem játszik szerepet.

A lokalizáció lehet relatív, amikor egy előző helyzethez vagy egyéb relatív referenciához viszonyított elmozdulást vagy helyzetet határozunk meg. A lokalizáció lehet abszolút is, amikor egy előzetesen definiált referenciarendszerben értelmezzük a helyzetet.

A repülés a szárazföldi navigációtól eltérően további speciális követelményeket támaszt a navigációval, illetve helymeghatározással szemben. A légi jármű helyzete

háromdimenziós, az X és Y koordináták mellett a magasság meghatározására is szükség van. A repülés közben a légi jármű helyzete folyamatosan, gyakran gyorsan változik, emiatt a lokalizáció nem egyszeri feladat, hanem folyamatos helyzetbecslésre van szükség megfelelően nagy mérési gyakoriság és kis késleltetés mellett. A helyzetmeghatározás kiesése a repülőgépeknél azonnali problémát jelent, amely a repülésbiztonságot is veszélyeztetheti. A légi járműveknél a helymeghatározásnak tehát kellően pontosnak és folyamatosnak kell lennie, továbbá nagy rendelkezésre állást kell biztosítania.

A katonai alkalmazás további különleges követelményeket támaszt a navigációval, illetve a helymeghatározással szemben. A katonai célú pilóta nélküli repülőgép rendeltetésétől függően ellenséges környezetben tevékenykedik, ahol a lokalizáció hibája már nemcsak repülésbiztonsági probléma, hanem veszélyezteti a művelet végrehajtását, a küldetés sikerét, és a repülőgép elvesztéséhez is vezethet. A műveleti környezetben azzal is számolni kell, hogy az ellenfél igyekszik akadályozni vagy megtéveszteni a lokalizációs rendszert. Tehát további fontos követelmény, hogy a pilóta nélküli repülőgép navigációs rendszerének degradált és szándékosan zavart környezetben is fenn kell tartania valamilyen szintű saját helyzetmeghatározási képességet.

A pilóta nélküli repülőgépeknél (UAV – Unmanned Aerial Vehicle) egy további sajátos helyzetet is figyelembe kell venni: a pilóta fizikailag „elszakad” (távol van) a repülőgéptől. A hagyományos, pilóta vezette repülőgép esetén az ember funkcionális értelemben egy összetett érzékelő-, információfeldolgozó és döntési rendszernek tekinthető, aki a tapasztalata és intelligenciája segítségével képes döntéseket hozni. A pilóta közvetlenül érzékeli a környezetet, vizuálisan felismeri a terepet, ezt képes összevetni a térképi információval, ezek alapján tudja korrigálni a repülési pályát. Emellett szükség esetén képes áttérni alternatív navigációs módszerekre is. A pilóta nélküli repülőgépen az ember közvetlen fedélzeti érzékelése nem áll rendelkezésre. Távirányítású UAV-nál az operátor csak a fedélzeti szenzorokból származó és az adatkapcsolaton keresztül a vezérlőrendszerig eljutó információkra támaszkodhat, míg az autonóm (távvezérlést is nélkülöző) pilóta nélküli repülőgépeknél egyre több helyzetbecslési és döntési funkció kerül a repülőgép fedélzetére.

Az előzőekben megfogalmazott követelményeket összegezve, a pilóta nélküli repülőgépeken használatos ideális navigációs (lokalizációs) módszerrel szembeni főbb követelmények az alábbiak lehetnek:

– kompakt felépítésű (kis méretű és kis tömegű) eszközzel megvalósítható,
– alacsony energiafogyasztású,
– képes abszolút helyzetet szolgáltatni,
– közvetlenül háromdimenziós pozíciót ad megfelelő pontosság mellett,
– folyamatosan és valós időben működik,

– nagy területen (lehetőség szerint globálisan) rendelkezésre áll,
– nem igényel jelentős helyi infrastruktúrát,
– zavarásvédett,
– automatizálható,
– költséghatékony.

Látható, hogy normál működési körülmények között a globális műholdas navigációs rendszer a felsorolt műszaki és üzemeltetési követelmények különösen kedvező, de nem tökéletes kombinációját valósítja meg. Ebből látható, hogy miért vált megkerülhetetlen helyzetmeghatározó technológiává az UAV-oknál a GNSS, valamint az is megérthető, hogy a sérülékenysége miért vált egyre nagyobb problémává a pilóta nélküli repülőgépek helymeghatározásánál.

2. A GNSS-alapú lokalizáció és sérülékenysége

A globális műholdas navigációs rendszerek biztosítják napjainkban a legelterjedtebb abszolút lokalizációs technológiát, amelyet széles körben használnak a szárazföldi, tengeri és légi alkalmazásokban. Kedvező tulajdonságai miatt egyúttal a pilóta nélküli repülőgépek alapvető helymeghatározó technológiájává vált.

Az első műholdas navigációs rendszerek az 1960-as években jelentek meg. Ilyen volt az 1960-as évek elején bevezetett amerikai Transit rendszer, valamint a hasonló elven felépülő szovjet Ciklon konstelláció az 1960-as évek második feléből. Az alacsony Föld körüli pályán (LEO – Low Earth Orbit)[3] keringő navigációs műhold fix frekvenciájú rádiójelet sugárzott. A közeledő vagy távolodó műhold rádiójelének frekvenciája a Doppler-eltolódás miatt változott. A földi vevőberendezés a frekvenciaváltozást mérte, és a műholdpálya ismeretében ebből számította a pozíciót. Ezzel a megoldással néhány száz méteres pontosságot lehetett elérni, ami a tengerészeti alkalmazáshoz abban az időben megfelelőnek számított. A pontosságot később kétfrekvenciás méréssel már 50 m alá lehetett csökkenteni. Ezeknek a rendszereknek az alapvető problémája volt, hogy az alacsony Föld körüli pályán keringő kevés műhold valamelyike csak szakaszosan látszódott a Földről,[4] és a mérés pontosságát a vevőberendezés saját mozgása is csökkentette.

2.1. A GNSS technológiai alapjai

A Doppler-hatáson alapuló rendszerek után jelentős technológiai ugrás volt az 1970-es évek végén megjelent első globális műholdas navigációs rendszer, az ame-

[3] 200–2000 km közötti pályamagasság.
[4] A Transit rendszernél esetenként akár másfél, két órát is kellett várni két mérés között.

rikai NAVSTAR[5] (később GPS – Global Positioning System), amely a jelfutási idő mérésének elvén alapul. Ennek kulcsfontosságú eleme a rendszerben az atomórák alkalmazása volt a jelfutás idejének pontos mérése miatt.

A műholdak fedélzetén elhelyezett atomórák biztosítják az időszinkront. A műhold által küldött üzenet tartalmazza a műhold pályaadatait és a jel kibocsátásának pontos időpontját. A vevő a jel futási ideje (a jel kibocsátása és vétele között eltelt idő) alapján számítja ki a műhold és a vevő közötti pszeudotávolságot (amely egy hibákkal terhelt nyers mérési adat). Geometriai értelemben ismert helyzetű műholdtól mért távolság egy gömbfelületet határoz meg, amelyen a vevő elhelyezkedhet. Három műhold távolságadatából meghatározható lenne a vevő három térbeli koordinátája. A gyakorlatban azonban a vevő órája nincs pontosan szinkronizálva a műholdak atomórái által biztosított rendszeridővel, ezért a három térbeli koordináta mellett a vevő órahibája is ismeretlenként jelenik meg. A helyzetmeghatározás során így négy ismeretlen – az X, Y és Z koordináta, valamint a vevő órahibája – meghatározására van szükség, amihez legalább négy műholdtól származó, egymástól független pszeudotávolság-mérés szükséges.

A pszeudotávolság tartalmazza a valódi távolságot, a vevő órahibáját és a légköri késleltetéseket (ionoszférikus és troposzférikus késleltetést), valamint a földfelszíni reflexiók miatt keletkező hibákat. A hibák közül alapvető jelentőségű az órahiba, ami abból ered, hogy a vevőberendezésben egyszerű és olcsó kvarcoszcillátoros órák működnek. Nagyságrendileg ez azt jelenti, hogy a műholdak pályamagasságából adódóan egy mikroszekundumos időhiba is 300 m-es távolsági hibát okoz. [1]

Az egyszerű és olcsó vevőberendezés mellett a globális műholdas navigációs rendszerek összetett, jelentős földi és űrbeli infrastrukturális elemeket tartalmaznak. Egy ilyen GNSS műholdas konstelláció űrszegmensét alkotják a műholdak, amelyek közepes Föld körüli pályán (MEO – Medium Earth Orbit) keringenek.[6] A közepes föld körüli pálya biztosítja, hogy az egész Föld 24–30 műholddal lefedhető. A közepes pályamagasság használata egy optimumra törekvő kompromisszum. Az alacsonyabb pálya erősebb vételi szintet biztosít ugyan a Föld felszínén, de az egy műhold által lefedett terület kisebb, gyors az áthaladás a horizont felett, így sok műholdra lenne szükség a lefedettség biztosításához. A magasabb pálya nagyobb területi lefedettséget biztosít, hosszabb ideig látható a műhold, de nagyobb jelterjedési veszteséget és hibát okoz. A földi szegmens több vezérlő állomás és monitoring állomás hálózatából áll, amelyek feladata a pályaadatok folyamatos karbantartása annak érdekében, hogy a műholdak pontos pozícióadatokkal rendelkezzenek. Vagyis az egyszerű vevőberendezés mögött egy jelentős földi és űrszegmens található, nagy és költséges alapinfrastruktúrával.

[5] A NAVSTAR (GPS) rendszer alapjait az 1970-es évek első felében dolgozták ki. Az első műholdat 1978-ban állították Föld körüli pályára, és a rendszer az 1990-es évek közepére érte el a teljes kiépítettséget.

[6] Napjaink működő GNSS rendszereinek műholdjainak pályamagassága 19 000 és 23 000 km közötti.

Napjainkban négy teljesen kiépített globális műholdas navigációs rendszer működik. Az Amerikai Egyesült Államok működteti a GPS-t (korábban NAVSTAR). Az európai Galileo tisztán polgári felügyelet alatt működő rendszer. A kínai BeiDou sajátossága, hogy a MEO pályán keringő műhold mellett regionális lefedettséget biztosító, geostacionárius és geoszinkron pályákon[7] lévő műholdakat is tartalmaz. Az orosz GLONASZSZ[8] rendszer speciális tulajdonsága, hogy az alkalmazott műholdpálya nagyobb inklinációja miatt jobb sarkvidéki lefedettséggel rendelkezik.[9] A nagyobb inklináció miatt ugyanis magasabban jelennek meg a műholdak a sarkvidékhez közeli régiók égboltján, így ott stabilabb vétel biztosított. [2]

További hasonló műholdas rendszer az indiai NavIC. Fejlesztés alatt áll a dél-koreai KPS rendszer, amely 2035-re érheti el a teljes kiépítettségét. A japán QZSS rendszer teljesen kiépített, de csak regionális szolgáltatást nyújt.

Napjaink modern vevőberendezései több GNSS rendszer jeleit képesek fogadni és feldolgozni. A több konstelláció együtt több, akár 30–40 műholdat eredményez, ami kedvezőbb műholdgeometriát és nagyobb rendelkezésre állást biztosít. További fontos jellemzője a modern vevőberendezéseknek a kétfrekvenciás vételi lehetőség (pl. jellemzően a GPS-nél az L1 és L5, a Galileonál az E1 és E5 jelek), amivel a légköri hiba közül az ionoszféra késleltetésének jelentős része kompenzálható.

A globális műholdas rendszerek pontosságát kiegészítő rendszerekkel (Augmentation System) tovább lehet növelni. Ezek lehetnek űralapú vagy földi bázisú kiegészítő rendszerek, amelyek földi referenciaállomások hálózatával mérik a GNSS jelek hibáját és korrekciós adatokat biztosítanak a vevőberendezésnek, így egyes technológiákkal akár cm alatti pontosság is elérhető.

A GNSS rendszerek elterjedésében a jelentős fordulópont volt a 2000-es év, amikor az amerikai GPS-nél kikapcsolták a civil felhasználók számára a GPS-jeleket szándékosan lerontó Selective Avaibality-t. Ez nagyságrendileg javította a polgári GPS helymeghatározás pontosságát, ami elindította a polgári és kereskedelmi alkalmazások gyors terjedését.[10]

A GNSS napjainkra nem csupán helymeghatározási szolgáltatást jelent, hanem nagypontosságú időreferenciát is biztosít, amelyre stratégiai fontosságú alapinfrastruktúrák épülnek, például a távközlésben, a villamosenergia-rendszerben, vagy a pénzügyi rendszereknél. De a katonai rendszereknél (kommunikációs hálózatok, szenzorhálózatok, radarok, elektronikai hadviselési rendszerek és el-

[7] Geoszinkron pályán a műhold keringési ideje megegyezik a Föld forgási periódusával, a pályamagasság 35 786 km. A geostacionárius pálya a geoszinkron pálya speciális esete, amikor a pálya inklinációja 0º.

[8] Cirill betűkkel ГЛОНАСС – Глобальная навигационная спутниковая система, Globajnaja Navigacionnaja Szputnyikovaja Szisztema, magyarul: globális műholdas navigációs rendszer.

[9] A GLONASZSZ műholdak pályájának inklinációja 64,8º, míg a többi rendszernél 55–56º körüli.

[10] A GPS.gov 2026-ban nyílt égbolt mellett, okostelefonba épített vevőre 4,9 átlagos vízszintes hibát ad meg. URL: https://www.gps.gov/gps-accuracy (Hozzáférés: 2026.07.24.)

osztott C4ISR-rendszerek[11]) is fontos szerepet játszik a közös időreferencia biztosításában.

Összegezve, a GNSS egyetlen rendszerben számos előnyös tulajdonságot egyesíti:

– abszolút földrajzi pozíciót szolgáltat;
– közvetlen 3D pozíciót ad;
– globális vagy közel globális lefedettséget biztosít;
– folyamatos lokalizációt nyújt;
– a vevő oldalon passzív vevőberendezést igényel;
– kis méretű, tömegű és alacsony energiaigényű vevővel használható;
– olcsó vevőberendezést használ;
– nem igényel kiterjedt helyi infrastruktúrát a vevő oldalon;
– nincs az idővel növekvő halmozódó hibája;
– a lokalizáció mellett pontos időreferenciát is szolgáltat.

2.2. A GNSS korlátjai és a szándékos zavarás

A pilóta nélküli repülőgépeknél a fenti tulajdonságok között különösen fontosak a SWaP-előnyök (Size, Weight and Power, tehát a méret, tömeg és fogyasztás). Mindez oda vezetett, hogy a GNSS-en alapuló navigáció napjainkra domináns lokalizációs módszerré vált ezen a területen. A kialakult széles körű függőség miatt ugyanakkor kritikussá vált a GNSS sérülékenysége.

A számos előnyös tulajdonság mellett a GNSS-technológia jelentős technológiai korlátokkal is rendelkezik, amelyek az alábbi jelenségekből erednek:

– *Jelárnyékolás és a kitakarás:* Beépített területen az épületek, a domborzat, a növényzet gátolja a rédiójelek terjedését. Beltéren, épületekben, alagutakban ugyancsak akadályozott a rádióhullámok terjedése.
– *Többutas terjedés:* A vevőhöz közvetlen és visszavert jelek is eljutnak, ami különböző úthosszt jelent a jelterjedésnél. Ez különösen a nagy épületekkel beépített városi területeken jellemző (ld. városi kanyonok jelenség).
– *Atmoszférikus hatások*: Az ionoszféra szabad elektronjai, valamint a semleges légkör, elsősorban a troposzféra vízgőztartalom-, nyomás- és hőmérsékletváltozásaiból eredő törésmutató-változásai késleltetik a jelterjedést.
– *Műholdgeometria hatása:* A műholdak megfigyelési geometriája miatt a magassági komponens pontossága kedvezőtlenebb a vízszintes komponensénél.

A fenti technológiai korlátokhoz tartozik, de jelentősége miatt külön ki kell emelni az alacsony vételi jelszint problémáját, hiszen katonai szempontból ez okozza elsősorban a zavarhatóságot. A közepes Föld körüli pályára jellemző nagy, 20 000 km

[11] A katonai döntéshozatalt támogató integrált vezetés-irányítási, kommunikációs, támogató és hírszerzési, megfigyelési és felderítési funkciót is tartalmazó rendszer.

körüli pályamagasság miatt a jel terjedési távolsága jelentős, emiatt a Föld felszínén tiszta égbolt mellett a vételi szint -130 dBm körül alakul (városi környezetben pedig még alacsonyabb is lehet).[12] Ez a vételi teljesítmény annyira alacsony, hogy nagysága a vételi sávban jelen levő termikus zaj teljesítménye alatt is lehet. A jelek detektálását a GNSS-jelek ismert kódstruktúráját kihasználó korrelációs jelfeldolgozás teszi lehetővé. Az alacsony jelszint azt eredményezi, hogy egyrészt megfelelő nyereségű antennára, érzékeny vevőre és speciális jelfeldolgozásra van szükség a vételi oldalon, másrészt a GNSS különösen érzékeny mind a véletlen, mind a szándékos zavarásra.

Az alacsony jelszint miatt a GPS-jel erősebb zavarójellel elnyomható vagy módosítható. A GNSS-zavarás három fő kategóriája: a jelelnyomás, a jelhamisítás, és a késleltetett jeltovábbítás.[13]

A *jelelnyomás (jamming)* során a vevő által használt frekvenciasávban a jammer a kis teljesítményű GNSS-jelhez képest akkora teljesítményű zavaró jelet generál, hogy lehetetlenné teszi a jelfeldolgozást. A zavaró jel lehet zajszerű vagy más modulált jel. Célja, hogy megakadályozza a GNSS-jelek detektálását, ezáltal a lokalizáció részlegesen vagy teljesen kiesik.

A *jelhamisítás* vagy *jeltrükközés (spoofing)* során a támadó olyan mesterséges GNSS-jelet állít elő, amelyet a vevőberendezés valódi műholdjelként érzékel. A jel navigációs paramétereinek manipulálásával a vevő hibás pozíciót, sebességet vagy időt kap. A spoofing a rendszer integritását rombolja. Azért kiemelten veszélyes zavarási eljárás, mert látszólag működőképes a GNSS, valójában azonban hamis és hibás adatokat szolgáltat. A spoofing során lehet kizárólag az időszinkront is hamisítani, így a GNSS időszolgáltatásán alapuló rendszerek is támadhatók.

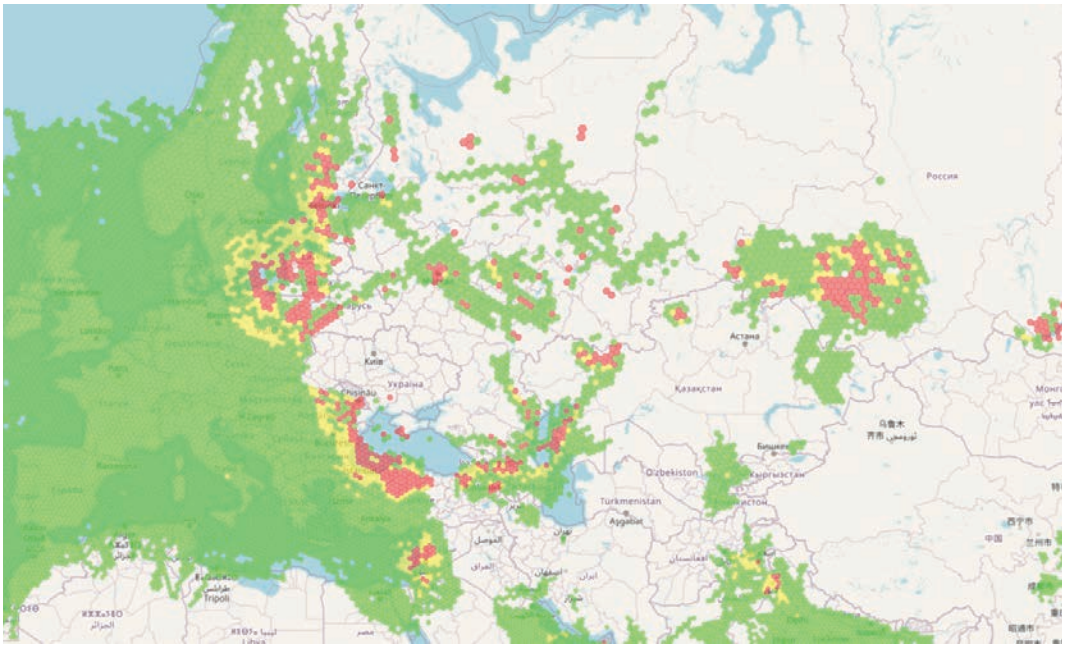
A *késleltetett újra sugárzás (meaconing)* esetén nem kell új hamis GNSS-jelet generálni. A támadó valódi műholdjeleket vesz, majd azokat késleltetve újra sugározza. Maga a jel navigációs tartalma tehát valódi, de a hozzáadódó késleltetés miatt a vevő nagyobb pszeudotávolságot számít, ami hibás lokalizációhoz és rossz órahiba meghatározáshoz vezet. A késleltetett újra sugárzás tehát a spoofinghoz hasonlóan a GNSS integritását rombolja.

A GNSS-jelek zavarásának különféle eljárásai napjaink katonai konfliktusaiban napi szintű bevett módszernek számítanak az elektronikai hadviselés terén. Ez azonban nem csak katonai probléma. A katonai konfliktusok nyomán az erősödő jamming- és spoofing-tevékenység – különösen Kelet-Európában és a Közel-Keleten – egyre nagyobb repülésbiztonsági kockázatot jelent a polgári légi közlekedésben is.[14]

[12] *Receiver sensitivity testing,* LabSat, URL: https://www.labsat.co.uk/en/applications/receiver-sensitivity-testing

[13] A késleltetett jeltovábbítást gyakran a jelhamisítás változataként kategorizálják.

[14] *EASA and IATA outline comprehensive plan to mitigate GNSS interference risk,* EASA, 2025, URL: https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-and-iata-outline-comprehensive-plan-mitigate-gnss (Hozzáférés: 2026. 08. 11.)



1. ábra. A GNSS-interferenciával összefüggő navigációs pontosságromlás területi eloszlása Európában és környezetében 2026. augusztus 26-i állapot szerint. A térkép a repülőgépek ADS-B üzeneteiben közölt navigációs pontossági adatok alapján készült. Forrás: GPSJAM, ADS-B Exchange.[15] *(Az térkép azt ábrázolja, hogy az adott területen átrepülő repülőgépek mekkora hányada jelentett alacsony navigációs pontosságot. A piros területeken ez >10%, a sárgán 2–10%.)*

A zavarással szembeni védelem és a GNSS ellenállóképességének növelése érdekében mind vevő oldalon, mind rendszerszinten több fejlesztés történt az elmúlt időszakban, amelyek többféle sérülékenységet is kezelnek.

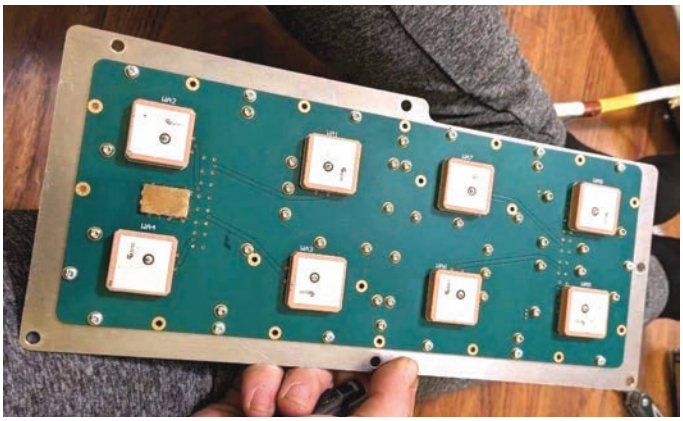
Vételi oldalon ezt szolgálja a többkonstellációs és többfrekvenciás vétel (bár ez nem jelent általános jamming-védelmet), a fejlettebb jelfeldolgozás alkalmazása, a zavarójelek felismerése és szűrése, valamint a jelintegritás-vizsgálat és spoofing-felismerés.

A vevő oldalán használt zavarásvédelmi eljárások közé tartozik a GNSS antennatömbök és irányított vételi karakterisztika *(CRPA – Controlled Reception Pattern Antenna)* alkalmazása. A CRPA-nél a vevőn antennatömböt használnak, amely2 × 4, 4 × 4, 16 × 16 darab, vagy akár még ennél is több antennaelemből áll. A tömb elemei különböző fáziseltolódással észlelik a zavaró jeleket. A vevő jelfeldolgozó processzora valós időben elemzi az egyes fázisokat, majd a rendszer kizárja a feldolgozásból a zavarás irányából érkező jeleket, azaz lényegében egy vakfoltot képez a

[15] URL: https://gpsjam.org, alaptérkép: OpenStreetMap. A szolgáltatás csak a pontosság romlását ábrázolja, arra vonatkozó adatot nem tartalmaz, hogy a jelentés mögött mekkora részben áll zavarás, de a korreláció valószínűsíthető. (Hozzáférés: 2026.08.26.)

jammer irányába, míg az égbolt többi részéről fogadja a GNSS jeleket. *(N* elemű antenna *N-1* számú jammer zavarójelét tudja semlegesíteni).

Maga a technológia nem új, az 1990-es években jelent meg amerikai repülőgépeken és hajókon. Az akkori nagyméretű, nehéz vevőberendezéseket emiatt főleg stratégiai eszközökön használták. A 2020-asévek közepére ezen a téren is jelentős technológiai fejlődés ment végbe, így a méretek és a tömeg jelentős csökkenésének köszönhetően már a kisebb pilóta nélküli repülőgépeken is alkalmazzák. Az orosz–ukrán háborúban mind az ukrán, mind az orosz oldalon széles körben elterjedten használják ezt a megoldást.



2. ábra. Az orosz VNIIR-Progressz vállalat által gyártott Kometa vevő antennatömbje ×4 db antennaelemmel.[16]

Az utóbbi időben nem csak a vevőknél, hanem a rendszer szintjén is történtek, illetve történnek olyan fejlesztések, amelyek a GNSS zavarvédelmének javítását célozzák. Az amerikai GPS-nél az ilyen irányú fejlesztések részeként megjelentek a GPS Block III típusú új műholdak, amelyeknél nagyobb a jelteljesítmény és erősödött a zavarvédettség. Ez a műholdsorozat már alapból rendelkezik a katonai M-code[17] támogatással. A műholdak fedélzetén elhelyezett korszerűbb atomóráknak köszönhetően javult a pontosság is.

A GPS fejlesztése más területeket is érint. A fejlesztés részeként az új műholdsorozaton megjelent az új L1C polgári jel, amelynél számos más tulajdonság mellett az egyik legjelentősebb lépés, hogy a GPS kompatibilissé válik az európai Galielóval (E1 frekvencia) és a japán QZSS-el (L1C frekvencia), amelyekkel így nagy virtuális konstellációt alkot.[18]

[16] Міліtарний, URL: https://militarnyi.com/en/news/new-chinese-crpa-antenna-found-on-russian-shahed/

[17] Military code. A GPS katonai alkalmazásra szolgáló, titkosítást tartalmazó és nagyobb zavvédelmet biztosító navigációs jele.

[18] *Global Positioning System (GPS),* Public ICWG Post Presentation, 2025, URL: https://www.gps.gov/sites/default/files/2025-08/2025 Public ICWG Post Presentation_Approved_20250625.pdf

A vezérlőrendszer ellenállóképességének növelését célozza a műholdak közötti optikai link kialakítása, így a GPS űrszegmensének autonómiája növekedni fog.

A harctéri zavarás elleni védelem rendszerszintű megoldása lesz a Regional Military Protection (RMP) technológia, amely már a GPS III műholdsorozat utolsó tagjánál megjelent, de majd csak a GPS Bolck IIIF (Follow-on) műholdaknál lesz alapértelmezett funkció. Itt a katonai M-code-t sugárzó antennák elfordításával egy koncentrált, szűk nyalábot lehet létrehozni, amellyel egy katonai művelet szempontjából fontos régióra lehet koncentrálni a rádiójeleket. Ez sokszoros jelszintemelkedést jelent az adott régióban, ami csökkenti a jamming lehetőségét.[19]



3. ábra. GPS Block III műhold. Forrás: U.S. Air Force, közkincs (Public domain)[20]

A GNSS zavarvédelme tehát jelentősen fejleszthető, de a fizikai működési elvből eredő sérülékenység teljesen nem szüntethető meg, ezért szükség van GNSS-től független lokalizációs képességekre is. Itt a cél nem feltétlenül a GNSS teljes kiváltása. A GNSS számos előnyös tulajdonsággal rendelkezik ahhoz, hogy egyszerűen mással helyettesítsük, viszont napjainkban a katonai alkalmazásokban már nem elegendő kizárólag a GNSS-re alapozni a helymeghatározást.

3. GNSS-független navigációs technológiák

A GNSS-en alapuló helymeghatározás előzőekben vázolt bizonytalansága, zavarhatósága miatt az utóbbi években egyre erősebb igény jelentkezett a GNSS rendszereket kiváltó, vagy csak ideiglenesen helyettesítő, más elveken és technológiá-

[19] *U.S. Space Force delivers final GPS III to orbit, advancing its most resilient constellation for military civil capabilities,* USSF Space Systems Command, 2026, URL: https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/4465444/us-space-force-delivers-final-gps-iii-to-orbit-advancing-its-most-resilient-con

[20] URL: https://www.af.mil/News/Photos.aspx?igphoto=2001638810 (Hozzáférés: 2026.07.24.)

kon alapuló helymeghatározó rendszerek alkalmazására. Az ilyen GNSS-mentes technológiák kutatása és fejlesztése napjaink egyik legfontosabb fejlesztési iránya a katonai pilóta nélküli repülőgépek területén.

A helyzeti adatok keletkezési módja szerint négy alapelvet különböztethetünk meg:

– *Elmozdulás mérésén alapuló helyzetinformáció:* Itt a rendszer a mozgásállapot változását méri, és ebből vezeti le a helyzetváltozást. Nincs szükség külső térbeli referenciára, ezért az eredmény relatív és a hibák halmozódhatnak. Klaszszikus példája ennek az inerciális navigáció.
– *Külső, ismert helyzetű forráshoz történő viszonyítás:* A jármű egy vagy több külső jelforráshoz viszonyított mérésekből határozza meg a helyzetét. Ide tartoznak a rádiónavigációs megoldások. Ez a módszer abszolút helyzetet is szolgáltathat, ha a források helyzete ismert.
– *A környezet megfigyeléséből származó relatív helyzetinformáció:* A szenzor a környezet geometriai vagy más fizikai jellemzőit érzékeli, és azok változásából, illetve ismételt megfigyeléséből megbecsüli a mozgást vagy a pozíciót. A környezet itt nem feltétlenül rendelkezik georeferenciával. Szenzorként ilyen célból kamera, radar és LiDAR is használható. Ebbe a csoportba tartozik a vizuális odometria, valamint a vizuális megfigyelésen, radaros mérésen és a LiDAR-on alapuló egyidejű helymeghatározás és térképezés (SLAM – Simultaneous Localization and Mapping).
– *Georeferált környezeti referenciához történő viszonyítás:* A fedélzeti szenzoros megfigyelést a környezet előzetesen ismert, georeferált reprezentációjával vetjük össze. Ebbe a csoportba tartozik a digitális magassági modell, georeferált légi- vagy műholdfelvétel, térképi adat, georeferált radar- és LiDAR-adat, valamint mágneses vagy gravitációs anomáliatérkép referenciaadatként történő felhasználása. Ez a módszer már abszolút földrajzi lokalizációt tesz lehetővé.

A környezeti megfigyelésen alapuló helymeghatározási eljárásoknál egységesen arról van szó, hogy a fedélzeti szenzor valamilyen helyfüggő környezeti jellemzőt mér, a referencia-adatbázis pedig ugyanezen vagy azzal kapcsolatba hozható jellemző georeferált térbeli reprezentációját tartalmazza. A kettő megfeleltetésével határozható meg a szenzor térbeli helyzete.

Másik, főként gyakorlati szempontú megközelítésben a szenzor működési elve, tehát az adatnyerés technológiája szerint is lehet csoportosítani a módszereket. Az alábbiakban a GNSS-független lokalizációs technológiák rövid bemutatása következik a szenzortechnológia alapján.

3.1. Inerciális lokalizáció

A tehetetlenségi, vagy más néven inerciális navigáció olyan eljárás, amelynél kizárólag a jármű gyorsulásának és szögsebességének mérésével számítható az eszköz

pillanatnyi pozíciója, sebessége és iránya. Ez egy relatív eljárás, amely az utolsó ismert pozícióból kiindulva számítja folyamatosan az elmozdulást és az elfordulást.

Az inerciális navigáció eszköze az inerciális mérőegység (IMU), amely kétfajta szenzorból áll: gyorsulásmérő (X, Y, Z irányban), és elfordulásmérő, vagy más néven giroszkóp (X, Y, Z tengely körüli elfordulás). Az IMU-kat gyakran kombinálják mágneses iránytűvel is, ekkor a Z tengely körüli elfordulást a mágneses északhoz képes tudja mérni az eszköz az abszolút referenciarendszerben is.

Az inerciális navigáció, illetve az inerciális mérőegység meglehetősen régi eszköz, már a 20. század elején megjelent. Kezdetben csak iránymérésre és iránytartásra használták. Az első gyakorlati alkalmazására a második világháborúban került sor a német V–2 ballisztikus rakéták irányítórendszerében.

A gyorsulásmérő műszaki alapja a megalkotása óta változatlan, vagyis egy tehetetlen tömeg gyorsulás hatására történő elmozdulását mérik. Ennek a mérési módja azonban többféle lehet, de közös bennük, hogy elektromos jeleket mérnek. A hagyományos megoldásoknál kapacitív vagy piezoelektromos módszerrel mérik az elmozdulást. A nagyobb pontosságot igénylő katonai és repülési területen a műszakilag összetettebb elektromechanikus (vagy szervó-) gyorsulásmérőt szokás használni, amelynek a driftje kedvezőbb. Hasonlóan nagy pontosságot biztosítanak a rezgőhúros gyorsulásmérők is.

A szögelfordulást mérő giroszkópok fejlődése volt a legnagyobb az elmúlt száz évben. Az 1920-as években megjelent több kilogrammos mechanikus pörgettyűs giroszkópok a perdületmegmaradás és a giroszkópos tehetetlenség elvén működtek, és használatuk az 1980-as évekig általános volt, bár több olyan terület van (pl. hajózás és a repülésben), ahol az alkalmazásuk bizonyos előnyös tulajdonságaik miatt napjainkig is megmaradt. Az 1980-as években jelentek meg a lézergiroszkópok, amelyek elsősorban a repülésben és az űrhajózásban, valamint fegyvereknél (pl. ballisztikus rakétákon) terjedtek el. Két fő változatuk a gyűrűs lézergiroszkóp (RLG – Ring Laser Gyroscop) és a száloptikás gyűrűs giroszkóp, amelyek az alkalmazott fényvezető csatornában különböznek elsősorban, de mindkettő esetén az elfordulás érzékelése az ellentétes irányba futó fénysugarak fáziseltolódásának (Sagnac-effektus) mérésén alapul.

A giroszkópok területén az igazi nagy áttörést a mikro-elektromechanikai rendszereken (MEMS – Micro-Eletro-Mechanical System) alapuló eszközök megjelenése jelentette. Az olcsón gyártható, minimális energiafogyasztású, kis tömegű és igen kisméretű, chipbe integrált giroszkóp, egybeépítve a gyorsulásmérővel, jelentős költségcsökkenést eredményezett, és széles körben elterjedtek a mindennapi elektronikában és a közepes pontosságot igénylő területeken is, így a pilóta nélküli repülőgépekben. Speciális gyártási eljárásokkal (pl. egyedi kalibrálás), rázkódásvédelemmel a MEMS alapú giroszkópok akár katonai és egyéb, nagyobb pontosságot igénylő területeken is alkalmazhatók.

Az inerciális navigációs rendszer nem függ külső navigációs rádiójelektől, azért rádiófrekvenciásan nem zavarható. Problémája azonban a sodródás, vagy elterjedt

angol elnevezéssel a drift. Az IMU integráló jellegű eszköz, a gyorsulásmérők adataiból az elmozdulást az idő kétszeres integrálásával, a szögelfordulást a mért szögsebesség egyszeres idő szerinti integrálásával számítja. Emiatt az inerciális mérőegységnél a hibák összeadódnak, halmozódó hiba jelentkezik.

A drift főbb összetevői: a statikus és dinamikus nullponteltolódás (bias), skálatényező-hiba, tengelyferdeségi és szerelési hibák, a szenzorok nem lineáris viselkedése, keresztérzékenységi hibák (amikor pl. a giroszkóp rezgő elemeire a lineáris gyorsulás is hatással van), valamint a fehér zajból eredő véletlen bolyongás (random walk).[21]

Az inerciális mérőegységek további hibaforrása a gravitációs anomáliák, illetve a szenzornál alkalmazott gravitációs modell és a tényleges gravitációs mező eltéréseiből adódó hiba. A pilóta nélküli repülőgépek esetében ez más hibaforrásokhoz viszonyítva legtöbbször elhanyagolható, de nagyobb hatótávolságú eszközöknél, pl. ballisztikus rakétáknál interkontinentális ballisztikus rakétáknál ez már jelentős hibaforrás. A hiba csökkentése érdekében az ilyen eszközök pontos gravitációs modellel dolgoznak.

Működési elve és a környezetre való mérsékelt érzékenysége miatt ideális navigációs eszköz lenne, de a halmozódó hiba miatt általában más navigációs eljárásokkal kell kombinálni. A leggyakoribb szenzorfúziós megoldás, főként a pontatlanabb MEMS alapú inerciális mérőegységeknél a GNSS-el együtt történő használat. (De a lézergiroszkóp az alacsony driftje miatt már alkalmas arra, hogy rakétafegyvereknél önállóan is biztosítsa a helymeghatározást.)

3.2. Domborzatalapú helymeghatározás

A domborzat alapú helymeghatározás (TRN – Terrain Referenced Navigation) alapelve, hogy a terepi profil előzetesen elkészített digitális reprezentációját használja referenciaadatként. Ehhez a repülőgép fedélzetén a terep feletti magasság (AGL) mérése történik lézeres vagy radaros magasságmérővel. A repülőgépen mér (pl. barometrikus magasságmérővel) mért referenciaszint feletti magasság és a mért terep feletti magasság összevetésével előállítják a terepprofilt. A mért terepprofilt korrelációs eljárással illesztik a domborzat digitális reprezentációjához, majd a legjobb illeszkedés helye fogja megadni a keresett pozíciót. Az eljárás abszolút helymeghatározást biztosít, ha a referenciaként használt digitális magassági modell rendelkezik georeferenciával.

Első gyakorlati megvalósítása az 1970-es évekre nyúlik vissza, amikor a TERCOM (Terrain Contour Matching) navigációs rendszert kidolgozták az amerikai BGM–109 Tomahawk robotrepülőgéphez. A TERCOM azonban csak szakaszo-

[21] Varga Attila, Jancsó Tamás, Udvard Péter: *Typical Errors, Accuracy Classes and Currently Expected Accuracy of Inertial Measurement Units,* in: Acta Avionica 23, 2021, pp. 8–14.

san, markáns és jellegzetes terepszakaszokon végez domborzatalapú helymeghatározást, ezek között inerciális navigációra támaszkodik.

A TERCOM modernebb változata a brit TERPROM (Terrain Profile Matching) rendszer, amelyet pl. a Storm Shadow robotrepülőgépen is használnak.[22] Az eredetileg a brit BAE Systems által kifejlesztett navigációs rendszer folyamatos magasságmérést és folyamatos terepi illesztést végez.

Rádióelektronikai zavarásra érzéketlen és független bármilyen külső navigációs infrastruktúrától. Ugyanakkor a lokalizáció pontossága függ a terep jellegétől, valamint a referenciaadatok minőségétől. A domborzatalapú helymeghatározás sem tekinthető megtéveszthetetlen módszernek. Radaros magasságmérésnél a radarvisszaverődési tulajdonságok mesterséges módosításával (pl. radarreflektív álcahálók, radarreflektorok alkalmazásával) vagy a terep átalakításával a referenciaadat és a mért terepprofil közötti korreláció lerontható.

3.3. Radaralapú lokalizáció

A radaralapú lokalizációnál a mikrohullámú rádiójeleket használó szenzor érzékeli a környezetet. Az előzőekben bemutatott radaros domborzatalapú eljárástól eltérően ez esetben a radar-visszaverődésnek a térbeli mintázata szolgáltatja a lokalizációhoz szükséges környezeti információt. A radar által kibocsátott, majd a tereptárgyakról visszaverődött mikrohullámú rádiójeleket a radar antennája érzékeli. A visszaver rádiójelekből a tereppontra távolságot és irányszögeket számít. Ha a tárgy vagy maga a radar mozog, akkor a Doppler-elv alapján a visszavert jel frekvenciaváltozásából a radiális sebesség is számítható.

A lokalizáció szempontjából a radarok három csoportját érdemes kiemelni:

– Az *impulzusradarok* rövid rádióimpulzusokat bocsátanak ki és a jel futásidejéből számítanak távolságot. Ezeket a radarokat elsősorban magasságmérésre használják.
– A *frekvenciamodulált folyamatos hullámú radar* (FMCW – Frequency-Modulated Continous Wave) folyamatos, de változó frekvenciájú rádiójelet bocsát ki, és a pillanatnyilag kibocsátott és visszavert jel frekvenciájának változásából számítja a távolságot, a Doppler-hatás alapján pedig sebesség radiális komponensét. Pontos távolságmeghatározást tesz lehetővé a technológia. Nem igényel nagyteljesítményű impulzusokat, ezért kis teljesítményigénnyel, valamint kis tömegben is megvalósítható. Emiatt a pilóta nélküli repülőgépeknél is főként ezeket a radarokat használják, elsősorban magasságmérésre, akadályérzékelésre és -akadályelkerülésre, a leszállás támogatására, célfelderítésre és célkövetésre, valamint lokalizációs célból radar-odometriára és radaralapú SLAM-re.

[22] URL: https://www.rtx.com/collinsaerospace/what-we-do/industries/military-and-defense/navigation/weapons-products/guidance-navigation-control/terprom-digital-terrain-system (Hozzáférés: 2026.07.24.)

– A *szintetikus apertúrájú radar* (SAR – Synthetic Aperture Radar) egy olyan képalkotó technológiát valósít meg, amelynél a platform mozgását használják fel arra, hogy virtuálisan egy nagyméretű radarantennát hozzanak létre. A platform mozgása során egymást követő radarmegfigyeléseket koherensen dolgozzák fel, amivel azimutirányban a fizikai antennánál jóval nagyobb virtuális apertúra hatása hozható létre. A szintetikus antenna lényegében egy térképszerű radarképet állít elő. A SAR-adat a terep egy adott pontjának visszaverődési jellemzőit, a visszavert jel amplitúdóját (erősségét) és a fázist. Az így keletkezett radartérkép a felszín radarvisszaverési tulajdonságainak térbeli eloszlását reprezentálják.

A radaralapú lokalizáció két nagy csoportja a relatív, valamint az abszolút pozícióbecslést adó módszerek. Előbbiek közé tartozik a radaros odometria és a radaralapú SLAM. A radar-odometria esetén a radar egymást követő méréseiből kinyert pontfelhők vagy sebességadatok összehasonlításával határozzák meg az elmozdulást a két mérés között. A SLAM hasonlóan működik, csupán az eszköz a radarképekből folyamatosan egy saját, lokális térképet épít fel.

– A radartérkép alapú illesztés (Radar Map Matching) már abszolút helymeghatározást tesz lehetővé, hiszen a szintetikus apertúrájú radarral előállított radartérképet egy előzőleg előállított, georeferenciával rendelkező referencia-radartérképpel hasonlítják össze.
– A radartérkép alapú illesztés továbbfejlesztett változata, amikor a radarképből jellegzetes képi jellemzőket (feature-öket, pontokat, éleket és sarkokat) nyerünk ki és ezt illesztjük a referenciaadatokkal. Egy további lépés, a mikor AI segítségével a jellegzetes pontokból összetett alakzatokat kinyerve történik a referenciaadatokkal történő összevetés.
– Az abszolút lokalizáció előzőleg elkészített, georeferált radartérképet igényel, az érintett területet előzetesen fel kell mérni. Erre a célra főleg radarműholdakat használnak, amelyek nagy területek gyors felmérésére alkalmasak. A referenciaadat-előállítás egy érdekes új iránya a meglévő 3D adatokon alapuló radarszimuláció. Itt számítógépes modellezéssel egy szoftver szimulálja a radar működését, és kiszámítja, hogy egy adott 3D-s objektumról hogyan verődne vissza a radarjel. A realisztikus visszaverődési intenzitás és szórás modellezéséhez azonban már szükség van az elektromágneses tulajdonságokra vagy a megfelelő anyag- és felszíntulajdonságokra is.
– A radar aktív eszköz, a célt saját rádiónyalábbal világítja meg, tehát nem igényel külső navigációs rádiójeleket. Ez azonban egyúttal az eszköz felderíthetőségét és rádióelektronikai eszközzel történő zavarhatóságát is lehetővé teszi. Alkalmazhatósága kevésbé függ az időjárási viszonyoktól (esőben, ködben is működőképes) és a megvilágítási körülményektől (éjszakai is használható). Számos hátrányos tulajdonsága is van: alacsony a szögfelbontása, zaj és többszörös visszaverődés jellemző rá, továbbá az RGB képektől eltérően az objektumok felismerése és szemantikai értelmezése az emberi szem számára nehezebb.

3.4. LiDAR-alapú lokalizáció

A LiDAR-alapú lokalizáció elve jelentős hasonlóságot mutat a 3.3. pontban bemutatott radaros lokalizáció elvével, a legfőbb különbség a szenzor fizikai alapjaiban van. A LiDAR (Light Detection and Ranging) olyan aktív optikai távérzékelési eszköz, amely lézersugarat bocsát ki, majd a terepi pontokról visszaverődő jel futási idejéből meghatározzák a terepi pont távolságát, a lézersugár ismert kibocsátási irányával együtt pedig megkapjuk a pont térbeli helyzetét a sugárforráshoz képest. Ezekből a mérésekből a környezet 3D pontfelhője állítható elő. Az egymást követő pontfelhők illesztésével megvalósítható a LiDAR-odometria és a LiDAR-alapú SLAM. Ha pedig a LiDAR által előállított pontfelhőt egy előzetesen előállított, georeferált referencia-pontfelhővel vagy más, szintén georeferált 3D modellel (pl. digitális felszínmodellel) illesztjük, akkor abszolút helymeghatározás végezhető.

A radarhoz viszonyítva a LiDAR a jobb szögfelbontásának köszönhetően sokkal részletesebb geometriai reprezentációt ad a környezetről. Nem függ a környezet megvilágítási viszonyaitól. Viszont érzékeny az időjárásra, ködben, csapadéknál, poros levegőben szóródnak a lézernyalábok, így a környezeti robusztussága alacsonyabb. A LiDAR működésének eredményeként nagy adatmennyiség áll elő, amelynek feldolgozása számításigényes. Napjainkban a kis tömegű és méretű LiDAR-ok is elérhetővé váltak, így kis és közepes pilóta nélküli repülőgépekhez is alkalmazhatóvá váltak. A LiDAR kisebb hatótávolsága miatt főleg kis magasságban használható, míg a radarok akár több száz km-es hatótávolsággal is rendelkeznek. Emiatt a LiDAR-t pilóta nélküli repülőgépeken inkább kis magasságban használják lokalizációra (főleg SLAM-re) és akadálykerülésre.

3.5. Mágneses anomálián és gravitációs anomáliákon alapuló lokalizáció

Mind a mágneses, mind a gravitációs anomálián alapuló lokalizáció alapelve egy geofizikai jellemző mintázatának mérése és összehasonlítása egy georeferált referenciatérképpel.

A mágnesesanomália-alapú lokalizáció (MagNav) a Föld inhomogén mágneses mezőjét használja ki helyfüggő adatok kinyerésére. A mágneses mező regionális és lokális eltéréseit részben a földkéreg eltérő mágneses tulajdonságú kőzetei okozzák, ezekről az eltérésekről geofizikai felméréssel mágnesesanomália-térkép készíthető. A repülőgép fedélzetén elhelyezkedő magnetométerrel mért mágneses teret a georeferenciával rendelkező mágnesesanomália-térképhez illesztve becsülhető az abszolút lokalizációs. A lokalizáció pontosságát a referenciatérkép pontossága és felbontása befolyásolja. Alkalmazhatóságát korlátozza, hogy nem minden terület rendelkezik egyformán karakterisztikus mágneses mintázattal.

A mágneses mező méréséhez szenzorként a magnetométer áll rendelkezésre. Ezek kisméretű, könnyű és kis fogyasztású eszközök, ezért már a kis- és közepes méretű pilóta nélküli repülőgépeken is jól alkalmazhatók. Ez a lokalizációs

módszer is passzív eljárás, azonban a környezet egyéb zavaraira érzékeny. A pontosságot befolyásolják a mesterséges mágneses terek és a hordozó platform saját mágneses tere. A Föld mágneses terének időben változó összetevői is vannak, ezért referenciaadatként történő használata időbeli korrekciót igényelhet. A pilóta nélküli repülőgépek fedélzetén a berendezések keltette mágneses terek által okozott zavarást a szenzor optimális elhelyezésével, kalibrációval és fejlett jelfeldolgozással lehet kompenzálni.

A gravitációs anomália alapú lokalizáció (GravNav) elve hasonlít a mágnesesanomália alapú navigációhoz, de a fizikai megvalósítása, a pontossága és a felhasználhatósága jelentősen eltér attól. Szenzorként gravimétert használnak. Ez lényegében egy nagyon érzékeny gyorsulásmérő, amely képes érzékelni a nehézségi gyorsulás kis változásait is, amit elsősorban a felszín alatti tömegeloszlás, ezen belül a földkéreg kőzeteinek eltérő sűrűsége okoz.[23] A gravitációs anomáliákat okozó kőzettömeg időben csak nagyon lassan változik, ezért az eljárás nagy előnye az időbeli stabilitás. Passzív, külső rádiójelet nem igénylő eljárás, rádiófrekvenciás zavarással nem tehető működésképtelenné. A hordozó platform gyorsulása, rezgései és mozgása viszont nehezíti a gravitációs anomália detektálását.

A gravitációs anomálián alapuló helymeghatározás gyakorlati alkalmazása a pilóta nélküli repülőgépeken korlátozott. Ennek elsődleges oka, hogy a graviméterek nagy tömegű szenzorok, és érzékenyek a repülőgépekre jellemző erős vibrációra. A graviméterekét napjainkban elsősorban hajókon és tengeralattjárókon, nagyméretű repülőgépeken használják, többek között gravimetriai felmérésekre, a navigációs célú felhasználásuk korlátozott. A referenciaadatot tartalmazó gravitációsanomália-térképek előállítása költséges, az ilyen adatbázisok stratégiai fontosságú, különösen védett adatbázisnak számítanak egyes országokban.

Gyakorlati szempontól a két geofizikai módszer között alapvető különbség, hogy a mágneses tér könnyebben mérhető kis méretű fedélzeti szenzorral, ugyanakkor érzékenyebb a lokális zavarokra, míg a gravitációs anomáliák időben stabilabb referenciaadatot biztosítanak, de nagy és nehéz szenzort igényelnek és a pontos fedélzeti mérésük lényegesen nehezebb.

3.6. Külső rádiójeleken alapuló lokalizáció

A külső rádiójeleken alapuló lokalizációs eljárás elvi alapja, hogy ismert helyzetű rádióforrás rádiójeleinek valamely tulajdonságát mérve végzünk helymeghatározást. Az eljárásnak a GNSS-el összehasonlítva a fő különbség az, hogy itt a rádióforrások jellemzően földi adók vagy más műholdas rendszerek, amelyek lehetnek navigációs célra telepített, illetve eredetileg más célra létrehozott rádióforrások.

[23] Zhao, J., Zhou, Z., Zhang, Z. (2026): *A Review of Key Technologies in Gravity Matching Navigation.* Sensors, 26(13), 4208., URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC13364145/ (Hozzáférés: 2026.07.24.)

A rádiójelek jellemzőinek mérési módszere alapján az alábbi módszerek használatosak:

- *Érkezési idő és futási idő (TOA – Time of Arrival, TOF – Time of Flight):* a jel futási idejéből távolságot határozunk meg, akárcsak a GNSS-nél.
- *Érkezésiidő-különbség (TDOA – Time Difference of Arrival):* több adó jelének beérkezési időeltéréséből történik a helymeghatározás. Itt nem feltétlenül szükséges a vevő órájának szigorúan szinkronban lennie az adókkal, viszont az adók egymás közötti időszinkronja fontos.
- *Érkezési szög (AOA – Angle of Arrival):* a jel érkezési irányát mérjük antennatömb (iránymérő antenna) segítségével, és több ismert helyzetű adó irányából határozzuk meg a pozíciót.
- *Vételi jelszint (RSS – Received Signal Strength, RSSI – Received Signal Strenght Indicator):* a vett jelerősségből (RSS) vagy a jelerősség-indikátorból (RSSI) következtetünk az adótól való távolságra. Ez a módszer általában lényegesen pontatlanabb, mert a rádiójel terjedési viszonyai erősen befolyásolják a vételi jelszintet.
- *Érkezési frekvenciakülönbség (FDOA – Frequency Difference of Arrival):* az adó és a vevő relatív mozgása miatt bekövetkező frekvenciaeltolódást használja fel helyzetinformáció meghatározására.

A forrásként használt rádióadók két nagy csoportba tartozhatnak: a kifejezetten navigációs célra telepített rádióadók, valamint nem navigációs célra telepített adók. Utóbbiak az ún. signals of opportunity (SoOP) jellegű adók, amelyek lehetőségként állnak rendelkezésre a lokalizációhoz. Ilyen célra felhasználhatók például mobilkommunikációs bázisállomások, rádió- és televízióadók, Wi-Fi hálózatok, illetve bizonyos esetekben műholdas kommunikációs rendszerek jelei. Ha az adó helyzete ismert, illetve a jel megfelelő tulajdonsága mérhető, akkor az eredetileg kommunikációs célú infrastruktúra lokalizációs referenciaforrássá válhat.

Az opportunisztikusan felhasználható földi rádióforrások egyik legfontosabb csoportját a mobilkommunikációs hálózatok bázisállomásai jelentik. Már a GSM-, UMTS- és LTE-hálózatok jelei is felhasználhatók helymeghatározásra, az 5G rendszerek pedig már fejlettebb idő- és iránymérési lehetőségeket is biztosítanak.

Új kutatási és fejlesztési terület napjainkban az alacsony Föld körüli pályán mozgó távközlési műholdak rádiójeleinek lokalizációs célú felhasználása. A lokáció egyik lehetséges műszaki megoldása a rádiójelek Doppler-eltolódásának vizsgálata, hasonlóan az 1960–1970-es évek Transit és Ciklon navigációs rendszereihez. A modern LEO műholdkonstellációk – pl. Starlink – esetén nagyszámú műhold áll rendelkezésre, így nagyobb rendelkezésre állás és kedvezőbb műholdgeometria érhető el, mint régen a Transit és Ciklon rendszereknél.

A módszer előnyös tulajdonsága, hogy abszolút lokalizációt biztosít, nincs drift, illetve halmozódó hiba. Fontos szem előtt tartani, hogy a módszer ugyan GNSS-független, de nem infrastruktúra-független, egy működő rádiós infrastruktúra meglé-

tét feltételezi. A vevőnek nem kell a hálózathoz csatlakoznia, passzívan érzékelheti a kisugárzott jeleket. A külső rádióforrások előnye, hogy a GNSS-től eltérő frekvenciák, jelszintek és geometria miatt a GNSS-zavarás nem feltétlenül teszi használhatatlanná. A rádiós rendszerekre jellemző zavarhatóság azonban fennáll.

3.7. Új szenzortechnológiák

A GNSS-független navigáció teljesen új kutatási irányát jelentik a kvantumtechnológián alapuló szenzorok. A kvantumnavigáció azonban nem új navigációs elvet jelent, hanem olyan új szenzortechnológiákat, amelyek az itt bemutatott inerciális, gravitációs és mágneses navigációs módszerek pontosságát növelhetik. Ezek a szenzorok az atominterferencián alapulnak, ahol az atomok hullámtermészetét használják ki. Az atomi anyaghullámot két eltérő pályára választják szét, így az két eltérő utat jár be. Majd a két részt újra egyesítik, és a gyorsulás vagy elfordulás hatására létrejött, azokkal arányos fáziskülönbséget mérik. Ezzel meghatározható a gyorsulás, az elfordulás, vagy a gravitációs mező kis változása.



4. ábra. A Q-CTRL cég pilóta nélküli repülőgépekre szánt Ironstone Opan GNSS-független, kvantummagnetométert és kvantumgravimétert használó navigációs rendszere. Forrás: Q-CTRL[24]

A kvantumtechnológián alapuló szenzorokkal nagy elméleti pontosság érhető el, de jelenleg a jelentős mértük és tömegük, nagy energiaigényük, a környezeti érzékenységük, valamint a technológia kiforratlansága miatt a repülőgépeken történő alkalmazásuk egyelőre korlátozott.[25]

[24] URL: https://q-ctrl.com/ironstone-opal

[25] Michael J. Wright, Luke Anastassioz, Chinmaya Mishra, James M. Daveies, Alexander M. Phillips, Simon Maskell: *Cold atom inertial sensors for naviógation applications,* Frontier in Phisics, 2022/10, URL: https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2022.994459/full (Hozzáférés: 2028.08.05.)

4. Vizuális lokalizáció

Az előzőekben áttekintettük a GNSS alternatívájaként napjainkban előforduló lokalizációs módszereket és szenzorokat. Ezek között nem szerepelt azonban jelen cikk központi témáját képező vizuális lokalizáció, amely külön fejezetben kapott helyet.

A vizuális lokalizáció szenzora a digitális kamera, amely egyszerű, olcsó, kis méretű, kis tömegű és alacsony energiaigényű eszköz, és a legtöbb pilóta nélküli repülőgépen egyébként is rendelkezésre áll. A kamera a környezetről nagy információtartalmú adatot szolgáltat. A kamerakép a környezet számos geometriai, radiometriai és szemantikai tulajdonságáról egyidejűleg hordoz információt. A képfeldolgozás ugyan összetett folyamat, de a hardverek teljesítményében bekövetkezett ugrás a számítási teljesítmény növekedésével járt, ezért mára a képfeldolgozási technológiák könnyen elérhető mindennapos módszerekké váltak.

Ennek következtében a digitális kamerát mint szenzort használó vizuális lokalizáció napjainkra fontos kutatási területté és fejlesztési iránnyá vált, és a GNSS-en alapuló lokalizáció egyik gyakran használt alternatívája lett. A kamera alapú szenzoradatok feldolgozásánál a gépi látás (CV – Computer Vision) és a fotogrammetria játszik főszerepet.

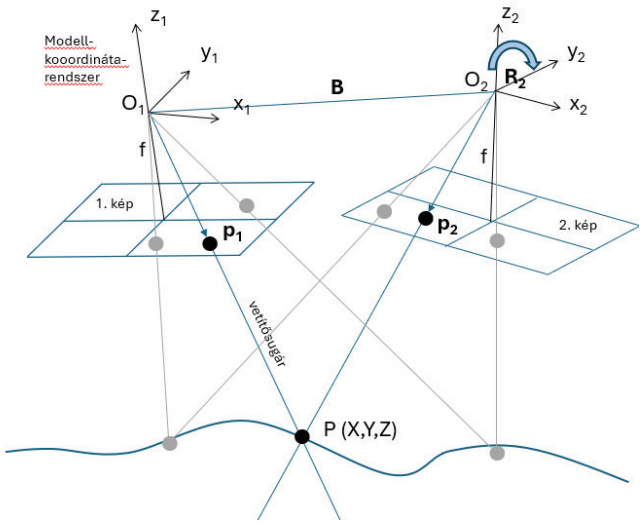
4.1. Geometriai alapok és a fotogrammetriai háttér

A vizuális lokalizáció során a 3D térről a szenzor 2D-s, síkbeli képi reprezentációt állt elő centrális vetítéssel. A lokalizáció érdekében ennek a 2D-s képi reprezentációnak a helyzetét kell térben újra rekonstruálni, ami fotogrammetriai eljárással történik. Ennek első lépése a belső tájékozás (a kamera geometriai modelljének megalkotása), majd a külső tájékozás, vagyis a kamera helyzetének és irányának a meghatározása (ezt együttesen kamerapóznak szokás nevezni), ami egyúttal a lokalizáció célja egyben.

A fotogrammetriai eljárás alapja, hogy a terepről több, egymást átfedő kép készül különböző pozícióból a kamera folyamatos mozgása miatt *(4. ábra).* Így ugyanazon *P* terepi pont több képen jelenik meg *(p_1, p_2),* amelyek geometriai kapcsolatot jelentenek a képek között. Sztereó képpárokat alapul véve megfelelő számú kapcsolópont *(p_1, p_2* párok) meghatározására van szükség a képeken, így a kamerák (pontosabban kamerapozíciók) egymáshoz viszonyított helyzete (azaz általában az egyik képhez rögzített lokális koordináta-rendszerben a másik kép pozíciója), illetve a 3D geometria rekonstruálható. A sztereó fotogrammetria alapját a kollinearitási feltétel (a tárgypont, ennek képi pontja és a vetítési középpont – *P, p_1, O_1 és P, p_2, O_2* – egy egyenesen helyezkedik el) és a koplanaritási feltétel (amely szerint a két vetítési középpont és a tárgypont egy síkban helyezkedik el). Utóbbi az epipoláris geometria alapvető feltétele is. Ezt a geometriai feltételt matematikai formában megadva és az egyenletrendszert megoldva meghatározhatók a kamera ismeretlen külső tájé-

kozási[26] elemei, vagyis a második kamera relatív helyzete és orientációja (azaz O_2 vetítési középpont és az R forgatási mátrix).

A 3D rekonstrukció során napjainkban szinte kizárólag a gépi látás módszereit használják, amelyek alapelve a klasszikus fotogrammetriai módszerekkel megegyezik, de részben eltérő matematikai formalizmust használ. [3][4]



5. ábra. A centrális vetítés és a geometriai kényszerek sztereó képpárnál. A P térbeli pont p_1 és p_2 képi megfelelői, valamint az O_1 és O_2 vetítési középpontok meghatározzák a két vetítősugarat. Forrás: a szerző korábbi ábrája alapján átdolgozva

4.2. Relatív és abszolút koordináta-rendszer

A vizuális navigáció egyik alapvető jellemzője, hogy a fedélzeti szenzor lokális koordináta-rendszerében végez megfigyeléseket, amelyet a georeferált környezeti referenciával kell összehasonlítani. A klasszikus fotogrammetriában a lokális koordinátarendszer és földi abszolút koordinátarendszer között földi illesztőpontokkal lehet kapcsolatot teremteni. A fotogrammetriában ez az abszolút tájékozás, ahol a két koordinátarendszer közötti térbeli hasonlósági transzformáció paramétereit meghatározzuk.

A vizuális lokalizáció során tehát a fő feladat az, hogy a fedélzeti lokális rendszerben történt megfigyelés és az abszolút rendszerben értelmezett georeferált tér közötti kapcsolatot kell automatikusan és folyamatosan meghatározni. Itt viszont nem földi illesztőpontokat mérünk közvetlenül a terepen, hanem georeferenciával rendelkező

[26] A tájékozás a fotogrammetriában a kamera felvételkori térbeli helyzetének és orientációjának a meghatározása adott koordinátarendszerben.

geoinformatikai referenciaadatokat használunk és ezekből nyerünk illesztőpontokat. A klasszikus fotogrammetriában a relatív tájékozással valósul meg a lokális rendszerben történő feldolgozás, majd ezt követően egy külön lépésben térbeli hasonlósági transzformációval történik a földrajzi rendszerbe történő átszámítás.

Attól függően, hogy a szenzoradatot egy korábbi szenzorállapothoz vagy georeferált referenciaadathoz viszonyítjuk, relatív vagy abszolút vizuális lokalizációról beszélhetünk. Az előbbi esetben a kamera elmozdulását egy lokális koordináta-rendszerben, az utóbbiban a kamera helyzetét egy abszolút földi koordináta-rendszerben határozzuk meg.

4.3. Automatikus képegyeztetés

A lokalizáció folyamatossága érdekében a valós idejű térbeli rekonstrukcióhoz a képeken a kapcsolópontok automatikus egyeztetésére van szükség, amelyhez a gépi látásban használt különböző képegyeztetési eljárásokat használnak. Ennek során különféle korrelációs eljárásokkal keresik meg ugyanannak a terepi pontnak az összetartozó képi megfelelőjét a sztereó képpár mindkét képén. Ez történhet régió alapú korrelációval vagy objektum (feature) alapú egyeztetéssel. A folyamat első lépése a jellegzetes képi elemek megkeresése. Erre általában éleket és sarokpontokat célszerű keresni. Terület alapú képegyeztetésnél a jellegzetes pont körüli adott régiót hasonlítják össze korrelációs eljárással. Hátránya, hogy az eljárás a méretarány-változásra és a forgatásra érzékeny. Hatékonyabbak az objektumalapú képegyeztetési eljárások. Itt a detektált sarokpontok környezetében egy adott régióban egy leíró adatsort (descriptor) állítanak elő. A két kép descriptorait összehasonlítva az összetartozó képpárok azonosíthatók. A képegyeztetés utolsó lépéseként geometriai ellenőrzés történik az outlierek kiszűrése érdekében, amivel az eljárás hibája csökkenthető.

Számos képegyeztető eljárást dolgoztak ki, amelyeket széles körben használnak a képfeldolgozó szoftverekben. Klasszikus példa az ilyen módszerekre a SIFT módszer.[27] Ez jellegzetes foltokat (blob) detektál a képen. A kulcspont környezetét 4×4 cellára osztja, amelyekben a lokális intenzitásgradiens irányából és nagyságából nyolcirányú hisztogramot képez. Az így kapott 4×4×8 érték alkotja a 128 elemű descriptort. A másik képen egy hasonló descriptorral rendelkező detektált kulcspontot keresünk. A SIFT jól kezeli a méretbeli eltéréseket (skálainvariáns) és a jó a forgatás-invarianciája is. A SIFT-hez hasonló elven működik a SURF és az ORB eljárás. Előbbinél 64 számot használnak a descriptorhoz, utóbbinál a környező régiók pixelintenzitásának összehasonlítását bináris számokkal végzik. A SURF és az ORB eljárás lényegesen gyorsabb, mint a SIFT módszer. Az ORB a skálázást egyszerűsített képpiramissal kezeli, ezért az gyengébb, mint a SIT és a SURF módszernél, ugyanakkor forgatással szembeni invarianciája jó.

[27] *Introduction to SIFT (Scale-Invariant Feature Transform),* OpenCV, URL: https://docs.opencv.org/4.13.0/da/df5/tutorial_py_sift_intro.html (Hozzáférés: 2026.07.24.)

A descriptorok összehasonlítása után számos hibás kulcspontpárosítást is kapunk, amelyeket ki kell szűrnünk a 3D rekonstrukcióból. Ennek egyik elterjedt módja a véletlenszerű mintavételezésen alapuló RANSAC robusztus modellbecslési eljárás, amely a geometriai modellnek nem megfelelő pontpárok (outlierek) azonosítására és kizárására használható. [5]

A képegyeztetési eljárások fejlődési iránya napjainkban egyre inkább az AI alapú megoldások felé mutat. Míg az előzőekben érintett hagyományos detektorok adott, beégetett matematikai szabályrendszeren alapulnak és mindig ugyanazokat a lépéseket végzik, addig az AI alapú, elsősorban a mélytanulást alkalmazó módszerek adatvezéreltek, sok mintaképből önállóan tanulják meg a legstabilabb vizuális jellemzők felismerését. Ennek köszönhetően képesek alkalmazkodni a képek szemantikai tartalmához is, és extrém körülmények között (pl. gyenge textura, hirtelen nézőpontváltozás) is jobb eredményeket adnak, mint a hagyományos detektorok. Az AI alapú eljárásokkal a kapcsolópontok detektálása mellett az outlierek kiszűrése is hatékonyabban megoldható.

4.4. A vizuális lokalizáció korlátjai

A vizuális navigáció működőképessége és minősége alapvetően függ attól, hogy a környezet a használt optikai szenzor számára megfigyelhető-e, és a kép tartalmaz-e elegendő, felismerhető és térben megkülönböztethető információt. Ami gyakorlati szempontból azt jelenti, hogy a megbízható pontos helyzetbecsléshez a képi információk alapján elő lehet-e állítani megfelelő számú, megbízható és kedvező geometriai eloszlású kapcsolópontot.

A vizuális lokalizáció korlátait három nagy csoportba lehet sorolni:

– *Nem megfelelő érzékelési feltételek:* A nem megfelelő megvilágítás, köd, füst, por, csapadék, ellenfény, árnyék, tükröződés jelentléte a szenzor képalkotási képességét rontja.
– *A környezet elégtelen információtartalma:* A jellegtelen és homogén, vagy ismétlődő felszín miatt (pl. víz, hóborította felszín, sivatag) kevés a stabil képi jellemző, a feature-alapú képegyeztető eljárások nem találnak elegendő megbízható kapcsolópontot. Két szélsőséges példaként említhető a sok kapcsolópontot biztosító városi környezet és egy kapcsolópontok keresésére kevésbé alkalmas vízfelszín.
– *Időbeli változás:* A növényzet, a járművek, az építkezések, az évszakos változások időben változó környezetet eredményeznek, emiatt a szenzor által érzékelt aktuális kép eltérhet a korábbi felméréssel létrehozott referenciaadattól.

A fenti korlátok bizonyos eljárásokkal – pl. infravörös vagy multispektrális szenzor alkalmazása, képjavítás, szenzorfúzió – mérsékelhetők, de nem szüntetik meg az alapvető környezetfüggést.

5. Relatív vizuális navigáció

Relatív vizuális lokalizációról beszélünk, ha a kamera aktuális megfigyelését egy korábbi megfigyelésekhez viszonyítva, külső abszolút referencia felhasználása nélkül határozzuk meg a kamera elmozdulását.

Minden új pozíció számítása az előző lépésen alapul, halmozódó hibák jelentkeznek, ez egyre növekvő hiba a relatív vizuális navigációnál is driftet okoz. Abszolút lokalizáció úgy valósítható meg, ha a repülőgép mozgása során bizonyos pozíciókban más lokalizációs eljárással kapunk abszolút pozíciót.

Az alábbiakban a jellemző relatív vizuális navigációs eljárások rövid bemutatása található, amelyek matematikai és műszaki alapja az előző fejezetben bemutatott fotogrammetriai eljárás.

5.1. Optikai áramlás

Az egyik legegyszerűbben megvalósítható eljárás, amely lefele néző kamerát használ. A módszer a pixelek vagy pixelcsoport látszólagos elmozdulását (optikai áramlását) vizsgálja a képen. Ebből a kamera tényleges térbeli elmozdulása még nem határozható meg, de a kamera geometriai modellje és a repülési magasság ismeretében már jól becsülhető a relatív elmozdulás. Egyszerű eljárás, ezért hobbidrónokon is népszerű. Lefelé néző kamera, ismert magasság és közel sík terep esetén nagyon jól használható. Problémája, hogy csak relatív elmozdulást mér, abszolút pozíció becslésére nem alkalmas. Egyszerűbb esetekben jól használható stabilizálásra (pozíciótartás, leszállás támogatása) és kisebb GNSS-jelvesztések kompenzálására.

5.2. Vizuális odometria (VO) és vizuális-inerciális odometria

Lokális koordinátarendszerben megvalósuló eljárás, amely az egymást követő képkockák közötti transzformációt számítja ki. Ennek eredményeként relatív elmozdulást kapunk. Ezekből a relatív elmozdulásokból pedig felépíthető a jármű trajektóriája.

A robusztusság növelésére a vizuális odometriát gyakran inerciális mérőegységgel kombinálják. A szenzorfúzióval két egymást kiegészítő rendszer fúziója valósul meg, amely alkalmas a robusztusság növelésére és a drift mérséklésére, de az abszolút referencia hiánya továbbra is fennáll. A vizuális-inerciális odometria a rövid távú mozgásbecslésre és lokalizációra jól használható, a két szenzor jól kiegészíti egymást. Az IMU követi a nagy frekvenciájú, gyors mozgásváltozásokat, miközben a kamera geometriai kényszerei korrigálják az IMU hibáját.

5.3. Vizuális SLAM

A vizuális szenzor (kamera) adatain alapuló egyidejű lokalizáció és térképépítés (SLAM) hasonlóan működik a LiDAR- és radaralapú SLAM-hez. A módszerrel az

egymást követő képkockák folyamatos 3D rekonstrukciójával egyidejűleg térképépítés valósul meg a kamera lokális koordinátarendszerében.

A térképépítés kezdetén a rendszer megfelelő képkockákat kulcsképkockaként (keyframe) választ ki. Az ezen képkockákon meghatározott kapcsolópontok alapján a képek tájékozásával a lokális rendszerben tereppontokat (landmarkokat) határoz meg. A további képkockák kamerapózát a már ismert landmarkokból számítható. A kamera tovább haladásával újabb területek kerülnek a látómezőbe, amelyek újabb kulcskockákat és újabb landmarkokat jelentenek, amelyekből további kamerapózokat számol. A folyamat során az algoritmus a landmarkokat nem dobja el, hanem megőrzi és ezekből folyamatosan egy térképet épít fel. Ha a kamera visszatér egy olyan területre, amely már szerepel a térképen (loop closure*),* akkor az időközben felgyűlt hibát korrigálni tudják. A trajektóriabecslés javítására a belső geometriai ellentmondások mérséklésére szolgáló sugárnyaláb-kiegyenlítést (bundle adjustment), valamint szenzorfúziót lehet alkalmazni.

A loop closure javíthat ugyan a pontossági problémákon, hiszen a korábbi helyre történő visszatérés olyan geometriai kényszert jelent, amely javítja a lokalizáció belső konzisztenciáját. Ám ennek feltétele, hogy a repülőgép olyan területen mozogjon, ahol van esély a korábban már bejárt területre történő visszatérésre. Alkalmazhatósága a repülési útvonal jellegétől függ. Egy csapásmérő pilóta nélküli repülőgép alapvetően egy cél felé repül, a visszatérés nem valószínű, de egy felderítő UAV esetében előfordulhat egy korábban bejárt területre történő visszatérés.

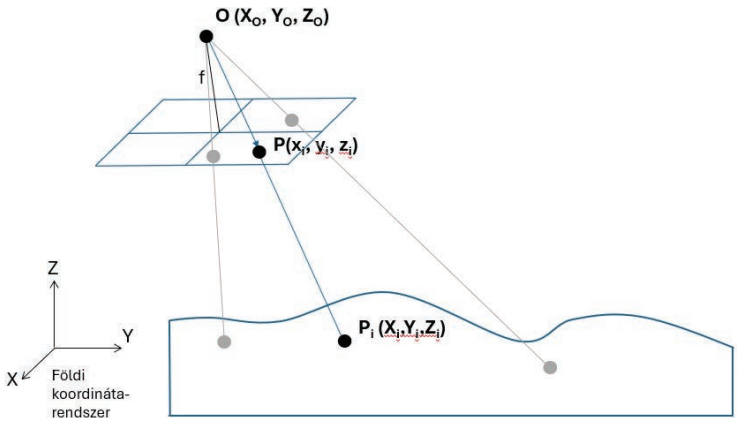
Míg a vizuális odometria elsődleges célja a kamera egymást követő pózainak és ezáltal a trajektóriának a becslése, addig a SLAM a lokalizációval egyidejűleg a környezet belső térképét is létrehozza és fenntartja.

6. Georeferált referenciaadaton alapuló vizuális navigáció

Az abszolút vizuális lokalizáció olyan referenciaadatot használ, amelynek térbeli helyzete egy földi, georeferált koordináta-rendszerben ismert. Az ilyen referenciaadaton alapuló lokalizáció eredményeként ezért a kamera helyzete és orientációja közvetlenül ebben a koordináta-rendszerben határozható meg.

6.1. A georeferált referenciaadatokon alapuló lokalizáció alapelve

Az eljárás alapvető feladata a fedélzeti kamerával megfigyelt környezeti információ (kamerakép) és a georeferált referenciaadat közötti megfeleltetés létrehozása. A legegyszerűbb geometriai esetben a kameraképen azonosított *pi* képpontokhoz a referenciaadatban ismert *Pi (Xi,Yi,Zi)* térbeli pontokat rendelünk (6. ábra). Az így létrejövő 2D–3D megfeleltetések alapján meghatározható a kamerapozíció (geometriai értelemeben az *O* vetítési középpont). Fotogrammetriai szempontból ez a térbeli hátrametszés, amelynek eredményeként megkapjuk a kamera külső tájékozási elemeit (pozíció és orientáció).



6. ábra. A kamera abszolút helyzetének és orientációjának meghatározása térbeli hátrametszéssel ismert földi koordinátájú pontok alapján

Ez némileg eltér a klasszikus fotogrammetriai munkafolyamattól, ahol több felvételből relatív tájékozással először egy lokális modell hozható létre, majd ezt ismert földi illesztőpontok segítségével abszolút koordináta-rendszerbe transzformálják. Az abszolút vizuális lokalizáció esetében ezzel szemben a georeferált referenciaadat már közvetlenül részt vesz a kamerapóz meghatározásában, ezért nincs szükség arra, hogy előbb egy önálló lokális modellt hozzunk létre, majd azt külön transzformáljuk az abszolút rendszerbe.

Az abszolút lokalizáció megvalósításában a legnagyobb problémát nem a geometriai helyzetmeghatározás (a térbeli hátrametszés) jelenti, hanem az, hogy a kamerakép megfelelő pontjait és az ezeknek megfelelő térbeli referenciaelemeket automatikusan és megbízhatóan összerendeljük. Ennek módszere függ a referenciaadat típusától. Georeferált légi- vagy műholdfelvételnél képi jellemzők, 3D pontfelhő vagy felszínmodell esetén képi és térbeli jellemzők, vektoros térképnél pedig geometriai vagy szemantikai objektumok között kell kapcsolatot teremteni. Ezért a referenciaadat reprezentációja határozza meg a lokalizációs eljárásban használt összerendelési módszereket.

6.2. Ortofotó mint referenciaadat

Elterjedt módszer az ortofotók (légifelvételek vagy műholdképek) alkalmazása referenciaadatként. Itt a szenzoradat és a referenciaadat is a 3D-s környezet 2D-s képi reprezentációja, a feladat tehát az előzőekben tárgyalt 2D–2D képegyeztetési feladattá egyszerűsödik. A megoldást nehezíti azonban, hogy a kamerakép és az ortofotó a 3D környezetnek nem ugyanazzal a leképezéssel készített reprezentációja. A kamerakép centrális vetítéssel előállított perspektivikus kép. Az ortofotó viszont ortorektifikált kép, a perspektivikus és magassági torzulásokat korrigálták, és egy vetületi térképi koordinátarendszerben van értelmezve. Tovább nehezíti a feladat

megoldását, hogy a kameraképek többnyire ferde kameranézettel készülnek (oblique felvételek), ezért a tereptárgyak ortofotón látható képe a kameraképen teljesen eltérhet. (Pl. magas épületeknél az ortofotón a tető látszik, de egy oblique felvételen már az oldalfalak is hangsúlyosan megjelennek.) Emiatt az ilyen feladatokhoz robusztus képegyeztető eljárások kellenek, amelyeknél már egyre nagyobb szerepet kap a mesterséges intelligencia.

Az ortofotó alkalmazásának egyszerűsített esete, amikor sík, vagy közel sík terepen nadír kameranézettel valósítjuk meg a lokalizációt. Ilyen esetben a kamerakép és az ortofotó közötti geometriai kapcsolat homográfiával jól közelíthető.

Az ortofotón alapuló lokalizáció általános eseténél a terepen domborzat található, a kamerakép ferde kameranézettel készül. A magassági és perspektivikus torzulások miatt csupán a két 2D-s képpel nem oldható meg a feladat. Az egyik megoldási lehetőség magassági adatokat tartalmazó digitális magassági modell (DEM – Digital Elevation Model) igénybevétele a feladathoz. Ekkor az ortofotó egy adott X, Y pontjához a magassági modellből kiolvasható a hozzá tartozó Z érték, így a feladat már 2D–3D megfeleltetéssé alakul, amely megoldható.

A feladatnak hat ismeretlenje van: a vetítési középpont koordinátái és a kamera forgatási szögei. A megoldandó geometriai feladat – a már korábban ismertetett kollinearitási feltétel alapján – a térbeli hátrametszés. A hat ismeretlen meghatározásához legalább három pont és ezek képpontjainak az összerendelésére van szükség. A maradékhibák csökkentése érdekében ennél rendszerint több pont meghatározása történik. A fölös mérésekkel az egyenletrendszer túlhatározott lesz, emiatt kiegyenlítést kell alkalmazni. A hiba csökkentése érdekében a kiválasztásánál figyelembe kell venni, hogy a képen egyenletesen eloszló pontokat célszerű használni.

Fotogrammetriai oldalról az eljárás szoros rokonságot mutat az egyképes fotogrammetriai kiértékeléssel (monoplotting). A geometriai modell ugyanaz, de a monoplottingnál a kamerapóz ismert és a terepi pont az ismeretlen, míg a magassági modellt használó ortofotó alapú lokalizációnál a terepi pont koordinátája ismert, a kamerapóz az ismeretlen. A gépi látás fogalomrendszerében ugyanez ez a feladat az ún. Perspective-n-point (PnP) probléma.

Az ortofotón alapuló lokalizációs feladat egy másik megoldási lehetősége a szintetikus perspektivikus referencia-nézet előállítása. Adott a centrális vetítéssel létrehozott kamerakép és a vetületi rendszerben lévő ortofotó, amelyek az eltérő vetítési geometria miatt közvetlenül nem egyeztethetők. A közvetlen egyeztetés helyett a referencia-ortofotóból olyan perspektivikus képet kell generálni, amely egy feltételezett helyzetű és orientációjú kamera képének felel meg. Vagyis az ortofotóból készítünk a valós kamera várható képéhez geometriailag hasonló referencia-képet, egy ún. szintetikus referenciaképet. A szintetikus kép előállításához meg kell adni egy virtuális-kamera pózt. Ez azonban ismeretlen, ezért különböző pozíció- és orientáció-hipotézisekkel kell alkalmazni és ezekkel létrehozni a szintetikus képet, majd azt összehasonlítani az aktuális kameraképpel. Ez történhet például feature matchinggel, korrelációval vagy gépi tanulás alapú képegyeztetési eljárással.

A nagyszámú lehetséges pózhipotézis miatt nagy a keresési tér, ez nagy számítási kapacitást igényel. A keresési tér csökkentésére célszerű felhasználni valamilyen rendelkezésre álló kamerapóz-információt. A kamerapozíció ismeretlen, de a pilóta nélküli repülőgépek kamerájának orientációja az IMU-adatok alapján rendszerint ismert, sőt, többnyire a repülési magasság is rendelkezésre állthat a barometrikus magasságmérő alapján. Így már csak az X, Y koordináta lesz az ismeretlen, tehát egy síkbeli pozíciókereséssé redukálható a feladat.

6.3. 3D modell, mint referenciaadat

A 3D modellek, mint a 3D pontfelhő, a mesh-háló szintén felhasználhatók abszolút lokalizáció céljára. A 3D-s modell eleve a környezet háromdimenziós geometriáját tartalmazza. Amennyiben a modell georeferált, a *P* terepi pont X, Y és Z abszolút koordinátája közvetlenül kiolvasható. A 3D modell problémája lokalizáció szempontjából ugyanaz, mint az ortofotónál: a 3D modellek térképi vetületben értelmezettek, míg a szenzor által generált kamerakép centrális vetítés eredménye.

A lokalizáció kétféle módon történhet. Egyik lehetséges módszer az előző pontnál bemutatott 2D–3D illesztési (térbeli hátrametszés vagy PnP-probléma) feladat a detektált képi jellemzők alapján.

A másik lehetőség a renderelésen alapuló lokalizáció, amely a 3D modell esetében könnyen megvalósítható. A 3D modellről különböző feltételezett kamerapózokkal és a kamerageometriára jellemző centrális vetítéssel renderelt nézet készül, majd ennek eredményét lehet összehasonlítani a referenciaképpel. Ez lényegében megegyezik az ortofotónál bemutatott szintetikuskamerakép-módszerrel, de azzal a különbséggel, hogy itt eleve teljes 3D referenciaadat áll rendelkezésre.

A 3D pontfelhő olyan reprezentációja a térnek, ahol nincs folytonos felület, csak diszkrét pontok állnak rendelkezésre. Emiatt a referenciaadat és a kamerakép összevetése során a pontfelhőt folytonossá kell, ami vagy felületillesztéssel, felületrekonstrukcióval, vagy interpolációval oldható meg. A mesh-háló ilyen szempontból kedvező, mert felületi geometriát tartalmaz, így renderelhető. Ennél is erősebb a textúrázott mesh, mert a felület vizuális információt is tartalmaz, így a renderelés során fotórealisztikus szintetikus kép állítható elő, amely a kamerakép illesztése szempontjából kedvezőbb.

Ez a lokalizációs módszer napjainkban már erősen kutatott téma.[28, 29]

[28] Liu et al.: *Enhancing visual localization with only imperfect 3D models, in: Applied Earth Observation and Geoinformatics,* Volume 132, 2024 August, URL: https://www.sciencedirect.com/science/article/pii/S1569843224003418 (Hozzáférés: 2026.08.13.)

[29] Linton Zhang, Yifu Tao, Jiarong Lin, Fu Zhang, Maurice Fallon: Visual localization in 3D maps: comparing point cloud, mesh, and NeRF representations, in: Autonomous Robots, Volume 50, 2026, Springer, URL: https://link.springer.com/article/10.1007/s10514-025-10232-5 (Hozzáférés: 2026.08.13.)

6.4. Vektoros térkép, mint referenciaadat

Újszerű megoldás a vektoros térképek felhasználása referenciaadatként az abszolút lokalizáció céljából. A vektoros térkép lényegében egy geoadatbázis, amelyből egy lekérdezés és renderelés eredményeként lesz vizuálisan látható térkép. A vektoros térkép térképi objektumokat tartalmaz. Ezek az objektumok rendelkeznek egyrészt geometriával, valamint különféle metaadattal. Geometria szerint a vektoros térképi elem lehet pont, vonal vagy poligon. A térkép tehát nem a környezet vizuális reprezentációját tárolja, hanem annak geometriai struktúráját, ami nehézséget okoz a képi szenzoradat és a referenciaadat összehasonlításában, mivel nem lehet egyszerű feature matchinget használni a képek összehasonlításánál. Természetesen itt is jelen van az eltérő geometriai projekció (centrális vetítés vs. térképi vetület) problémája, de amint az előzőekben láthattuk, erre léteznek már jó megoldások. A vektoros térkép ugyanakkor előnyös, mert kompakt, kis méretű adatbázisban tárolható.

A megfeleltetéshez a kameraképből először ki kell nyerni olyan geometriai elemeket, amelyekhez hasonló objektumok találhatók a vektoros térképen, majd ezeket lehet összehasonlítani. Ha a geometriai megfeleltetés lehetséges, akkor az előző pontokban bemutatott módszerekkel már becsülhető a kamerapóz. Ilyen jellegzetes objektumok az úthálózat és az útkereszteződések, az épületek, partvonalak, vasútvonalak és egyéb markánsan elkülöníthető lineáris objektumok, valamint maguknak az objektumoknak az egymáshoz viszonyított térbeli elhelyezkedése.

Az eljárás fő problémája a szenzoradat és a referenciaadat közötti reprezentációs különbség. A kameraképen egy út például a vektoros térképen lehet vonal, de poligon is, a kameraképen viszont egy textúrával rendelkező felület. Egy épület a térképen az alaprajzával jelölt poligon, a kameraképen egy perspektivikus 3D objektum. Emiatt szükség van valamilyen köztes reprezentációra, amely olyan geometriai struktúrát használ, amely lehetővé teszi az összehasonlíthatóságot. Ehhez olyan képfeldolgozási eljárások használhatók fel, mint az él- és vonaldetektálás, az objektumdetektálás, valamint a szegmentáció, különösen a szemantikus szegmentáció.[30]

6.5. A szemantikus térképek jövőbeni szerepe

A vektoros térképen alapuló lokalizáció kiterjesztésének tekinthető a szemantikus térképek lokalizációra történő használata, amely egy teljesen újszerű fejlesztési irány. Az újszerű volta annak köszönhető, hogy erősen támaszkodik a mesterséges intelligencia használatára, amelyben az utóbbi években robbanásszerű fejlődés ment végbe. Ez a megközelítés már az emberi vizuális tájékozódás gépi megvaló-

[30] Chenguang Ouyang, Suxing Hu, Fengqi Long, Shuai Shi, Zhichao Yu, Kaichun Zhao, Zheng You, Junyin Pi, Bowen Xing: *A semantic vector map-based approach for aircraft positioning in GNSS/GPS denied large-scale environment,* in: Defence Technology vol.ume 34., April 2024, p. 1-10.
URL: https://www.sciencedirect.com/science/article/pii/S2214914723001903

sításának irányába vezet. A szemantikus térképek referenciaadatként történő felhasználása lokalizációra már egy kutatott, de még nem kellően kidolgozott és nem kiforrott területe a vizuális lokalizációnak.[31]

A vektoros térképi lokalizációval ellentétben itt nem csak a geometriai megfeleltetést használjuk, hanem az objektumokhoz kapcsolódó egyéb jelenségeket, szemantikus tartalmakat is bevonjuk a megfeleltetésbe. Például a szemantikus térképen szereplő poligon lehet egy épület, vízfelület vagy erdő is. A szemantikus térkép tartalmaz erre vonatkozó információkat is, de mellette tárolja pl. a környezeti kontextust és szabályrendszert (pl. egy repülőteret jelölő poligonhoz tartozó szabályrendszer lehet, hogy ott no-drone zóna van), továbbá jelölhet topológiai és ontológiai kapcsolatokat is (pl. egy ház a telek része, vagy egy út a vasútvonal felett halad). A geoinformatikában használatos vektoros térképek objektumai is tartalmaznak attribútum-adatokat, de a szemantikus térképen ez szélesebb körű, kiegészül a környezetobjektumainak jelentéseivel, az objektum osztályba sorolásával, továbbá az objektumok közötti kapcsolatok és a környezeti kontextus a reprezentáció fontos részét képezik.

A kamerakép és a referenciaadat megfeleltetésénél a szenzoradatból szemantikus szegmentációval objektumokat kell meghatározni, ezekhez objektumosztályokat és jelentést kell rendelni, és ezeket az adatokat kell megfeleltetni a szemantikus térkép objektumaival, illetve a hozzájuk tartozó objektumosztályokkal és szemantikus tartalommal.

7. A geoinformatikai referenciamodellen alapuló lokalizáció általános modellje

A különböző geoinformatikai adatok ugyanazon valós környezet eltérő reprezentációi. Ezek referenciaadatként akkor használhatók lokalizációra, ha a fedélzeti érzékelésből kinyerhető információ és a georeferált reprezentáció közötti megfeleltetés létrehozható.

Az ortofotó, a pontfelhő, a mesh-háló, a vektoros térkép és a szemantikus térkép látszólag nagyon eltérő geoadat. Valójában azonban mindegyik ugyanannak a georeferált környezetnek egy adott reprezentációja, de a valós környezet más-más tulajdonságait tartalmazza. Az ortofotó elsősorban radiometriai és texturális, valamint síkbeli geometriai információt tartalmaz. A 3D modell elsősorban térbeli geometriát, esetleg textúrát tartalmaz. A vektoros térkép tartalma absztrakció útján létrejött geometria és topológia, míg a szemantikus térkép az objektumok jelentését és térbeli kapcsolatait is tartalmazza.

[31] Natalia Trukhina, Vadim Vashkelis: SASGeo: *Stability-Aware Semantic Map Localization for GNSS-Denied UAVs – A Framework and Synthetic Proof of Concept,* 2026, URL: https://arxiv.org/html/2607.07737v1

A vizuális lokalizáció általános problémája tehát nem a képegyeztetés (image matching), hanem a megfigyelt és a referenciaként tárolt környezeti információ közötti megfeleltetés.

Az egyes geoinformatikai referenciaadatok (ortofotó, 3D modell, vektoros és szemantikus térkép) nem kell, hogy egymást kizáró alternatívák legyenek, hanem a referenciaadatbázis egy-egy rétegét képezhetik. Egy referencia-adatbázis tartalmazhat képi, 3D geometriai, vektoros és szemantikai adatokat is. (Ez a gyakorlatban azt jelenti, hogy egy épülethez tartozhat például az ortofotón megjelenő képe / textúra/, pontfelhő vagy mesh, az alaprajzát ábrázoló poligon, szemantikai osztály, valamint további attribútumok). A fedélzeti lokalizációs rendszer pedig az aktuális körülményektől függően használhatja a legjobban használható reprezentációt, vagy azok kombinációit. Ez a többrétegű geoadat-megközellítés funkcionálisan lényegében teljesen analóg a szenzorfúzió szerepével, így itt már referenciaadat-fúzióról beszélhetünk.

8. Összegzés és értékelés

A kizárólagosan a GNSS-en alapuló navigáció napjainkban már nem tekinthető kellően robusztus megoldásnak. A katonai alkalmazásnál figyelembe kell venni, hogy a GNSS szolgálttás időszakosan szünetelhet, vagy teljesen elérhetetlenné válik. A cél nem feltétlenül a GNSS használatának mellőzése, hanem olyan megoldások alkalmazása, ami biztosítja, hogy ezzel együtt ne szűnjön meg a navigációs képesség. Vagyis, ahol rendelkezésre áll és megbízhatóan működik a GNSS, ott továbbra is jól használható abszolút helymeghatározásra.

Nincs univerzális GNSS-t helyettesítő technológia. Ahogyan a cikkben is látható, ezeknek a navigációs technológiáknak is vannak műszaki korlátjai. Az inerciális navigációs rendszernek driftje van, a vizuális navigációt korlátozza a környezet megfigyelhetősége és az információtartalma. A térképalapú módszerek megfelelő minőségű és aktualitású, előzetes felmérésen alapuló referenciaadatot igényelnek, a radar és LiDAR alkalmazását korlátozhatja a nagyobb tömeg, a magas energiaigény és költségek, a rádióalapú rendszerek erősen függenek a rádiós infrastruktúrától és ugyancsak zavarhatóak. A mágneses és gravitációs módszerek pedig szintén rendelkeznek korlátokkal, mint pl. a szenzorérzékenység kérdése, a referenciaadatok felbontása és minősége, valamint a fizikai jellemzők térbeli változékonysága.

A robusztus navigációs rendszerek legígéretesebb megvalósítására a legígéretesebb megoldásnak a szenzorfúzió tűnik. Nem egymást helyettesítő, hanem egymást kisegítő technológiákra van szükség. A szenzorfúzió nem csupán redundanciát jelent, hanem egymást kiegészítő információforrások használatát a navigációhoz, ahol az egyes technológiák hibajellemzői kompenzálják egymást.

A szenzorfúzió terén a jövőt az adaptív navigációs rendszerek megjelenése jelentheti. Nem minden vesz részt azonos súllyal a navigációs feladatok megoldásában, hanem a rendszer a szenzorokból kinyerhető információ minősége és megbízható-

sága alapján változtathatja a források súlyát. Jó GNSS jeleknél a GNSS és az inerciális rendszer dominálhat. Míg a GNSS jelek zavarása esetén az inerciális navigációs rendszer mellé a látáson alapuló rendszerek járulnak hozzá a navigációhoz. Rossz látási viszonyoknál viszont az inerciális rendszer mellé a vizuális rendszer helyét a radar vagy a LiDAR veheti át.

Hosszabb távon az ilyen adaptív navigációs rendszerek már az autonóm eszközök felé vezetnek. Az autonóm pilóta nélküli jármű nem csak navigálni fog, hanem képesnek kell lennie felismerni, hogy a fedélzeten rendelkezésre álló többféle szenzor közül melyek biztosítanak megbízható navigációs adatot.

A különféle GNSS-független és abszolút lokalizáción alapuló eljárások egy közös geoinformatikai keretben értelmezhetők. A fedélzeti szenzor valamilyen helyfüggő jellemzőt érzékel, a referencia-adatbázis pedig ennek vagy egy ezzel összefüggésben hozható más jellemzőnek a georeferált reprezentációját tartalmazza. A lokalizáció általánosságban ezeknek a jellemzőknek a megfeleltetését jelenti. Ez a közös geoinformatikai keret egyúttal lehetővé teszi a többféle reprezentáción alapuló referenciaadat fúzióját.

Összegezve: a jövő az UAV-ok navigációja területén várhatóan a többféle fizikai és információs elven működő navigációs eljárások intelligens fúziója, amelyeknél kiemelt szerepet fognak kapni a geoinformatikai referenciaadatokon alapuló eljárások.

Források:

1. Clement A. Ogaja: *Introduction to GNSS Geodesy – Foundations of Precise Positioning Using Global Navigation Setellite Systems,* Springer, 2022, ISBN 978-3-030-91820-0
2. Ivan G. Petrovski: *GPS, GLONASS. Galileo, and BeiDou for Mobile Devices – From Instant to Precise Positioning,* Cambridge University Press, 2014, ISBN 978-1-107-03584-3
3. Karl Kraus: *Photogrammetry – Geometry from Images and laser Scans,* Walker de Gruyter, Berlin – New York, 2004, SBN 978-3-11-019007-6
4. Rafael C. Gonzalez: *Digital Image Processing Using MATLAB,* Gatesmark Publishing, 2009, ISBM 978-0-9820854-0-0
5. Vasileos Argyriou, Jesús Martínez del Rincón, Barbara Villarini, Alexis Roche: Image, Video & 3D Data Registration – Medical, Satellite and Video Processing Applications with Quality Metrics, John Wiley & Sons, 2015, ISBN 978-1-118-70246-8

Ladányi Éva[1]**:**

Űrdivat: a védelmi-ipari paradigmától a bioadaptív textíliákig

Absztrakt:

Az űrruha a világűr kutatásának egyik legösszetettebb technológiai rendszere: évtizedeken át kizárólag katonai-ipari vállalatok fejlesztették, ahol a funkcionalitás, a túlélés és a szabványosítás volt az elsődleges szempont. A pilóták és űrhajósok ruházata minden országban védelmi-ipari háttérrel készült, a NASA-tól a Roszkoszmoszon át a kínai, japán és indiai űrügynökségekig.

Ezzel párhuzamosan a sci-fi filmek világa – a Star Warstól az Orion űrhajó fantasztikus kalandjain át Lem Solarisáig – a divat és a jelmeztervezés esztétikai terét formálta, létrehozva a klasszikus értelemben vett, de a valós technológiától ekkor még teljesen elkülönült „űrdivat" kulturális igényét. A két világ között sokáig nem volt átjárás.

A 2020-as években azonban fordulópont következett: a divatipar először lépett be a valós űrtechnológiába, amikor az Axiom Space a Prada szakértelmét is bevonta az Artemis-program új űrruhájának fejlesztésébe. Ezzel megnyílt az út a high-tech textíliák, a varrástechnológiai innovációk és a kulturális-esztétikai szemlélet fúziója előtt. A bioalapú anyagok – így a különböző selyemstruktúrák, algatextilek, baktériumcellulózok és pókfonal-származékok – megjelenése új lehetőséget teremt a fenntartható, adaptív, heterogén összetételű űrruházat számára.

A cikk áttekinti az űrruhák történeti fejlődését, a jelenlegi nemzetközi technológiai helyzetet, a divatipar belépésének okait, valamint a bioanyagok integrációs lehetőségeit a jövő hibrid űrtextiljeiben, különös tekintettel a micéliumalapú kompozitok funkcionális szerepére.

Kulcsszavak: űrdivat, extravehikuláris mobilitási egység (EMU), interdiszciplináris textiltechnológia, bioadaptív anyagok, micéliumkompozitok, funkcionális ergonómia.

[1] HM EI Zrt. Űrmunkacsoportjának társelnöke, a Pécsi Tudományegyetem címzetes egyetemi docense.

Abstract:

The spacesuit is one of the most complex technological systems used in space exploration. For decades, it was developed exclusively by military-industrial companies, where functionality, survival, and standardization were the primary considerations. In every country, the protective garments of pilots and astronauts emerged from a defense-industrial background, from NASA and Roscosmos to the Chinese, Japanese, and Indian space agencies.

In parallel, the world of science-fiction film-from Star Wars and Raumpatrouille – Die phantastischen Abenteuer des Raumschiffes Orion to Lem's Solaris-shaped the aesthetic domain of fashion and costume design, creating a cultural demand for "space fashion" in the classical sense, although it remained entirely separate from real-world technology at the time. For a long period, there was little exchange between these two domains.

The 2020s, however, marked a turning point: the fashion industry entered operational space technology for the first time when Axiom Space also engaged Prada's expertise in developing the new spacesuit for the Artemis program. This collaboration opened the way for the convergence of high-tech textiles, garment-construction innovations, and cultural-aesthetic perspectives. The emergence of bio-based materials-including various silk structures, algal textiles, bacterial cellulose, and spider-silk derivatives-creates new opportunities for sustainable, adaptive, and compositionally heterogeneous space apparel.

This article reviews the historical development of spacesuits, the current international technological landscape, the factors behind the fashion industry's entry into the field, and the potential integration of biomaterials into future hybrid space textiles, with particular emphasis on the functional role of mycelium-based composites.

Keywords: space fashion, extravehicular mobility unit (EMU), interdisciplinary textile technology, bioadaptive materials, mycelium composites, functional ergonomics.

Bevezetés

Az emberi jelenlét fenntartása az alacsony Föld körüli pályán (LEO), valamint a mélyűr-kutatási missziók során – különös tekintettel a visszatérésre a Hold felszínére és a tervezett Mars-utazásokra – olyan technológiai architektúrákat igényel, amelyek képesek az emberi szervezet és a fiziológiai integritás teljes körű megóvására és izolációjára a világűr extrém, életellenes fizikai környezetével szemben. Ezen rendszerek csomópontjában az antropomorf életfenntartó rendszerek, vagyis az űrruhák állnak. Az űrruha-tervezés hagyományos paradigmája a 20. század közepétől fogva a merev mérnöki funkcionalitás és a katonai-ipari szabványosítás

koordinátarendszerében mozgott. Ebben a struktúrában az elsődleges prioritást a nyomástartás, a hőszabályozás és a sugárzásvédelem jelentette, miközben a viselő biomechanikai komfortja, a pszichológiai jóllétet támogató esztétika és az anyagfenntarthatóság marginális tényezők maradtak.

Ezzel párhuzamosan a huszadik századi vizuális kultúra és a spekulatív fikció létrehozta a maga autonóm „űrdivat" kánonját, amely a technológiai realitásoktól elszakadva, tisztán szemiotikai és esztétikai alapon reflektált a jövő űrutazóira. Ez a dichotómia – a zárt, hierarchikusan szervezett védelmi-ipari technológiai modell és a nyitottabb, expresszív, esztétikai fókuszú dizájn között – évtizedekig nehezen átjárhatónak tűnt.

A 2020-as évek közepére azonban a magánűrhajózás térnyerése, a hosszú távú missziók (long-duration spaceflight) felerősödése, valamint a globális textildizájn anyagtudományi áttörései együttesen új értelmezési keretet hoztak létre. Az űrdivat fogalma ennek nyomán nem pusztán fikciós jelmeztervezést vagy felszíni stylingot jelöl, hanem egy hibrid, konvergens kutatási és tervezési területként írható le, amely a csúcstechnológiás mérnöki tervezést ötvözi az anyagtudománnyal, a fejlett szabástechnológiával és a bioadaptív megközelítésekkel.

Jelen tanulmány célja ezen konvergenciafolyamat strukturális elemzése. Első lépésben áttekintjük a domináns állami űrügynökségek historikus védelmi-ipari modelljeit, majd bemutatjuk a divatipar intézményesült belépését a reál-űrtechnológiába. Végezetül a tanulmány a jövőbe mutató, heterogén és fenntartható anyaginnovációkat vizsgálja, különös tekintettel a zárt ökológiai rendszerekben is tenyészthető, bioalapú textilalternatívákra (alga-, selyem- és baktérium-alapú rendszerek), kiemelten elemezve a micéliumkompozitok funkcionális integrációjának lehetőségeit az űrruházat jövőbeli architektúrájában.

I. fejezet:
Az űrruhafejlesztés védelmi-ipari paradigmája és históriku s struktúrája

Az űrruha-fejlesztés (hivatalos nómenklatúrával: Extravehicular Mobility Unit – EMU, illetve Anthropomorphic Space Suit System) történetileg és strukturálisan a globális védelmi-ipari komplexumok része. Nem pusztán ruházati elemet, hanem egy antropomorf, autonóm életfenntartó rendszert (Life Support System) testesít meg, amelynek primer funkciója a fiziológiai homeosztázis fenntartása extrém barometrikus, termikus és sugárzási környezetben. A fejlesztési trajektóriákat a kezdetektől fogva a katonai-ipari szabványosítás, a hibatűrő tervezés (fault-tolerant design) és a szigorú állami-védelmi finanszírozás határozta meg.

A szkafanderek és a nagy magassági repülőruházat gyártása univerzálisan a hadiipari infrastruktúrához kapcsolódott. Ez a nemzeti védelmi logika képezte az alapját a nagyhatalmi fejlesztéseknek, de ugyanezen elv alapján működnek a regionális védelmi szereplők is: Magyarországon például a HM EI Zrt. és a hazai védelmi-ipari szabászati

és textilgyártó kapacitások képviselik azt a specifikus technológiai és szabványosítási tudásbázist, amely a katonai célú védőruházatoktól a magas hozzáadott értékű, extrém környezeti igénybevételre tervezett funkcionális textíliák felé mutat.

1. Az amerikai modell: Az ILC Dover és a NASA fúziója

Az Egyesült Államok űrruha-fejlesztési programjának egyik legnagyobb technológiai paradoxona, hogy a merev katonai beszállítói láncok helyett egy vágástechnológiai és alakformálási tapasztalattal rendelkező konvencionális gyártó, az International Latex Corporation (ILC Dover) vált a domináns szereplővé az Apollo-program során.

A klasszikus nehézipari és repülőgépgyártó konglomerátumok korai prototípusai merev, ízületi mobilitást gátló páncélzatok voltak. Ezzel szemben az ILC Dover mérnökei felismerték, hogy a gáznyomás alatt lévő rétegek rugalmasságát speciális neoprén konform rétegekkel, valamint fém csuklópontok helyett bonyolult, textíliába integrált kábel- és csigarendszerekkel (cord-and-pulley systems) lehet biztosítani. Az A7L típusú Hold-szkafander 25 védőanyag-rétegből álló kompozit textilszerkezet volt, amelyhez a belső folyadékhűtéses ruha (Liquid Cooling Garment – LCG), a mikrometeorit- és hővédelmi burkolat, valamint többek között aluminizált Mylar- és Nomex-rétegek kapcsolódtak. Az amerikai megközelítés a mai napig a moduláris, többrétegű, lágytextil-orientált struktúrára épül, amely magas taktilis visszacsatolást és ízületi mobilitást biztosít, ám rendkívül kifinomult, egyedi varrástechnológiát igényel.

2. A szovjet-orosz iskola: Az NPP Zvezda és a monolitikus tervezés

A szovjet, majd orosz fejlesztési filozófia, amelyet az NPP Zvezda kutatóintézet testesít meg, több ponton eltér az amerikai modularitástól. Az orosz tervezési doktrína a monolitikus integrációra és a mechanikai robusztusságra helyezi a hangsúlyt. Ennek egyik legismertebb példája az Orlan-széria, amely az 1970-es évektől a mai napig a Nemzetközi Űrállomás (ISS) orosz szegmensének standard űrséta-ruhája.

Az Orlan nem különálló nadrág- és felsőrészből áll, hanem egy félig merev, egybeöntött alumínium torzó- és hátizsákrendszerből (semi-rigid backpack entry). Az űrhajós nem felveszi a ruhát, hanem a hátul elhelyezkedő, ajtóként funkcionáló életfenntartó rendszeren keresztül lép be a szkafanderbe. Ez a konstrukció minimalizálja a kritikus tömítési pontok és gázszivárgási zónák számát, kiküszöböli a külső segítség szükségességét az öltözésnél, és drasztikusan csökkenti a fel- és levétel időszükségletét. Az orosz megközelítés a standardizált méretezésre törekszik: a végtagok belső zsinórrendszerekkel állíthatók, így egyetlen ruhatípus képes lefedni az űrhajós populáció jelentős részét, háttérbe szorítva az antropometrikus testreszabást a rendszerszintű megbízhatóság javára.

3. Az ázsiai szereplők: Kína, Japán és India technológiai trajektóriái

A 21. századi űrprogramokban az ázsiai űrügynökségek saját védelmi-ipari és kutatás-fejlesztési képességeikre támaszkodva alakítottak ki egyre önállóbb technológiai rendszereket:

- **Kína (CNSA):** A Feitian (Fejtien) űrruha-generáció az orosz Orlan-M konstrukciójától erősen befolyásolt, félig merev, hátulról felvehető architektúrát alkalmaz; a korai kínai programban importált Orlan-M ruhák is szerepet kaptak. A Tiangong űrállomás programjához fejlesztett későbbi változatok ugyanakkor már önálló kínai anyag-, kommunikációs, telemetriai és vezérlőrendszereket integrálnak.
- **Japán (JAXA):** Japán hagyományosan a NASA hardveres és műveleti ökoszisztémájába integrálódik, és a JAXA kutatás-fejlesztési programjai többek között fejlett űrruhaanyagokkal, ember-gép interfészekkel és az extravehikuláris tevékenységet támogató robotikai megoldásokkal foglalkoznak.
- **India (ISRO):** A Gaganyaan-misszióhoz India saját fejlesztésű intravehikuláris (IVA) nyomásruhát készít a Vikram Sarabhai Space Centre vezetésével. A könnyű, többrétegű ruha normál körülmények között kabinnyomáson működik, vészhelyzetben pedig nyomás- és oxigénellátást biztosít; fejlesztése az importfüggőség csökkentését és a hazai gyártási képességek kiépítését szolgálja.

II. fejezet:
A sci-fi esztétika és a valós technológia konvergenciája:
Az űrdivat mint legitim diszciplína megjelenése

1. A fikciós vizuális kultúra hatása az antropomorf reprezentációra

Az „űrdivat” (space fashion) fogalma történetileg a spekulatív fikció és a filmművészet szemiotikai terében izoláltan fejlődött, éles dichotómiát képezve a fent bemutatott merev mérnöki valósággal. A 20. század közepének filmművészeti produkciói – kiemelten az európai és amerikai sci-fi sorozatok, mint a német *Raumpatrouille – Die phantastischen Abenteuer des Raumschiffes Orion* (1966), vagy a későbbi hollywoodi produkciók – nem pusztán funkcionális jelmezeket, hanem egy határozott, progresszív társadalmi és nemi esztétikát vizualizáltak.

Az Orion űrhajó karakterei, mint Tamara Jagellovsk (Eva Pflug alakításában), olyan strukturált, testvonalat követő, geometrikusan tiszta és maszkulin elemeket feminin eleganciával ötvöző sziluetteket viseltek, amelyek a korabeli nők számára a technológiai egyenjogúság és a futurisztikus vonzerő szimbólumává váltak.

Ez a vizuális kánon szorosan korrelált a kor avantgárd divattervezőinek (André Courrèges, Pierre Cardin, Paco Rabanne) Space Age kollekcióival.



1. ábra: Paco Rabanne (1966)[2].
Fotó: Rue des Archives (©Rue des Archives/RDA / Cordon)

Ezek a darabok hűen tükrözik az ő *„Manifesto: 12 Unwearable Dresses in Contemporary Materials”* (12 hordhatatlan ruha kortárs anyagokból) című kollekcióját. Kisebb alumínium- vagy fémlemezekből áll, amelyeket fémgyűrűkkel kapcsolt össze. Ez nem klasszikus textil, hanem strukturált páncélzat – azaz a védelmi szkafanderek divatmegfelelője. Audrey Hepburn is Paco Rabanne-ruhát viselt a Stanley Donen rendezte Ketten az úton (1967) című filmben. A tervező ihlette Jane Fonda ruhatárát a Barbarellában, abban a sci-fi filmben, amelyben a színésznő egy űrkalandort alakított.



2. ábra: Pierre Cardin (Ikonikus buborék-ruha és sisak).
Fotó: Getty Images

[2] https://elpais.com/smoda/el-universo-de-paco-rabanne-de-las-curvas-de-barbarella-al-perfume-mas-vendido-del-mundo.html

Pierre Cardin munkáiban gyakran jelentek meg geometrikus formák, különösen körök és gömbszerű struktúrák, amelyek a futurisztikus divat vizuális nyelvének meghatározó elemeivé váltak. A képen látható buborékformák és sisakszerű plexielemek a Space Age esztétika játékos, technológiai asszociációkat keltő megközelítését szemléltetik.



3. ábra: André Courrèges (1964/1965 – „Moon Girl" esztétika).
Fotó: Peter Knapp, Courrèges collection – paru dans le journal ELLE de septembre 1964, Elle France, [3]

André Courrèges munkája, amely meghatározta a hatvanas évek „Moon Girl" (Holdlány) stílusát: a jellegzetes, fehér gyapjú- vagy gabardin-csuklya (ami a szkafander sisakjának absztrakciója), a prémes szegély, a tiszta fehér minimalizmus és a hangsúlyos, geometrikus smink.



4. ábra: A Courrèges-ház 1993-as kiotói (Kyoto) bemutatójának sziluettje.
Fotó: Kurita Kaku/Gamma-Rapho via Getty Images, Courrèges-divatbemutató, Kiotó, 1993. április 27.

[3] 1964. szeptember: Zürcher Hochschule der Künste / Museum für Gestaltung Zürich, Grafiksammlung, PH C KNAP 3.

A planetáris gyűrűstruktúrát idéző szoknyaforma és a telekommunikációs sisak-absztrakció a retrofuturizmus 1990-es évekbeli újjáéledésének egyik példájaként értelmezhető.

Azonban amíg a divat és a filmvászon a textíliák vizuális dinamikájára és a karakteres antropomorf reprezentációra fókuszált, a valós űrtechnológia funkcionális, robusztus és esztétikailag semleges maradt. A két terület között évtizedekig hiányzott a strukturális transzfermechanizmus.

2. A Prada és az Axiom Space együttműködése: Paradigmaváltás a funkcionális dizájnban

Ez az évtizedes izoláció tört meg a 2020-as évek közepén, jelezve, hogy az űrdivat elhagyta a fikció és a spekulatív kifutók világát, és integrálódott a repülőmérnöki gyakorlatba. A fordulópontot az Axiom Space és az olasz Prada luxusdivatház közötti intézményesített partnerség jelentette a NASA Artemis III Hold-missziójához készülő Axiom Extravehicular Mobility Unit (AxEMU) fejlesztésében.

A Prada bevonása nem pusztán esztétikai felszínformálásként vagy márkaépítésként értelmezhető, hanem anyagtudományi és szabástechnológiai transzferként is. A luxusiparban felhalmozott szövési, szabási és illesztési kompetenciák hozzájárulhatnak a ruha külső védőrétegének, valamint a belső, közvetlenül a bőrrel érintkező komfort- és hűtőrétegek optimalizálásához. A dizájnerek és mérnökök együttműködése olyan komplex textilmegoldások fejlesztését támogathatja, amelyek egyszerre javíthatják a hőtágulás-menedzsmentet, a kritikus mozgástartományokat és az antropometrikus illeszkedést. Ez a kollaboráció azt jelzi, hogy az esztétika, az ergonómia és a csúcstechnológiás textiltervezés az extrém környezeti életfenntartásban egymást erősítő szempontokká válhatnak. Az űrdivat ezáltal a spekulatív jelmeztervezés mellett egyre inkább a funkcionális bioergonómia és a fejlett textiltervezés interdiszciplináris területeként értelmezhető.

III. fejezet: Heterogén bioanyagok és a jövő adaptív űrtextíliái: A zárt ökológiai rendszerek anyaginnovációi

A mélyűr-kutatás és a planetáris felszíni missziók logisztikai korlátai, különösen a hasznos teherszállítási költségek és a zárt rendszerek erőforrás-limitációi, indokolttá tehetik az anyagtudományi fókusz részleges eltolódását a petrolkémiai szintetikumoktól a regeneratív, bioalapú és hibrid textilrendszerek felé. Az űrdivat és a funkcionális dizájn konvergenciája ebben az összefüggésben olyan kutatási irányként értelmezhető, amely a statikus mesterséges szálak mellett zárt ökológiai életfenntartó rendszerekben (Controlled Ecological Life Support Systems – CELSS) előállítható vagy reciklálható heterogén, bioadaptív kompozitok vizsgálatát is előtérbe helyezi.

1. Strukturális fehérjék és algabázisú polimerek az űrruházatban

A hibrid biotextil-architektúra alapját olyan természetes és géntechnológiával módosított polimerek képezhetik, amelyek kedvező mechanikai tulajdonságokkal és potenciális biológiai funkcionalitással rendelkeznek:

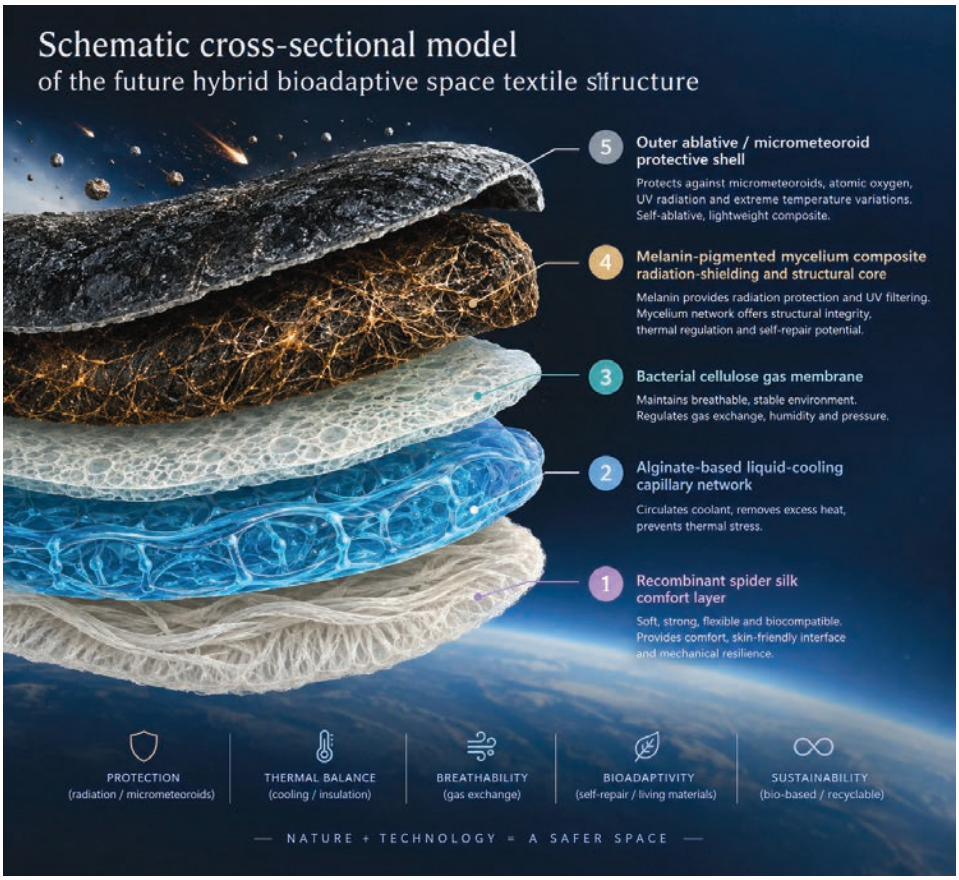
- **Fejlett selyemstruktúrák és pókfonál-származékok:** A hernyóselyem (*Bombyx mori*) fibroinfehérjéje, valamint a rekombináns DNS-technológiával előállított mesterséges pókfonál (spidroin) kedvező szakítószilárdság-tömeg aránnyal rendelkezhet. Az űrruházat belső rétegeiben e fehérjealapú anyagok termoregulációs, biokompatibilitási és mechanikai tulajdonságaik alapján vizsgálhatók, de alkalmazásukhoz az űrkörnyezeti terhelések melletti tartósság további validációja szükséges.
- **Algatextilek (alginate-based fibers):** A tengeri barna- és vörösalgákból kivont nátrium-alginátból nedves szálképzéssel előállított filamentumok megfelelő felületkezeléssel lángálló és funkcionális textilrendszerek alapanyagaként vizsgálhatók. Nedvességkezelési és ionmegkötő tulajdonságaik miatt a folyadékhűtéses alsóruházat következő generációjához kapcsolódó kutatásokban is relevánsak lehetnek, de ilyen alkalmazásuk teljesítményét űrkörnyezeti körülmények között még igazolni kell.
- **Baktériumcellulóz (microbial cellulose):** A *Komagataeibacter xylinus* baktériumtörzsek által glükózfermentáció során termelt extracelluláris cellulóznanoszálak sűrű, háromdimenziós hálót képeznek. E nanostrukturált cellulóz porozitása, nedvességkezelése és kompozitálhatósága alapján köztes membránrétegek fejlesztésében vizsgálható, de szelektív gázáteresztő és folyadékzáró űrruházati alkalmazása további célzott tesztelést igényel.

2. A micéliumalapú kompozitok funkcionális integrációja és in situ növesztése

Míg a selyem és az algatextilek elsősorban a flexibilis, bőrrel érintkező rétegek funkcionalitásáért felelnek, a gombafonalakból álló hálózat, a micélium (mycelium), a szilárdabb, kompozit struktúrák terén nyit új dimenziót. A micélium-technológia nem kizárólagos, hanem az űrruha-architektúra azon komponenseiben jelenthet áttörést, ahol a vibrációvédelem, a sugárzás-pufferelés és a strukturális tartás együttes jelenléte szükséges (például a torzó-elemeknél, csizmatalpaknál vagy külső védőpajzsoknál).

A micéliumalapú anyagok előnye a heterotróf növekedési mechanizmusukban rejlik: mezőgazdasági vagy akár asztronautikai hulladékáramokon (lignocellulóz hordozókon) minimális energia- és vízigénnyel növeszthetők ki a kívánt antropometrikus formára. Anyagtudományi szempontból a kitinből és glükánból álló sejtfalszerkezet természetes módon csillapítja a mikrovibrációkat, és alacsony sűrűsége ellenére magas nyomószilárdsággal bír.

Különösen fontos kutatási irány a mélyűri alkalmazások szempontjából a melanin-pigmentált micéliumok sugárzásvédelmi potenciálja. Egyes radiotróf gombafajok, például a Cladosporium sphaerospermum, kísérleti eredmények alapján képesek lehetnek a sugárzás egy részének elnyelésére, illetve a melanin szerepet játszhat a sugárzási energiával szembeni biológiai válaszfolyamatokban. Ez arra utal, hogy a micéliumkompozitok külső rétegekbe történő integrálása hosszabb távon passzív sugárzáscsökkentő elemként vizsgálható, bár gyakorlati űrruházati alkalmazásuk további anyagtudományi, biológiai és mérnöki validációt igényel.



5. ábra: Sematikus keresztmetszeti modell a jövő hibrid bioadaptív űrtextil-rétegrendjéről. Fotó: Saját koncepcionális modell és saját szerkesztés; a hibrid bioadaptív űrtextil rétegrendjének elméleti felépítése a szerző micéliumalapú anyagkutatási koncepcióján alapul.

Alulról fölfelé: 1. Rekombináns pókfonál komfortréteg; 2. Alginát-alapú folyadékhűtéses kapilláris hálózat; 3. Baktériumcellulóz gázmembrán; 4. Melanin-pigmentált micélium-kompozit sugárzásvédelmi és strukturális mag; 5. Külső ablatív/mikrometeorit védőburok.

3. A micéliumalapú textilplatformok tudományos konvergenciája: a „fungal cloth” és a mélyűri kompozitok párhuzamai

A 2026-os Science Advances publikáció fontos mérföldkő a bioalapú textiltechnológiák fejlődésében, mivel bemutatta, hogy a gombafonalakból álló hifahálózat programozható anyagtudományi platformként vizsgálható. A Cordyceps-alapú „fungal cloth” létrehozása során a kutatók a gombát formába növesztették, majd glicerin-alapú stabilizálással bőrszerű mechanikai tulajdonságú anyagot hoztak létre. A demonstrált környezeti válaszok és javítási lehetőségek ígéretesek, de a hosszú távú működés, a reprodukálhatóság és az űrkörnyezeti alkalmazhatóság további vizsgálatot igényel.

Ez a viselkedés különösen releváns lehet a mélyűri alkalmazások szempontjából, ahol a szkafander külső rétegeit folyamatos mikrometeoritterhelés, hőingadozás és mechanikai kopás éri. A Cordyceps-textil földi demonstrációja arra utal, hogy a micéliumhálózat nem csupán biológiai struktúraként, hanem környezeti ingerekre reagáló funkcionális kompozitként is értelmezhető. A mélyűri alkalmazhatóság ugyanakkor további vizsgálatokat igényel, különösen vákuum-, hőciklus-, sugárzási és sterilizációs körülmények között.

A Cordyceps-textil ezért hasznos proof-of-conceptként értelmezhető arra, hogy a micélium, mint anyagfenntartható és mérnöki szempontból programozható platform vizsgálható, amely megfelelő feldolgozás és validáció mellett adaptív funkciók hordozására is alkalmassá válhat. Ezek a tulajdonságok elméletileg olyan irányok felé mutatnak, amelyek a mélyűri szkafanderekben is relevánsak lehetnek.

A két kutatási irány közötti különbség elsősorban az alkalmazási környezetben és a validációs követelményekben ragadható meg: míg a fungal cloth földi divatipari és anyagtudományi demonstrációként kínál új lehetőségeket, addig a melanin-micéliumkompozitok mélyűri sugárzási, vibrációs és mechanikai terhelések szempontjából vizsgálhatók. A közös nevező a micélium, mint biológiai eredetű, mérnökileg alakítható anyagplatform, amely hosszabb távon földi és űrbeli alkalmazások között is kapcsolatot teremthet.

4. Cordyceps „fungal cloth” és melaninmicélium űrtextil: két bioalapú platform konvergenciája

A micéliumalapú textiltechnológiák két különböző, de egymást kiegészítő irányban fejlődnek: (1) a fenntartható divatipar számára fejlesztett Cordyceps-alapú „fungal cloth”, (2) a mélyűri környezetekhez tervezett melanin-pigmentált micéliumkompozitok.

Az alábbi összehasonlítás bemutatja a két rendszer főbb különbségeit és átfedéseit:

Tulajdonság	Cordyceps „Fungal Cloth”	Melanin-micélium űrtextil
Biológiai alap	Cordyceps hyphae	Radiotróf, melanin-pigmentált micélium
Fő cél	Fenntartható, önjavító divattextil	Sugárzásvédelem, strukturális tartás
Mechanikai tulajdonság	Bőrszerű, hajlítható	Kompozit jellegű, nagy nyomószilárdság
Önjavítás	Párás környezetben aktiválódik	Integrálható, de a sugárzásvédelem dominál
Sugárzásvédelem	Alacsony	Magas (melanin radiotropikus tulajdonságai miatt)
Biodegradáció	~1 hónap alatt lebomlik	Irányított biodegradáció, zárt rendszerekben reciklálható
Energiaigény	Minimális (heterotróf növesztés)	Minimális (heterotróf növesztés)
Alkalmazási környezet	Földi divatipar	Mélyűri szkafanderek és védőpajzsok

1. táblázat: a két rendszer összehasonlítása

5. K+F lehetőségek, kettős felhasználás (dual-use) és a meglévő gyártókapacitások átalakulása

A bioadaptív űrtextíliák és a high-tech funkcionális ruházat kutatás-fejlesztése nem szigetelődik el a globális és nemzeti ipari stratégiáktól; sokkal inkább a kettős felhasználású (dual-use) technológiák mintapéldája. Az extrém környezeti életfenntartásra kifejlesztett szövési, rétegzési és anyagtudományi áttörések közvetlenül csatornázhatók át a földi védelmi iparba, a speciális mentőerők felszereléseibe és a katonai egyéni védőeszközökbe (Personal Protective Equipment – PPE).

Ebben a kontextusban kiemelt jelentőséggel bír a meglévő védelmi-ipari és szabászati infrastruktúra transzformációja:

Hagyományos gyártókapacitások újragondolása: Az olyan komplex védelmi-ipari szereplők, mint a hazai HM EI Zrt., vagy más szabászati és textilipari gyártókapacitásokkal rendelkező intézmények, historikusan a katonai egyenruházat és védőfelszerelések szabványosított, robusztus gyártására rendezkedtek be. A high-tech funkcionális textíliák és bioalapú hibrid anyagok megjelenése nem teszi túlhaladottá ezeket a kapacitásokat, hanem új értéklánc-pozíciót kínál számukra.

Pontos szabástechnológia és precíziós illesztés: Az űrruházat – ahogy azt a Prada és az Axiom Space együttműködése is mintázza – extrém szabástechnológiai pontosságot és varrástechnológiai fegyelmet követel meg. A védelmi iparban meglévő minőségbiztosítási és konfekcionálási rendszerek alkothatják azt a fizikai hidat, amely a laboratóriumi szintű bioinnovációkat (pl. micélium-kompozit panelt vagy baktériumcellulóz membránt) képes ipari léptékű, integrált ruházati rendszerekké formálni.

Kettős felhasználású K+F szinergiák: A radiotróf gombakompozitok sugárzásvédelme, az algatextilek lángállósága és a pókfonál-származékok kopásállósága a katonai taktikai ruházatban (pl. CBRN védőruhák, repülőhajózó-öltözékek) éppúgy kritikus tényező, mint a Hold- vagy Mars-missziókban. A védelmi-ipari szereplők K+F hálózataiba történő integrálással a bioadaptív textiltechnológiák nemcsak a világűrben, hanem a Földön is közvetlen védelmi és nemzetgazdasági hozzáadott értéket teremtenek.

Elemző összegzés:

A Cordyceps-textil és a melanin-micéliumkompozitok közötti legfontosabb közös pont a micéliumhálózat programozhatósága: mindkét rendszer képes funkcionális mikroorganizmusokat integrálni (szín, UV-védelem, sugárzáselnyelés). A különbség a környezet extrémitásában rejlik: míg a Cordyceps-textil a földi körülmények között mutat adaptív viselkedést, addig a melanin-micéliumkompozitok a mélyűri sugárzás és mechanikai terhelés kihívásaira adnak választ.

Ez a párhuzam lehetővé teszi, hogy a micéliumalapú anyagok fejlődése két irányból konvergáljon: a földi fenntarthatósági innovációk és az űrkutatás anyagtudományi fejlesztései egymást erősítik, és közös technológiai platformot hoznak létre.

A III. fejezet konklúziójaként megállapítható, hogy a jövő űrdivatja és funkcionális ruházata egy olyan komplex biopolimer-ökoszisztéma, ahol nincs egyedüli „befutó" anyag. A jövő fenntartható űrruháját a selyem rugalmassága, az algák transzspirációs kontrollja, a baktériumcellulóz szűrési finomsága és a micélium strukturális, sugárzásvédelmi robusztussága együttesen, hibridizált formában fogja létrehozni.

IV. fejezet: Konklúzió és jövőkép – A kozmosz gardróbjának megnyitása

Az antropomorf életfenntartó rendszerek evolúciója elérte azt a kritikus csomópontot, ahol a technológiai túlélés és az esztétikai-ergonómiai önkifejezés már nem feltétlenül egymást kizáró tényezők. A 20. század erősen funkcionális, szabványosított védelmi-ipari paradigmája, amely az űrhajóst elsősorban egy zárt gépészeti rendszer biológiai komponenseként kezelte, fokozatosan kiegészül egy hibrid, konvergens megközelítéssel.

A divatipar – élén a Prada és az Axiom Space strukturális fúziójával – sikeresen igazolta, hogy a szabástechnológiai és textilmérnöki örökség közvetlenül képes javítani az űrhajósok mozgáskényelmét és fiziológiai biztonságát. Ez a lépés végleg legitimálta az „űrdivat" fogalmát, kiemelve azt a sci-fi filmek (mint a klasszikus Orion vagy a Solaris) tisztán fikciós és vágy-vezérelt jelmeztervezési közegéből.

A jövő mélyűri és planetáris misszióiban meghatározó kutatási irányt jelenthetnek a fenntartható, részben in situ előállítható vagy zárt rendszerekben újrahasznosítható bioalapú anyagok. Ahogy azt a jelen tanulmány anyagtudományi áttekintése

bemutatta, a jövő űrruházata várhatóan nem kizárólag statikus kőolaj-származékokra épül, hanem fokozatosan egy heterogén biopolimer-ökoszisztéma elemeit is integrálhatja.



6. ábra: Vizuális jövőkép: A kozmikus elegancia és az organikus textíliák fúziója.
Forrás: saját prompt alapján AI-generált illusztráció, saját szerkesztés.

Egy fénylő, csillagközi gázfelhőkből és biopolimer-szövetből álló, haute couture esztétikájú galaxis-szoknyás űrruha-koncepció (AI-generált illusztráció), amely a funkcionális dizájn és a kulturális önkifejezés végső szintézisét reprezentálja a jövő planetáris kifutóin.



7. ábra: A funkcionális űrdesign és a high-fashion szintézisének végső evolúciója.
Forrás: saját prompt alapján AI-generált illusztráció, saját szerkesztés.

A hagyományos, merev felsőtörzs (HUT) teljes dekonstrukciója: egy áramvonalas, strukturált, magabiztos eleganciát sugárzó futurisztikus egyenruha-architektúra (AI-generált illusztráció), amely az áttetsző, ergonomikus arcvédő maszkkal és az örvénylő planetáris gyűrűstruktúrákkal az emberközpontú, bioadaptív esztétika diadala a planetáris kifutóin.

Amikor a rekombináns selyem rugalmasságát, az algák transzspirációs kontrollját, a baktériumcellulóz szűrési finomságát és a melanin-pigmentált micélium-kompozitok sugárzásvédelmi potenciálját egyetlen hibrid textíliává integráljuk, az űrruházat fogalma a tisztán védelmi funkciótól az adaptív, emberközpontú és fenntartható rendszerek irányába mozdul el. Ebben a folyamatban a védelmi ipar és a meglévő szabászati-gyártási infrastruktúra (mint pl. a HM EI Zrt. vagy a nemzeti textilipari K+F központok) nélkülözhetetlen szerepet játszanak: ők biztosítják azt a technológiai fegyelmet és szabványosítási hátteret, amely a bioadaptív textilforradalmat a laboratóriumi asztalról eljuttatja a planetáris felszínek éles bevetéseiig.



8. ábra: Komparatív infografikai modell az intravehicularis (IVA) és extravehicularis (EVA) űrruházati rendszerek anyagtudományi rétegrendjéről és funkcionális felépítéséről. Forrás: saját koncepcionális modell és saját szerkesztés; az IVA és EVA űrruházati rendszerek anyagtudományi rétegrendjének összehasonlító felépítése a szerző bioadaptív űrtextil-koncepcióján alapul.

A modell részletesen bemutatja a belső kényelmi és szenzoros rétegek, valamint a külső kompozit védő- és hőszabályozó rendszerek integrációját.

V. fejezet:
Rendszerszintű tudományos szintézis és koncepcionális összefoglalás

A jelen tanulmányban feltárt technológiai, anyagtudományi és kultúrtörténeti folyamatok alapján az antropomorf életfenntartó rendszerek fejlődése három, részben egymásra épülő értelmezési szakasz mentén írható le. Az alábbi rendszerszintű szintézis a cikk főbb elméleti és anyagtudományi következtetéseit foglalja össze.

1. A paradigmaváltások evolúciós modellje

Az űrruházat története a tiszta gépészeti izolációtól a komplex biológiai integrációig terjed:

1. **Elsődleges védelmi-ipari paradigma (20. század közepe – 2010-es évek):** Az űrruha mint zárt, merev, mechanikus nyomástartó edény és életfenntartó gép. A fejlesztést a katonai szabványosítás, a hibatűrés és a merev mérnöki logika uralta (USA: ILC Dover, Szovjetunió/Oroszország: NPP Zvezda). Ebben a modellben a viselő biomechanikai kényelme és az anyagi fenntarthatóság másodlagos maradt.
2. **Interdiszciplináris fúziós paradigma (2020-as évek közepe):** A magánűrhajózás térnyerése és a high-fashion (Axiom Space – Prada együttműködés) belépése a reál űrtechnológiába. A szabástechnológia, az ergonómia és a fejlett szövési eljárások integrálása igazolta, hogy az esztétikai és ergonómiai megközelítés közvetlenül növeli az űrhajós mozgásszabadságát, hőtágulási kontrollját és fiziológiai biztonságát.
3. **Regeneratív bioadaptív kutatási irány (jövőbeli mélyűri missziók):** A szintetikus és petrolkémiai alapú textíliák mellett egyre nagyobb szerepet kaphatnak az in situ előállítható, zárt ökológiai életfenntartó rendszerekbe (CELSS) illeszthető biopolimerek és élő vagy részben élő kompozitok.

2. A hibrid biotextil architektúra anyagtudományi mátrixa

A mélyűri szkafanderek jövőbeli architektúrája nem egyetlen univerzális anyagból, hanem egy funkcionálisan degradált, többrétegű biopolimer-ökoszisztémából épül fel. Ennek összetevői és specifikus feladataik:

- **Belső ergonómiai és szerkezeti réteg (Rekombináns selyem és spidroin):** A rendkívüli szakítószilárdsággal és rugalmassággal rendelkező fehérjestruktúrák biztosítják a közvetlen bőrkomfortot, a mechanikai nyírásállóságot és a hőtágulás-menedzsmentet.
- **Kapilláris hőszabályozó réteg (nátrium-alginát / Algatextil):** A nedves szálképzéssel előállított algaszálak kiemelkedő transzspirációs és lángálló tulajdonságaik révén az aktív hűtőruházat (LCVG) alapját képezik, hatékonyan szabályozva a nedvesség- és hőháztartást.

- **Gáz- és mikroszűrési membrán (baktériumcellulóz):** A *Komagataeibacter xylinus* által szintetizált nanostrukturált cellulózhálózat szelektív gázáteresztő, de folyadékzáró gátként működik.
- **Strukturális, rezgéscsillapító és potenciális sugárzáscsökkentő mag (melanin-micélium kompozitok):** A heterotróf gombafonalak kitin-glükán sejtfala rezgéscsillapító és kompozit tartóelemként vizsgálható, míg a radiotróf gombafajok melanintartalma kísérleti eredmények alapján passzív sugárzáscsökkentő funkciók szempontjából is kutatható.

3. Összegző konklúzió

A tanulmány arra mutat rá, hogy az „űrdivat" fogalma fokozatosan túllép a spekulatív jelmeztervezés és a sci-fi esztétika hagyományos keretein, és egyre inkább a fejlett anyagtudomány, a bioergonómia és a repülőmérnöki tervezés interdiszciplináris metszéspontjaként értelmezhető.

A Földön demonstrált micéliumtechnológiák, például a Cordyceps-alapú adaptív textilek, valamint a mélyűri alkalmazások szempontjából vizsgált melaninpigmentált gombakompozitok párhuzamos fejlődése arra utal, hogy a fenntartható földi textilinnovációk és az extrém környezeti életfenntartó rendszerek fejlesztései között közös anyagtudományi és tervezési kapcsolódási pontok azonosíthatók.

E megközelítés alapján a jövő űrruházata a technológiai túlélés eszköze mellett az emberi jelenlét adaptív, részben bioalapú és fenntartható kiterjesztéseként is vizsgálható a világűrben.

Irodalomjegyzék

1. Averesch, N. J. H., Shunk, G. K., & Kern, C. (2022). Cultivation of the dematiaceous fungus *Cladosporium sphaerospermum* aboard the International Space Station and effects of ionizing radiation. *Frontiers in Microbiology, 13*, 877625. https://doi.org/10.3389/fmicb.2022.877625
2. Axiom Space. (2023, October 4). *Axiom Space, Prada join forces on tech, design for NASA's next-gen lunar spacesuits*. https://www.axiomspace.com/release/prada-axiom-suit
3. Axiom Space. (2024). *Axiom Space, Prada unveil spacesuit design for Moon return*. https://www.axiomspace.com/release/axiom-space-prada-unveil-spacesuit-design-for-moon-return
4. Brandić Lipińska, M., Dade-Robertson, M., Maurer, C., Morrow, R., Senesky, D. G., Theodoridou, M., Zhang, M., & Rothschild, L. J. (2021). *Growth as an alternative approach to the construction of extra-terrestrial habitats* [Conference paper]. NASA Technical Reports Server. https://ntrs.nasa.gov/citations/20210021668

5. De Micco, V., Amitrano, C., Mastroleo, F., Aronne, G., Battistelli, A., Carnero-Diaz, E., De Pascale, S., Detrell, G., Dussap, C.-G., Ganigué, R., Jakobsen, Ø. M., Poulet, L., Van Houdt, R., Verseux, C., Vlaeminck, S. E., Willaert, R., & Leys, N. (2023). Plant and microbial science and technology as cornerstones to bioregenerative life support systems in space. *npj Microgravity, 9*, 69. https://doi.org/10.1038/s41526-023-00317-9
6. García, B. (2023, February 3). El universo de Paco Rabanne: De las curvas de Barbarella al perfume más vendido del mundo. *El País: S Moda*. https://elpais.com/smoda/el-universo-de-paco-rabanne-de-las-curvas-de-barbarella-al-perfume-mas-vendido-del-mundo.html
7. Li, K., An, B., Zhang, J., Xun, D., Yuan, X., Song, Y., Wang, X., & Zhong, C. (2026). A programmable fungal platform for engineered living textiles. *Science Advances, 12*(30), eaed6937. https://doi.org/10.1126/sciadv.aed6937
8. National Aeronautics and Space Administration. (n.d.). *Spacesuits*. https://www.nasa.gov/humans-in-space/astronauts/spacesuits/
9. Provin, A. P., dos Reis, V. O., Hilesheim, S. E., Bianchet, R. T., Dutra, A. R. A., & Cubas, A. L. V. (2021). Use of bacterial cellulose in the textile industry and the wettability challenge-A review. *Cellulose, 28*(13), 8255-8274. https://doi.org/10.1007/s10570-021-04059-3
10. Ramezaniaghdam, M., Nahdi, N. D., & Reski, R. (2022). Recombinant spider silk: Promises and bottlenecks. *Frontiers in Bioengineering and Biotechnology, 10*, 835637. https://doi.org/10.3389/fbioe.2022.835637
11. Zheng, C., Sun, Y., Cui, Y., Yang, W., Lu, Z., Shen, S., Xia, Y., & Xiong, Z. (2021). Superhydrophobic and flame-retardant alginate fabrics prepared through a one-step dip-coating surface-treatment. *Cellulose, 28*(9), 5973-5984. https://doi.org/10.1007/s10570-021-03890-y

Kassai Károly:[1]

Kiberbiztonsági összetevők – a felelősség

Absztrakt:

A cikk az elektronikus információs rendszerek kiberbiztonságához szükséges szakmai felelősök kérdésével foglalkozik.

A vonatkozó jogszabályban meghatározott szereplők összehangolt tevékenysége, illetve az egész keretrendszer felügyelete és irányítása nélkül nem lehetséges egy szervezetnél hatékony kibervédelmi eljárásokról vagy kontrollokról beszélni.

A cikk megoldást keres az összeférhetetlen felelősségi körök azonosítására, ami gyakori bajok elkerülését segítheti és támogathatja a szervezetnél a szükséges kijelöléseket. E mellett egy három részre tagolt szerepkör modell kialakításával megtörténik a kiberbiztonsággal kapcsolatos felelősségek áttekintése és a szervezeti rendbe történő integrálás érdekében egy megoldási változat bemutatása.

A végzett vizsgálat támogatja a szervezeteknél szükséges felelősségi rend kialakítását, ezzel együtt a más szakterületekhez történő kapcsolódási pontok és a külső szolgáltatásokkal történő együttműködési vonalak azonosítását.

Kulcsszavak: elektronikus információs rendszer, kiberbiztonság, kontroll, felelősség, összeférhetetlenség.

Abstract:

This article examines the professional roles required to ensure the cybersecurity of electronic information systems. It argues that without coordinated action among the actors defined in the relevant legislation, and without proper oversight and governance of the entire framework, effective cybersecurity controls cannot be achieved within an organization.

The article aims to identify conflicting responsibility areas that may lead to operational issues, and to support organizations in assigning clear and appropriate roles. It also introduces a three-part role model that provides an overview of cybersecurity responsibilities and presents an option for integrating them into the organizational structure.

[1] Dr. Kassai Károly (Ph.D.), c. egyetemi docens, NKE

The analysis supports the development of a coherent responsibility framework within organizations, including the identification of connection points to other professional areas and cooperation lines with external service providers.

Keywords: electronic information system, cybersecurity, control, responsibility, conflict of interest.

Bevezetés:

Az elektronikus információs rendszerek védelme (a kiberbiztonság megvalósítása) komplex feladatkör. A szükséges mértékű védelmet a korábban gyakran egyediként elképzelt technikai megoldások mellett összehangolt fizikai biztonsági rendszabályokkal, adminisztratív intézkedésekkel együttesen kell alkalmazni.

A jogszabályi követelmények (esetleg szabványok alkalmazása) nem mechanikus végrehajtást igényel, hanem szervezeti és rendszerspecifikus értelmezést. Az általánosan megfogalmazott követelmények specifikálása, szervezeti és rendszerspecifikus jellemzők figyelembevétele lehet az a megoldás, melyet a szervezet vezetőjének jóváhagyásával kell kialakítani, fenntartani és folyamatosan fejleszteni.

A továbbiakban a magyar jogszabályi követelmények szerinti kiberbiztonsági kontroll rendszer kialakításának kiemelt kérdései következnek. A vizsgálat kiindulási kérdése, hogy a jogszabályokban megfogalmazott általános követelmények alapján kialakítható-e olyan, szervezeti szinten alkalmazható keretrendszer, amely elősegíti a kiberbiztonsági feladatok szervezeti folyamatokba és szervezeti kultúrába történő integrálását.

A vonatkozó rendelet (MK, 2024) az elektronikus információs rendszer biztonsági osztályának megfelelő (alap, jelentős, magas) jelöléssel ellátva 15 követelménycsoportra osztva 331 kötelezően alkalmazandó és 122 ajánlott védelmi rendszabályt (kontrollt) fogalmaz meg, melyek szervezeti, adminisztratív, technikai és fizikai követelményeket, felelősségi területeket és működési eljárásokat tartalmaznak.

Az alkalmazandó irányítási, menedzsment és üzemeltetési kontrollok száma nem tekinthető a szervezet közvetlen mutatójának, mivel azokat elsősorban az elektronikus információs rendszer biztonsági osztálya határozza meg (tehát előfordulhat, hogy kis létszámú szervezet nagyságrendekkel bonyolultabb kontroll készletet alkalmaz, mint egy lényegesen nagyobb, strukturált szervezet).

Vizsgálati hipotézis, hogy az alkalmazó szervezeteknél kialakítható olyan testre szabott működési keret, amelyben a kiberbiztonsági felelősségek (mint szervezeti kontroll eszközök) nem különálló alrendszert alkotnak, hanem a szervezeti folyamatokban integráltan jelennek meg.

Ennek megfelelően a továbbiakban a szervezetnél szükséges felelős személyek kijelölésének megvilágítása következik, kifejezetten a szervezeti alkalmazás támogatása érdekében, javaslatokkal, kerülve a jogszabályi követelményekben olvasható

kontrollok felesleges ismétlését. Követendő logikai vonal a jogszabályban megfogalmazott követelmények – az értelmezés – a szervezeti döntés – az implementáció, a kontrollok kialakítása – ciklusának támogatása.

A vizsgálati módszer célzott, kvalitatív dokumentumelemzés az elsődleges források feldolgozásával, a kiemelt témáknál egyéb forrásokra támaszkodva a jelenlegi (2026) érvényességi időben.

A jogszabály követelményei adottnak tekintendők, így azok elemzése, értelmezése vagy véleményezése nem tartozik a vizsgálat szakmai feladatai közé.

A kiberbiztonsági felelősségi keretrendszer kialakítása

Szervezeti sajátosságoktól független állítás, hogy az elektronikus információs rendszerek kiberbiztonságához vezető úton az első lépés a felelősségek kijelölése. A felelős személyek hatásköre, a végzett szabályozási és biztonságfelügyeleti tevékenység képezi a szervezet kiberbiztonságának gerincét a szervezet vezetésétől kezdve a munkavállalókig (Hunorfy, 2024).

Kifejezetten fontos annak megértése, hogy a jogszabályban meghatározott normák a szervezetnél milyen lépésekkel alakíthatók kiberbiztonsági szereplőkké.

Bevezető információ, hogy a jogszabály 24, később pontosabban látható felelős személy kijelölését határozza meg a szervezet vezetői számára. Ez a szám elrettentő lehet nemcsak a kislétszámú (pl. 30-50 fős) szervezetek számára, hanem a nagyvállalati körbe tartozó, több telephelyes szervezetek számára is.

A felelősségi körök azonosítási követelménye egyértelmű fogalmazású, de nem tartalmazza azt az – irreális – követelményt, hogy ezeket a szerepköröket csak önálló beosztással vagy megbízással lehet ellátni. Így logikus megoldás a szerepkörök összevonása más munkakörökkel.

A kiberbiztonsági feladatok ellátásához szükséges felelősségi rend kialakítása – és a jelen vizsgálat – nem egy új szervezeti egység megalakítását vagy a létszám bővítését célozza. A megoldás a szervezeti kultúrába illesztett, a működési rendbe integrált felelősségi struktúra kialakítása, a meglévő erőforrásokra, folyamatokra és feladatokra támaszkodva.

Megállapítható, hogy a kiberbiztonsági felelős szerepkörök kijelölése az érintett személyek és szervezeti elemek esetében többlet feladatokat jelent, ami szükségszerűen erőforrás-versenyt eredményez a szervezeti alrendszerek között. Ennek megoldása vezetői és humán szakterületű feladat azzal az iránymutató gondolattal, hogy a szervezeti célok megvalósításához esetenként szükség lehet az alrendszerek elkülönült igényeinek a módosítására.

A kiberbiztonsági szerepkör-elosztási modell

A kiberbiztonsági funkciók ellátását, a szükséges vezetői kijelöléseket egy egyszerű, szervezeti struktúrát alkalmazó kiberbiztonsági szerepkör-elosztási modell

támogathatja. A modell a szervezet kiberbiztonsági felelőseit három, egymástól független kategóriába rendezi, mint:

– dedikált kiberbiztonsági szerepkörök;
– elektronikus információs rendszer üzemeltetéshez kapcsolódó feladatok (pl. irányítás, tervezés, technikai feladatok), valamint
– más szervezeti egységekhez kapcsolható feladatok (pl. humán, infrastruktúra biztonság, beszerzés).

Mindhárom kategória esetében további választási lehetőség az adott feladatkör saját munkavállalóval történő ellátása vagy külső, szerződéses partner igénybevétele. A kiszervezésnél a nyilvánvaló anyagi kérdés mellett kiberbiztonsági szempontként kell figyelembe venni az így megismerhető adatokkal kapcsolatos fenyegetéseket, az összeférhetetlenségi szempontokat, az együttműködés gyakorlati kérdéseit és a szükséges ellenőrzési, felügyeleti kontrollok működőképességének biztosítását, illetve a jelentési kötelezettségek teljesítését. A szervezet adataiért és információs folyamataiért való felelősséget nem lehet áthárítani („kiszervezni"), így a szolgáltató felé támasztott követelmények és az átláthatóság (auditálhatóság, nyomon követhetőség) kérdéseinek specializált megoldása elengedhetetlen.

A szervezeti sajátosságoknak megfelelő modell kialakításához nélkülözhetetlen az elkülönítési[2] (vagy összeférhetetlenségi) irányelvek egyértelmű meghatározása és következetes betartása (pl. távollét esetén szükséges helyettesítés esetén is). Az elkülönítés alapvetően szélesebb körben értelmezett kiberbiztonsági módszer, vonatkozhat a fizikai létesítményekre, hardverekre, szoftverekre vagy tudatossági programokra is (Demann, 2023). E kérdés részletesebb feldolgozásához önálló vizsgálatra lenne szükség, így most csak a legfontosabb, személyekre vonatkoztatható kérdések következnek.

A hatályos jogszabály szerint a szervezet szétválasztja az egyéni felelősségeket, azt dokumentálja, illetve a szétválasztás érdekében meghatározza az elektronikus információs rendszer hozzáférési jogosultságait (MK, 2024, 1. sz. melléklet, 2.59.). Szakmai érdekesség, hogy a korábbi (már hatályon kívüli) 2013-as változatban (NFM, 2013, 4. sz. melléklet, 3.3.6.5.1.), illetve a 2015-ös változatban (BM, 2015, 4. sz. melléklet, 3.3.10.5.) is hasonló megfogalmazás olvasható, tehát a kérdés jogszabályi megítélése egy évtized alatt nem változott.

Az irányadó nemzetközi ISO[3] szabvány szerint a visszaélésre lehetőséget adó kapcsolódó feladatokat és felelősségi területeket[4] el kell különíteni annak érdekében, hogy csökkenjen az illetéktelen vagy véletlen módosítás vagy visszaélés lehetősége (ISO, 2022, 6.1.2.).

[2] separation of duties – SoD
[3] International Organization for Standardization – Nemzetközi Szabványügyi Szervezet
[4] conflicting duties and areas

Az amerikai NIST szabvány szerint a hatáskörök elkülönítése a jogosultságokkal történő visszaélést akadályozza és segíti a rosszindulatú tevékenységek összejátszási kockázatának csökkentését (NIST, 2020, AC-5).

Az elkülönítési szabályok technikai szintű megoldása már fejlődő ágazatnak számít; különböző SoD tulajdonságok mentén már modellek üzemelnek (pl. statikus-, dinamikus-, objektum alapú- vagy művelet alapú SoD), ahol a szerepkör kijelölés, a jogosultság aktivizálás engedélyezett vagy tiltott (Groll, Ludwig, & Pernul, 2025).

Az említett források elemzése alapján megállapítható, hogy nem adnak szervezeti szintű elkülönítésre vonatkozó iránymutatás (pl. megfogalmazható elvek formájában), a követelmények a különböző szabályozási területeken, általános megfogalmazásban jelennek meg. Ez aláhúzza, hogy minden szervezetre érvényesíthető megoldás nem adható, ugyanakkor a legfontosabb vizsgálati szempontok meghatározhatók.

Az elkülönítési irányelvek szervezeti szintű meghatározásához a következő szempontok segítséget nyújtanak a jogszabályban megfogalmazott követelmények gyakorlati implementálása érdekében:

Elkülönítendő feladat		**Indoklás**
Szerepkör 1	**Szerepkör 2**	
döntési jogkörök	végrehajtási feladatok	döntés és a végrehajtás egy kézben kockázatot jelent
adatgazdai döntési jogosultságok	rendszeradminisztrátori feladatok	döntés és technikai végrehajtás ne legyen egy kézben
üzemeltetés	üzemeltetés ellenőrzés	független ellenőrzés szükséges
kritikus műveletek kezdeményezése	kritikus műveletek jóváhagyása	a kezdeményezés, jóváhagyás, végrehajtás és ellenőrzés elkülönítésének hiánya szervezeti szintű kockázatot jelent
kockázatmenedzsment	üzemeltetés	a kockázatok felmérése, kezelése és az üzemeltetési feladatok összemosása kockázatos
hozzáférési jogosultságok meghatározása	hozzáférési fiókok technikai kezelése	a jogosultságok tartalmának meghatározása és azok technikai megvalósítása (adminisztrációja) nem kezelhető kockázatokat jelentenek
hozzáférés-kezelés	konfiguráció-módosítás	a hozzáférési döntések és a rendszerparaméterek módosításának együttes kezelése konfliktust hordoz magában
naplózás üzemeltetés	incidenskezelés, kivizsgálás	az üzemeltető és vizsgáló szerepek elkülönítésének hiánya veszélyezteti az objektivitást
fizikai hozzáférés (pl. helyiség) biztosítása	felhasználói hozzáférés kiosztása és adminisztrációja	a két feladatkör elkülönítésének hiánya megkönnyíti a jogosulatlan hozzáféréseket
elektronikus információs rendszer beszerzésének (kialakításának) előkészítése, átvétele	rendszer üzemeltetés	a két fázis összemosása esetén későbbi vizsgálatok objektivitása megkérdőjelezhető
fejlesztési, tesztelési feladatok	rendszer üzemeltetés	a két feladat összemosása megakadályozza az objektív megítélést

1. sz. táblázat: Az elkülönítésre vonatkozó irányelvek (saját szerkesztés)

Az előbbiekből az adott szervezetnél csak az értelmezhető eseteket kell mérlegelni (pl. ahol nincs saját üzemeltetésű elektronikus információs rendszer, ott felesleges a fejlesztésről rendelkezni).

Nem kiberbiztonsági területű megállapítás, de ezen a területen is érvényes, hogy az IT felügyeleti és irányítási[5] feladatok – különösen a szabályozás, megfelelőség és audit – elkülönítése az operatív IT-tevékenységektől alapvető követelmény a felelősségek elmosódásának elkerülése érdekében (Juiz, Duhamel, Isis, & Luna-Reyes, 2022).

A feladatok nemcsak szerepkörök, hanem konkrét műveleti lépések szintjén is elkülönítést igényelhetnek. A kritikus műveletek (pl. kezdeményezés, jóváhagyás, végrehajtás és ellenőrzés) egy kézben történő összpontosulása ugyanis a kontrollok gyengüléséhez vezethet és visszaélési lehetőséget adhat (Groll, Ludwig, & Pernul, 2025).

Inkább technikai területen szükség lehet speciális helyzetek kezelésére a kétszemélyes szabály[6] alkalmazásával, ahol csak két, dedikált személy együttes tevékenysége kezdeményezheti az adott folyamat indítását (pl. rendszer leállítás vagy indítás, rejtjelzéssel kapcsolatos bizalmi folyamatok), így az elkülönítés mellett e feladatok megoldására is gondolni kell a szabályozásnál.

A továbbiakban a szervezeti felelősségi körök funkcionális csoportosítása következik azzal az iránymutató gondolattal, hogy a csoportosítás nem a szervezeti hierarchiát, hanem az egyes szerepkörök elsődleges szervezeti funkcióját veszi figyelembe.

A jogszabályban meghatározott felelős funkciók részletes áttekintése példát adhat a szervezeti modell kialakításához, ahol a rendelkezésre álló erőforrások ismerete adja az elsődleges támpontokat a szükséges személyi kijelölésekhez.

A nehezebbnek tűnő kiberbiztonsági felügyeletért, szabályozásért felelős funkciók esete bonyolultabb, ezért erről a következőkben kicsit részletesebb gondolatok következnek.

Ennél a területnél kulcsfontosságú annak felismerése, hogy a szükséges szaktudás megléte nélkül illúzió szakértői megoldásokról beszélni. A gyakorlat az, hogy a szervezeteknél lassan kialakul a felelősségi rend, amibe a kiberbiztonság is beilleszkedik. Ehhez tanulásra, gyakorlati tapasztalatokra van szükség; vagy meg kell fizetni a szaktudást és felkészült szakértőt kell toborozni, ahol már csak a szervezeti sajátosságok megismerése jelenthet kihívást.

A másik lényegi kérdés annak felismerése, hogy a szervezet elektronikus adatkezelése nem nulláról induló feladat (nem „zöldmezős beruházás”). Előzmények (örökölt rendszerek, elemek, vezetői döntések, megvalósult vagy félbemaradt projekt eredmények) vannak, csak esetleg nem tisztán ismertek (dokumentáció hiány, üzemeltető állomány és a felelős vezetők fluktuációja miatt). Ez az állapot mutatja,

[5] governance
[6] two-man rule, four-eyes principle

hogy az említett nagy számú kontroll ellenére nem biztos, hogy minden területen egyidejűleg kell szabályozási, irányítási folyamatokat kialakítani és technikai vagy üzemeltetés fejlesztési lépéseket megtenni, valamint azokat a napi ügyintézés mellett dokumentálni.

A jogszabályban megfogalmazott kiberbiztonsági funkciókat egy vagy több személy láthatja el az elektronikus információs rendszerek bonyolultsága, biztonsági osztálya, illetve a szervezet sajátosságainak (pl. több telephelyes elhelyezkedés) figyelembe vételével.

A következő táblázat a szerepkör-elosztási modell első kategóriájának eseteit mutatja be.

Kontroll megnevezése (Az előfordulás (MK, 2024) azonosításával) **(feladatkör összefoglalása)**	**Kontroll területe** **(Összeférhetetlenség)**
Biztonságért felelős személy a szervezeti szintű információbiztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására (2. mell., 1. fejezet 1.2. p.) (megfelelés koordinálása) (felelős a rendszerek védelméért, a kockázatmenedzsment rendszerért, incidensbejelentésért – Kibertv. 11.§.)	kiberbiztonsági felügyelet és irányítás (gazdasági vezető, üzemeltetést irányító vagy annak alárendeltségében lévő)
Kockázatkezelésért felelős személy (2. mell., 1. fejezet 1.20.1. p.) (folyamatok összehangolása)	kiberbiztonsági felügyelet és irányítás (üzemeltetés irányítás)
Kockázati vezető (2. mell., 1. fejezet 1.20.2. p.) (szervezeti szintű áttekintés, elemzés)	vezetői megbízás (kockázatmenedzsment irányításáért felelős személy)
A biztonságértékelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 5. fejezet 5.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	kiberbiztonsági felügyelet és irányítás (biztonságértékelést végző személy)
Biztonsági értékelést végző személy vagy csoport (2. mell., 5. fejezet 5.2. 1. p.). (értékelő személy)	kiberbiztonsági feladat (biztonságértékelési szabályozásért felelős személy)
Az engedélyezésért felelős személy, aki az EIR-ért felelős (2. mell., 5. fejezet 5.12.1. p.). (engedélyező személy)	vezetői megbízás (biztonságért felelős személy)
A más rendszerekből áthozott biztonsági követelményekért felelős személy (2. mell., 5. fejezet 5.12.2. p.) (megfelelés elfogadásért felelős)	kiberbiztonsági felügyelet és irányítás (üzemeltetés)
A biztonsági eseménykezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 9. fejezet 9.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	kiberbiztonsági felügyelet és irányítás
A biztonságtervezési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 13. fejezet 13.1.2. p.) Szabályzat menedzselése, szabályozás irányítása	kiberbiztonsági felügyelet és irányítás

Kontroll megnevezése (Az előfordulás (MK, 2024) azonosításával) **(feladatkör összefoglalása)**	**Kontroll területe** **(Összeférhetetlenség)**
A kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 15. fejezet 15.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	kiberbiztonsági felügyelet és irányítás (kockázati vezető)
Az üzletmenet-folytonosságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 7. fejezet 7.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	kiberbiztonsági felügyelet és irányítás (üzemeltetés irányítás)
Az azonosítási és hitelesítési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 8. fejezet 8.1.2. p.)	kiberbiztonsági felügyelet és irányítás (üzemeltetés irányítás)
A rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 17. fejezet 17.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	kiberbiztonsági felügyelet és irányítás (üzemeltetés irányítás)

2. sz. táblázat: A kiberbiztonsági feladatok megvalósítási változata (saját szerkesztés)

A táblázatban látható megoldás – mint egy szervezeti modell változat – kialakítása kizárólag a szervezet sajátosságaihoz igazítottan lehet hatékony.

Megállapítható, hogy a tizenhárom kiberbiztonsági felügyeleti funkcióból kettőt vezetői megbízással szükséges megoldani; kettő összeférhetetlenséget tartalmaz, így megoldásként a biztonságértékelési feladatokat más szervezeti elemhez kell rendelni (pl. belső ellenőrzés, kontrolling), a kockázatelemzés végzését és vezetői jóváhagyását el kell különíteni. A maradék esetekben mérlegelési szempont, hogy a szervezetnél alkalmazott elektronikus információs rendszerek összetettsége, biztonsági osztálya szerint egy fő el tudja-e látni ezeket a feladatokat. Ezt a kérdést egyedileg lehet megválaszolni, kiegészítve azzal a szervezési kérdéssel, hogy biztonságért felelős személy a szervezeti hierarchiában hol fog elhelyezkedni, illetve milyen megoldással biztosítható a helyettesítése.

Civil szakterületű kutatás mutatja az általános tendenciát, hogy növekszik a biztonságért felelős funkció[7] rendszeresítésére vonatkozó igény, közvetlen jelentési kötelezettséggel a vezető[8] felé az alacsonyabb IT szervezeti vezető felé történő jelentés helyett (Karanja & Rosso, 2017, old.: 39), ami megerősíti a feladatkör fontosságát.

Strukturált megközelítés szerint a biztonságér felelős személy feladatai a védelem és megelőzés, a felügyelet, érzékelés és keresés, a reagálás, helyreállítás és fenntartás, valamint az irányítás, felügyelet, megfelelőség, képzés és kockázat menedzsment négyesére tagolhatók (Allen, és mtsai., 2015, old.: 1), ami szemléletesen igazolja a 2. sz. táblázatban foglaltakat.

[7] Chief Information Security Officer – CISO
[8] Chief Executive Officer – CEO

Az összetett feladatok és a különböző területek közötti összehangolás sikere szempontjából kritikus fontosságú a biztonságért felelős személy hitelessége és a hatékony kommunikációja a különböző menedzsment szinteken, mint szervezeti felsővezetés vagy IT üzemeltetés (Triplett, 2022).

A szervezeteknél a kiberfenyegetések következményei túlmutatnak a technikai problémákon és súlyosan befolyásolják az üzletmenet folytonosságot, a partnerek felé mutatott megbízhatóságot és a versenyképességet, így létfontosságú a kiberbiztonsági kockázatmenedzsment integrálása a szervezet stratégiai szintű feladatai közé (Mizrak, 2023).

Az incidenskezelés – tágabban incidensmenedzsment – hatékony működése az előbbiek figyelembe vételével szintén stratégiai fontosságú témakör. A felkészülés – detektálás – elemzés – reagálás – helyreállítás – tapasztalatok integrálása és fejlesztés ciklikus feladatai hatékony kommunikációval kiegészítve már régen nem tekinthető csak technikai kérdésnek, így ezt csak összetett szabályozási és felügyeleti lépésekkel lehet biztosítani (Jebaraj, 2022).

Az üzletmenet folytonosság – más megfogalmazásban kiber ellenállóképesség[9] – átfogó megközelítést kíván, ami az irányítás és felügyelet), az együttműködés, a technológia és a folyamatos értékelés együttes kezelését jelenti. A szervezet vezetésének kiemelt szerepe van a helyesen működő kiberbiztonsági kultúra kialakításában, a szükséges döntések döntéshozatalba történő integrálásában, illetve a megosztott kiberbiztonsági felelősségi rend kialakításában és működtetésében (AL-Hawamleh, 2024).

Specifikus és különösen érzékeny területnek tekinthető az azonosítási és hitelesítési folyamatok felügyelete, így a jogosultságok kiosztása, módosítása és visszavonása a leggyakoribb összeférhetetlenségi pontok közé tartozik (Sharma, 2026).

A szervezeti céloknak megfelelő kiberbiztonsági szabályozás érdekében az irányítás és felügyeleti területnek a hatékony technikai kontrollokat összetett jogi megfelelést biztosító struktúrával és dinamikus szervezeti kockázatmenedzsment eljárásokkal kell integrálni (Moreira & Larissa, 2024). Ennek megoldása a szervezeti elemek összehangolása és a különböző szakterületi képviselők szoros együttműködése nélkül nem képzelhető el.

A továbbiakban az üzemeltetési, illetve más területekhez dedikálhatók kiberbiztonsághoz kapcsolódó felelősségek bemutatása történik.

Kontroll megnevezése (Az előfordulás (MK, 2024) azonosításával) **(Feladatkör összefoglalása)**	**Kontroll területe** **(Összeférhetetlenség)**
A naplózásra és elszámoltathatóságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 4. fejezet 4.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	Üzemeltetés felügyelet és irányítás (üzemeltetés végrehajtás)

[9] resilience

Kontroll megnevezése (Az előfordulás (MK, 2024) azonosításával) **(Feladatkör összefoglalása)**	**Kontroll területe** **(Összeférhetetlenség)**
A konfigurációkezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 6. fejezet 6.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	Üzemeltetés felügyelet és irányítás (üzemeltetés végrehajtás)
A karbantartási szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 10. fejezet 10.1.2. p.) (szabályzat menedzselése, szabályozás irányítása)	Üzemeltetés felügyelet és irányítás (üzemeltetés végrehajtás)
Az információk nyilvánosan hozzá férhetővé tételét biztosító személyek (2. mell., 2. fejezet 2.124.1. p.) (adatok szabályozott nyilvánosságra hozatala)	Kommunikációs terület
A tudatossági és képzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 3. fejezet 3.1.2. p.) (tudatossági feladatok szabályozása és irányítása)	Humán/képzési szakterület
Az adathordozók védelmére vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 11. fejezet 11.1.2. p.) (adathordozók védelmének szabályozása)	Ügyviteli terület
A fizikai védelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 12. fejezet 12.1.2. p.) (az elektronikus információs környezet fizikai védelmének szabályozása)	infrastruktúra biztonsági terület
A személyi biztonságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel (2. mell., 14. fejezet 14.1.2. p.) (az elektronikus adatfeldolgozó eszközök hozzáférési jogosultságának szabályozása)	Humán terület
A beszerzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 16. fejezet 16.1.2. p.) (az elektronikus információs eszközök és szolgáltatások beszerzésének szabályozása)	logisztikai/beszerzési szakterület
Az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy (2. mell., 19. fejezet 19.1.2. p.) (az ellátási lánc kockázatmenedzsment feladatok szabályozása)	logisztikai/beszerzési szakterület

3. sz. táblázat: Az üzemeltetési és egyéb területekhez kapcsolható feladatok megvalósítási változata (saját szerkesztés)

Az említett esetek nem jelenthetik a szabályozási terület önálló irányba történő megvalósulását, a végrehajtásnak a jogszabályban meghatározott követelmények szerint kell megvalósulnia, melyhez nélkülözhetetlen a biztonságért felelős személy tevékenysége. E mellett a szükséges eljárások és követelmények kialakításához

nélkülözhetetlen a csoportmunka, mivel az adott szakterület képviselőjének a kapcsolódó kérdésekben támogatásra van szüksége.

A naplózás, a hálózat monitorozása, illetve az átláthatóság és megfigyelhetőség szempontjainak integrálása lehetőséget teremt a különböző típusú adatok korrelációjára, ami értékes eszköz lehet a biztonsági incidensek kivizsgálásakor, illetve az üzemeltetés közbeni események hatásainak megértésében (Burramukku, 2024). A hálózaton belüli elszigetelt megoldások helyett integrált szolgáltatások kialakítása és folyamatos fejlesztése a vezetés, a biztonsági menedzsment és az üzemeltetési szakterületek szoros együttműködését igényli.

A karbantartás segítheti a kiberbiztonság megerősítését a karbantartó és menedzsment állomány képzésével, a rendszerek naprakészen tartásával csökkentheti a kiberfenyegetések okozta incidensek és sérülések hatásait, a minőségbiztosítás gondozásával támogatja a detektálási, elemzési és reagálási képességek szinten tartását illetve fenntarthatja a rendelkezésre állás szükséges mértékét (Zarreha, Wan, Leea, Saygina, & Al Janahia, 2019), így jól érzékelhetően ez a terület is szerteágazó, az üzemeltetésbe ágyazott folyamatokat és tevékenységeket takar.

A kiberbiztonsági tudatosság hiánya súlyos következményekkel járhat nem csak a felhasználók, hanem az üzemeltetők és vezetők esetében is, ami felhívja a figyelmet a képzés és tudatosításra, valamint tudatos vezetői kommunikációra a szabályok betartása érdekében (Triplett, 2022). Emiatt a humán faktorra történő támaszkodás kiemelt fontosságú a kiberbiztonsági tudatosság erősítése és a viselkedés átalakítása érdekében (Balzano & Giacomo, 2025).

Az adathordozókra vonatkozó védelmi rendszabályok kialakítása és fenntartása a napi gondolkodásban nem kiemelt jelentőségű téma, a felhasználók és üzemeltetők gyakran néhány fizikai védelmi rendszabály (pl. pendrive azonosítás, személyes felügyelet) segítségével megoldottnak gondolják a feladatot. A kérdéshez tartozik azonban a bonyolultabb adattároló infrastruktúrák biztonságos kialakítása és használata, a kezelt adatok védelme (beleértve a titkosítást is), a tároló kapacitások hozzáférési mechanizmusai (fizikai és hálózati) és az izoláció. A biztonsági mentések diverzifikált tárolása, a mentett adatok helyreállíthatóságának biztosítása, illetve a rendszerből kivont eszközök archivált adatainál az adatkezelési lehetőség (pl. olvashatóság) rendelkezésre állása bonyolult elektronikus információs rendszerek esetében összetett feladat, melyet strukturáltan felépített eljárások mentén, folyamatszemlélettel lehet csak helyesen megoldani.

A beszerzés, valamint az ellátási lánc biztonságára megszámolhatatlan, többszintű fenyegetés irányul a technológiai sérülékenységektől kezdve a humán szempontokig. Emiatt komplex kockázatelemzésre épülő, többszintű megközelítés szükséges a szükséges mértékű védelmi rendszabályok kialakítása és fenntartása érdekében, bevonva az összes érintett szereplőt (pl. fejlesztő, szállító, auditor, külső partnerek) a szükséges képzési és tudatosítási programokkal megerősítve (Koppisetti, 2026).

A 3. táblázat jól szemlélteti a felelősök kijelölésénél a feladatokhoz szükséges kompetenciák meglétének fontosságát. Egyértelmű – bár szervezeten belül elle-

nérdekeltségbe ütközhet –, hogy meglévő kompetenciák (tudás, szervezeti ismeret, kapcsolati rendszer, infrastruktúra vagy pénzügyi keretek) az esetek nagy részében jól felhasználhatók a kiberbiztonsági háló kialakítása és fenntartása során.

A konkrét megoldás kialakításakor figyelembe kell venni azt a kihívást is, hogy a kijelöléseknél (megbízásoknál) az auditor vagy az ellenőrző hatóság számára is érthető legyen az adott munkaköri megoldás valamint a kiberbiztonsági struktúra, illetve világos legyen az összeférhetetlenségre vonatkozó szervezeti elgondolás is.

Hirtelen helyzetek mindig adódhatnak – mint baleset, betegség, váratlan távollét vagy szervezettől való hirtelen távozás –, így arra is fel kell készülni, hogy ezekben a helyzetekben milyen ideiglenes, helyettesítő megoldások alkalmazhatók. Erre kiforrott megoldás nem adható, de a vezető a fennálló kockázatok tudatában kiegészítő védelmi rendszabályok alkalmazásával, dokumentálással és fokozott ellenőrzéssel kiegészítve rövid távon kényszerülhet az összeférhetetlenségi szabály ideiglenes módosítására (mert pl. egyszerűen más megoldással nem biztosítható a funkció ellátása).

A működőképesség megköveteli, hogy a kiberbiztonsági felelősségi rend szereplői ismerjék egymást és egymás feladatait, illetve alakuljon ki az a szakmai rend, ami biztonságért felelős személytől indítva végrehajtható feladatokat eredményez, a közbeeső, más hatáskörű vezetőkön átívelve. Ez két származtatott feladatot jelent a hatékony működés érdekében:

– a felelősök, helyetteseik és elérhetőségeik naprakész azonosítása („szakmai telefonkönyv”) és
– szervezeti belső rendelkezés, ami rögzíti a szakmai működési, együttműködési és koordinációs feladatokat (pl. eseménykezelés vagy szabályozó elem változtatása esetén).

Szabályozási modell szempontok

A jogszabály első, 2013-as változata a szervezet feladataként általánosságban határozta meg az elektronikus rendszerekkel kapcsolatos felelősségek és feladatok kijelölését. A felelősségi rend ekkor három konkrét szerepkörben jelent meg (biztonságért felelős személy, rendszerelemek adminisztrációjáért felelős személy, valamint a rendszerelemek kiszállítását engedélyező személy) (NFM, 3. sz. melléklet). A 2015-ös módosítás ugyanezt a megközelítést követte, új felelősi szempontot nem vezetett be (BM, 2015, 4. sz. melléklet).

A 2024-es módosítás nagyságrendi változást hozott a jogszabály 24 különálló felelős szerepkör kijelölési kötelezettségével. Ez a változás nem csak mennyiségi kérdés, inkább a jogalkotó szemléletváltását, a szabályozási modell átalakulását jelzi.

A jogszabály által alapul vett amerikai NIST SP 800-53 szabvány alapvetően technikai és folyamat-alapú, és csak két kontrollban[10] határoz meg név szerint definiált szerepkört. A többi kontroll esetében a szabvány általános feladatkijelölést alkalmaz, mint „ki kell jelölni egy meghatározott tisztségviselőt,[11] aki a politika és az eljárások[12] kidolgozásáért és fenntartásáért felel".

A magyar jogszabályalkotó a 2024-es frissítéskor ezt az általánosan megfogalmazott feladatkijelölési (implicit) modellt alakította át név szerint meghatározott (explicit) felelősségi körökké. A kontrollok kialakítására és fenntartására vonatkozó folyamatkezelés megmaradt, de kiegészült a személyes felelősség kötelező kijelölésével: minden kontrollhoz szervezeti felelős tartozik, aki a kialakításért, fenntartásért, felülvizsgálatért és megújításért felel, beleértve a hatálybalépést biztosító jóváhagyást is. A jogszabály által alkalmazott megfogalmazás az amerikai szabványhoz képest közvetlenebb megfogalmazást alkalmaz: „a szervezet (…) kijelöl egy, a szervezet által meghatározott személyt, aki a (név szerint azonosított) szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel".

Ez a változás az európai szabályozási szemléletet tükrözi, amelyben a biztonság nem csak technikai folyamatok összessége, hanem a szervezetbe illesztett felelősségi pontok rendszere is. A magyar modell így az amerikai szabvány általános folyamatleíró megközelítését továbbfejleszti: a feladatkijelölési kötelezettséget pontosabban meghatározva, számonkérhető felelősségi körökké alakítja.

Speciális eset, de az egyre gyakoribb előfordulás miatt említeni kell a multinacionális cégek országhatárokon átnyúló hatásait. Ennek egyik megnyilvánulása, hogy a magyar telephelyen az elektronikus információs rendszerek szabályozása (pl. felügyeleti megoldásai, biztonsági követelményei) a tulajdonosnál honos szabályok szerint kell, hogy történjen. Részletes elemzést mellőzve kijelenthető, hogy a Magyarországon üzemelő szervezet – amennyiben tevékenysége alapján a jogszabályok hatálya alá tartozik – nyugodtan követhet más szabványokat, ajánlásokat, ugyanakkor a magyar jogszabály követelményeit maradéktalanul be kell, hogy tartsa. Ez egyszerűen kizárja azt a provokatív kérdést, hogy „ugye nem gondolják, hogy az X ország szabványa gyengébb, mint a magyar kiberbiztonsági követelmény"? Az auditor, vagy hatósági ellenőr ugyanis nem fog idegennyelvű ajánlásokat böngészni, csak a magyar jogszabályi követelmények végrehajtására kíváncsi. Ebben az esetben kulcsfontosságú a külföldi szabályozó és a magyar követelmények közötti megfelelőségi táblázat[13] kialakítása, támogatva az auditálhatóságot is.

[10] Authorizing Official – CA-6; Configuration Management Responsible Individual – CM-9
[11] organization-defined official
[12] policy and procedures
[13] mapping

A multinacionális szervezetek másik kihívása a szükséges szervezeti kultúra kialakítása és fenntartása területén a központi szabályozók (ajánlások eljárások) és a helyi megoldások, szokások szinkronba hozatala (Troublefield, 2025), amit nehezít, hogy a jogszabályokban rögzített sarokpontoknál nem tehető könnyítés.

Összefoglalás

Az elhangzottak szemléletesen igazolják, hogy a kiberbiztonsági területen belül a felelősségi rend kialakítása nem egyszerűen megoldható kérdés, kitekintve arra is, hogy a személyi változások miatt ez nem egyszeri feladat, hanem folyamatosan felügyelt kérdés kell, hogy legyen.

A bevezetésben felvillantott kiberbiztonsági területtel foglalkozó szerepkörök száma a vezetői reakciókat az érdeklődés és a merev visszautasítás közötti skála valamelyik pontjára sodorja. Megjelenhet az a látszólag egyszerű megoldás is, hogy rendben, akkor mindent rá kell bízni a biztonságért felelős személyre…

A hasonló bizonytalanságok mellett világítótoronyként ad tiszta jelzést az adatok és az adatkezelő képességek szervezeti védelmének követelménye, melynek egyszemélyi felelőse a szervezet vezetője a szükséges erőforrások biztosítása, a védelmi eljárások felügyelete és a szükséges vezetői reagálások formájában. Mert, amíg nincs kiberbiztonsági probléma, addig könnyű a feladatok könnyebb megúszása irányába navigálni a szervezeti lépéseket, csak nem biztos, hogy ez stratégiai szempontból valóban eredményes megoldás.

A jogszabályban megfogalmazott követelmények megértése után következik a szervezetnél a megvalósítás fázisa, az általános keretekből egy speciális, a szervezeti keretekbe (struktúra és folyamatok) történő formálás, integrálás, melyre a cikk gyakorlati példát mutat. A három táblázat a szervezeti felépítés szerint szervezeti egységig és beosztásig terjedően pontosítható, így gyakorlati támogatást nyújt a szervezetek kiberbiztonságának szakterületi kialakításához.

Kiemelten fontos annak megértése, hogy a jogszabályban meghatározott szerepkörök szervezeti megfeleltetése önálló tervezési feladat és nem csak másolás. A jogszabályban a felelősök azonosítása még nem alakítja ki a szervezetnél a működőképes felelősségi rendszert. Ehhez kapcsolódó további következtetés, hogy a kijelölt személyek megfelelő szervezeti felhatalmazás és a szükséges erőforrások biztosítása kiemelt vezetői feladat, ahol a hiányosságok stratégiai kockázatokkal járnak.

Fontos eszköz az 1. sz. táblázat, melynek szervezeti sajátosságokat követő pontosítása támpontot ad a szervezet vezetőjének és a biztonságért felelős személynek arra nézve, hogy melyik területeken kerülendők a káros összefonódások. Ugyanez a lépés segíti a szervezetet abban is, hogy az elkerülhetetlen helyzetekben alkalmazott ideiglenes megbízásokhoz milyen kockázatcsökkentő kiegészítő kontrollok alkalmazása szükséges.

A 2. és 3. sz. táblázat tételes felsorolása egyszerű ellenőrzési lista arra nézve, hogy szervezet maradéktalanul teljesíti-e a jogszabályban megfogalmazott felelősök kinevezésére vonatkozó követelményt.

Ugyanígy segítség a szervezet számára annak azonosításában, hogy mely feladatokat kell szervezeten belül ellátni, esetleg mely feladatok megoldása történik szervezeten kívüli megbízással, illetve melyek azok a felelősségi körök, melyekre központi szolgáltatások igénybevétele miatt a szervezetnek nincs hatása. Fontos tehát annak pontos ismerete, hogy mely feladatokat ki lát el a szervezetnél, és melyek azok az esetek, ahol más szervezethez tartozó szolgáltatásokat kell igénybe venni. Itt tehát előkerül a szervezetek közötti és a belső együttműködés, a napi kapcsolattartás, a vészhelyzeti protokollok kérdése, ahol a nevek, telefonszámok ismerete és a szükséges közlendők vagy kérdések előzetes körvonalazása stratégiai előnyöket jelenthet például kiberbiztonsági incidens megoldásakor.

A bemutatott eszközökre hivatkozva kijelenthető, hogy a jogszabályban meghatározott kiberbiztonsági felelősségi körök és a szervezeti felépítés vizsgálatára támaszkodva kialakítható egy egyedi sajátosságokkal rendelkező felelősségi modell, ahol a meglévő kompetenciákhoz történő delegálással a kiberbiztonsági feladatok integráltan jelennek meg a szervezet folyamataiban és feladataiban, igazolva a bevezetés szerinti hipotézist.

A szervezeti kiberbiztonsági feladatok menedzselése erőteljes koordinációt jelent a különböző szakterületek tevékenysége között, így záró gondolatként meg kell jeleníteni a biztonságért felelős személy felhatalmazásának, szervezőképességének, agilitásának és elfogadottságának kiemelt fontosságát, mint a szervezet adatvagyonának és adatfeldolgozó képességeinek védelméhez szükséges alapvető erőforrást.

Hivatkozások

1. AL-Hawamleh, A. (2024). Strengthening Defenses and Enhancing Continuity in Business Security. *, International Journal of Computing and Digital Systems, 15, No.1 (Mar. 24).* doi:http://dx.doi.org/10.12785/ijcds/150193
2. Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). Structuring the chief information security officer organization. Letöltés dátuma: 2026. 08 12, forrás: https://www.researchgate.net/profile/Julia-Allen-11/publication/282646726_Structuring_the_Chief_Information_Security_Officer_Organization/links/5615205808ae983c1b41e6fb/Structuring-the-Chief-Information-Security-Officer-Organization.pdf
3. Balzano, M., & Giacomo, M. (2025). At the Cybersecurity Frontier: Key Strategies and Persistent Challenges for Business Leaders. *Strategic Change 2025.* doi:https://doi.org/10.1002/jsc.2622
4. BM. (2015). 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben

meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre (...) vonatkozó követelményekről.
5. Burramukku, N. R. (2024). Monitoring, Logging, and Observability in Secure Infrastructure Operations. *International Journal for Novel Research in Economics , Finance and Management, Volume 2, Issue 5*. doi:http://doi.org/10.5281/zenodo.18467412
6. Demann, Y. (2023). Separating Privacy Awareness From Security Awareness Training. Letöltés dátuma: 2026. 08 17, forrás: https://www.isaca.org/resources/news-and-trends/industry-news/2023/separating-privacy-awareness-from-security-awareness-training
7. Groll, S., Ludwig, F., & Pernul, G. (2025). Separation of Duty in Information Security. *ACM Computing Surveys, Volume 57, Issue 7 (2025)*. doi:https://doi.org/10.1145/3715959
8. Hunorfy, P. (2024). Az ISO/IEC 27001 szabvány elmélete és gyakorlati alkalmazása OT/ICS-rendszerek kiberbiztonsági jelentéseinek tükrében. *Scientia et Securitas, Volume 5: Issue 3*. doi:10.1556/112.2024.00228
9. ISO. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls.
10. Jebaraj, S. (2022). Incident response and mamagement: resolving cybersecurity issues. *Practical Applications of Cyber Security*. Letöltés dátuma: 2026. 08 16, forrás: http://alexispress.in/wp-content/uploads/2022/09/Practical-Applications-of-Cyber-Security.pdf
11. Juiz, C., Duhamel, F., Isis, G.-M., & Luna-Reyes, L. F. (2022). IT Managers' Framing of IT Governance Roles and Responsibilities in Ibero American Higher Education Institutions. doi:https://doi.org/10.3390/informatics9030068
12. Karanja, E., & Rosso, M. A. (2017). The Chief Information Security Officer: An Exploratory Study. *Journal of International Technology and Information Management, volume: 26, Issue. 2, 2017*. doi:https://doi.org/10.58729/1941-6679.1299
13. Koppisetti, V. S. (2026). Cybersecurity Challenges and Risk Mitigation Strategies in Digitized Procurement and Supply Chain Systems. *AIJCST, vol. 8, no. 1*. doi:10.63282/3117-5481/AIJCST-V8I1P105
14. Mizrak, F. (2023). Integrating cybersecurity risk mamagement into strategic management: a comprehensive literature review. *Research Journal of Business and Management- RJBM (2023), 10(3)*. doi:10.17261/Pressacademia.2023.1807
15. MK. (2024). *7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről*.
16. Moreira, T., & Larissa, C. (2024). Legal and Regulatory Considerations in Cybersecurity and Information Assurance: Managing Privacy, Responsibility,and Compliance in Digital Systems. *Journal of Applied Computational Science, Numerical Methods, and Scientific Computing in*

Engineering, Vol. 14 No. 11. Letöltés dátuma: 2026. 08 12, forrás: https://soloncouncil.com/index.php/JACSNMSCE/article/view/2024-nov-04
17. NFM. (2013). 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó (...).
18. NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800 53, Rev. 5).
19. Sharma, S. (2026). Balancing Access and Control: Identity Management with Segregation of Duties. *International Journal of Computer Techniques, 13(3)*. Letöltés dátuma: 2026. 0825, forrás: https://ijctjournal.org/wp-content/uploads/2026/05/Balancing-Access-and-Control-Identity-Management-with-Segregation-of-Duties-1.pdf
20. Triplett, W. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy, 2022, 2(3)*. doi:https://doi.org/10.3390/jcp2030029
21. Troublefield, T. C. (2025). Cultural Dimensions of Cybersecurity: A Cyberpsychology Analysis of Multinational Corporate Security. *Journal of Information Security Vol.16 No.3*. doi:DOI: 10.4236/jis.2025.163019
22. Zarreha, A., Wan, H., Leea, Y., Saygina, C., & Al Janahia, R. (2019. Alireza Zarreha, HungDa Wana, Yooneun Leea, Can Saygina, Rafid Al Janahi). Cybersecurity Concerns for Total Productive Maintenance in Smart Manufacturing Systems. *ScienceDirect*. doi:10.1016/j.promfg.2020.01.067

Tóth Dávid[1]**:**

Az uniós jog nem büntetőjogi válaszai a digitális megszemélyesítésre

Absztrakt:

A jelen tanulmányban azt vizsgálom, hogy az Európai Unió milyen nem büntetőjogi eszközökkel lép fel a digitális megszemélyesítéssel szemben. E gyűjtőfogalom alá vonom a hitelesítő adatok megszerzésén alapuló online személyazonosság-lopást, az abból következő identitáscsalást, valamint azokat az eseteket is, amelyekben az elkövető úgy jár el más személy vagy intézmény nevében, hogy annak adatait technikailag nem szerezte meg. Három eltérő szabályozási területet elemzek. Ezek az eIDAS 2.0 európai digitális személyazonossági tárcája, a mesterséges intelligenciáról szóló rendelet 50. cikkének átláthatósági kötelezettségei, valamint a pénzforgalmi szolgáltatásokról szóló rendelettervezet megtévesztéssel kiváltott, mégis engedélyezett fizetésekre vonatkozó károlosztási szabályai. Az elemzésben a megelőzés, a felismerhetőség és a kárrendezés szintjét különítem el. Ennek alapján az erős hitelesítés nem zárja ki a felhasználó megtévesztését, a deepfake-tartalmak jelölése korlátozott védelmet nyújt a szándékosan jogellenes felhasználással szemben, a fizetési szabályozás pedig csak meghatározott megszemélyesítési esetekben ír elő visszatérítést. A három szabályozási eszköz kiegészíti egymást, de nem alkot egységes sértettvédelmi rendszert.

Kulcsszavak: digitális megszemélyesítés; online személyazonosság-lopás; identitáscsalás; eIDAS 2.0; európai digitális személyazonossági tárca; AI Act; deepfake; pénzforgalmi szolgáltatásokról szóló rendelettervezet

Abstract:

This study examines the non-criminal-law instruments through which the European Union responds to digital impersonation. The term is used here as an umbrella covering online identity theft based on the acquisition of authentication credentials, the identity fraud that follows from it, and those cases in which the perpetrator acts in the name of another person or institution without having technically obtained their credentials. Three distinct regulatory areas are analysed: the European Digital Identity Wallet established by eIDAS 2.0, the transparency

[1] a szerző a PTE-ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék adjunktusa

obligations under Article 50 of the Artificial Intelligence Act, and the loss-allocation rules in the proposed Payment Services Regulation for fraudulently induced yet authorised payments. The analysis distinguishes three levels of intervention, namely prevention, recognisability and redress. It shows that strong authentication does not exclude the manipulation of users, that deepfake labelling offers limited protection against intentionally unlawful use, and that payment regulation provides reimbursement only in defined impersonation scenarios. The three instruments complement one another, but they do not form a unified system of victim protection.

Keywords: digital impersonation; identity theft; identity fraud; eIDAS 2.0; EUDI Wallet; AI Act; deepfake; Payment Services Regulation

Bevezetés

Az online térben egyre gyakrabban merül fel a személyazonosság fontossága és védelme, valamint az ezzel kapcsolatos kihívások kezelése. Az online pénzügyi tranzakciók miatt az azonosítás megbízhatósága közvetlen vagyoni következményekkel is járhat. Emellett meg kell még említenünk a mesterséges intelligencia fejlődését, amely lehetővé tette a valósághű képi, hang- és szöveges tartalmak tömeges előállítását. A technológiai fejlődés miatt az identitással kapcsolatos visszaélések már túlnőttek a hitelesítő adatok megszerzésén, és sok esetben egy másik személy vagy intézmény hitelesnek tűnő megjelenítését, valamint az így kiváltott vagyoni rendelkezést is jelenthetik. Az identitáslopással, illetve identitáscsalással összefüggő bűncselekmények elleni fellépésben elsődleges szerepe van a büntetőjognak, de emellett más jogi és nem jogi eszközökkel is szükséges hozzájárulni a prevencióhoz. Az Európai Unió a közelmúltban több jogforrást fogadott el, amelyek érintőlegesen ezeket a problémákat is kezelik.

Fogalmilag fontos elhatárolni egymástól az identitással kapcsolatos különféle visszaéléseket. Jelen tanulmányban a digitális megszemélyesítést használom gyűjtőfogalomként, amely alá három, egymással részben átfedő jelenség tartozik. Az online személyazonosság-lopás azt az esetet jelöli, amikor az elkövető más személyhez kapcsolódó azonosító adatokat, hitelesítő eszközt, illetve hozzáférési jogosultságot szerez meg jogellenes módon. Az identitáscsalás fogalmába azokat az eseteket soroljuk, amikor az elkövető a már megszerzett adatokkal visszaéléseket követ el, így például vagyoni haszonra tesz szert vagy reputációs veszteséget okoz. A szűkebb értelemben vett megszemélyesítés pedig azt az esetkört fogja át, amelyben az elkövető úgy lép fel más személy vagy intézmény nevében, hogy annak hitelesítő adatait technikailag nem szerezte meg. A három jelenség így részben átfedheti egymást. Közös elemük, hogy a sértett vagy az információs rendszer az online térben tévesen tulajdonít identitást, jogosultságot vagy intézményi minőséget az elkövetőnek. Az ilyen jellegű támadások elsősorban arra építenek, hogy a

hitelesítő adatokat technikai szinten kompromittálják, illetve, hogy az identitáshoz fűződő bizalmat manipulálják.[2]

A kutatás aktualitását az adja, hogy két, a téma szempontjából meghatározó uniós jogforrás a közelmúltban lépett hatályba, egy harmadik szabályozás jogalkotási folyamata pedig előrehaladott állapotban van. Az eIDAS 2.0 2024. május 20-án lépett hatályba, a tagállamoknak pedig a kapcsolódó végrehajtási rendeletekre figyelemmel 2026 végéig kell legalább egy európai digitális személyazonossági tárcát biztosítaniuk. Az AI Act 2024. augusztus 1-jén lépett hatályba, az 50. cikk vizsgált szabályai pedig 2026. augusztus 2-től alkalmazandók. A pénzforgalmi rendelettervezet 2026. augusztus 7-én még a Tanács első olvasatbeli álláspontjára várt. A jelenség pénzforgalmi jelentőségét az EBA és az EKB 2025-ös közös jelentése is mutatja. Az EGT-ben a jelentett fizetési csalások összértéke 2024-ben 4,2 milliárd euró volt. Ezen belül az átutalási csalások értéke megközelítette a 2,5 milliárd eurót, az azokból eredő veszteség pedig 2,2 milliárd eurót tett ki. Az átutalási csalások veszteségének mintegy 85 százalékát a felhasználók viselték, főként a fizető felek megtévesztésére épülő csalások miatt.[3]

Tanulmányom célja annak vizsgálata, hogy e jogforrások milyen védelmet biztosítanak a digitális megszemélyesítéssel szemben, milyen szabályozási korlátok figyelhetők meg, és a rendszerek a jövőben hogyan fejleszthetők tovább. A módszertan[4] egyrészt kritikai jogi elemzésre épül, másrészt feldolgozom a vonatkozó szakirodalmat, és ezek alapján jogalkotási javaslatokat fogalmazok meg.

Az eIDAS 2.0 és az európai digitális személyazonossági tárca

Az első, a tanulmány szempontjából releváns jogforrás az úgynevezett eIDAS 2.0 rendelet. Az elektronikus azonosítás és a bizalmi szolgáltatások első közös uniós keretét a 2014-ben elfogadott eIDAS-rendelet hozta létre. Ezt módosította a 2024. április 11-én elfogadott eIDAS 2.0, amely 2024. május 20-án lépett hatályba. A módosítás középpontjában az európai digitális személyazonossági tárca áll. A tagállamoknak legalább egy ilyen tárcát kell biztosítaniuk, amely köz- és magánszolgáltatásokhoz nyújt biztonságos, megbízható és határokon átnyúló hozzáférést.

[2] Idomeneas Mokkas: An In-Depth Examination of GDPR and eIDAS in the Prevention of Identity Theft. Information Law Journal, 2024, 2. sz. 2–4. DOI: 10.26262/infolawj.v5i2.10491.

[3] Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete, 2. cikk és az e rendelettel módosított 910/2014/EU rendelet 5a. cikk (1) bekezdés; Európai Bizottság: European Digital Identity (EUDI) Regulation, https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation;
az Európai Parlament és a Tanács (EU) 2024/1689 rendelete, 50. és 113. cikk; az Európai Parlament és a Tanács (EU) 2026/1744 rendelete, 1. cikk 39. pont b) alpont; Európai Parlament, Legislative Observatory: Payment services in the internal market, 2023/0210(COD), https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023%2F0210%28COD%29;
Európai Bankhatóság – Európai Központi Bank: Joint EBA-ECB report on payment fraud: strong authentication remains effective but fraudsters are adapting. 2025. december 15. https://www.eba.europa.eu/publications-and-media/press-releases/joint-eba-ecb-report-payment-fraud-strong-authentication-remains-effective-fraudsters-are-adapting (utolsó hozzáférés: 2026. augusztus 7.).

[4] A fordítási és szövegellenőrzési feladatokhoz nagy nyelvi modelleket, Claude Opus 5-öt és OpenAI ChatGPT 5.6-ot használtam.

A rendelkezés jelentősége az identitáslopás szempontjából abban áll, hogy egységesen ellenőrzött azonosítási infrastruktúrát teremt. Erre az infrastruktúrára adatvédelmi, biztonsági, tanúsítási és incidenskezelési követelmények épülnek, amelyek megnehezítik a hamis vagy jogosulatlan identitáshasználatot, és egyúttal lehetővé teszik a már bekövetkezett kompromittálódás gyorsabb kezelését (5a. cikk (1) bekezdés és 5c. cikk).[5]

A tárca használata során a felhasználónak nem kell minden esetben a teljes személyes adatkészletét átadnia. Ha például egy szolgáltatás igénybevételéhez kizárólag a nagykorúság igazolása szükséges, elegendő lehet ennek a tulajdonságnak a közlése a név, a pontos születési idő és a lakcím feltárása nélkül. A szelektív adatközlés így nemcsak az adatvédelem szintjét emeli. Az identitáslopás lehetséges alapanyagát is szűkíti, mert egy adatot kérő fél vagy egy későbbi adatszivárgás révén kevesebb, más személy megszemélyesítésére alkalmas információ válhat hozzáférhetővé (5a. cikk (4) bekezdés a) pont).

A magas biztonsági szint, a beépített biztonság és a tárcaadatok más adatoktól való logikai elkülönítése tovább csökkenti annak kockázatát, hogy egy bűnelkövető egyszerűen átvegye a felhasználó digitális identitását. Másik oldalról viszont e követelmények nem teszik lehetetlenné a hitelesítő eszköz kompromittálását. Egy feloldott állapotban megszerzett telefon, rosszindulatú program vagy a felhasználót távoli hozzáférés engedélyezésére rávevő megtévesztés mellett a technikailag biztonságos tárca is támadási felületté válhat. Mivel a tárca több azonosító adatot és jogosultságot egyetlen infrastruktúrában kapcsol össze, kompromittálódása egyszerre több szolgáltatásban is növelheti a visszaélés következményeit. A szabályozás tehát az illetéktelen hozzáférés valószínűségét és a megszerezhető adatok körét mérsékli, de a felhasználói magatartást kihasználó támadásokat nem zárja ki (5a. cikk (11), (12) és (14) bekezdés).[6]

Prevenciós szempontból fontos az is, hogy a felhasználó egy közös kezelőfelületen áttekintheti a tárcával végzett műveleteket és az adatot kérő feleket. Innen kérheti személyes adatainak törlését, és jelezheti a gyanús adatkérést is. A tárcára támaszkodó szolgáltatónak előzetesen regisztrálnia kell, meg kell jelölnie a kért adatok körét, majd a felhasználó előtt is azonosítania kell magát. Ennek gyakorlati jelentősége különösen akkor mutatkozik meg, amikor a bűnelkövető banknak vagy hatóságnak adja ki magát. Az ellenőrzött tárcakörnyezetben a felhasználó nem pusztán saját magát igazolja, hanem arról is megbízhatóbb információt kaphat, hogy valóban a megjelölt szervezet kéri-e az adatot. A védelem ugyanakkor nem

[5] Az (EU) 2024/1183 rendelettel módosított 910/2014/EU rendelet 5a. cikk (1) bekezdés és 5c. cikk; Sanna Wong-Toropainen: Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework. In: K. Prifti et al. (szerk.): Digital Governance. T.M.C. Asser Press, 2024, 117–123., DOI: 10.1007/978-94-6265-639-0_6.

[6] Az (EU) 2024/1183 rendelettel módosított 910/2014/EU rendelet 5a. cikk (4) bekezdés a) és d) pont, (8), (11), (12) és (14) bekezdés, valamint 5b. cikk (1)–(3) és (7)–(9) bekezdés; Mokkas: i. m., 3–4.; Maryline Laurent – Claire Levallois-Barth: European Digital Identity Wallets: How Secure Are They and What Are the Risks? The Conversation, 2026. április 14. DOI: 10.64628/AAK.3ttgpkpvd; HAL: hal-05624583.

terjed ki automatikusan a telefonon, elektronikus levélben vagy más külső csatornán megvalósuló megtévesztésre (5a. cikk (4) bekezdés d) pont és 5b. cikk (1)–(3), valamint (7)–(9) bekezdés).

A rendelet a kompromittálódás felismerését követő beavatkozás kérdéskörével is foglalkozik. A tárca érvényességét vissza kell tudni vonni, ha annak biztonsága sérült, és a felhasználó számára könnyen elérhető technikai segítséget, valamint incidensbejelentési lehetőséget kell biztosítani. A biztonsági rés által érintett tárcák használatát késedelem nélkül fel kell függeszteni, súlyos vagy tartós probléma esetén pedig vissza kell vonni. Ez az identitáslopás szempontjából azért fontos, mert az első jogosulatlan felhasználást követően megakadályozhatja ugyanazon hitelesítő eszköz ismételt felhasználását. A rendelkezések így nem feltétlenül előzik meg az első károkozást, de korlátozhatják a megszerzett digitális identitással elkövethető további visszaéléseket (5a. cikk (9) és (10) bekezdés, valamint 5e. cikk).

Az eIDAS 2.0 rendelet korlátai

A szabályozás egyik érzékeny pontja a kizárólagos felhasználói kontrollra épülő modell. A technikai értelemben vett kontroll azt biztosítja, hogy a tárcával végzett művelet a jogosult felhasználó eszközéhez legyen köthető. Ebből azonban nem következik, hogy a felhasználó a művelet valódi célját ismerte, vagy döntését külső befolyástól mentesen hozta meg. Az elkövető például telefonon ráveheti a sértettet arra, hogy maga mutasson be egy igazolást vagy hagyjon jóvá egy műveletet. A rendszer ilyenkor technikailag szabályosan működik, miközben a döntést megtévesztés alakítja. Kjørven, Gjøsteen és Wærstad arra figyelmeztetnek, hogy a kriptográfiai kontroll jogi vélelemmé alakítása a csalás, a kényszer és a társadalmi manipuláció kockázatát a felhasználóra terhelheti. Különösen azok kerülhetnek hátrányba, akik digitális készségeik, fogyatékosságuk vagy más személy segítségére utaltságuk miatt a gyakorlatban nem tudnak teljes önállósággal eljárni. A szerzők ezért olyan jogi és technikai biztosítékokat sürgetnek, amelyek a csalárd használat lehetőségét elismerik, de nem teszik automatikusan felelőssé a sértettet. Az ellenérv ugyanakkor az, hogy a kizárólagos kontroll az illetéktelen hozzáféréssel szembeni alapvető biztonsági garancia. Ezért nem annak gyengítése, hanem a manipulált felhasználói döntéshez kapcsolódó kiegészítő helyreállítási szabályok kialakítása indokolt (5a. cikk (4) bekezdés a) pont és (14) bekezdés).[7]

A tárcához kapcsolódó felelősségi szabályok sem jelentenek minden identitáslopással összefüggő helyzetben automatikus kártalanítást. A rendelet a szándékosan vagy gondatlanul okozott kárért fennálló felelősségből indul ki, a részletes igényérvényesítés azonban továbbra is a nemzeti szabályokhoz kapcsolódik. A károsultnak

[7] Az (EU) 2024/1183 rendelettel módosított 910/2014/EU rendelet 5a. cikk (4) bekezdés a) pont és (14) bekezdés; Marte Eidsand Kjørven – Kristian Gjøsteen – Tone Linn Wærstad: Safe and Inclusive or Unsafe and Discriminatory? European Digital Identity Wallets and the Challenges of 'Sole Control'. Computer Law & Security Review, 60 (2026), 106235, DOI: 10.1016/j.clsr.2025.106235.

ezért rendszerint azt is igazolnia kell, hogy a kárt a tagállam, a tárca biztosítója vagy az azonosítási rendszer működtetője által elkövetett kötelezettségszegés okozta. Más a helyzet, ha a tárca technikailag hibátlanul működött, de az elkövető a felhasználót vette rá az adatközlésre vagy a művelet jóváhagyására. Erre a helyzetre az eIDAS 2.0 nem ad önálló kárelosztási szabályt. A szabályozás ezért erős megelőzési és incidenskezelési keretet teremt, de a manipulációból eredő kár rendezését csak közvetetten segíti. A védelem akkor lehetne teljesebb, ha a biztonságos hitelesítést könnyen hozzáférhető helyreállítási eljárás és a felhasználó tényleges döntési helyzetét is értékelő felelősségi gyakorlat egészítené ki (5a. cikk (19) bekezdés és 11. cikk).[8]

A mesterséges intelligenciáról szóló rendelet 50. cikke

A második releváns jogforrás a mesterséges intelligenciáról szóló rendelet, amelyet 2024. június 13-án fogadtak el, és 2024. augusztus 1-jén lépett hatályba. A jogszabály az első átfogó, kockázatalapú uniós keretet hozta létre a mesterséges intelligencia fejlesztésére, forgalomba hozatalára és használatára. Az 50. cikk a szintetikus tartalmak felismerhetőségének hiányából eredő kockázatokat kívánja csökkenteni. A generatív mesterségesintelligencia-rendszer szolgáltatójának biztosítania kell, hogy a rendszer kimenete géppel olvasható formában megjelölt és mesterségesen előállítottként vagy manipuláltként észlelhető legyen. Ettől elkülönül a deepfake-tartalmat előállító vagy manipuláló alkalmazó kötelezettsége, akinek a közzétételkor tájékoztatnia kell a címzettet a tartalom mesterséges eredetéről. Az identitáslopás és az identitáscsalás szempontjából e szabályok azért jelentősek, mert segíthetik a valós személyt, banki ügyintézőt vagy hatósági szereplőt utánzó képi, hang- vagy mozgóképes tartalom felismerését. Az 50. cikk vizsgált kötelezettségei 2026. augusztus 2-től alkalmazandók. A korábban forgalomba hozott, szintetikus tartalmat létrehozó rendszerek szolgáltatói az 50. cikk (2) bekezdésének 2026. december 2-ig kötelesek megfelelni (50. cikk (2), (4) és (5) bekezdése, valamint a 2026/1744 rendelettel módosított 111. cikk (4) bekezdése).[9]

Az AI Act előremutató szabályai

A szabályozás előnye, hogy a speciális átláthatósági kötelezettségeket nem kizárólag egyes magas kockázatú felhasználásokhoz köti. A szolgáltatói jelölés az automati-

[8] Az (EU) 2024/1183 rendelettel módosított 910/2014/EU rendelet 5a. cikk (9), (10) és (19) bekezdés, 5e. cikk és 11. cikk; Kjørven – Gjøsteen – Wærstad: i. m.; Wong-Toropainen: i. m., 130.

[9] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete, 50. cikk (2), (4) és (5) bekezdés; az Európai Parlament és a Tanács (EU) 2026/1744 rendelete (2026. július 8.), HL L, 2026/1744, 2026. július 24., 1. cikk 39. pont b) alpont; Európai Bizottság: Code of Practice on Transparency of AI-Generated Content. 2026. június 10.;
Európai Bizottság: Guidelines on Transparency Obligations for Providers and Deployers of AI Systems. 2026. július 20.; Nicolaj Feltes: Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft? *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 16 (2025), 224–228. és 232–235.

zált felismerést és a tartalom eredetének utólagos vizsgálatát segíti, az alkalmazó tájékoztatása pedig a közzététel társadalmi környezetében figyelmezteti a felhasználót. A két kötelezettség együtt azért lehet hasznos, mert a digitális megszemélyesítés több pontján is ellenőrizhető nyomot hoz létre. A kötelezettségek azonban nem helyettesítik egymást. Az alkalmazó saját, ember számára érzékelhető tájékoztatását nem teljesítheti pusztán a szolgáltató által beágyazott géppel olvasható jelöléssel. Ha például egy mesterségesen előállított banki vezető videóüzenetben sürgős átutalást kér, a technikai jelölés a platformi felismerést, a látható tájékoztatás pedig a címzett óvatosságát támogathatja. Ez nem szünteti meg a megtévesztést, de csökkentheti annak valószínűségét, hogy a szintetikus személyt valódi döntéshozóként fogadják el.

Az AI Act korlátai

Fogalmi bizonytalanságot okozott, hogy a deepfake meghatározása létező személyhez, tárgyhoz, helyhez, szervezethez vagy eseményhez kapcsolja a valósághű utánzást. A Bizottság 2026-ban közzétett iránymutatása azonban a „létező" elemet úgy értelmezi, hogy az olyan személyre vagy más tárgyra is kiterjed, amely a valóságban létezhet vagy létezhetett volna. E megközelítés alapján egy teljesen fiktív, mégis hitelesnek tűnő banki ügyintéző vagy rendőr sem marad szükségképpen kívül a fogalmon. Łabuz korábban cél szerinti értelmezést javasolt, mert álláspontja szerint a kizárólag nyelvtani megközelítés indokolatlan védelmi rést hagyott volna. A gyakorlati védelmi rés ezzel szűkült, jogdogmatikai bizonytalanság azonban maradt, mert a Bizottság iránymutatása nem módosítja a rendelet szövegét, és a bírósági értelmezést sem köti (3. cikk 60. pont).[10]

További probléma, hogy az átláthatósági kötelezettség jogkövető címzettre épül. A megtévesztési céllal eljáró alkalmazó éppen a tartalom mesterséges eredetét kívánja eltitkolni, ezért tőle nem várható, hogy önként elhelyezze a csalást leleplező tájékoztatást. Feltes ennek kapcsán arra mutat rá, hogy a végleges szabályozás előrelépést jelent a bizottsági javaslathoz képest, de a címzetti szerkezet és a kivételek miatt a gyakorlati végrehajtás továbbra is nehéz. Az identitáslopás elleni védelem ezért nem alapulhat kizárólag a tartalmat létrehozó vagy közzétevő személy önkéntes megfelelésén. Szükség van olyan platformi és hatósági ellenőrzésre is, amely a hiányzó vagy eltávolított jelölést képes felismerni.[11]

Az 50. cikk művészi, kreatív, szatirikus vagy fiktív művek esetében korlátozottabb tájékoztatást követel meg, a közérdekű tájékoztatás céljából közzétett szintetikus szövegnél pedig emberi felülvizsgálat és szerkesztői felelősség mellett kivételt

[10] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete, 3. cikk 60. pont; Európai Bizottság: Guidelines on Transparency Obligations for Providers and Deployers of AI Systems. 2026. július 20., 107. pont;
Mateusz Łabuz: A Teleological Interpretation of the Definition of DeepFakes in the EU Artificial Intelligence Act–A Purpose-Based Approach to Potential Problems With the Word 'Existing'. Policy & Internet, 17 (2025), e435, DOI: 10.1002/poi3.435.

[11] Feltes: i. m., 232–236.

enged. E megoldások az alkotói szabadság és a sajtó működésének védelmét szolgálják. A Bizottság iránymutatása ugyanakkor a kedvezményes szabályt megszorítóan, csak a nyilvánvalóan művészi, kreatív, szatirikus, fiktív vagy ezekhez hasonló tartalmakra alkalmazza. A pusztán tájékoztató vagy kereskedelmi jelleg önmagában nem alapozza meg a kedvezményt, bár az összetett tartalmak minősítésénél továbbra is maradhat értelmezési vita. Romero Moreno emberi jogi megközelítése jól érzékelteti, hogy a szabályozásnak az átláthatóság mellett a megszemélyesített személy jogait és a tartalom címzettjének védelmét is mérlegelnie kell. Az 50. cikk közvetlen célja ugyanis nem a személyazonosság önálló jogi védelme, hanem a mesterséges tartalmak felismerhetősége és az információs környezet átláthatósága (50. cikk (4) bekezdés és (134) preambulumbekezdés).[12]

A szakirodalmi és végrehajtási vita két irányban mutat. Łabuz a létező személyre utaló fogalom szűkösségét emelte ki, a Bizottság 2026-os iránymutatása viszont tágabb értelmezéssel igyekszik elkerülni ezt a védelmi rést. Meding és Sorge ezzel párhuzamosan arra figyelmeztetnek, hogy a manipuláció és a jogszerű tartalomfeldolgozás közötti határ elmosódhat, Makauskaite-Samuole pedig az átláthatósági kötelezettségek arányosságát és egyensúlyát vizsgálja kritikusan. Az eltérő álláspontok az identitáslopás szempontjából ugyanarra a szabályozási dilemmára vezethetők vissza. A túl szűk fogalom védtelenül hagyhat valós megtévesztési helyzeteket, a túl tág fogalom viszont olyan ártalmatlan szerkesztést is azonos kötelezettség alá vonhat, amely nem alkalmas identitáscsalásra. A végrehajtásban ezért a megtévesztésre való alkalmasságot és az utánzott személyhez vagy intézményi minőséghez kapcsolódó bizalmi hatást is értékelni kell.[13]

Az AI Act továbbfejlesztésének lehetséges irányai

Az identitáslopással összefüggő kockázatok csökkentése érdekében az átláthatósági szabályokat gyors bejelentési, vizsgálati és tartalomkorlátozási eljárásokkal kell összekapcsolni. A teljesen fiktív, de valós intézményi minőséget utánzó személyek bevonását jogszabályi szinten is egyértelművé kellene tenni. Emellett olyan műszaki szabványokra van szükség, amelyek a tartalom eredetét a létrehozástól a közzétételig ellenőrizhetővé teszik, és jelzik azt is, ha a jelölést eltávolították vagy megsértették. A platformoknak könnyen elérhető bejelentési csatornát kell biztosítaniuk a megszemélyesített személy és a megtévesztett címzett számára.

---

[12] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete, 50. cikk (4) bekezdés és (134) preambulumbekezdés; Európai Bizottság: Guidelines on Transparency Obligations for Providers and Deployers of AI Systems. 2026. július 20., 119–123. pont; Felipe Romero Moreno: Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content. International Review of Law, Computers & Technology, 38 (2024) 3, 297–326, különösen 305–317. DOI: 10.1080/13600869.2024.2324540.

[13] Łabuz: i. m.; Kristof Meding – Christoph Sorge: What Constitutes a Deep Fake? The Blurry Line Between Legitimate Processing and Manipulation under the EU AI Act. In: Proceedings of CSLAW '25, 2025, 152–159., DOI: 10.1145/3709025.3712218;
Gintare Makauskaite-Samuole: Transparency in the Labyrinths of the EU AI Act: Smart or Disbalanced? Access to Justice in Eastern Europe, 8 (2025) 2, 38–68., DOI: 10.33327/AJEE-18-8.2-a000105.

A jövőbeli védelemnek a tartalom felismerhetőségén túl a további károk megelőzésére is ki kell terjednie. Ha a szintetikus tartalom pénzügyi szolgáltató, hatóság vagy más bizalmi szereplő nevében kér adatot vagy fizetést, a platformi jelzést gyorsan továbbíthatóvá kell tenni az érintett szervezetnek, a hírközlési szolgáltatónak és szükség esetén a pénzforgalmi szolgáltatónak. Ilyen együttműködés mellett a jelölési kötelezettség nem pusztán tájékoztatási szabály maradna, hanem egy szélesebb megelőzési rendszer kiindulópontjává válhatna.

Az említett platformi intézkedések részben a digitális szolgáltatásokról szóló rendelet már hatályos rendszerére építhetők. A DSA 16. cikke a jogellenes tartalmak bejelentésére és kezelésére, 22. cikke a megbízható bejelentőkre, 34–35. cikke pedig a nagyon nagy online platformok és keresőprogramok rendszerszintű kockázatértékelésére és kockázatcsökkentésére tartalmaz szabályokat. E rendelkezések azonban nem állapítanak meg minden szintetikus tartalomra általános jelölési kötelezettséget, ezért az AI Act 50. cikkét kiegészítik, nem helyettesítik.

A pénzforgalmi szolgáltatásokról szóló rendelettervezet és a megtévesztéssel kiváltott, mégis engedélyezett fizetések

A harmadik releváns jogforrás a belső piaci pénzforgalmi szolgáltatásokról szóló rendelettervezet, amelyet az Európai Bizottság 2023. június 28-án terjesztett elő. A Parlament és a Tanács közötti intézményközi megállapodás szövegét az ECON bizottság 2026. május 5-én jóváhagyta. Az eljárás 2026. augusztus 7-én még a Tanács első olvasatbeli álláspontjára várt, ezért a rendelet ekkor nem lépett hatályba. A végleges kompromisszumos szöveg szerint a jövőbeli rendelet a Hivatalos Lapban való kihirdetését követő huszadik napon lép hatályba, és fő szabályait huszonegy hónappal később kell majd alkalmazni. Kivételt képez többek között a kedvezményezett nevének és egyedi azonosítójának egyezését ellenőrző szolgáltatáshoz kapcsolódó 50. és 57. cikk, amelyek huszonhét hónappal a hatálybalépés után válnának alkalmazandóvá (112. cikk). A javaslat célja a pénzforgalmi szabályok egységesítése, a fogyasztóvédelem erősítése és az új csalási módszerek kezelése. Az identitáslopás szempontjából azért releváns, mert a megszerzett vagy megtévesztően felépített identitás használata gyakran egy fizetési rendelkezés kiváltásával okoz vagyoni kárt.[14]

[14] Európai Bizottság: Proposal for a Regulation on payment services in the internal market, COM(2023) 367 final, 2023. június 28.; Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations, PE787.675, 2026. május 5.; Az Európai Unió Tanácsa: ST 8221/26, 2026. április 17., 112. cikk; Európai Parlament, Legislative Observatory: Payment services in the internal market, 2023/0210(COD), https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023%2F0210%28COD%29 (utolsó hozzáférés: 2026. augusztus 7.).

Paradigmaváltás az engedélyezett, mégis csalárd fizetési műveletek kezelésében

A hatályos második pénzforgalmi irányelv az engedélyezés tényéhez köti a veszteségviselés kiindulópontját. Ha az elkövető a sértett hitelesítő adataival, de annak akarata nélkül indít fizetést, a művelet nem engedélyezett. Ha viszont a sértett a megtévesztés hatására maga hagyja jóvá az átutalást, a művelet főszabály szerint engedélyezett marad. Ez a különbség az identitáscsalásoknál különösen jelentős. Az első esetben az elkövető technikailag átveszi a sértett fizetési identitását, a másodikban pedig a bank, hatóság vagy más megbízható szereplő identitásával visszaélve a sértett saját közreműködését váltja ki. A második pénzforgalmi irányelv az utóbbi helyzetre nem biztosít általános visszatérítési jogot.[15]

A kompromisszumos szöveg fenntartja az engedélyezett és a nem engedélyezett műveletek elhatárolását, de az eltérő jogkövetkezmények közötti rést részben szűkíti. Nem engedélyezett műveletnél a szolgáltatónak főszabály szerint haladéktalanul, legkésőbb a következő munkanap végéig vissza kell térítenie az összeget. A megtévesztés hatására jóváhagyott fizetés ezzel szemben engedélyezett marad, mégis önálló visszatérítési kötelezettség kapcsolódhat hozzá, ha a törvényben meghatározott megszemélyesítési feltételek teljesülnek. A megoldás erőssége, hogy felismeri a technikai jóváhagyás és a valós döntési szabadság közötti különbséget. Korlátja, hogy a védelem nem minden megtévesztéssel kiváltott fizetésre, hanem csak szűken meghatározott esetkörre terjed ki (54., 56. és 59. cikk).[16]

A szabályozás jelentőségét növeli, hogy az azonnali átutalásoknál a pénz rövid idő alatt elhagyhatja a sértett számláját, így a téves vagy csalárd rendelkezés visszahívására egyre kisebb gyakorlati lehetőség marad. Az (EU) 2024/886 rendelet a kedvezményezett nevének és számlaazonosítójának ellenőrzését az euróövezeti pénzforgalmi szolgáltatóknál 2025. október 9-től már alkalmazandóvá tette. A készülő pénzforgalmi rendelet ezt az ellenőrzést az (EU) 260/2012 rendelet hatályán kívüli átutalásokra is kiterjesztené, és a fizetési művelet mindkét oldalán végzett megfigyeléssel egészítené ki. Ezek a megoldások még a teljesítés előtt jelezhetik, ha az elkövető által megadott címzett eltér attól, akinek a sértett fizetni kívánt. Az identitáscsalás azonban akkor is sikeres lehet, ha a sértett a figyelmeztetés ellenére a megszemélyesített személy utasítását követi. A megelőzési és a visszatérítési szabályoknak ezért együtt kell működniük.[17]

---

[15] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (PSD2), 64. és 72–74. cikk; Nanne Johanna Taavitsainen: Trust to Exploitation: The Legal and Societal Implications of Payment Fraud and the Path Toward Stronger Protections. Åbo Akademi University, mesterszakos szakdolgozat, 2025, 19. és 58–62.

[16] Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations, PE787.675, 2026. május 5., 54., 56. és 59. cikk; Európai Parlament, Legislative Observatory, 2023/0210(COD), https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023%2F0210%28COD%29.

[17] Az Európai Parlament és a Tanács (EU) 2024/886 rendelete (2024. március 13.), az (EU) 260/2012 rendeletbe beillesztett 5c. cikk (1) és (9) bekezdés; Európai Parlament, ECON: Payment Services in the Internal Market – Text Agreed at Early Second Reading Interinstitutional Negotiations. PE 787.675, 2026. május 5., 50. és 57. cikk; Taavitsainen: i. m., 44–49.

A védelem személyi és tárgyi határai

A visszatérítési védelem csak akkor nyílik meg, ha a fogyasztót olyan harmadik személy manipulálta, aki a fogyasztó saját fizetési szolgáltatójának adta ki magát, és ehhez a szolgáltatóhoz köthető kommunikációs csatornát használt. A fogyasztónak a csalást indokolatlan késedelem nélkül jeleznie kell a szolgáltatónak, és rendőrségi feljelentést is kell tennie. A feltételek teljesülése esetén a szolgáltató főszabály szerint a csalárd módon engedélyezett fizetés teljes összegét visszatéríti. A szabály előremutató, mert a banki identitással való visszaélést nem egyszerűen a fogyasztó hibás döntésének tekinti, hanem olyan kockázatnak, amelyhez a szolgáltató oldalán is felelősséget kapcsol. A védelem ugyanakkor csak fogyasztót illet meg, és nem terjed ki minden olyan helyzetre, amelyben a fizetést más személyazonosságának vagy intézményi minőségének felhasználásával csalták ki (59. cikk).[18]

A jogalkotási folyamatban ennél szélesebb megoldás is felmerült. Az Európai Parlament 2024-es álláspontja a fizetési szolgáltató mellett más releváns köz- vagy magánjogi szervezet megszemélyesítésére is kiterjesztette volna a védelmet, ez azonban nem került be a végleges kompromisszumba. A jogalkotói különbségtétel kockázatelosztási szempontból azzal indokolható, hogy a szolgáltatóhoz köthető kommunikációs csatorna a bank ellenőrzési köréhez kapcsolódik, míg más személyek vagy intézmények megszemélyesítése rendszerint kívül esik azon. Kriminológiai és sértettvédelmi szempontból ugyanakkor a különbség kevésbé egyértelmű. A rendőrnek, adóhatóságnak, ügyvédnek vagy bajba jutott családtagnak kiadott elkövető ugyanúgy az identitáshoz kapcsolódó bizalmat használja fel, mint a bank nevében fellépő csaló. A szűkebb hatály kiszámíthatóbbá teszi a szolgáltatói kockázatot, de éppen azokat az áldozatokat hagyhatja védelem nélkül, akik a leginkább meggyőző társadalmi szerepeknek hisznek. Indokolt lenne ezért a későbbi felülvizsgálat során azt vizsgálni, hogy a visszatérítés a hasonlóan erős bizalmi helyzetet kihasználó megszemélyesítésekre is kiterjeszthető-e.[19]

A súlyos gondatlanság szerepe a kárelosztásban

A visszatérítés tényleges terjedelmét jelentős részben a súlyos gondatlanság kivétele határozza meg. Ez nem büntetőjogi bűnösségi forma, hanem a fogyasztó és a fizetési szolgáltató közötti veszteségviselést befolyásoló magatartási mérce. Ha a fogyasztó csalárdul vagy súlyosan gondatlanul járt el, nem részesül visszatérítésben. A bizonyítás a szolgáltatót terheli, amelynek az értékelés előtt lehetőséget kell adnia a fogyasztó számára az események ismertetésére. Az információ hiánya önmagá-

[18] Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations, PE787.675, 2026. május 5., 59. cikk.

[19] Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations, PE787.675, 2026. május 5., 59. cikk; az Európai Parlament 2024. április 23-i jogalkotási állásfoglalása a belső piaci pénzforgalmi szolgáltatásokról, P9_TA(2024)0298.

ban nem elegendő a súlyos gondatlanság megállapításához. Figyelembe kell venni a csalás újszerűségét és összetettségét, a manipuláció módját, a fogyasztó korábbi áldozattá válását, sérülékenységét és a szolgáltató konkrét figyelmeztetését is. Ez a megközelítés azért fontos az identitáscsalásnál, mert a sértett döntése rendszerint nem elszigetelten, hanem egy hitelesnek tűnő szereplő által felépített nyomáshelyzetben születik (59. cikk (3) és (4) bekezdés, valamint (82) preambulumbekezdés).[20]

Braithwaite a súlyos gondatlanságot olyan nehezen megragadható fogalomként írja le, amely több pénzforgalmi kárelosztási rendszer kritikus pontján a bank visszatérítési felelősségének legfontosabb gyakorlati korlátjává válik. Az angol jog, az uniós és brit pénzforgalmi szabályozás, valamint a pénzügyi ombudsmani gyakorlat elemzése alapján arra jut, hogy a mérce tartalma és konkrét alkalmazása között jelentős bizonytalanság marad. A modern csalási ügyekben egy egyszeri kód átadása, egy banki alkalmazásban elvégzett művelet vagy a távoli hozzáférés engedélyezése önmagában nem mutatja meg, hogy a sértett magatartása mennyire tért el az észszerűen elvárhatótól. Ehhez a megtévesztés felépítését és a sértett helyzetét is vizsgálni kell. A szerző ezért a jelenlegi megoldás újragondolását és egy világosabb szabályozási mérce kialakítását sürgeti. Ez az identitáscsalás áldozatai számára azért lényeges, mert a súlyos gondatlanság túl tág értelmezése a látszólagos fogyasztóvédelem ellenére visszaháríthatja rájuk a teljes kárt.[21]

Kárelosztás és közvetítői felelősség

A rendelettervezet a megtévesztéssel okozott fizetési kárt nem az elkövető büntetőjogi felelősségének megállapításával kezeli. A veszteséget a fogyasztó és a fizetési szolgáltató között osztja el, és ezzel a csalás gazdasági következményét rendezi. Ez önmagában nem akadályozza meg az identitás megszerzését vagy a megtévesztő kapcsolatfelvételt, mégis jelentős megelőzési hatása lehet. Ha a szolgáltató meghatározott esetekben viseli a kárt, erősebb érdeke fűződik a megszemélyesítési minták felismeréséhez, a kommunikációs csatornák védelméhez és a célzott figyelmeztetésekhez. A szakirodalomban ugyanakkor vita van arról, hogy a bankokra helyezett szélesebb felelősség mennyiben arányos, illetve milyen költségeket hárít át a pénzforgalmi rendszer egészére. A szélesebb visszatérítési kötelezettség morális kockázatot is teremthet, mert gyengítheti a felhasználók óvatossági ösztönzőit, és a költségeket díjak formájában a fogyasztók szélesebb körére háríthatja. A felelősség bővítését ezért célzott figyelmeztetésekhez, együttműködési kötelezettséghez és a súlyos gondatlanság világos mércéjéhez kell kapcsolni. A szabályozás értéke

[20] Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations, PE787.675, 2026. május 5., 59. cikk (3) és (4) bekezdés, valamint (82) preambulumbekezdés.

[21] Jo Braithwaite: Gross Negligence in Bank Payments Law. Oxford Journal of Legal Studies, 46 (2026) 2, 308–337., DOI: 10.1093/ojls/gqag002.

nem pusztán a visszatérített összegben, hanem az ösztönzők megfelelő elosztásában mérhető.[22]

A csalás megelőzése nem marad kizárólag a bankok feladata. A kompromisszumos szöveg a tárhelyszolgáltatók, az elektronikus hírközlési szolgáltatók, valamint a nagyon nagy online platformok és keresőprogramok közötti gyorsabb információcserét is előírja. A hírközlési szolgáltatóknak technikai és szervezési intézkedéseket kell tenniük a hívószám vagy az elektronikus levélcím manipulációjával megvalósuló megszemélyesítés felismerésére és megelőzésére. A nagyon nagy platformoknak a szabályozott pénzügyi szolgáltatások hirdetőiről is ellenőrző információkat kell kérniük. Ezek a szabályok az identitáscsalás korábbi szakaszában avatkoznak be, mert a hamis kommunikáció és a megtévesztő hirdetés terjedését célozzák. A közvetítők azonban nem válnak a fogyasztóval szemben általánosan visszatérítésre kötelezetté. Egy tárhelyszolgáltató csak szűk feltételek mellett köteles megtéríteni a fizetési szolgáltató által viselt veszteséget. A javaslat tehát helyesen ismeri fel a több szereplőn átívelő megelőzés szükségességét, de a közvetlen sértetti igény továbbra is alapvetően a fizetési szolgáltatóval szemben érvényesíthető (59a., 59b. cikk és 78. cikk (1a) bekezdés).[23]

Összegzés

A három szabályozási eszköz eltérő ponton avatkozik be a digitális megszemélyesítés folyamatába. Az eIDAS 2.0 az azonosító adatok és jogosultságok biztonságos használatával elsősorban a megelőzést szolgálja. A mesterséges intelligenciáról szóló rendelet 50. cikke a szintetikus megszemélyesítés felismerhetőségét javítja. A pénzforgalmi rendelettervezet pedig a megtévesztéssel kiváltott fizetés után rendezi a veszteség viselését, és egyes közvetítőket a csalás megelőzésébe is bevon. E szabályozások közös értéke, hogy a büntetőjogi felelősség megállapításától függetlenül is képesek csökkenteni a kockázatot vagy enyhíteni a már bekövetkezett kárt.

A három funkció mentén az eIDAS 2.0 a megelőzésben a legerősebb, az AI Act a felismerhetőséget szolgálja közvetlenül, a PSR pedig a kárrendezéshez kapcsolódik. A funkciók ugyanakkor nem válnak el teljesen. Az eIDAS incidenskezelése a további károkat is korlátozhatja, az AI Act jelölése megelőző hatást fejthet ki, a PSR felelősségi szabályai pedig erősebb megelőzésre ösztönzik a szolgáltatókat. Közvetlen kártalanítási mechanizmust azonban csak a PSR tartalmaz, és az is szűk feltételek mellett.

Előremutató, hogy az uniós szabályozás nem kizárólag a felhasználó hitelesítésére összpontosít. Az eIDAS 2.0 az adatot kérő fél ellenőrizhetőségét és a komp-

[22] Matthias Bauer – Andrea Dugo – Dyuti Pandya: Shared Liability: The European Parliament's Misstep in Fighting Financial Fraud. ECIPE Policy Brief, 21/2024, különösen 1–7. és 12–13.; Taavitsainen: i. m., 58–62.

[23] Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations, PE787.675, 2026. május 5., 59a–59b. cikk és 78. cikk (1a) bekezdés; Az Európai Unió Tanácsa: ST 8221/26, 2026. április 17., 59a–59b. cikk, 78. cikk (1a) bekezdés és (96b)–(96d) preambulumbekezdések.

romittált tárca felfüggesztését is biztosítja. Az AI Act a tartalom létrehozóján túl a közzétevőt is kötelezi, a pénzforgalmi rendelettervezet pedig felismeri, hogy a technikailag engedélyezett fizetés mögött is állhat megtévesztés. A három megoldás ezzel a támadás különböző összetevőire reagál. Védi a hitelesítő infrastruktúrát, növeli a megtévesztő tartalom felismerhetőségét és bizonyos esetekben leveszi a teljes vagyoni veszteséget a sértettről.

A szabályozási környezet ennek ellenére töredezett marad. A biztonságos tárcahasználat nem bizonyítja a felhasználó valós és befolyásmentes akaratát. A szintetikus tartalmak jelölése a tudatosan jogellenes alkalmazóval szemben önmagában kevés, a teljesen fiktív intézményi személyek bevonása pedig jelenleg a Bizottság tág, nem kötelező erejű iránymutatására épül. A pénzforgalmi visszatérítés pedig a fizetési szolgáltató megszemélyesítésére szűkül, miközben a hatóság, az ügyvéd vagy a családtag nevével visszaélő elkövető azonos bizalmi mechanizmust használhat. További bizonytalanságot okoz, hogy a súlyos gondatlanság értelmezése a gyakorlatban jelentősen meghatározhatja a sértetti védelem terjedelmét.

A büntetőjog az elkövető utólagos felelősségre vonását és szankcionálását biztosítja, de önmagában nem hozza létre a biztonságos azonosítási infrastruktúrát, nem teszi felismerhetővé a szintetikus tartalmat, és nem rendezi automatikusan a sértett és a szolgáltató közötti veszteségviselést. A vizsgált nem büntetőjogi eszközök ezért nem helyettesítik, hanem az elkövetés előtti megelőzés, az elkövetés közbeni felismerés és az azt követő kárrendezés oldaláról egészítik ki a büntetőjogi fellépést.

Magyarországon az eIDAS 2.0 és az AI Act közvetlenül alkalmazandó uniós rendelet, a PSR pedig elfogadása után szintén közvetlenül alkalmazandó lesz. Ettől függetlenül a tárca biztosítása, a felügyeleti hatáskörök gyakorlása, valamint a panasz- és visszatérítési eljárások működtetése hazai intézményi és jogalkalmazási feladatokat keletkeztet. A szabályok gyakorlati értéke ezért azon is múlik, hogy a magyar hatóságok, pénzforgalmi szolgáltatók és bíróságok összehangoltan kezelik-e a technikailag szabályos, de megtévesztéssel kiváltott identitás- és fizetési műveleteket.

A jövőbeli fejlesztés irányát ezért nem egy új, minden részletet egységesítő jogszabályban, hanem a meglévő rendszerek közötti működő kapcsolatok kialakításában látom. A tárcaszolgáltatóknak, a platformoknak, a hírközlési és a pénzügyi szolgáltatóknak gyorsan továbbítható jelzésekkel kellene összekapcsolniuk a gyanús identitáshasználatot, a szintetikus megszemélyesítést és a rendellenes fizetési műveletet. A helyreállítási eljárásoknak figyelembe kell venniük a felhasználó sérülékenységét és a manipuláció körülményeit. Indokolt továbbá a fiktív intézményi személyek jogszabályi szintű egyértelműsítése, a pénzforgalmi védelem hasonló bizalmi helyzetekre való kiterjesztésének vizsgálata és a súlyos gondatlanság kiszámíthatóbb meghatározása. Így a három eszköz nem csupán egymás mellett működne, hanem összehangoltan járulhatna hozzá a digitális megszemélyesítés megelőzéséhez és felismeréséhez, valamint az abból eredő károk csökkentéséhez.

Irodalomjegyzék

1. Bauer, Matthias – Dugo, Andrea – Pandya, Dyuti: Shared Liability: The European Parliament's Misstep in Fighting Financial Fraud. ECIPE Policy Brief, 21/2024.
2. Braithwaite, Jo: Gross Negligence in Bank Payments Law. Oxford Journal of Legal Studies, 46 (2026) 2, 308–337. DOI: 10.1093/ojls/gqag002.
3. Nicolaj Feltes: Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft? J. Intell. Prop. Info. Tech. & Elec. Com. L. 16 (2025) 222–237.
4. Kjørven, Marte Eidsand – Gjøsteen, Kristian – Wærstad, Tone Linn: Safe and Inclusive or Unsafe and Discriminatory? European Digital Identity Wallets and the Challenges of 'Sole Control'. Computer Law & Security Review, 60 (2026), 106235. DOI: 10.1016/j.clsr.2025.106235.
5. Laurent, Maryline – Levallois-Barth, Claire: European Digital Identity Wallets: How Secure Are They and What Are the Risks? The Conversation, 2026. április 14. DOI: 10.64628/AAK.3ttgpkpvd; HAL: hal-05624583.
6. Łabuz, Mateusz: A Teleological Interpretation of the Definition of DeepFakes in the EU Artificial Intelligence Act–A Purpose-Based Approach to Potential Problems With the Word 'Existing'. Policy & Internet, 17 (2025), e435. DOI: 10.1002/poi3.435.
7. Makauskaite-Samuole, Gintare: Transparency in the Labyrinths of the EU AI Act: Smart or Disbalanced? Access to Justice in Eastern Europe, 8 (2025) 2, 38–68. DOI: 10.33327/AJEE-18-8.2-a000105.
8. Meding, Kristof – Sorge, Christoph: What Constitutes a Deep Fake? The Blurry Line Between Legitimate Processing and Manipulation under the EU AI Act. In: Proceedings of CSLAW '25, 2025, 152–159. DOI: 10.1145/3709025.3712218.
9. Mokkas, Idomeneas: An In-Depth Examination of GDPR and eIDAS in the Prevention of Identity Theft. Information Law Journal, 2024, 2. sz. DOI: 10.26262/infolawj.v5i2.10491.
10. Romero Moreno, Felipe: Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content. International Review of Law, Computers & Technology, 38 (2024) 3, 297–326. DOI: 10.1080/13600869.2024.2324540.
11. Taavitsainen, Nanne Johanna: Trust to Exploitation: The Legal and Societal Implications of Payment Fraud and the Path Toward Stronger Protections. Åbo Akademi University, 2025.
12. Wong-Toropainen, Sanna: Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework. In: Prifti, K. et al. (szerk.): Digital Governance. T.M.C. Asser Press, 2024, 115–136. DOI: 10.1007/978-94-6265-639-0_6.

Jogforrások

1. Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) az elektronikus tranzakciók belső piacon történő elektronikus azonosításáról és bizalmi szolgáltatásairól, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
2. Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról (PSD2).
3. Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet).
4. Az Európai Parlament és a Tanács (EU) 2024/886 rendelete (2024. március 13.) az azonnali euroátutalások tekintetében az (EU) 260/2012 és az (EU) 2021/1230 rendelet módosításáról.
5. Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) az (EU) 910/2014 rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról. HL L, 2024/1183, 2024. április 30.
6. Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (AI Act). HL L, 2024/1689, 2024. július 12.
7. Az Európai Parlament és a Tanács (EU) 2026/1744 rendelete (2026. július 8.) az (EU) 2024/1689, az (EU) 2018/1139 és az (EU) 2023/1230 rendeletnek a mesterséges intelligenciára vonatkozó harmonizált szabályok végrehajtásának egyszerűsítése tekintetében történő módosításáról (Digital Omnibus on AI). HL L, 2026/1744, 2026. július 24.

Hivatalos uniós dokumentumok

1. Európai Parlament, ECON: Payment services in the internal market – text agreed at early second reading interinstitutional negotiations. PE787.675, 2026. május 5.
2. Az Európai Unió Tanácsa: Proposal for a Regulation on payment services in the internal market – Confirmation of the final compromise text with a view to agreement. ST 8221/26, 2026. április 17.
3. Európai Bankhatóság – Európai Központi Bank: Joint EBA-ECB report on payment fraud: strong authentication remains effective but fraudsters are adapting. 2025. december 15. https://www.eba.europa.eu/publications-and-media/press-releases/joint-eba-ecb-report-payment-fraud-strong-authentication-remains-effective-fraudsters-are-adapting (utolsó hozzáférés: 2026. augusztus 7.).

4. Európai Bizottság: Code of Practice on Transparency of AI-Generated Content. 2026. június 10. https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content (utolsó hozzáférés: 2026. augusztus 5.).
5. Európai Bizottság: Guidelines on transparency obligations for providers and deployers of AI systems. 2026. július 20. https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems (utolsó hozzáférés: 2026. augusztus 5.).
6. Az Európai Parlament 2024. április 23-i jogalkotási állásfoglalása a belső piaci pénzforgalmi szolgáltatásokról és az 1093/2010/EU rendelet módosításáról. P9_TA(2024)0298, 2023/0210(COD).
7. Európai Parlament, Legislative Observatory: Payment services in the internal market. 2023/0210(COD). https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023%2F0210%28COD%29 (utolsó hozzáférés: 2026. augusztus 7.).

Mogyoródi Gergely[1]– Sallai János[2]:

A lengyel-magyar rendőri kapcsolat és a lengyel rendőrtisztképzés

Absztrakt:

A magyar-lengyel barátság több mint ezer évre nyúlik vissza. A magyar és a lengyel rendőrség történetében is nagy szerepet játszik a lengyel-magyar barátság és szakmai kapcsolat. Ebben meghatározó, hogy bár eltérő okok miatt, de közel azonos időben jött léte mind két ország állami rendőrsége. A 20 és 21. századok hasonló történelmi tapasztalatai, a hasonló földrajzi, geopolitikai környezet is determinálja a két rendőrség szorosabb együttműködését, amelynek egyik színtere az oktatás, a rendőrtiszt és tiszthelyettes képzés. Ahhoz, hogy képzésben együtt tudjon a két szervezet működni, illik ismerni a másik ország rendőrségének szervezetét, meghatározó jogszabályokat és a képzési rendszerét. E cél megvalósításához nyújt segítséget a tanulmányunk, amikor bemutatja magyar-lengyel rendőri kapcsolat történetét és a lengyel tisztképzés jelenlegi rendszerét.

Kulcsszavak: magyar lengyel, barátság, rendőr, rendőrség, rendőrtisztképzés, főiskola, rendőrakadémia

Abstract:

The friendship between Hungary and Poland dates back more than a thousand years. Polish-Hungarian friendship and professional ties also play a major role in the history of the Hungarian and Polish police forces. A key factor in this is that, although for different reasons, the national police forces of both countries were established at roughly the same time. Similar historical experiences in the 20th and 21st centuries, as well as a similar geographic and geopolitical environment, also drive closer cooperation between the two police forces, one area of which is education–specifically, the training of police officers and non-commissioned officers. In order for the two organizations to collaborate effectively in training, it is essential to understand the structure of the other country's police force, its

[1] Dr Mogyoródi Gergely, főosztályvezető. Nemzetközi Bűnügyi Együttműködési Központ, Bűnügyi Együttműködési Főosztály

[2] Dr Sallai János egyetemi tanár. Kodolányi János Egyetem https://orcid.org/0000-0001-6674-1942 sallai.janos@uni-nke.hu

key legislation, and its training system. Our study contributes to this goal by presenting the history of Hungarian-Polish police relations and the current system of officer training in Poland.

Keywords: Hungarian-Polish, friendship, police, police force, police officer training, college, police academy

1. Bevezető

A lengyel-magyar barátság, kapcsolatok hosszú múltra tehető és kezdete a hasonló időpontra (államalapításra) datálható. Az uralkodó házak közötti kapcsolatok, perszonáluniók, az ezer évig fennállt közös határszakasz, a magyar diákok lengyelországi tanulmányai mind-mind hozzájárultak a jó kapcsolatokhoz, a két nép közötti barátsághoz.

A magyar-lengyel rendőri együttműködésnek a kiinduló alapja, hogy közel azonos időben, az első világháború után jött létre mindkét országban a központi állami rendőrség.

A nemzetközi bűnözés elleni közös fellépés gondolata Magyarországon már az első világháború alatt megszületett és Irk Albert munkájából adódóan ma is olvasható. Irk kriminológiai jegyzeteiben világított rá a nemzetközi együttműködés szükségességére, amely a nemzetközi üzletszerű gonosztevők ellen az egyetlen megoldás lehet. Véleménye szerint a „*kriminalitás modern fejlődésének két legfőbb szimptómája a gonosztevő specializálódásában és elnemzetköziesedésében mutatkozik*."[3] Irk szerint a nemzetközi gonosztevők ellen nem lehet hatékony, ha csak izoláltanlépnek fel az államok. Csak a szervezett nemzetközi fellépés a megoldás. Véleményünk szerint Irk a korát meghaladva jelentette ki, hogy a „szervezés központjában a nemzetközi rendőri tudakozó hivatal állana. Ide futnának össze az egyes államok rendőrhatóságainak telefonhálói." Ennek az új nemzetközi rendőr szervezetnek a fő feladata egyrészt elméleti, tudományos kérdések megoldása és gyakorlati fellépés[4] lenne a legveszélyesebb nemzetközi gonosztevők ellen (nemzetiközi szálloda-tolvajok, kasszafúrók, leánykereskedők stb. ellenőrzése, továbbá nemzetközi pénzpiac, börze kontrolálása). Irk a gyakorlati együttműködéshez elengedhetetlenül fontosnak tartotta egy nemzetközi laboratórium létrehozását, hogy a nyomozásokat ki tudják szolgálni. Mindezeket a háború miatt, csak a háborút követően látta kivitelezhetőnek.

---

[3] Irk Albert (1915) Nemzetközi küzdelem a bűntettesek nemzetközi osztályai ellen. in. Bűnügyi szemle, 1914-1915. 3. évfolyam, 7. sz. 1-5. o.

[4] *„Vegyük fel a következő esetet: mondjuk Budapestre megérkezik egy „nemzetközi" és egy előkelő szállodába köt ki, ahol ugyan nem „dolgozik", de egy „caup"-ot készít elő. A pesti rendőrség a nemzetközi bűntettes albumból felismeri. Ha most a nemzetközi rendőrhivatal szervezve van, ugy haladéktalanul bejelenteni annak megérkezését. A nemzetközi rendőrhivatal pedig erre azonnal az összes államokba szétküldi kérdését, hogy a jelzett nemzetközi gonosztevő ellen nincs-e kibocsátva letartóztatási rendelet? Ha valahonnan igenlő választ kap, értesiti rögtön a pesti rendőrséget, amelyik a mit sem sejtő és pesti működését még meg nem kezdett bűntettest azonnal letartóztatja."*
Forrás: Irk Albert (1915) Nemzetközi küzdelem a bűntettesek nemzetközi osztályai ellen. in. Bűnügyi szemle, 1914-1915. 3. évfolyam, 7. sz. 1-5. o.

Ebben a szellemben a „Nagy Háború" után egyrészt folytatódott az 1914-es monacói rendőrkongresszus elhangzottak szerint újabb nemzetközi rendőrkonferenciák, kongresszusok[5] megszervezése, száz évvel ezelőtt 1923-ban, Bécsben megszületett az Interpol elődje a Nemzetközi Bűnügyi Rendőrség Szervezete.[6] E szervezet újdonsága, hogy immár közbeeső szervezetek kizárásával működtek együtt a tagállamok hivatali szervei.

A fentiekkel párhuzamosan elindult több európai és a világ más államainak rendőrségei között a kétoldalú kapcsolatok[7] felvétele. Ennek keretében magyar rendőr és csendőrtisztviselők szakmai tanulmányutakon jártak Németországban, Lengyelországban, Finnországban[8]. Természetesen a viszonosság elve alapján német, finn, lengyel rendőrtisztviselők is jártak Magyarországon.

2. Lengyel-magyar rendőri kapcsolatok áttekintése.

A nemzetközi kapcsolatok kiépítésében a nemzetközi sport, kulturális rendezvények mindig úttörő szerepet játszottak. Így volt ez a magyar-lengyel rendőri kapcsolatok kezdetén is, amikor sorra került 1927-ben Lengyelországban a magyar-lengyel rendőr futball válogatottak mérkőzésére. A mérkőzés[9] a lengyel felsőszileziai rendőrség fennállásának 5. évfordulójáról szóló megemlékezés rendezvénysorozatába illeszkedett. A mérkőzés mellett több kulturális rendezvényre, szívélyes vendéglátásra is sor került.

A lengyel-magyar rendőri kapcsolatok kiemelkedő állomása volt az 1936-os év, amikor először szeptemberben lengyel delegáció látogatott Magyarországra, majd viszonzásul magyar rendőr-csendőr delegáció járt Varsóban.

Zamorski Kordian a lengyel rendőrség főparancsnoka a látogatás során szívesen tett eleget a magyar rendészeti szaksajtó képviselői kérésének és interjút adott. Az interjúban tájékoztatta az újságírókat, hogy a lengyel kollégáknak két szaklapjuk van a tiszteknek és az altiszteknek, ezen kívül még egy kriminológiai szakfolyóiratuk. Továbbá elmondta, hogy ismerik a magyar csendőrségi és rendőrségi szaklapokat, azokat le is fordítják. Ezen kívül elmondta, hogy Lengyelországban csak egy központi rendőrség van és nincs csendőrség, mint Magyarországon. Zamorski elmondta még a lengyel rendőrségről, hogy a „*Varsóban székelő főparancsnokságnak négy osztálya van: 1. a szemlélőké, 2. a törzsé, amely külön szervezési, sze-*

[5] Sallai János (2022): Nemzetközi rendőr konferencia turizmus. https://uni-pen.hu/files/konferencia/2021/VI.%20Turizmus%20%C3%A9s%20biztons%C3%A1g%20tudom%C3%A1nyos%20konferencia%20tanulm%C3%A1nyk%C3%B6tete_2022.pdf Letöltve 2023.05.13.

[6] Johann Schober (1927): Nemzetközi rendőrség. Az Ujság jubiláris karácsonyi számáénak. Újság 1927. december 25. 8.o.

[7] Borszéki Judit – Sallai János (2022): A nemzetközi rendőri együttműködés kezdetei. BM Szemle 2022. 5. sz. https://ojs.mtak.hu/index.php/belugyiszemle/article/view/8529 letöltve 2023.05.13.

[8] Sallai János (2021): A finn-magyar nemzetközi rendészeti együttműködés a két világháború között. In: V. Turizmus és Biztonság Nemzetközi Tudományos Konferencia tanulmánykötet. 60-75. o.

[9] *„A meccs nívós játékot produkált. Első félidőben a magyarok voltak fölényben (2:0). Második félidőben a vezetést a lengyelek veszik át; azután a magyar kapus egy szép gixerével a meccs eldöntetlenül fejeződött be (3:3)."* **Forrás:** Magyar detektív. 1927. 15. sz. 29. o.

mélyzeti és katonai csoportokra tagozódik, 3. a gazdasági osztály és 4. a bűnügyi központ. Az ország közigazgatásilag ú.n. vajdaságokra oszlik, amelyek székhelyein egy-egy, összesen 17 kerületi rendőr parancsnok áll a kerületekre osztott rendőrség élén. Ezek alá tartoznak a helyi rendőrparancsnokságok, amelyek alatt a biztosságok, kisebb városokban és falvakban pedig az őrsök alkotják a legkisebb egységeket. Varsóban még a zászlóaljparancsnokságnak megfelelő felügyelőségek – a főváros közigazgatási kerületeinek megfelelő számban – vannak közbe iktatva. A parancsnokságok mellett mindenütt bűnügyi nyomozószervek is állanak. A rendőrség működése kizárólag a rend fenntartására, közbiztonsági szolgálatra és bűnügyi nyomozásra szorítkozik, közigazgatási rendészeti tevékenységet és rendőri büntető bíráskodást nem folytatunk. Helyszíni bírságolási jogunk csupán 1 zloty összegű fizetési meghagyás (mandat) kibocsátásra terjed ki. Tisztikarunk és legénységünk a hadseregből egészül ki, csak katonaviselt egyén léphet rendőri szolgálatba. Szolgálatát mindenki, a tisztjelölt is, a legalsó fokon kezdi. A kiképzési időt iskolázottabb embereknél csökkenthetjük, a jogvégzetteknél is azonban körülbelül öt hónapig tart. Vannak azután különleges kiképzések is, pl. ilyen a detektívszolgálatra kiképzés. Erősen specializálunk, még rendőrségi botanikusunk is van."[10]
A lengyel rendőrségnél az altiszti állományt egy alapos 5-6 hónapos kiképzésben[11] részesítik. A lengyel rendőrségnél ekkor már voltak női rendőrök is mind egyenruhás, mint polgári ruhás állományban, és az ő vezetőjük is hölgy volt. Varsóban külön működött egy női rendőriskola, ahol katonai jellegű felkészítés folyt,[12] azzal a különbséggel, hogy a női rendőröket csak a pisztoly használatára készítették fel. A vidéki rendőrségeken nagyon szívesen látták a női rendőröket. A női rendőrök feladat és hatáskörébe a leánykereskedelem, a veszélyes csavargók, munkakerülők, a prostituáltak, a pornográfia, gyermekvédelem és a kábítószer elleni harc tartozott.[13]

A lengyel rendőrök egyenruhája már ekkor is sötétkék színű volt és a rendfokozati jelzésüket a vállukon viselték.

A lengyel főparancsnok és a delegáció tagjai látogatásuk során megtekintették a bűnügyi múzeumot, a budapesti és vidéki főkapitányságot.[14] Hősök emlékművet, ügetőpályán a díszszemlét, székesfehérvári rendőrkapitányságot, visegrádi csendőrőrsöt és a szentendrei csendőr szárnyparancsnokságot, valamint a budapesti Böszörményi utcai csendőrlaktanyát. A szakmai programok mellett nívós szabadidős elfoglaltságot is beiktattak a lengyel látogató csoport tagjainak, pl. a Balatonon. A lengyel rendőr delegáció útjáról hazaérve a lengyel rendőri szaksajtó is hírt adott és nagyon pozitívan értékelték a magyarországi látogatást.

---

[10] Zamorszki Kordian a lengyel rendőrség főparancsnoka Budapesten. Magyar Rendőr, 1936. 19. sz. 442-443. o.

[11] Külföldi szemle. A lengyel államrendőrség. In.: Magyar Közigazgatás. 1937. 13. sz. 7-8. o.

[12] Uo.

[13] Uo.

[14] A főkapitányságon „*Nagy Valér rendőrtanácsosnak mintegy háromnegyed órás németnyelvű előadása következett ezután a bűnügyi szolgálatról, a bűnügyi nyilvántartóról, a nő- és gyermekvédelemről, a híradó szolgálatról, a közlekedési rendőrségről, az erkölcsrendészetről, a rendőrségi jóléti intézményekről, majd dr. Cseténi Imre főkapitányhelyettes tartott rendkívül értékes előadást az ügykörébe tartozó rendőri tevékenységről.*"
Magyar Rendőr, 1936. 19. sz. 442-443. o

A magyar rendőr és csendőrtisztek viszont látogatására még ugyanebben az évben 1936-ben sor került. A lengyel delegáció sikerét igazolta, hogy a magyar rendészeti delegációt kiemelt figyelemmel, érdeklődéssel fogadták, már a határon. A határátkelést követően Poznámban fogadták a magyarokat, ahol a lengyel rendőrséggel megismerkedhettek. A célállomáson a varsói pályaudvaron a lengyel rendőrség főparancsnoka (Zamorski Kordian) fogadta magyar küldöttséget. Ezt követően a szívélyes fogadtatásban részesítették a magyar csoportot, majd Varsó nevezetességeit megmutatták nekik. A következő napon, istentiszteleten vettek részt a vendégek és vendéglátók, majd megkoszorúzták a lengyel rendőrök az emlékhelyét.[15] A magyar rendészeti delegációt a Lengyel Köztársaság elnöke és miniszterelnöke is fogadta, majd részt vettek a lengyel hadsereg díszszemléjén. A következő időszakban a magyar küldöttség Vilnóba utazott, ahol a protokolláris rendezvényeken túl megtekintették a város bűnügyi hivatalát. A vilnói kitérő után a csoport Varsóban a rendőrség tömegekkel szembeni fellépésének új korszerű módszerét tanulmányozhatta a lengyel rendőrkollégák bemutatója által, majd a modern lengyel bűnügyi labort tekintették meg. A tanulmányi út keretén belül megtekintették a lengyel rendőrtiszti és női rendőriskolákat, az ott folyó felkészítést[16]. A program második részét a rendőr lovas félezred bemutatója, akadályverseny és lovas futball zárta. Természetesen itt sem maradhatott ki a rendőrmúzeum meglátogatása, és a lengyel rendőrségi nyilvántartási rendszer megismertetése. A szakmai program végén a lengyel rendőr tartalékok, karhatalmi zászlóalj és egy riadó bemutatására került sor, amely során a helyszínen meggyőződhettek, hogy „*első szirénabúgást követő nyolcadik percben az első csapatszállító kocsi már vad iramban robogott az úton. Ezt követően különböző karhatalmi harcászati gyakorlatokat, majd gázálarcban könnyfakasztó gázgyertyadobásokat mutattak be a rendőrtartalék nagyszerűen képzett csapatai.”*[17]

A két szakmai út hosszú időre megalapozta a magyar-lengyel rendőri együttműködést, barátságot, amelynek a béke éveit lezáró második világháború sem vetett véget, sőt igazi kihívásokat hozott a két nemzetnek. A magyar-lengyel határ[18] történetének fontos fejezete az 1939-es esztendő, amikor visszaállt egy kisebb szakaszon a történelmi magyar lengyel határ. Lengyelország lakossága a náci Németország hadai által való lerohanása és a Molotov-Ribbentrop paktum eredményeként kiszolgáltatottá vált és jelentős részük az ország elhagyása mellett döntött. Ekkor értékelődött fel a nemrég visszaállított lengyel-magyar határ, amely menekülést jelentett a lengyelek tízezrei számára. A lengyel katonák[19] szeptember 20-án indult és a tömeges jellegű átlépése október elején befejeződött. A honvédségi források[20] szerint 4819 tisztet,

[15] A lengyelországi tanulmányút. Szemerjay-Kovács Dénes miniszteri tanácsos és a magyar rendőrségi és csendőrségi delegáció diadalútja Varsóban és lengyel földön. Magyar Rendőr. 1936. 538-542. o.

[16] Uo. 563. o.

[17] Uo. 564. o.

[18] Sallai János (2007) A magyar-lengyel határ története. HISTORIA GRANICY WEGIERSKO-POLSKIEJ. Országos Lengyel Kisebbségi Önkormányzat. Budapest.

[19] Sallai János (2010)Zachować człowieczeństwo. Witeź Zoltán Baló opiekunem polskich uchodźców. In: SLAVICA. XXXIX–XL kötet. 323-330. o.

[20] Sallai János (2011): Egy meg nem jelent cikk a lengyel haderőről. Valóság 2011. 4. szám. 85-91 o.

32.436 katonát[21] irányítottak az internáló táborokba. A lengyel polgári menekültek számát több mint százezerre becsülik, akik hazánkban leltek menedéket.

A második világháború után Magyarország és Lengyelország a közismert történelmi folyamtok révén szovjet befolyási övezetbe kerültek, amelynek egyenes következménye lett, hogy a rendészetben, rendőrségnél is a szovjet mintára való áttérés alól nem lehetett kibújni. A két világháború között kialakult lengyel-magyar rendőri barátság, szakmai kapcsolat azonban nem tört meg, hanem folytatódott. A kapcsolatok felvételének első jelentős eseménye ismét a lengyel-magyar rendőr sportolók találkozója[22] volt 1947-ben, amikor is a magyar rendőr labdarúgó és ökölvívó válogatott Lengyelországba látogatott. A következő állomásaként a „*Keleti pályaudvarra berobog a varsói gyorson Dénes r. őrgy. bajtárs kíséretében, mosolyogva száll le a „lengyel-magyar barátság hete“ keretében a Budapesti Rendőr Egyesület vendégeiként Budapestre érkező*). Konarzewski Józef *rendőrezredes, Varsó rendőri őrségének parancsnoka és Woliuska Heléna r. őrgy. bajtársnő, a varsói rendőrség elnöki osztályának vezetője.*”[23] A látogatás a lengyel rendőr delegáció részére Budapest bemutatásával indult, amely közben a beszélgetések fő témája a második világháború okozta pusztítások és a helyreállítás volt. Megállapították, hogy mindkét ország rendőrsége kiveszi a részét az újjáépítésből, miközben hasonló nehézségekkel küzdenek. Többek között: „*Akárcsak nekünk, lengyel bajtársainknak is meg kellett küzdeniük a kezdet minden nehézségével. Egyenruha, lábbeli, fizetés nélkül kezdték meg szolgálatukat a felszabadult Lengyelországban.*”[24] Mindezt tetőzi, hogy a korábban jól felkészített rendőr állomány nagyon kis része maradt mega testületnél, a bűnügyi statisztika pedig folyamatosan romló közbiztonsági eredményeket mutatott. Mind a két országban a rendőr testületből hiányzó állományt gyorsan kellett pótolni, ezért a rendőr állománynak minden erejét a felkészítésre kellett fordítani. Nemcsak a rendőriskolákon, hanem szabad időben a bajtársi közösségekben is folyamatosan képezték önmagukat. A szovjet minta átvételét jelezte Lengyelországban (is), hogy a „*nevelőtisztek felelősek az egyes alakulatok szaktanulmányi és politikai, világnézeti ismereteinek gyarapításáért, fejlődéséért. A nevelőtiszteket külön iskolákban képezik ki. Lengyelországban ez idő szerint mintegy kétezer rendőrbajtársi kör működik.*”[25] A látogatás során a lengyel rendőr delegáció megtekintett a Budapesti Rendőrfőkapitányságot, a gyermekbíróságot, rendőrkórházat. Továbbá találkoztak a Magyar Rendőr szerkesztőivel és szaklapokat cseréltek. A látogatás végén megállapodtak, hogy kölcsönösen további rendőrcsoportokat küldenek Lengyel-, és Magyarországra. Még ugyanebben az évben magyar rendőr delegáció utazott Lengyelországba dr. Münnich I Ferenc r. altá-

[21] Sallai János (2008): ősz a lengyel–magyar határon, 1939. In: Gorąca jesień na granicy polsko-węgierskiej, 1939. Újpesti Lengyel Kisebbségi Önkormányzat, Budapest.
[22] Magyar Rendőr, 1947. 1. évf. 16. szám 5. o.
[23] Magyar Rendőr, 1948. 2. évff. 4. sz. 4. o.
[24] Uo.
[25] Uo.

bornagy és Marschall László r. ezredes vezetésével, akik megtekintették a lengyel rendőrség képzését és technikai felszereléseit.

A későbbiekben folyamatossá volt a lengyel és magyar belügyi, rendőri szervek közötti együttműködés, szakmai delegációk kölcsönös látogatása. Valamint a magyar belügyi táncegyüttes[26] több alkalommal szerepelt sikeresen Lengyelországban. A Duna Művészegyüttes „*Fellépett egyebek között Varsóban, Gdanskban, Ostyiban, Krakkóban. Kétszer adott róla műsort a televízió, éspedig egyenes adásban. Közvetítette programját a kongresszusi palotából, s jó huszonöt perces rádióműsor mutatta be életét, munkáját.*"[27] A nagy sikert igazolja, hogy később több alkalommal kapott meghívást a Duna Művészegyüttes Lengyelországba.

Ugyanebben az évben a Magyar Rendőr folyóiratban jelent meg a lengyel miliciának ez első 20 évéről egy méltató írás. A szerző szerint a milícia felszerelése ekkor már korszerűnek mondható, és a „*rendőrségünk* (lengyel) *20 éves fennállásának évfordulóján nyugodtan állíthatjuk: lényegében minden rendőrtiszt elérte az általános műveltséget jelentő középfokú képzettséget és elvégezte a 2 éves rendőrtiszti iskolát. Apparátusunk tisztjeinek, munkatársainak 17%-a megszerezte a felsőfokú képzettséget. A rendőröknek általában tiszthelyettesi, de legalábbis általános ismereteket nyújtó 6 osztályos iskolai végzettségük van."*[28] Ekkorra a rendőrség már a „*közbiztonságot veszélyeztető és a gazdasági természetű bűncselekmények megelőzését"*[29] tartotta a legfontosabb feladatának.

A magyar lengyel kapcsolatokban üde színfoltként jelentkezett, amikor 1965-ben Zbigniew Bryczkowski lengyel rendőrtiszt látogatástát követően a Magyar Rendőr hasábjain jelentette[30] meg tapasztalatait. S bár írásából egyértelműen rózsaszínűnek tűnik a magyar rendőrökről festett kép, mindenképp jelzés értékű, hogy Lengyelország rendőre kiemelt érdeklődést tanúsított a magyar közbiztonsági viszonyok és a magyar rendőri szolgálatellátás iránt.

Az elkövetkezendő években folyamatosan jelentek meg mindkét ország rendőri szakajtójában a mások ország rendőrségéről, rendőri tevékenységéről szóló tudósítások. Ezen kívül különböző kulturális eseményekről is olvashattunk, amely a két nemzet rendőrsége is részt vett. Például 1981-ben lengyel-magyar barátság hete[31] alkalmából „*Tudjunk többet Lengyelországról!*" címmel folyt beszélgetés a Belügyminisztérium Központi Könyvtár olvasótermében.

Az 1980-as években a magyar lengyel rendőri kapcsolatok egyik meghatározó elem volt, hogy a magyar Rendőrtiszti Főiskolán lengyel, a Lengyelországban – Legionowoban – magyar bűnügyi technikusok tanultak. Később a 1990-es években a

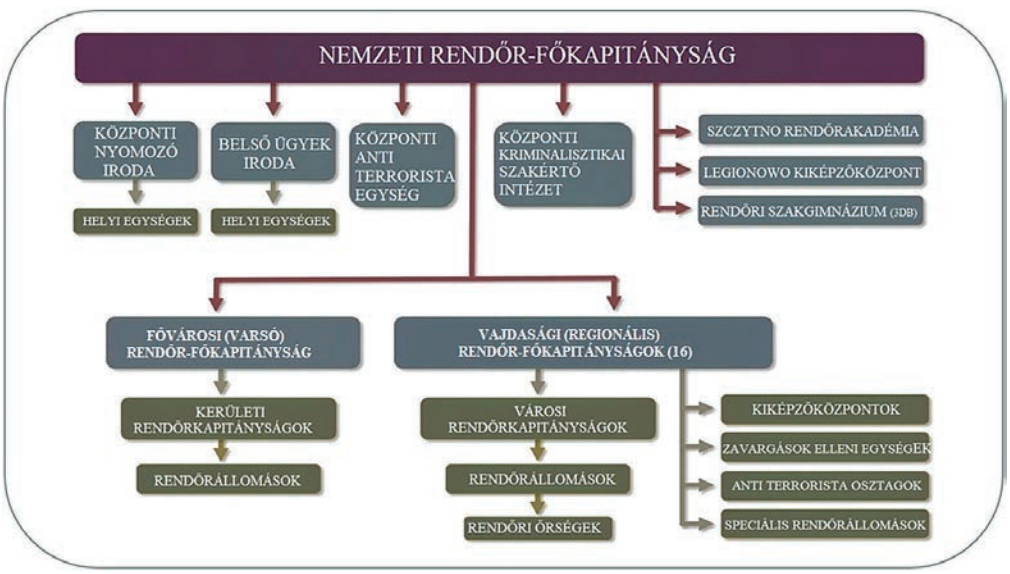
[26] Barátaink között. A Duna Művészegyüttes sikere a Lengyel Népköztársaságban. In.: Magyar Rendőr, 1964. 18. évfolyam, 44. szám. 5. o.
[27] Uo.
[28] Ryszard Kaezorowski (1964) A „W SLUZBIE NARQDU" 2o éve. In: Magyar Rendőr, 1964. 18.évf. 40. sz. 11. o
[29] Uo.
[30] Zbigniew Bryczkowski (1965): Egy lengyel rendőrtiszt szemével. Magyar Rendőr, 1965. 19. évfolyam, 42. sz.
[31] Magyar Rendőr, 1981. 35. évf. 10. szám

magyar rendőrtisztek, a Továbbképzési és Módszertani Központban folytatott néhány hónapos nyelvi felkészítés után bűnügyi ismereteket tanultak Lengyelországban.

Mindkét országban a ’80-as évek végén bekövetkezett politikai rendszerváltás hatásaként döntően megváltozott a korábbi állampártokat kiszolgáló népi, szocialista rendőrség tevékenységet meghatározó jogszabályok, szabályzatok és új demokratikus környezetben, új kihívásoknak megfelelve váltak a köztársaságok rendőrségévé, policiájává. A változás eredményeként átalakultak a rendőrség állományba kerülésének módjai, lehetőségei, és döntően megváltozott a rendőrtisztek felkészítése.

Rendőrtisztek kiválasztása Lengyelországban.

A Lengyel Nemzeti Rendőrség (eredeti nevén: Policja, röviden: lengyel rendőrség) centrális irányítású, fegyveres, egyenruhás szervezet, amelynek a munkáját a lengyel Közigazgatási és Belügyminisztérium irányítja. A szervezet a következő alapfeladatköröket végzi: a személyek életének és testi épségének, valamint vagyonuknak a védelme, a közrend és a közbiztonság védelme, a közösségi rendőrség kialakítása és szervezése, a bűnmegelőzés, a bűncselekmények és a szabálysértések észlelése, a bűnelkövetők letartóztatása, a közéleti és a közterületi szabályok betartatása, más országok rendőrségeivel és a nemzetközi szervezettekkel való együttműködés.[32] A lengyel rendőrségnél rendőr tiszthelyettesek, rendőr tisztek és rendőr tábornokok teljesítenek szolgálatot.



1. ábra: Lengyel Nemzeti Rendőrség (Az ábrát készítette: Dr. Kovács István)

[32] Mogyoródi Gergely (2023): A rendőrség hivatásos állománya kiválasztásának vizsgálata. Doktori (PhD) értekezés. NKE. Budapest. 98. o.

Lengyelországban minden lengyel polgár jelentkezhet rendőrtisztnek, aki elmúlt 18 éves és az alábbi feltételeknek megfelel:

- Igazolhatóan rendelkezik lengyel állampolgársággal.
- Kifogástalan hírneve van.
- Jogerősen nem ítélte el bíróság.
- Teljes közjogot élvez.
- Legalább középfokú végzettséggel rendelkezik.
- Megfelelő pszichikai és fizikai képességekkel rendelkezik.
- Egyéb titoktartási követelményeknek eleget tud tenni.[33]

A jelentkezés első lépcsője, hogy ha megfelel a feltételeknek, amelyeket dokumentumokkal is igazolni tud, a területi rendőrfőkapitányságon beadja a kérelmét. A jelentkezés során egy 30 pontból álló kérdőívet kell kitölteni. A kérdőívben meg kell neveznie egy rendőrségi szolgálati helyet a jelöltnek, ahol később szolgálni kíván.

A következő szakaszban a jelöltnek egy 40 kérdésből álló tudáspróbát kell teljesítenie, amelynek eredményét pontok formájában tovább viszi.

Ezt követi a jelölt fizikai alkalmassági vizsgálata. A teszt során a jelölt a sebességét, a mozgékonyságát, az erejét és az állóképességét mérik fel és a mért eredményt pontokká alakítják.

A fentiek után kerül sorra a pszichikai felmérés, amely során a jelölttel tesztet, kérdőívet töltetnek ki, interjút készítenek és megfigyelést hajtanak végre. „*A teszt során az intellektuális hajlamokat, a szociális viselkedést, a stabilitást és a munkahelyi attitűdöt ellenőrzik*.”[34]

A fenti szakaszok eredményes teljesítését után kerülhet sor a pályaalkalmassági beszélgetésre és orvosi vizsgálatra, valamint biztonsági ellenőrzésre.

A fenti követelmények teljesítése után a jelölt megkezdheti a rendőrség állományába a szolgálatot és jelentkezhet az alapképzésre.

Lengyel rendőrtisztképzés Szczytnóban

Az előző fejezetrészben tárgyaltak szerint a lengyel rendőri pályára alkalmas személyeket tiszthelyettesnek négy helyszínen: Słupskon, Pilan, Lodzon és Katowicen képzik, míg rendőrtiszti felkészítés csak egy helyen Szczytnóban folyik.

Szczytno kb. 27 000 lakosú város északkelet Lengyelországban, Mazuriában, ahova több évtizeddel ezelőtt a meglévő infrastruktúra miatt került a lengyel rendőrség tisztképző intézete.

[33] https://magazyn-ksp.policja.gov.pl/mag/poradniki/120995,Jak-przebiega-rekrutacja-do-sluzby-w-Policji.html letöltve 2023.06.24.

[34] https://hit.policja.gov.pl/hit/aktualnosci/209492,System-szkolenia-funkcjonariuszy-Policji-Panstwowej.html letöltve 2023.06.24.

A város vonzó erejét a mazuri tavak közül itt lévő két tó a Domowe Małe és a Długie, a városházával társbérletben lévő Mazúriai Múzeum, valamint Sienkiewicz történelmi regényéből ismertté vált vár jelenti.

A Wyzsza Szkola Policja (továbbiakban WSzPol) magyarul Lengyel Rendőrtiszti Főiskola a Szczytnó szélén, irigylésre méltó feltételek között található. A WSzPol[35] az 2018. július 20-i lengyel Felsőoktatási és tudományos életről szóló törvény szerint a belügyminiszter alárendeltségébe tartozik. A törvény szerint a WSzPol „*küldetése a társadalomtudományok igazságának feltárása és terjesztése a biztonság- és jogtudomány tudományágain, különös tekintettel a biztonságra és a közrendre, kutatások végzésével, oktatók, doktoranduszok, hallgatók, résztvevők oktatásával. tanfolyamok és képzések, valamint ezek terjesztése.*”[36]



2. ábra: Rendőrakadémia Szczytnó (Fotó: Dr Sallai János)

A szczytnói főiskola a társadalomtudomány területén biztonság és jogtudományi ágakban PhD doktori fokozatok adományozására jogosult. A főiskola egyben a rendőrség egyik kutatási központja is, amely tevékenységet hazai és nemzetközi partnerek bevonásával végzi.

Az WszPol élén a rektor (parancsnok áll), aki jelenleg dr hab. Iwona Klonowska hívnak rendőr dandártábornok, helyettese: Dr. Andrzej Zylinski, fejlesztési[37] helyettese: Dr. Porwisz Monika. A főiskola kancellárja: Agnieszka Lesniewska.

[35] 2003 óta tagja az Európai Rendőrfőiskolák Szövetségének (AEPC)
[36] https://www.wspol.edu.pl/g/uczelnia/o-szkole letöltve 2023.06.23.
[37] A főiskola fejlesztési projektjeit döntően (90 %) állami források bevonásával valósítja meg.

A rektor közvetlen alárendeltségébe tartoznak az alábbi szervezeti egységek:

- Rektori Hivatal,
- Emberi Erőforrások Főosztálya,
- Információbiztonsági Főosztály,
- Fegyelmi és Ellenőrzési Osztály,
- Társadalmi Kommunikációs Osztály,
- Munkavédelmi csoport,
- Jogi ügyekkel foglalkozó csoport,
- Belső ellenőr.

A rektor-helyettes közvetlen irányítása alá tartoznak:

- Biztonság- és Jogtudományi Kar,
- Képzésszervezési és Szakképzési Osztály,
- Vezetési Osztály.

A kancellár pedig felügyeli: a pénzügyeket, a Kommunikációs és Informatikai Szolgálatot, a Beruházási és Javítási Osztályt és az Ellátási és Közlekedési Osztályt.

A fejlesztési rektorhelyettes „felügyeli a Kutatási Koordinációs Intézet, a Kiadói és Nyomdai Osztály, a Könyvtár[38] és az Európai Integrációs és Nemzetközi Kapcsolatok Csoport munkáját."[39]

A WSzPol zöld környezetben, 37 hektáron, kiváló oktatói bázissal, tantermekkel, modern audiovizuális és speciális berendezésekkel, szimulátorokkal, speciális (kriminalisztika, nyelvoktatás oktatás számára) laboratóriumokkal, konferenciatermekkel, lőterekkel, sportpályákkal, uszodával, kantinnal, nyomdával, kiadóval, szállodával rendelkezik.

A főiskola, (amely része a bolognai rendszernek) fő tevékenységét az oktatást a Biztonság- és Jogtudományi Kar alábbi szervezeti egységei, tanszékei, intézetei biztosítják:

- Megelőző Szolgálat Intézet, (Megelőzési és Megelőzési Osztály, Közbiztonsági Tanulmányok Osztálya, Testnevelési Tanszék);
- A Bűnügyi Szolgálat Intézet (Bűnügyi Tanszék, Kriminalisztikai Tanszék);
- Jogtudományi Intézet;
- Társadalomtudományi Intézet;
- Nyelvoktatási Tanszék.[40]

A WSzPol-n tanulhatnak civilek és a lengyel rendőrség állománya, nappali és levelező (váltásos) munkarendben.

[38] A WszPol könyvtára több mint 220 000. főleg szakmai könyvvel, valamint korszerű elektronikus katalógussal, kutatóolvasó helységekkel rendelkezik.

[39] https://www.wspol.edu.pl/g/uczelnia/kierownictwo letöltve 2023.06.23.

[40] https://www.wspol.edu.pl/g/uczelnia/o-szkole letöltve 2023.06.23.

Civil képzési szakok:

A lengyel rendőrtisztképzés fellegvárában nemcsak rendőrségi állományú személyeknek van lehetősége tanulni, hanem civil szakokon a lengyel polgárok is tanulhatnak, akik a felvételi követelményeknek megfelelnek. A főiskola két szakon, a **kriminológia**[41] és **belső biztonság** szakokon indít posztgraduális képzéseket a témák iránt érdeklődőknek.

„A kriminológia oktatásának célja a diplomások átfogó felkészítése a bűnüldöző szerveknél, igazságügyi hatóságoknál, valamint más szolgálatoknál és szervezeteknél végzett munkára, beleértve a pártfogó hivatalokat, a szociális jóléti központokat, a családsegítő központokat és a krízisintervenciós központokat."[42]

„A belső biztonság témájú oktatás célja magasan kvalifikált szakemberek felkészítése az állami és önkormányzati szolgálatokban a válsághelyzetekben, természeti katasztrófákban és állami fenyegetettségben felmerülő csoportok irányításával kapcsolatos munkakörökben való munkavégzésre, valamint az állami szolgálatok támogatása tisztjeik szakmai képzettségének javítása a folyamatban lévő jogszabályi változásokban és a felmerülő új típusú fenyegetések mélyreható elemzésének szükségessége."[43]

Mindkét civil szak esetén a tanulmányokat nappali és levelezős munkarendben végezhetik a hallgatók.

Rendőri tudományi szak

A főiskolára a kiválasztást követően a rendőri szervek állományában szolgálatot teljesítő rendőrök jelentkezhetnek. A képzés moduláris formában zajlik, összesen 4 évben a következő fő szakaszokban.

1. **Bevezető (alapképzési) szakasz. 144 nap. Amelyen a következő fő tantárgyak[44] a megadott óraszámban kerülnek leoktatásra:**
   1. **modul:**
      JS01 – Bevezetés a joggyakorlatba 3 óra
      JS02 – Anyagi büntetőjog és általános jog 19 óra
      JS03 – Anyagi büntetőjog és a speciális bűncselekmények 48 óra
      JS04 – Különleges cselekmények büntetőjogi rendelkezései 10 óra
      JS05 – Helyszíni szemle végrehajtása 15 óra
      JS06 – A helyszín vizsgálata 12 óra
      JS07 – Bűnügyi információk feldolgozása 13 óra
      JS08 – Tanú kihallgatása 12 óra

[41] „Kriminológia" szakon érettségivel rendelkező civil jelentkezhet első ciklusú tanulmányaira, amely 3 évig tart.
[42] https://www.wspol.edu.pl/g/ letöltve 2023.06.23.
[43] Uo.
[44] DECYZJA NR 376. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego podstawowego

JS09 – A rendőrség története, 17 óra
JS10 – Információ kezelése és a tömegmédia

2. **modul:**
JS01 – (rádió) Kommunikációs eszközök alkalmazása 12 óra
JS02 – Személyazonosítás 23 óra
JS03 – Pénzügyi eszközök felhasználása (gazdálkodás) 28 óra
JS04 – Lőfegyver alkalmazásra felkészülés 31 óra
JS05 – Elsősegélynyújtás 42 óra
JS06 – Személy letartóztatása 31 óra
JS07 – Személyek, csomagok, rakományok átvizsgálása, ellenőrzése 9 óra
JS08 – Személyek, helyiségek és dolgok átkutatása 17
JS09 – Együttműködő szervekkel kapcsolattartás, együtt dolgozás 8 óra
JS10 – Kábítószer hatása alatt álló emberekkel való eljárás, tevékenység 92 óra
JS11 – Járőrszolgálat ellátása 9 + 40 óra

3. **modul:**
JS01 – Rendőrség információs rendszer és használata 20 tanóra
JS02 – Interjú, mint a rendőri munka módszere 8 óra
JS03 – A körözött személyek keresése, elfogása 7 óra
JS04 – Eljárás eltűnt személy esetén 8 óra
JS05 – Ismeretlen személlyel kapcsolatos eljárás 5 tanóra
JS06 – Eljárás eltűnt tárgyak megtalálása esetén 7 óra
JS07 – Az informátor 8 óra
JS08 – Ad hoc megfigyelés 11 óra
JS09 – Nemzetközi információs együttműködés 10 óra
JS10 – SPP-alkalmazások és hordozható terminálok használata, ellenőrzése 10 óra

4. **modul:**
JS01 – Konvoj szolgálat 11 óra
JS02 – Biztonsági szolgálat ellátása rendőri őrzött helyeken. (Fogda, kijózanító, gyerek szoba, ideiglenes helységek) 10 óra

5. **modul:**
JS01 – A közlekedés alapjai 15 óra
JS02 – Feladat ellátása az utakon 10 óra
JS03 – Dokumentumok megőrzése, törlése, járművek és kerék zárak 9 óra
JS04 – Alapvető tevékenységek a helyszínen közlekedési esemény esetén 15 óra
JS05 – Az úthasználók ellenőrzése 23 óra

6. **modul**
JS01 – Bevezetés vétség esetén azügyek kezelésébe 2 óra
JS02 – Szabálysértési és pénzbüntetési eljárások 13 óra
JS03 – Magyarázó tevékenységek 9 óra

JS04 – Gyanúsított személy kihallgatása 9 óra
JS05 – Büntetési indítvány 6 óra
JS06 – Gyorsított eljárás alkalmazása 6 óra

7. **modul:**
JS01 – Rendőri magatartás szabályai 6 tanóra
JS02 – Egyéni és csapatgyakorlatok végrehajtása 8 tanóra
JS03 – Kordonok és kettős kordonok kialakítása 6 tanóra
JS04 – Előőrs- és járőrvonalak bővítése és lezárása 2 tanóra
JS05 – Rendőrségi vonal kialakítása és manőverezése 8 tanóra
JS06 – Rendőr magatartása válsághelyzetekben 14 tanóra

8. **modul:**
JS01 – Diagnózis abnormális és kóros jelenségek megelőzése területén 6 tanóra
JS02 – Fiatalkorú elkövetők 86 tanóra

9. **modul:**
JS01 – A lövészet alapjai 16 tanóra
JS02 – Előkészületi és statikus lövés 30 tanóra
JS03 – Gyorslövés 22 tanóra
JS04 – Dinamikus lövés 22 tanóra
JS05 – SMG-lövés alapjai 13 tanóra
JS06 – A sima csövű sörétes lövés alapjai 14 tanóra
JS07 – Helyzetlövés 20 tanóra
Lövéspróba 7 tanóra

10. **modul:**
JS01 – Testnevelés 35 tanóra
JS02 – A fizikai erő alkalmazása kényszerítő eszközként 44 tanóra
JS03 – Technikai készségek a beavatkozások végrehajtásához 42 tanóra
JS04 – A rendőrtiszt elleni támadások visszaverése 32 tanóra
JS05 – Rendőr személyi biztonság 42 tanóra

Az alapszakon összesen 1123 órát kell teljesíteni mind a négy tiszthelyettes iskolán és a Szczytnoi Rendőrakadémián is.

2. **Altiszti szakasz**[45]
A szabályzat megismerése a képzés szervezése 2 tanóra
A program tevékenységei[46] 115 tanóra
Záróvizsga 2 tanóra
A képzés befejezése 1 tanóra

[45] DECYZJA NR 377. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego podoficerskiego

[46] Emberi jogok, rendőr etika, diszkrimináció és a korrupcióellenes magatartás, családon belüli erőszak, határon átnyúló üldözés, lövészet, ittas személyek elleni fellépés, …. stb. Kiválasztott témák, esetek kezelése, adminisztrálása, értékelése.

Az altisztképzési szakaszban 120 órát kell a hallgatóknak teljesíteni, amire 15 képzési nap áll rendelkezésre.

3. **Aspiránsi szakasz**[47]
   A szabályzat megismerése a képzés szervezése 2 tanóra
   A program tevékenységei[48] 146 tanóra
   Záróvizsga 2 tanóra
   A képzés befejezése 1 tanóra

A zászlósi aspiránsi szakasz rendszere hasonló az altisztképző szakaszhoz, de témában és óraszámban eltér. Az zászlósi aspiránsi szakaszban 155 órát kell a hallgatóknak teljesíteni, amire 19 képzési nap áll rendelkezésre.

4. **Tiszti szakképző szakasz (hadnagyig)**[49]
   A szabályzat megismerése a képzés szervezése 2 tanóra
   A program tevékenységei[50] 587 tanóra
   Záróvizsga 2 tanóra
   A képzés befejezése 1 tanóra

[47] DECYZJA NR 378. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego aspiranckiego

[48] Emberi jogok, szakmai etika, a rendőr diszkrimináció és a korrupcióellenes tevékenysége, kommunikációs műhelyek, pszichológiai módszerek, szervezés, irányítás, szolgáltatás, munkaszervezés, a civil ruhás rendőr fegyelmi és büntetőjogi felelőssége, bűntetőjogi esetek, kiber bűnözés, rendőri menedzsment, operatív tevékenység, bűnügyi információ elemzése, elsősegélynyújtás, lövészet, beavatkozás taktika.

[49] DECYZJA NR 379. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego oficerskiego

[50] • TÖRTÉNELEM, HAGYOMÁNY ETHOS
• A PSZICHOLÓGIA ELEMEI VEZETÉSBEN
• A SZOCIÁLIS KOMMUNIKÁCIÓ SZEMPONTJAI
• SZERVEZÉS ÉS IRÁNYÍTÁS
• KÖZIGAZGATÁSI JOG
• KÖZIGAZGATÁSI ELJÁRÁSJOG
• VÁLOGATOTT JOGI KÉRDÉSEK BÜNTETŐELJÁRÁS
• A KRIMINOLOGIA VÁLOGATOTT ELEMEI
• SZOCIÁLIS PREVENCIÓ
• MEGELŐZŐ SZOLGÁLTATÁS
• FORGALMI SZOLGÁLATI TAKTIKA
• VÁLSÁGKEZELÉS ÉS A RENDŐRSÉGI MŰVELETEK SZERVEZÉSE
• BŰNÜGYI TECHNOLÓGIA VÁLOGATOTT KÉRDÉSEI
• MŰVELETI TAKTIKA felderítés
• BŰNÜGYÜGYI TAKTIKA
• GZADASÁGI BŰNÖZÉS ELLENI HARC VÁLOGATOTT TAKTIKAI KÉRDÉSEK
• BŰNÜGYI ELEMZÉS
• A SZERVEZETT BŰNÖZÉS ELLENI KÜZDELEM
• FENYEGEZÉSEKTŐL A MODERN TERRORIZMUSBÓL
• KIBERBŰNÖZÉS
• RENDŐREK KÉPZÉSE SZAKMAI FEJLŐDÉS TÖRTÉNETE
• NEMZETKÖZI RENDŐRSÉGI EGYÜTTMŰKÖDÉS
• KIVÁLASZTOTT TÉMÁK TAKTIKÁJA ÉS BEAVATKOZÁSI TECHNIKÁK
• EGÉSZSÉGPROGRAM

A tiszti szakképzés szakaszában jól érzékelhető a témákban való minőségi ugrás, a vezetési témakörök előtérbe kerülése, a speciális témák megjelenése. A szakasz oktatására 74 oktatási nap áll rendelkezésre.



POLSKA IZBA HANDLU ZAGRANICZNEGO
CERTYFIKACJA
Polish Chamber of Foreign Trade
Certification

CERTYFIKAT

Nr 218/2007

Ten Certyfikat nadaje się jako dowód, że system zarządzania:
This Certificate is granted as evidence that the management system of:

WYŻSZA SZKOŁA POLICJI
w Szczytnie
12-100 Szczytno, ul. Marszałka Józefa Piłsudskiego 111; Polska (Poland)

spełnia wymagania Normy:
complies with the requirements of the Standard:

ISO 9001:2015

w zakresie:
in the scope of:

· świadczenie usług edukacyjnych

· *educational services*

Certyfikat został nadany 7 października 2004
The certificate was granted on 7th of October 2004

Ważność certyfikatu:
Expiry date:
1.09.2022

AC 070
QMS

Artur Szwoch
PREZES / PRESIDENT
Gdynia, 2.09.2019

PIHZ Certyfikacja Sp. z o.o.; 81-332 Gdynia, ul. Kołłątaja 1, Polska

3. ábra: A Rendőrakadémia ISO minőségbiztosítási diplomája

Befejezés

A magyar rendőrtisztképzés immár tradicionálisan főiskolai, egyetemi keretek között szemeszter jellegű több mint 50 éve. Megismerve a lengyel rendőrtisztképzést, azonnal szemebtűnő a szakaszos és moduláris rendszer. Ez azt jelenti, hogy a tisztképzésben résztvevő jelölt a szakmai testületbe való felvétel után, négy szakasz teljesítését követően válhat rendőrtisztté, (hadnaggyá). Közben bármelyik szakaszban kiszállhat és az elért eredményei és a teljesített követelmények alapján a gyakorlatban folytathatja a rendőrségnél őrmesterként, zászlósként a pályát. Ugyanakkor később visszatérhet és teljesítheti a képzés következő szakaszát és eljuthat a rendőrhadnagyi rendfokozatig.

A lengyel rendőrtisztképzés Északkelet-Lengyelországban található egy kisvárosban, míg a magyar a főváros szívében. Ezzel a lengyel rendőrtisztjelöltek többet a tanulmányaik során több közös rendezvényen tudnak részt venni, véleményem szerint erősebb baráti kollegiális kapcsolatokat tudnak kialakítani.

A szerzőknek Lengyelországban tett szakmai látogatásra 2023. júliusában került sor. Ezt követően 2023 augusztus 1.-től a lengyel Rendőrtiszti Főiskolán névváltoztatásra került sor, és a Wyzsza Skola Policji felvette a Akademia Policji nevet.

A magyar-lengyel rendészeti kapcsolatok tradicionálisan kiállták a próbát és több mint száz éve folyamatos a gyakorlati és a rendészeti oktatásban is az együttműködés.

Felhasznált irodalom:

1. A Lengyel rendőrtiszti Főiskola (Szczytno) honlapja https://www.wspol.edu.pl/g/ letöltve 2023.06.23.
2. A lengyelországi tanulmányút. Szemerjay-Kovács Dénes miniszteri tanácsos és a magyar rendőrségi és csendőrségi delegáció diadalútja Varsóban és lengyel földön. Magyar Rendőr. 1936. 1. sz.
3. Barátaink között. A Duna Művészegyüttes sikere a Lengyel Népköztársaságban. In.: Magyar Rendőr, 1964. 18. évfolyam, 44. szám.
4. Borszéki Judit – Sallai János (2023): 100 éves az Interpol. In. BM Szemle 71. évf. 11. sz.
5. Borszéki Judit – Sallai János (2022): A nemzetközi rendőri együttműködés kezdetei. BM Szemle 2022. 5. sz. https://ojs.mtak.hu/index.php/belugyiszemle/article/view/8529 letöltve 2023.05.13.
6. DECYZJA NR 376. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego podstawowego.
7. DECYZJA NR 377. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego podoficerskiego.
8. DECYZJA NR 378. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego aspiranckiego

9. DECYZJA NR 379. KOMENDANTA GŁÓWNEGO POLICJI z dnia 21 grudnia 2022 r. w sprawie programu szkolenia zawodowego oficerskiego.
10. https://legionowo.policja.gov.pl/ letöltve 2023.06.24.
11. https://magazyn-ksp.policja.gov.pl/mag/poradniki/120995,Jak-przebiega-rekrutacja-do-sluzby-w-Policji.html letöltve 2023.06.24.
12. https://magazyn-ksp.policja.gov.pl/mag/poradniki/120995,Jak-przebiega-rekrutacja-do-sluzby-w-Policji.html letöltve 2023.06.24.
13. https://www.wspol.edu.pl/g/ letöltve 2023.06.24.
14. Irk Albert (1915) Nemzetközi küzdelem a bűntettesek nemzetközi osztályai ellen. in. Bűnügyi szemle, 1914-1915. 3. évfolyam, 7. sz.
15. Joanna Stempinski (2009) A lengyel rendőrség és rendőrségi jog bemutatása. Rendvédelmi Füzetek 2009/5. sz. Rendőrtiszti Főiskola Budapest.
16. Johann Schober (1927): Nemzetközi rendőrség. Az Újság jubiláris karácsonyi számának. Újság 1927. december 25.
17. Kovács Gábor – Kovács Istvan – Piros Attila (2019): A magyar és lengyel rendőrség vezetés-irányítási rendszerének összehasonlító elemzése. Rendőrségi Tanulmányok II. Budapest RTT.
18. Külföldi szemle. A lengyel államrendőrség. In.: Magyar Közigazgatás. 1937. 13. sz.
19. Magyar detektív. 1927. 15. sz.
20. Magyar Rendőr, 1936. 19. sz.
21. Magyar Rendőr, 1947. 1. évf. 16. szám
22. Magyar Rendőr, 1948. 2. évff. 4. sz.
23. Magyar Rendőr, 1981. 35. évf. 10. szám
24. Mogyoródi Gergely (2021) A lengyel rendőrség hivatásos állományú személyzetének kiválasztási rendszere. In Belügyi Szemle. 69. Évf. 69 9. sz.
25. Mogyoródi Gergely (2023): A rendőrség hivatásos állománya kiválasztásának vizsgálata. Doktori (PhD) értekezés. NKE. Budapest
26. Németh Gábor (2021) A lengyel rendőri alapképzési rendszer Belügyi Szemle 69. évf. 9. szam
27. Ryszard Kaezorowski (1964) A „W SLUZBIE NARQDU" 20 éve. In: Magyar Rendőr, 1964. 18.évf. 40. sz.
28. Sallai János (2007) A magyar-lengyel határ története. HISTORIA GRANICY WEGIERSKO-POLSKIEJ. Országos Lengyel Kisebbségi Önkormányzat. Budapest.
29. Sallai János (2008): ősz a lengyel–magyar határon, 1939. In: Gorąca jesień na granicy polsko-węgierskiej, 1939. Újpesti Lengyel Kisebbségi Önkormányzat, Budapest
30. Sallai János (2010)Zachować człowieczeństwo. Witeź Zoltán Baló opiekunem polskich uchodźców. In: SLAVICA. XXXIX–XL kötet.
31. Sallai János (2011): Egy meg nem jelent cikk a lengyel haderőről. Valóság 2011. 4. szám.

32. Sallai János (2015): A rendészet kihívásai napjainkban. Magyar Hadtudomány. 25 évf. 1-2 sz
33. Sallai János (2016) Rendőr-, rendőraltiszt-, rendőrtörzsaltiszt-képzés a m. kir. rendőrség államosítása után. Magyar Rendészet 16. évfolyam 6. sz.
34. Sallai János (2021): A finn-magyar nemzetközi rendészeti együttműködés a két világháború között. In: V. Turizmus és Biztonság Nemzetközi Tudományos Konferencia tanulmánykötet.
35. Sallai János (2022): Nemzetközi rendőr konferencia turizmus. https://uni-pen.hu/files/konferencia/2021/VI.%20Turizmus%20%C3%A9s%20biztons%C3%A1g%20tudom%C3%A1nyos%20konferencia%20tanulm%C3%A1nyk%C3%B6tete_2022.pdf Letöltve 2023.05.13.
36. www.wspol.edu.pl/g/dobor-do-policji letöltve 2023.06.24.
37. Zamorski Kordian a lengyel rendőrség főparancsnoka Budapesten. Magyar Rendőr, 1936. 19. sz.
38. Zbigniew Bryczkowski (1965): Egy lengyel rendőrtiszt szemével. Magyar Rendőr, 1965. 19. évfolyam, 42. sz.

Hottó István[1]**:**

A svájci rendőrség szervezeti felépítése, képzési rendszere és technológiai eszközei a fenntartható közbiztonság kontextusában

Absztrakt:

A tanulmány a svájci rendőrség szervezeti felépítését, képzési rendszerét és a rendőri munkát támogató technológiai megoldásokat mutatja be, kitérve a rendőrség társadalmi megítélésére és a lakosság rendőrségbe vetett bizalmára is. Az elemzés nemzetközi szakirodalomra, hivatalos rendészeti dokumentumokra és nyilvánosan elérhető szakmai forrásokra épül, amelyet a szerző több éves svájci tartózkodása alatt szerzett személyes tapasztalatai egészítenek ki. A vizsgálat rámutat, hogy a kantonális alapokon nyugvó, decentralizált szervezeti modell és az egységes szakmai követelményrendszer jól összeegyeztethető egymással, a képzés pedig erőteljesen gyakorlatorientált, kiemelt figyelmet fordítva a kommunikációs és konfliktuskezelési készségek fejlesztésére. A rendészeti munkát korszerű digitális, kriminalisztikai és informatikai eszközök támogatják, a lakosság rendőrség iránti bizalma pedig nemzetközi összehasonlításban is kiemelkedően magas. A tanulmány mindezek alapján átfogó képet nyújt a svájci rendőrség működéséről, és támpontokat ad a külföldi rendészeti modellek hazai megismeréséhez, illetve a nemzetközi tapasztalatok szakmai hasznosításához.

Kulcsszavak: kantonális rendőrség, rendőrképzés, rendészeti technológia, társadalmi bizalom, rendészeti professzionalizmus, nemzetközi rendészeti tapasztalatok

Abstract:

This study examines the organizational structure of the Swiss police, its training system, and the technological solutions supporting police work, while also addressing public perceptions of the police and the level of public trust in law enforcement. The analysis draws on international academic literature, official law enforcement documents, and publicly available professional sources, complemented by the author's personal observations gained during several years of residence in Switzerland. The findings show that the decentralized, cantonally based organizational model is well reconciled with a uniform set of professional

[1] tudományos segédmunkatárs, PhD-hallgató, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Kriminológiai és Büntetés-végrehajtási Jogi Tanszék

standards, while training remains strongly practice-oriented, placing particular emphasis on the development of communication and conflict-management skills. Law enforcement work is supported by advanced digital, forensic, and information technologies, and public trust in the police is exceptionally high by international standards. The study thus provides a comprehensive picture of the functioning of the Swiss police and offers points of reference for the domestic reception of foreign policing models as well as for the professional application of international experience.

Keywords: cantonal police, police training, law enforcement technology, public trust, police professionalism, international policing experience

Bevezetés:

A rendészeti szervek működésének, felépítésének és képzési rendszerének vizsgálata túlmutat az adott ország közbiztonsági helyzetének megismerésén: lehetőséget teremt arra is, hogy a hazai és a külföldi rendészeti modelleket egymás mellé állítva gondolkodjunk a rendőri munka lehetséges fejlesztési irányairól. A nemzetközi kitekintés azért is fontos a rendészettudomány számára, mert az egyes országok eltérő történelmi, társadalmi és közigazgatási hagyományai gyökeresen különböző megoldásokhoz vezettek a rendőri feladatok ellátásában.

Svájc a köztudatban Európa egyik legbiztonságosabb országaként van jelen, és rendészeti rendszere több szempontból is megérdemli a figyelmet. A föderális államberendezkedésből fakadó decentralizált működés, a magas színvonalú, gyakorlatközpontú rendőrképzés és a technológiai megoldások következetes alkalmazása olyan jellemzők, amelyek nemzetközi összevetésben is kiemelkednek. Ehhez társul a svájci rendőrség iránti társadalmi bizalom szokatlanul magas szintje, ami önmagában is sokat elárul a rendészeti szervek működésének eredményességéről.

A témaválasztást a szerző több éves svájci tartózkodása is motiválta: ez idő alatt számos kantonban volt módja megfigyelni a rendőrség mindennapi munkáját és társadalmi megítélését. A személyes tapasztalatok közül különösen figyelemre méltónak bizonyult az állampolgárokkal szemben tanúsított udvarias, tiszteletteljes kommunikáció, amely a rendőri intézkedések és a hétköznapi kapcsolattartás során egyaránt megmutatkozott.

1. A svájci rendőrség szervezeti felépítése

A svájci föderális berendezkedés a rendőri tevékenység decentralizáltságában is megjelenik. Roché rámutat arra, hogy egy rendészeti rendszer decentralizáltsága nem következik automatikusan a föderális vagy unitárius államberendezkedésből – az egyes föderációk rendészeti modelljei jelentősen eltérhetnek a decentralizáció mértékét tekintve, és Svájc a rendkívül helyi szintű, kantonális szervezettség egyik

legszemléletesebb példájának tekinthető.[2] A bevezetőben említjük, hogy svájci rendőrség, mint egy entitás a gyakorlatban nem létezik, ugyanis a 26 különböző kanton sajátos kantonális rendőrséggel (Kantonspolizei) rendelkezik. E tagolt rendőri szervezet „felett" áll a Fedpol (Bundesamt für Polizei)[3], amely a határokon átnyúló vagy súlyos bűncselekményekkel, a szervezett bűnözéssel foglalkozik. A pénzügyi szektor felügyeletében a FINMA fontos szerepet játszik a gyanús pénzügyi tranzakciók felderítésében és jelentésében.[4]

A svájci rendőrképzés[5] decentralizált, nem egyetlen intézményben történik, hanem kantononként vagy régiónként rendőrakadémiákon, vagy rendőriskolákban történik.

A felvételi követelmények többlépcsősek és szigorúak, a jelentkezők –kantononként – átlag 80%-a nem felel meg felvételi követelményeknek.[6]

A rendőriskolákban a jelöltek az első évben intenzív bentlakásos képzés keretében sajátítják el a legfontosabb alapfokú és gyakorlati ismereteket, e körbe tartoznak a fizikai kiképzés, a lőfegyverhasználat, valamint az intézkedéstaktikai ismeretek és készségek. Az első év végén egy alkalmassági vizsgát (Einsatzfähigkeit) tesznek a jelöltek.

A második évben éles helyzetben teljesítenek gyakorlatot, jellemzően mentorok segítik tevékenységüket. A képzés végén „szövetségi okleveles rendőr" (Polizist/in mit eidgenössischem Fachausweis) címet szereznek.

A képzés időtartama két év, majd az innen kikerülő rendőrök járőrként vagy határrendészként dolgozhatnak.

A nyomozók jellemzően járőrként kezdik pályafutásukat, majd tovább tanulva nyomozókká, később parancsnokokká is válhatnak. Specializált nyomozói tanfolyamokon vehetnek részt, elsősorban az élet elleni bűncselekmények, a pénzmosás és más pénzügyi bűncselekmények, a gazdasági bűnözés, kiberbűnözés, terrorellenes képzési területeken. Nyomozókká válhatnak rendőrakadémiai vagy egyetemi képzés nélkül is.[7]

A rendőrakadémiák magasabb szintű képzést nyújtanak, jogi ismeretek, kriminológiai, kriminalisztikai, vezetéselmélet, pszichológiai és más a bűnügyi munkához nélkülözhetetlen tantárgyak, gyakorlati ismeretekkel vértezik fel a rendőrhallgatókat.[8]

Az egyetemi képzésből is – természetesen – beléphetnek a rendőrség kötelékébe. A kriminológiai képzés egyik meghatározó intézménye az University of Lausanne[9],

---

[2] Sebastian Roché: Federalism and Police Systems. Coginta, 2011. https://coginta.org/wp-content/uploads/2024/03/2011-COGINTA-policing-and-federalism.pdf

[3] https://www.fedpol.admin.ch/de

[4] https://www.newsd.admin.ch/newsd/message/attachments/55110.pdf

[5] https://www.edupolice.ch/de/

[6] https://www.blick.ch/politik/die-schlafqualitaet-leidet-personalmangel-bremst-schweizer-polizei-korps-reagieren-id21380174.html

[7] https://www.police.be.ch/de/start/karriere/polizei/bestpol/berufsbild-und-karriereperspektiven.html

[8] https://www.kompol-zh.ch/spezialisierungen/einsatztraining-polizei

[9] https://www.unil.ch/unil/en/home.html

valamint az ETH Zürich[10], ahol magas szintű kiberbiztonsági, információbiztonsági és digitális forenzikai képzés folyik.

A svájci rendészeti képzési rendszer az egységes szakmai követelmények és a decentralizált kantonális működés sajátos ötvözeteként írható le. Jellemzője a magas fokú gyakorlatorientáltság, a kompetenciaalapú képzés, valamint a többnyelvű társadalmi és intézményi környezethez való alkalmazkodás, amely a német, francia és olasz nyelvek, illetve bizonyos régiókban a rétoromán nyelv ismeretét is szükségessé teheti. Előtérbe helyezik a mediációs ismeretek és készségek az elsajátítását, mely rendkívül fontos szerepet tölt be a működésben.

A szerző személyes megfigyelései szerint a svájci rendőrség működését az állampolgárokkal szembeni udvarias és tiszteletteljes kommunikáció jellemzi, függetlenül attól, hogy rendőri intézkedésről vagy általános segítségnyújtásról van szó. A modern szemléletű képzés része a Video-Retex megközelítés, amelynek a lényege az, hogy szituációs gyakorlatok végzésekor a jelöltek testkamerát viselnek, majd e felvételeket oktatójuk, mentoruk, pszichológus segítségével elemzik a történteket. Hangsúlyt helyezve a jogszerű eljárásra, az intézkedés arányosságára, az udvariasságra, a hanghordozásra és más jelekre. A felvételek elemzése jelentősen hozzájárulhat a képzés eredményességéhez.[11]

2. Technológiai innovációk és speciális rendőri eszközök a svájci rendőrségnél

A svájci nyomozók és rendőri szervek munkájuk során a legkorszerűbb technológiai megoldásokat alkalmazzák. A digitális kriminalisztikai eszközök, a helyszínrögzítő rendszerek és a modern kommunikációs technológiák jelentősen hozzájárulnak a nyomozások hatékonyságához és a közbiztonság fenntartásához.

A nyomozás során a legkorszerűbb eszközöket használnak a svájci nyomozók. Kiemelendő a helyszínelés során használatos 3D-s lézerszkenner (pl. Faro Focus, Orbis készülékek). A szkenner percek alatt több millió térbeli pontot rögzít, amely megőrzi a helyszínt a későbbi eljárási cselekményekhez.

Ennek előnye, hogy a helyszín lezárásának időtartama jelentősen csökkenthető, ezáltal mérsékelhető a lakosságot és a közlekedést érintő korlátozások mértéke. Az elkészített „felvétel" segítségével az ügyészségen és a bíróságon a helyszín bemutatható, bejárható akár monitoron vagy VR szemüveg segítségével.

A svájci lausenne-i fejlesztésű PIX4D szoftver drónfelvételekből képes a helyszín és környezetének részletes 3D modelljét elkészíteni.[12]

[10] https://ethz.ch/en.html

[11] https://www.swissinfo.ch/ger/politik/so-lernt-der-nachwuchs-der-polizei-den-umgang-mit-extremsituationen/48416486?nab=0

[12] https://www.pix4d.com/about-us/

A berni IRM – Institut für Rechtsmedizin[13] intézetben boncolás nélkül a Virtopsy (CT-MRI-3D) szkennerrel az elhalt sértett belső sérülései, valamint a lövedékpálya is betekintést enged.

A DNS-azonosítás területén egyre nagyobb jelentőséget kapnak a gyors genetikai vizsgálati eljárások (Rapid DNA), amelyek lehetővé teszik a DNS-profil rövid időn belüli elkészítését. A kiberbűnözés elleni fellépés során a svájci hatóságok korszerű digitális kriminalisztikai eszközöket és szoftvereket alkalmaznak az elektronikus adatok elemzésére, helyreállítására és bizonyítékként történő rögzítésére.

A svájci automatizált ujjnyomat- és arcfelismerő rendszer is – bár Svájc nem tagja az Európai Uniónak – a schengeni adatbázisokhoz kapcsolódik.

A svájci rendészeti szervek kommunikációját az országos POLYCOM[14] digitális rádióhálózat támogatja, amely a rendőrség, a mentőszolgálatok, a tűzoltóság, a vám- és határvédelmi szervek, valamint a polgári védelem számára biztosít biztonságos és interoperábilis kommunikációt. A terepen szolgálatot teljesítő rendőrök munkáját mobil adatkommunikációs eszközök – okostelefonok és tabletek – segítik, amelyek lehetővé teszik a személyek, járművek és okmányok helyszíni ellenőrzését, valamint a releváns rendőrségi adatbázisok gyors elérését.

Fotokite[15] drónt használnak Svájcban a közterületi bűnözés, balesetek rögzítésében. A FLIR[16] hőkamerás helikopterek segítségével a sötét erdőkben és hegyekben bujkáló emberek is leleplezhetők.

Lézeres sebességmérők és rendszámfelismerő rendszerek (ANPR) segítik a rendőrség munkáját. Az útlezárásokat szöges láncokkal (Stinger Spike System) biztosíthatják. A Dräger digitális analizátor a helyszínen véralkoholszint és drogteszt készítésére alkalmas.

A svájci rendőrök szolgálati oldalfegyverként jellemzően Glock vagy SIG Sauer típusú pisztolyokat használnak. A hosszú lőfegyverek általában nem képezik a mindennapi járőrszolgálat általános felszerelését, ugyanakkor a járőrgépjárművekben rendelkezésre állhatnak a magasabb kockázatú rendőri intézkedések végrehajtásához. A repülőtereken, valamint a különleges rendőri feladatok ellátása során a hosszú lőfegyverek alkalmazása gyakoribb. Egyes kantonok speciális egységei (pl. Enzian, Skorpion) rendelkeznek további speciális fegyverekkel.

A svájci rendőrök egyéni védőfelszerelései közé tartoznak a modern ballisztikai védőmellények, amelyek a szolgálati követelményeknek megfelelően lőfegyverrel és egyes szúró-vágó eszközökkel szembeni védelmet is biztosíthatnak. A rendőri szervek a speciális műveletek során sörétes puskákat is alkalmazhatnak, amelyek egyebek mellett technikai célokra, például ajtónyitásra is használhatók. A magasabb kockázatú rendőri intézkedésekhez és különleges műveletekhez egyes egységek karabélyokkal, valamint egyéb speciális fegyverekkel és eszközökkel rendelkeznek.

[13] https://www.irm.uzh.ch/de.html
[14] https://www.avm.hu/marka/polycom/
[15] https://fotokite.com/
[16] https://www.flir.com/ots/search-rescue/

A svájci rendőrségnél több kantonban alkalmaznak elektromos sokkoló eszközöket (Taser), amelyek a kényszerítő eszközök rendszerének részét képezik. A rendőrök felszerelésében emellett rendőri botok – többek között teleszkópos kivitelű eszközök – is megtalálhatók.[17]

A különleges rendőri egységek – kantontól függően eltérő elnevezéssel és szervezeti formában – speciális kiképzéssel, valamint a hagyományos járőrszolgálat felszerelését meghaladó eszközrendszerrel rendelkeznek.

3. Társadalmi bizalom és a svájci rendőrség megítélése

A modern rendészeti rendszerek értékelése során nem elegendő kizárólag a szervezeti felépítés, a képzési rendszer vagy a technológiai háttér vizsgálata. Hasonló jelentőséggel bír a rendőrség társadalmi elfogadottsága, valamint a lakosság bizalmának mértéke is. A rendészeti szervek legitim működésének egyik alapvető feltétele ugyanis az, hogy tevékenységüket a társadalom jogszerűnek, szakszerűnek és arányosnak tekintse. Tyler eljárási igazságosság (procedural justice) elmélete szerint a lakosság bizalmát elsősorban nem a rendőri intézkedések kimenetele, hanem az eljárás módja – a tisztelet, a méltányosság és az átláthatóság – alakítja. [18]

A svájci rendőrség társadalmi megítélése e tekintetben figyelemre méltó. A rendelkezésre álló felmérések szerint a rendőrség iránti bizalom nemzetközi összehasonlításban is magasnak tekinthető, amely összefüggésben állhat a rendőri szervek szakmai működésével, a magas színvonalú képzéssel, valamint a lakossággal való együttműködés hagyományaival.

A svájci rendőrség jelentős társadalmi támogatottsággal rendelkezik, amit a rendelkezésre álló felmérések eredményei is alátámasztanak. A lakosság 90%-a bízik a svájci rendőrségben, tevékenységüket rendkívül pozitívan értékelte egy a 2022-ben készült felmérés szerint.[19]

Ez a bizalom megnyilvánult abban is, hogy a felmérést megelőző 12 hónapban a válaszadók 88,9 százaléka (a bizalommal szinte megegyező arányban) nyilatkozta, hogy nem félt attól, hogy bűncselekmény áldozatává váljon. A közvélemény nagyra értékeli a rendőrség objektív, professzionális és udvarias tevékenységét.

Egy rövid kitekintéssel összevetve a magyarországi bűnözési helyzettel, a 2022-es felmérés válaszadói a csalásra és annak kísérletére (befektetési -, árucsalásokra, sőt a romantikus csalásra) panaszkodtak. Ezt követte a kiberbűncselekményekre (pl. a jogosulatlan informatikai behatolások, adatlopások), a szexuális zaklatásra, fenyegetésre, majd a kerékpárlopásokra utalás.

[17] https://www.trooper.ch/collections/dienst-einsatzmaterial

[18] Tom R. Tyler: Enhancing Police Legitimacy. The ANNALS of the American Academy of Political and Social Science, 593(1), 2004, 84–99.

[19] https://www.kkpks.ch/de/meldungen/crime-survey-2022-hohes-vertrauen-in-die-polizei-%E2%80%93-erstmals-zahlen-zu-hate-crime-292

A rendelkezésre álló adatok alapján megállapítható, hogy a svájci rendőrség a társadalom széles körű támogatottságát élvezi, amely a svájci rendészeti rendszer egyik meghatározó sajátosságának tekinthető. Ezen felmérések alapján a svájci rendőrség rendkívül magas társadalmi elismertségnek örvend.

4. Összegzés

A svájci rendőrség működésének vizsgálata azt mutatja, hogy a föderális berendezkedésből eredő decentralizált rendészeti modell és az egységes szakmai követelményrendszer nem kizárják, hanem kiegészítik egymást. A kantonális rendőrségek széles önállósága mellett a szövetségi szintű koordináció biztosítja a hatékony fellépést a súlyosabb, illetve a határokon átnyúló bűncselekményekkel szemben.

A svájci rendészeti rendszer másik meghatározó vonása a gyakorlatközpontú képzés, a folyamatos szakmai továbbképzés, valamint a modern technológiai eszközök széles körű alkalmazása. A kriminalisztikai és informatikai fejlesztések, a digitális nyomozási módszerek, a korszerű kommunikációs hálózatok és a fejlett helyszínelési technológiák érdemben hozzájárulnak a rendőri munka eredményességéhez és a közbiztonság fenntartásához.

A magas társadalmi elfogadottság és a rendőrség iránti bizalom szorosan összefügg a professzionális működéssel, a színvonalas képzéssel, valamint a rendőrök és az állampolgárok közötti együttműködés kultúrájával. A svájci modell egyik tanulsága, hogy a rendőrség eredményessége nem kizárólag a szervezeti felépítésen vagy a technikai felszereltségen múlik: legalább ilyen súllyal esik latba a rendőri mentalitás, a kommunikáció minősége, valamint az udvarias, szakszerű és jogszerű intézkedési kultúra.

A svájci tapasztalatok a magyar rendészet számára is tanulságosak lehetnek. A kommunikációs és konfliktuskezelési készségek további fejlesztése, a lakossággal való együttműködés erősítése, valamint a modern rendészeti és kriminalisztikai technológiák szélesebb körű alkalmazása mind hozzájárulhat a rendőrség társadalmi elfogadottságának növeléséhez és a közbiztonság erősítéséhez.

Felhasznált irodalom

1. AVM Hungary, *POLYCOM.* Elérhető: https://www.avm.hu/marka/polycom/ [Letöltés dátuma: 2026. 08. 04.]
2. Blick, *„Die Schlafqualität leidet" – Personalmangel bremst Schweizer Polizei – Korps reagieren.* Elérhető: https://www.blick.ch/politik/die-schlafqualitaet-leidet-personalmangel-bremst-schweizer-polizei-korps-reagieren-id21380174.html [Letöltés dátuma: 2026. 08. 04.]
3. dupolice.ch, *Ausbildung Polizei Schweiz.* Elérhető: https://www.edupolice.ch/de/ [Letöltés dátuma: 2026. 08. 05.]

4. Eidgenössisches Finanzdepartement (é. n.). *FINMA-jelentés a pénzügyi szektor felügyeletéről.* Elérhető: https://www.newsd.admin.ch/newsd/message/attachments/55110.pdf [Letöltés dátuma: 2026. 08. 06.]
5. ETH Zürich (é. n.). *ETH Zürich – Home.* Elérhető: https://ethz.ch/en.html [Letöltés dátuma: 2026. 08. 06.]
6. Fedpol – Bundesamt für Polizei (é. n.). *Polizeiliche Aufgaben auf Bundesebene.* Elérhető: https://www.fedpol.admin.ch/de [Letöltés dátuma: 2026. 08. 07.]
7. FLIR Systems (é. n.). *Search & Rescue.* Elérhető: https://www.flir.com/ots/search-rescue/ [Letöltés dátuma: 2026. 08. 06.]
8. Fotokite (é. n.). *Fotokite – Home.* Elérhető: https://fotokite.com/ [Letöltés dátuma: 2026. 08. 06.]
9. Institut für Rechtsmedizin, Universität Zürich (é. n.). *IRM Zürich.* Elérhető: https://www.irm.uzh.ch/de.html [Letöltés dátuma: 2026. 08. 07.]
10. Kantonspolizei Bern. *Berufsbild und Karriereperspektiven.* Elérhető: https://www.police.be.ch/de/start/karriere/polizei/bestpol/berufsbild-und-karriereperspektiven.html [Letöltés dátuma: 2026. 08. 07.]
11. Kantonspolizei Zürich. *Spezialisierungen – Einsatztraining Polizei.* Elérhető: https://www.kompol-zh.ch/spezialisierungen/einsatztraining-polizei [Letöltés dátuma: 2026. 08. 07.]
12. Konferenz der Kantonalen Polizeikommandanten der Schweiz (2022). *Crime Survey 2022 – hohes Vertrauen in die Polizei, erstmals Zahlen zu Hate Crime.* Elérhető: https://www.kkpks.ch/de/meldungen/crime-survey-2022-hohes-vertrauen-in-die-polizei-erstmals-zahlen-zu-hate-crime-292 [Letöltés dátuma: 2026. 08. 06.]
13. Pix4D. *About us.* Elérhető: https://www.pix4d.com/about-us/ [Letöltés dátuma: 2026. 08. 07.]
14. Roché, S. (2011). *Federalism and Police Systems.* Coginta. Elérhető: https://coginta.org/wp-content/uploads/2024/03/2011-COGINTA-policing-and-federalism.pdf [Letöltés dátuma: 2026. 08. 07.]
15. Swissinfo. *So lernt der Nachwuchs der Polizei den Umgang mit Extremsituationen.* Elérhető: https://www.swissinfo.ch/ger/politik/so-lernt-der-nachwuchs-der-polizei-den-umgang-mit-extremsituationen/48416486 [Letöltés dátuma: 2026. 08. 07.]
16. Trooper.ch. *Dienst- und Einsatzmaterial.* Elérhető: https://www.trooper.ch/collections/dienst-einsatzmaterial [Letöltés dátuma: 2026. 08. 07.]
17. Tyler, T. R. (2004). *Enhancing Police Legitimacy.* The ANNALS of the American Academy of Political and Social Science, 593(1), 84–99.
18. University of Lausanne. *UNIL – Home.* Elérhető: https://www.unil.ch/unil/en/home.html [Letöltés dátuma: 2026. 08. 07.]

Tarkó Áron[1]**:**

A magánnyomozás szabályozása az USA-ban (Kalifornia)

Absztrakt:

A tanulmányban bemutatásra kerül az USA magánnyomozási szabályozása, szemléltetve, hogyan változott meg, és milyen fejlődésen, illetve átalakuláson ment keresztül a magánnyomozás jogszabályi háttere, valamint azt, hogy a magánnyomozói gyakorlat miként harmonizál a jogszabályi előírásokkal. Az elmúlt évszázadok társadalmi és politikai változásainak hatására a magánnyomozás és a vagyonvédelem területét speciális törvényi szabályozás jellemzi. Az USA magánnyomozásának 1989 és 2024 közötti evolúcióját áttekintve képet kapunk arról, hogy a magánnyomozói és vagyonvédelmi struktúra milyen változásokon ment keresztül az egyes régiókban.

Kulcsszavak: magánnyomozás, jogszabályi háttér, USA, adattárak, szabályozás

Abstract:

This study presents how the regulation of private investigation and asset protection in the USA has changed over time. It explores the development and transformation of the legal background of private investigation, as well as how the practice of private investigation aligns with legal regulations. Influenced by the social and political changes of past centuries, the field of private investigation and asset protection has come to be governed by specific legal frameworks. By reviewing the evolution of private investigation in the USA between 1989 and 2024, we gain insight into how the structures of private investigation and asset protection have changed in these regions.

Keywords: law, USA, private investigation, databases, regulation

A magánnyomozás nemzetközi kitekintése az USA-ban

A tanulmányban bemutatásra kerül, hogy az Amerikai Egyesült Államokban hogyan változott a magánnyomozás szabályozása, hogyan alakították át a jogszabá-

[1] Nemzeti Közszolgálati Egyetem, doktorandusz hallgató

lyokat, ezek milyen fázisokon mentek mentek át. A szabályozási rendszerek között vannak hasonlóságok és különbségek. A társadalmi és politikai változások miatt a magánnyomozás területét speciális törvényi előírások jellemzik.

Az USA-ban a magánnyomozás 1989–2024 közötti fejlődéséből kiderül majd, hogy a magánnyomozói és vagyonvédelmi struktúra milyen változásokon ment keresztül a régiókban, még akkor is, ha felépítésében és feladatrendszerében a lényeges eltérések mellett jelentős hasonlóságok is tapasztalhatók. A tanulmány – figyelembe véve a hazai és a regionális evolúciós tapasztalatokat – javaslatot tesz arra, hogy a hatályos törvényi szabályozásban milyen újszerű változtatásokra lenne szükség. Célom egy olyan javaslatcsomag kidolgozása, amely a magánnyomozói munkavégzés folyamatát átláthatóbbá, a törvényi szabályozást pedig specifikusabbá teszi, miközben kielégíti a megrendelői igényeket, megfelel a nemzeti értékeknek és érdekeknek, valamint a nemzetközi jogszabályok által előírt kötelezettségeknek.

Tanulmányomban a hazai és regionális tapasztalatokra építve teszek javaslatot a jogszabályi rendszer reformjára. A javasolt módosítások célja, hogy a magánnyomozás hatékonyan tudjon válaszolni a 21. század kihívásaiból és követelményeiből eredő elvárásokra, továbbá megfeleljen a technológiai, valamint a társadalmi fejlődés exponenciálisan változó hatásainak.

A tanulmányban javaslatot teszek az USA magánnyomozói tevékenységének szabályozásával kapcsolatos kiegészítésekre, a jogforrások specifikusabbá tételére, valamint a jelenlegi fogalmi rendszer pontosítására, hiszen általánosan elfogadott és jogszabályban rögzített egységes definícióval a magánnyomozás jelenleg nem jelenik meg.

A magánnyomozás törvényi szabályozása Kaliforniában

(2024. évi Kaliforniai Törvénykönyv, Üzleti és Szakmai Kódex – BPC 3. OSZTÁLY – SZAKMÁK ÉS HIVATÁSOK ÁLTALÁNOSSÁGBAN, 1.3. fejezet – Magánnyomozók, 3. cikk – Szabályozás, engedélyezés és regisztráció, 7524. szakasz)

7521.5. szakasz

(a) A magánnyomozó nyújthat személyvédelmi szolgáltatásokat, de vagyontárgy-védelmi szolgáltatást csak akkor, ha az közvetlenül kapcsolódik egy olyan nyomozáshoz, amelyre a magánnyomozót korábban megbízták.

(b) Amennyiben a magánnyomozó ilyen szolgáltatásokat nyújt, teljesítenie kell a 4. cikk (a 7540. szakasztól kezdődően) követelményeit, különösen a lőfegyvertartásra és a hivatal által kiállított, érvényes fegyveres képesítési igazolvány megszerzésére vonatkozó rendelkezéseket.

(c) Ha a magánnyomozó ilyen szolgáltatásokat nyújt, teljesítenie kell a 7583.39., 7583.40. és 7583.41. szakaszok előírásait is, amelyek a felelősségbiztosítási kötvény fenntartására vonatkoznak.

(d) Ha egy személy a magánnyomozó nevében vagy megbízásából jár el a szolgáltatások nyújtása során, az illető a magánnyomozó alkalmazottjának minősül a 7512.11. szakaszban meghatározottak szerint, és a felek között a 7512.12. szakasz szerinti munkáltató-munkavállaló kapcsolat áll fenn. Ezen személynek szintén teljesítenie kell a jelen szakasz követelményeit, kivéve a (b) és (c) alpontokban szereplő mentességeket.[2]

7523. szakasz

(a) Hacsak a 7522. szakasz kifejezett mentességet nem biztosít, senki sem folytathat magánnyomozói tevékenységet a 7521. szakaszban meghatározottak szerint, amíg az adott vállalkozási tevékenységre vonatkozóan engedélyt nem szerzett ezen fejezet alapján.

(b) Bármely személy, aki megsérti ezen fejezet rendelkezéseit, vagy összeesküvést sző a magánnyomozói engedélyre vonatkozó rendelkezések megsértésére, illetve aki tudatosan egy engedéllyel nem rendelkező személyt von be a tevékenységbe, vétséget követ el. Ez a cselekmény ötezer dollárig (5000 USD) terjedő pénzbírsággal, vagy egy évig terjedő megyei börtönbüntetéssel, illetve a kettő kombinációjával büntetendő.

(c) A (b) bekezdésben meghatározott bírság kiszabására irányuló eljárást Kalifornia állam lakosságának nevében a főügyész, a kerületi ügyész vagy a városi ügyész indíthatja meg bármely illetékes bíróságon. Ha az eljárást a megyei kerületi ügyész indítja, a beszedett bírságot a megyei pénztárosnak kell megfizetni. Ha az ügyet városi ügyész indítja, a beszedett büntetés fele a város, másik fele pedig a megye pénztárát illeti meg. Amennyiben az eljárást az állami ügyészség indítja, a teljes összeget a Magánbiztonsági Szolgáltatások Alapjába kell befizetni.[3]

(d) Vétséget követ el és tízezer dollárig (10 000 USD) terjedő pénzbírsággal, illetve egy évig terjedő megyei börtönbüntetéssel (vagy mindkettővel) büntetendő az a személy, aki:

1. magánnyomozói licencjogosultként mutatkozik be, miközben nem rendelkezik engedéllyel;
2. hamisan azt állítja, hogy egy engedéllyel rendelkező magánnyomozó alkalmazottja;
3. olyan jelvényt, azonosító kártyát vagy névjegykártyát visel/használ, amely jogosulatlanul magánnyomozói státuszra utal;

[2] California Business and Professions Code, section 7523 (2025). Letöltés ideje: 2025. 11. 23.
[3] California Business and Professions Code, section 7523 (2025). Letöltés ideje: 2025. 11. 23.

4. olyan levélfejet, írásos vagy elektronikusan generált anyagot használ, amely valótlanul engedélyezett státuszt sugall;
5. engedély hiányában magánnyomozói tevékenységet hirdet.

(e) A (d) bekezdés szerinti bírságok kiszabására irányuló eljárásokra a (c) bekezdésben rögzített illetékességi és pénzkezelési szabályok megfelelően irányadók.

(f) Bármely személy, akit a jelen szakasz rendelkezéseinek megsértése miatt elítélnek, az elítélést követő egy éven belül nem kaphat magánnyomozói engedélyt.

(g) Az (a), (b) vagy (d) bekezdések megsértése miatti első elítélést követően a magánnyomozói engedély megszerzése egy évig, második vagy későbbi elítélés esetén pedig öt évig kizárt.

(h) A hatóság vezetője köteles gyűjteni a licenc nélkül tevékenykedők szabályszegéseire vonatkozó bizonyítékokat, és azokat a vádemelés érdekében továbbítani az illetékes helyi ügyészségeknek.

(i) Az illetékes megyei vagy városi ügyészség köteles eljárást indítani a joghatósága területén történt minden ilyen jogsértés ügyében.

A magánnyomozói tevékenység gyakorlata

A magánnyomozóknak szigorú szakmai és etikai iránymutatásokat kell követniük annak érdekében, hogy tevékenységük jogszerű maradjon. Kaliforniában az Üzleti és Szakmai Kódex (BPC) 7523. szakasza előírja, hogy a magánnyomozónak érvényes engedéllyel kell rendelkeznie a munka megkezdése előtt. A sikeres hitelesítést követően a nyomozók az alábbi tevékenységeket végezhetik:

- **Megfigyelés és dokumentálás nyilvános helyeken:** Követhetik a célszemélyek mozgását, fényképeket és videófelvételeket készíthetnek róluk nyilvános területeken, amennyiben ezzel nem sértik meg a magánszférát és nem lépnek magánterületre.
- **Nyilvános nyilvántartások és adatbázisok elérése:** Jogszerűen kereshetnek a nyilvánosan hozzáférhető adatbázisokban (pl. bírósági iratok, ingatlan-nyilvántartások, cégbejegyzések), hogy ellenőrizzék a büntetett előéletet vagy a tulajdonjogokat.
- **Személyek felkutatása:** Közösségi média platformok és úgynevezett *skip tracing* adatbázisok segítségével (amelyek hiteljelentésekből, közüzemi számlákból és egyéb nyilvános adatokból építkeznek) kereshetnek eltűnt személyeket vagy jogi ügyekben érintett feleket, az adatvédelmi jogszabályok szigorú betartása mellett.
- **Háttérellenőrzések végzése:** Legális adatbázisok segítségével ellenőrizhetik a jelentkezők foglalkoztatási múltját, végzettségét és bűnügyi hátterét a vállalati felvételi folyamatok során.

- **Együttműködés a rendvédelmi szervekkel:** A magánnyomozók gyakran segítik a hatóságok munkáját azáltal, hogy kiegészítő információkat szolgáltatnak személyes ügyekben vagy folyamatban lévő nyomozásoknál.[4]

Tiltott tevékenységek (amit a nyomozók jogilag nem tehetnek meg):

Bár a magánnyomozók eszköztára széles, a jogi korlátok szigorúan kötik őket. Az alábbi tevékenységek elvégzése tilos és jogellenes:

- **Magánterület megsértése (birtoksértés):** Nem léphetnek be magánterületre a tulajdonos engedélye nélkül. A magánterület megsértése Kaliforniában bűncselekménynek minősül, és súlyos jogi következményekkel jár, még nyomozati célok esetén is.
- **Telefonok, számítógépek vagy e-mail-fiókok feltörése:** A digitális eszközökhöz és személyes fiókokhoz való jogosulatlan hozzáférés szigorúan tilos. A nyomozónak kizárólag jogszerű eszközöket szabad alkalmaznia az információgyűjtésre.
- **Rendőri vagy kormányzati szerep megszemélyesítése:** A magánnyomozók nem adhatják ki magukat rendőrnek vagy kormányzati tisztviselőnek. Ennek megszegése a kaliforniai büntető törvénykönyv 538(d) szakasza alapján súlyos bűncselekménynek minősül.
- **Megtévesztő telefonhívások:** Bár készíthetnek telefonos interjúkat, nem használhatnak hamis identitást vagy megtévesztést arra, hogy bizalmas, védett információkat csaljanak ki másokból.

A megbízó biztonsága érdekében kritikus fontosságú az engedéllyel rendelkező nyomozó alkalmazása, mivel a képesítetlen személyek igénybevétele komoly jogi kockázatot jelent a kliens számára is. Olyan professzionális ügynökségek, mint például a *Worldwide Intelligence Network*, garantálják az etikus és törvényes eljárást Kaliforniában, kiterjedt szolgáltatásokat nyújtva a háttérellenőrzéstől a megfigyelésen át az eltűnt személyek felkutatásáig.

Szövetségi és állami szabályozási hierarchia az USA-ban

A magánnyomozói tevékenységet szabályozó törvények többrétegű keretrendszerben működnek, amely ötvözi a szövetségi felügyeletet az államok egyedi követelményeivel. A szabályozás folyamatosan fejlődik a modern technológia és az új adatvédelmi normák hatására.

[4] Discreet PI Official Website. Letöltés ideje: 2025. 11. 23.

Főbb szövetségi szabályozások (Federal Trade Commission – FTC felügyelete alatt):

- **Fair Credit Reporting Act (FCRA):** Szabályozza a háttérellenőrzéseket és a fogyasztói jelentések felhasználását.
- **Gramm-Leach-Bliley Act (GLBA):** Védelmet biztosít a személyes pénzügyi adatok számára.
- **Drivers Privacy Protection Act (DPPA):** Korlátozza a gépjármű-nyilvántartási adatokhoz való hozzáférést.[5]
- **Electronic Communications Privacy Act (ECPA):** Szabályozza az elektronikus megfigyelést és a lehallgathatóságot.
- **Health Insurance Portability and Accountability Act (HIPAA):** Szigorúan védi az egészségügyi információkat.
- **Computer Fraud and Abuse Act (CFAA):** Megtiltja a jogosulatlan számítógépes rendszerbe történő belépést.[6]

Állami szintű szabályozás:

Az Országos Állami Törvényhozási Konferencia (NCSL) adatai szerint a részletes szabályozási jogkörök az egyes államok kezében vannak, így az előírások jelentősen eltérhetnek a következő területeken:

- Engedélyezési követelmények (oktatás, szakmai múlt, vizsgák).
- A tevékenységi kör és a tiltott magatartások pontos meghatározása.
- Helyi adatvédelmi és megfigyelési korlátozások.
- Etikai és fegyelmi eljárások normái.
- Díjszabási és számlázási előírások.
- Kötelező felelősségbiztosítási minimumok.

A magánélethez való alkotmányos jog

A magánnyomozói törvényeknek egyensúlyt kell teremteniük a nyomozati érdekek és az alkotmányos jogok között. Az USA Legfelsőbb Bíróságának joggyakorlata alapján az Alkotmány Negyedik Kiegészítése alapvető adatvédelmi jogokat garantál, amelyek közvetlenül kihatnak a magánnyomozásra is:

- **A magánélethez való észszerű elvárás elve *(Reasonable Expectation of Privacy):*** Erős védelem illeti meg a polgárokat az otthonukban és a magánjellegű kommunikációjuk során.

[5] Foglight Investigations: Top 10 Private Investigation Agencies in the US. Letöltés ideje: 2025. 11. 23.
[6] California Business and Professions Code, section 7523 (2025). Letöltés ideje: 2025. 11. 23.

- **A nyilvános helyek doktrínája:** Nyilvános helyeken a magánélethez való elvárás korlátozott, így ott a megfigyelés és fotózás főszabály szerint legális.[7]
- **Hozzájárulási kötelezettségek hangfelvételnél:** Az államok megoszlanak a tekintetben, hogy a beszélgetés rögzítéséhez minden fél beleegyezése szükséges-e (*Two-Party Consent States*, mint Kalifornia), vagy elegendő csupán az egyik fél tudomása (*One-Party Consent States*). A hangmegfigyelés szövetségi szinten is lényegesen szigorúbb szabályozás alá esik, mint a videómegfigyelés.[8]
- **GPS nyomkövetés és digitális technológia:** A modern törvények szigorúan korlátozzák a járművek beleegyezés nélküli GPS-követését, a közösségi média zárt profiljainak manipulatív elérését, valamint a mobileszközök szoftveres megfigyelését.[9]

Bizonyítékgyűjtés és a rendőri jogkörök hiánya

A bírósági eljárásokban való felhasználhatóság érdekében a magánnyomozóknak szigorúan be kell tartaniuk a bizonyítékok kezelésére vonatkozó szabályokat, beleértve a **bizonyítási lánc *(Chain of Custody)*** pontos dokumentálását a gyűjtéstől a bemutatásig.[10]

Kiemelendő, hogy a magánnyomozóknak **nincsenek hatósági (rendőri) jogköreik**:

- Nem kérhetnek és nem hajthatnak végre bírósági házkutatási vagy lefoglalási parancsot (*Search Warrant*).
- Nincs önálló okirat-beidézési (kikényszerítési) jogkörük (*Subpoena*).
- Az állampolgári letartóztatás jogintézménye (*Citizen's Arrest*) csak rendkívül korlátozott, specifikus körülmények között illeti meg őket.
- Nem kényszeríthetnek ki tanúvallomást vagy beismerést.[11]
- Nincs közvetlen hozzáférésük a zárt kormányzati és rendőrségi bűnügyi adatbázisokhoz.
- A nyomozóknak minden tevékenységükről (időbeosztás, bizonyítéknapló, interjúk, ügyfélszerződések) részletes, objektív és a szabályozásnak megfelelő nyilvántartást kell vezetniük, ami védi mind a nyomozót, mind az ügyfelet.

[7] Bureau of Security and Investigative Services (BSIS): Frequently Asked Questions – Private Investigator (PI). Letöltés ideje: 2025. 11. 25.

[8] McDuffie Law Office: Understanding the Legal Aspects of Private Investigation in California. Letöltés ideje: 2025. 11. 24.

[9] U.S. Government Accountability Office (GAO): Personal Privacy Protection. Letöltés ideje: 2025. 11. 24.

[10] Bureau of Security and Investigative Services (BSIS): Frequently Asked Questions – Private Investigator (PI). Letöltés ideje: 2025. 11. 25.

[11] Investigate NC | Private Investigator Raleigh, NC, USA. Letöltés ideje: 2025. 12. 23.



1.számú fénykép [12]

Magyarország

Hazánkban a 2005. évi CXXXIII. törvény – a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól – kiegészítése a jelen időszak egyik fontos kihívása lehet. A téma aktualitása fontos mert a magánnyomozói tevékenységgel kapcsolatosan nem készült jelentős mennyiségű tudományos cikk az elmúlt években, így a terület további kutatása főleg a gyakorlati felhasználás oldaláról mindenképpen indokoltnak tűnik.

A magánnyomozás fogalma törvényileg nem került meghatározásra. A magánnyomozó tevékenysége egy polgári jogi megbízás alapján végzett, nem hatósági adatgyűjtés, melyet az arra jogosult személy végez (a tevékenységre jogosító igazolvánnyal kell rendelkeznie, tevékenységét a rendőrségen be kell jelentenie, melyet ott nyilvántartásba vesznek) ellenszolgáltatás fejében, a megbízó magánérdekének kiszolgálására. Helyzete könnyebb mert nem vonatkoznak rá a hivatásos szolgálattal járó szigorú előírások. Nehezebb mert nem áll mögötte széles szakapparátus.

[12] Konferencia – Biztonsági Expo/letöltés ideje:2026.06.16.

Adatot gyűjt, rendszerez, a beszerzett tárgyi eszközöket felhasználhatja bizonyítékként, büntető és polgári perben.

A magánnyomozás egy gyakorlati tevékenység melynek során több tudományág (például kriminalisztika, kriminológia, pszichológia, bűnügyi szolgálati ismeretek, büntető jog) törvényszerűségeit felhasználva jut el magánnyomozó egy-egy ügy megoldásához.

Magyarországon jelenleg nincs pontos definíciója a magánnyomozásnak. A jelen helyzetben fontosnak tartom a jogforrás szövegében meghatározni a magánnyomozás fogalmát, melyre a következő javaslatot teszem.

Magyarországon a rendszerváltozás komoly hatással volt a politikára, a társadalomra, a gazdaságra, melyek átrendeződése, változása természetszerűen hatott a magánnyomozásra.

A rendszerváltást követően új jogszabályok jöttek létre, melyek még hiányosak (1998. évi IV. törvény, 2005. évi CXXXIII. törvény) a magánnyomozás rendelkezéseinek vonatkozásában.

A jelenleg hatályos személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvényre, az 1998. évi IV. törvényre és végrehajtására megalkotott 24/1998. (VI. 9.) BM rendeletre jellemző, hogy ellentmondásos szabályozásokat fogalmaz meg a magánnyomozásra vonatkozóan; mivel a magánnyomozás továbbá a személy-és vagyonvédelmi tevékenység nem azonos nyomozati cselekményeket foglal magában ezért eltérő szabályozásra van szükség mindkét tevékenység esetében. A technikai információszerzés a fentebb említett két jogforrás esetében nem határozza meg egyértelműen, hogyan lehet információt gyűjteni technikával (rejtett kamera, rejtett toll, rejtett távirányító).

A szektorban szélesebb körű együttműködésre lenne szükség a rendvédelmi szervek és a magánnyomozó között a hatékonyabb információáramlás érdekében.

Lehetőség biztosítása arra vonatkozóan, hogy külön ügyszámmal megkérve szolgáltassanak információt a rendőrségi bűnügyi adattárból a magánnyomozónak, a bűnügyi felderítés eredményessége miatt.

A magánnyomozó ügyével kapcsolatos lakcím/bűnügyi adatkérést az állami apparátus (ügyészség) ellenőrizné, hogy jogos-e az adatkérés megadott ügyben. Ezáltal a magánnyomozó törvényes úton tudna hozzájutni információkhoz. Fontos lenne az is, hogy magánnyomozó az Ügyészség és a Bíróságtól kapjon egy általános tájékoztatást a megbízási ügyében. Amennyiben a magánnyomozó rendelkezik információkkal azt átadja a megfelelő hatóságnak, amelyből mindkét fél profitál.

A magánnyomozás tekintetében szükség lenne jogszabályi kiegészítésre vagy új jogforrás megalkotására, mely konkrétan megfogalmazná a nyílt nyomozás, a titkos nyomozás erőit, eszközeit, módszereit; valamint azt, milyen módon gyűjthet titkos /nyílt információt a magánnyomozó, fontos lenne a magánnyomozói tevékenység szétválasztása a vagyonvédelmi tevékenységtől. Alapvetően a rendőrségi belső utasításokban megtalálható erők, eszközök, módszerek tananyaga, részletesebb szabá-

lyozást biztosítana a magánnyomozó számára átvehetnének egyes részeket a törvény alkotó [13].

Komoly problémát jelent a jogi háttér hiányossága is: a törvényalkotó adós maradt a legendák és a megtévesztő taktikák alkalmazási feltételeinek pontos meghatározásával[14]. Amit fontos kiemelni, hogy a rendőrségi és nemzetbiztonsági törvényben le vannak írva speciális utasításban, hogyan kell használni a fedettség szabályait, ellenben a magánnyomozói törvényben ez nincsen megfogalmazva.

Elengedhetetlen lenne kitérni a magánnyomozók által alkalmazható felderítési eszközök és módszertanok tételes jogszabályi rögzítése, pontosan kijelölve a legális működés határait [15]. Továbbá arra is, hogy specifikusan próbavásárlást hogyan végezhet el szabályosan a magánnyomozó; konkrétan milyen jogai és kötelezettségei vannak úgy, mint ahogyan a nyugat-európai magánnyomozói törvények (francia, német, angol) is szabályozzák[16].

A hazai szabályozás reformjához alapul szolgálhatna a németországi gyakorlat. Ott az ügyészség ellenőrzése mellett, egyedi ügyszám alapján nyílik lehetőség a bűnügyi adattárból történő adatszerzésre, így a magánnyomozók törvényes és konspirált keretek között juthatnak hozzá a szükséges lakcím- és háttéradatokhoz. A magánnyomozó számára törvény által lehetőséget kapjon, hogy a hatóságtól adatot kérhessen (Rendőrség, Ügyészség, Bíróság, BV). Az adatkérés jogosságát a magánnyomozónak igazolnia kellene pl. a megbízási szerződéssel. Az adatkérés jogosságának elbírálását az ügyészség hatáskörébe kellene utalni. A törvényeket a GDPR-t, a Legfelső Bíróság 4. számú elvét, a magánnyomozói törvényt harmonizációba kellene hozni. A jogszabályban szükséges lenne meghatározni, a magánnyomozói tevékenység, illetve nyomozás határait. Nyugat-Európában vannak olyan országok, mint például Németország, ahol egyes ügyekben a Rendőrség ad ki adatot a magánnyomozó számára, például egy biztosítási ügyben a rendőrség tájékoztatást magánnyomozónak.

Összegzés

Az Amerikai Egyesült Államokban a magánnyomozói tevékenység szabályozása államonként eltérő képet mutat. Kaliforniában a magánnyomozói tevékenységet a *2024. évi Üzleti és Szakmai Kódex* részletesen és szigorúan szabályozza, pontosan rögzítve a jogköröket és a végezhető nyomozati cselekményeket.

Bár az USA magánnyomozói törvényei évszázados múltra tekintenek vissza és világszerte mintaként szolgálnak, a modern kor kihívásai (például a nyílt és fedett nyomozások pontos elhatárolása, a minősített információk legális gyűjtése, valamint a legendák és ürügyek alkalmazhatóságának határai) folyamatos finomhango-

[13] Tarkó Áron: A HUMINT szerepe a nemzetbiztonsági szolgálatoknál (polgári és katonai) és a magánnyomozásban
[14] B2/2013. (I. 31.) BM utasítás (minősített norma)
[15] B2/2013. (I. 31.) BM utasítás (minősített norma)
[16] Tarkó Áron: A HUMINT szerepe a nemzetbiztonsági szolgálatoknál (polgári és katonai) és a magánnyomozásban

lást igényelnek. A szakmai szövetségek és kamarák (amelyekből számos működik az országban) kulcsszerepet játszanak a tagok képzésében, az információáramlás segítésében és a szakmai hálózatok építésében.

A jövőre nézve a bűnügyi felderítés eredményességének növelése érdekében indokolt lenne egy szélesebb körű és strukturáltabb együttműködés kialakítása a hatóságok és a magánnyomozók között. Célszerű lenne olyan legális eljárásrendet biztosítani, amely lehetővé tenné, hogy a magánnyomozók hivatalos ügyszám alapján, ellenőrzött keretek között kaphassanak specifikus adatokat (pl. lakcím- vagy korlátozott bűnügyi információkat) a rendőrségi adattárakból, amennyiben az a megbízás sikeres teljesítéséhez vagy a hatósági munka támogatásához szükséges, biztosítva ezzel a kölcsönös szakmai előnyöket.

A magánnyomozói törvény jelenleg nem dolgozza ki kellőképpen a nyílt nyomozás és a fedett nyomozás formai követelményeit. Továbbá azt is szükséges meghatározni a törvényben, hogy hogyan gyűjthet minősített információt a magánnyomozó legálisan. A törvényeket tagolni szükséges külön-külön törvényben tevékenységi körnek megfelelően. Érdemes lenne figyelembe venni a nyugat-európai törvényeket, hogyan szabályozzák a magánnyomozóitevékenységet. Külön figyelmet érdemel annak vizsgálata, hogyan alkalmazzák a bizonyítást a bírósági eljárásokban. Továbbá ki kell dolgozni álláspontom szerint olyan részt a törvényben, amely konkrétan taglalja a tárgyi bizonyítást. A törvénynek szabályoznia kellene, hogy használhat-e a magánnyomozó legendát és ürügyet, a nyomozás során. Szükséges lenne a magánnyomozó részére bírósági védelmet biztosítani, hogy a konspiráció és a fedettségszabályainak meg tudjon felelni és inkognítóban tudjon maradni a munkája során. Védettséget kell biztosítani a magánnyomozó számára. A tanulmányozott országokban megállapítást nyert, hogy különbségek fedezhetők fel, a fentnevesített szervezetek esetében, magánnyomozói, struktúrák működése tekintetében, kamarai felépítésben és a törvényi szabályozásában és utasítási szinteken, oktatási képzésben is. Érdemes megvizsgálni, hogy a cseh, magyar, szlovák magánnyomozói és vagyonvédelmi kamarák között megfelelő módon történik-e az információ csere.

Felhasznált irodalom:

1. B2/2013. (I. 31.) BM utasítás (minősített norma).
2. Bureau of Security and Investigative Services. (é. n.). *Frequently Asked Questions – Private Investigator (PI).* California Department of Consumer Affairs. Letöltve 2025. november 25-én.
3. California Business and Professions Code, § 7523 (2024). *Justia US Law.* Letöltve 2025. november 25-én.
4. California Business and Professions Code, section 7523 (2025). Letöltve 2025. november 23-án.
5. Discreet PI Official Website. (é. n.). Letöltve 2025. november 23-án.

6. Foglight Investigations. (é. n.). *Top 10 Private Investigation Agencies in the US*. Letöltve 2025. november 23-án.
7. Investigate NC | Private Investigator Raleigh, NC, USA. (é. n.). Letöltve 2025. december 23-án.
8. Konferencia – Biztonsági Expo. (é. n.). Letöltve 2026. június 16-án.
9. McDuffie Law Office. (é. n.). *Understanding the Legal Aspects of Private* Investigation in California. Letöltve 2025. november 24-én.
10. Tarkó, Á. (é. n.). A HUMINT szerepe a nemzetbiztonsági szolgálatoknál (polgári és katonai) és a magánnyomozásban.
11. The Investigator's Journal – CPIRC. (é. n.). Letöltve 2025. november 23-án.
12. U.S. Government Accountability Office. (é. n.). Personal Privacy Protection. Letöltve 2025. november 24-én.

Nagy János[1]**:**

A rendkívüli események kezelése a rendőri intézkedések során

Absztrakt:

Pályafutásom során egy rendkívüli intézkedés hatására a traumaérzékeny szemlélet és a mentális egészségvédelem vált szakmai munkám központjává. A Nemzeti Közszolgálati Egyetemen a rendkívüli események pszichés hatásait és a poszttraumás stressz-zavar rendvédelmi sajátosságait kutatom. Tapasztalataim és Dr. Máté Gábor kutatásai is igazolják, hogy a rendőri szolgálatban átélt traumák lelki és testi szinten egyaránt megjelennek, miközben a feldolgozás gyakran elmarad. A parancsnokok szerepe kulcsfontosságú a trauma felismerésében és a támogatás biztosításában. E felismerés nyomán hoztam létre a „PTSD – A Magyar Rendvédelemben" zárt online közösséget, amely biztonságos teret ad a tapasztalatok megosztására. Kutatásom célja, hogy a traumaérzékeny vezetői szemlélet és a pszichológiai innováció beépüljön a rendőri kultúrába, erősítve a szolgálat biztonságát és a rendőrök hosszú ávú egészségét.

Kulcsszavak: mentális egészség, PTSD, poszttraumás stressz zavar, innováció

Abstract:

A specific, extraordinary incident during my career led me to make a trauma-informed approach and mental health protection central to my professional work. At the University of Public Service, I conduct research on the psychological impact of extraordinary events and the specific characteristics of post-traumatic stress disorder (PTSD) within law enforcement.

Both my own experiences and the research of Dr. Gabor Maté confirm that traumas experienced during police service manifest on both psychological and physical levels, yet the necessary processing often fails to occur. Commanders play a pivotal role in recognizing trauma and ensuring support.

[1] Nagy János r. százados, BRFK

Driven by this realization, I established the „PTSD – In Hungarian Law Enforcement" private online community, which provides a safe space for sharing experiences. My research aims to integrate a trauma-informed leadership mindset and psychological innovation into police culture, thereby enhancing operational safety and the long-term health of police officers.

Keywords: mental health, PTSD, innovation

Bevezetés

A rendőri intézkedéssel összefüggő rendkívüli események jelentősége a magyar rendvédelemben

A rendőri hivatás sajátossága, hogy a szolgálatot teljesítők rendszeresen kerülnek olyan helyzetekbe, amelyek fokozott fizikai, pszichés és mentális terheléssel járnak.

A közterületi állomány tagjai nap mint nap találkoznak olyan szituációkkal, amelyekben a veszélyhelyzet, a kiszámíthatatlanság és a gyors döntéshozatal együttesen jelenik meg.

A rendkívüli események – legyen szó erőszakos támadásról, életveszélyes helyzetről, öngyilkossági kísérletről, családon belüli erőszakról vagy fegyveres konfliktusról – nem csupán az intézkedés taktikai és jogi kereteit teszik próbára, hanem a rendőr személyiségét, lelki stabilitását és hosszú távú mentális egészségét is.

A rendőri állomány körében a traumás élmények feldolgozása gyakran háttérbe szorul, noha a tapasztalatok szerint a poszttraumás tünetek megjelenése nem kivételes, hanem rendszeresen előforduló jelenség. A tudományos munkámban szerepel az a fontos megállapítás, hogy ***„a magyar rendőrségnél a stressz folyamatosan jelen van, és amikor egy rendkívüli eseménybe belekerülünk, az még hatványozottabban fogja a szervezetünket megviselni".***

Ez a felismerés jól mutatja, hogy a rendkívüli események kezelése nem csupán intézkedéstaktikai, hanem mentálhigiénés kérdés is.

A rendőri állomány mentális terhelésének vizsgálata különösen aktuális a 2019 óta növekvő tendencia miatt, amelyet az **Országos Rendőr-főkapitányság forrás adatai is alátámasztanak**[2]. A dokumentum szerint *„2023 első félévében 948.211 főt igazoltattak, ami 22,25%-os növekedést jelent az előző évhez képest"*, és ezzel párhuzamosan nőtt a rendőrök elleni erőszakos cselekmények száma is. A 2020-as Budapest IV. kerületi, illetve a 2023 januárjában történt, országos visszhangot ki-

[2] (ORFK, Közrendvédelmi statisztikai adatok, 2024)

váltó Budapest XI. kerületi tragédiák pedig rávilágított arra, hogy a rendőri intézkedések során a veszélyhelyzet valós és közvetlen.

A rendkívüli események feldolgozásának hiánya nemcsak a rendőrök szolgálatkészségét, hanem családi életét és társas kapcsolatait is érinti. A dokumentumban szereplő személyes reflexió szerint *„a traumát hazavisszük, és a szeretteink is elszenvedik”*. Ez a jelenség nemzetközi kutatásokkal is összhangban áll, amelyek szerint a trauma közvetetten a családtagokra is hatással lehet.

A tanulmány célja, hogy:

– bemutassa a rendkívüli események jogi, intézkedéstaktikai és pszichológiai hátterét,
– feltárja a rendőröket érő mentális terhelések sajátosságait,
– rövidített esettanulmányon keresztül szemléltesse a trauma hatásmechanizmusát,
– empirikus adatokkal támassza alá a probléma súlyosságát,
– és innovációs javaslatokat fogalmazzon meg a rendőri állomány támogatására.

A rendkívüli események kezelése nem csupán szakmai feladat, hanem emberi felelősség is. A cél egy olyan rendőri kultúra kialakítása, amelyben a mentális egészség megőrzése ugyanolyan fontos, mint a fizikai biztonság.

Rendkívüli események rendőri sajátosságai – személyes tapasztalat szakmai kontextusban

A rendőri hivatás egyik legmeghatározóbb sajátossága, hogy a szolgálatot teljesítők időről időre olyan helyzetekbe kerülnek, amelyek túlmutatnak a hétköznapi intézkedéseken. A rendkívüli események – különösen az élet elleni támadások, a fegyveres helyzetek vagy a súlyos sérüléssel járó intézkedések – nemcsak szakmai kihívást jelentenek, hanem mély és tartós pszichés lenyomatot hagyhatnak a beavatkozó rendőrben. Ezek az élmények nem izoláltan hatnak: olyan belső mintázatokat alakítanak ki, amelyek akár **transzgenerációs úton is továbbadhatók**, és így a trauma feldolgozatlan elemei a következő generációk érzelmi és stresszreakciós rendszerében is megjelenhetnek.

A rendőri állomány körében a traumás élmények feldolgozása gyakran háttérbe szorul, noha a tapasztalatok szerint a poszttraumás tünetek megjelenése nem kivételes, hanem rendszeresen előforduló jelenség.

A tudományos munkámban szerepel az a fontos megállapítás, hogy ***„a magyar rendőrségnél a stressz folyamatosan jelen van, és amikor egy rendkívüli eseménybe belekerülünk, az még hatványozottabban fogja a szervezetünket megviselni”.***

Ez a felismerés jól mutatja, hogy a rendkívüli események kezelése nem csupán intézkedéstaktikai, hanem mentálhigiénés kérdés is.

A rendőri állomány mentális terhelésének vizsgálata különösen aktuális a 2019 óta növekvő tendencia miatt, amelyet az Országos Rendőr-főkapitányság adatai is alátámasztanak.

A forrás adatok alapján[3] ***2024-es évben 1 317 760 főt igazoltattak, majd a 2025-ös évben már 1 611 463 fő került igazoltatásra, ami 22,3%-os növekedést jelent az előző évhez képeset*** és ezzel párhuzamosan növekedett a rendőrök elleni erőszakos cselekmények száma is.

A rendkívüli események pszichológiai háttere

A rendőri intézkedések során bekövetkező rendkívüli események nem csupán fizikai veszélyt jelentenek, hanem olyan pszichés terhelést is, amely azonnali és hosszú távú hatást gyakorol a beavatkozó rendőr mentális működésére.

A stresszreakciók, a traumafeldolgozás és a poszttraumás tünetek megértése nélkülözhetetlen ahhoz, hogy a rendvédelmi állomány megfelelő támogatást kapjon és a szolgálat biztonságosan, stabil mentális háttérrel legyen ellátható.

A tudományos munkámban szerepel az a lényeges megállapítás, hogy ***„a magyar rendőrségnél a stressz folyamatosan jelen van, és amikor egy rendkívüli eseménybe belekerülünk, az még hatványozottabban fogja a szervezetünket megviselni”***.

Ez a mondat pontosan rávilágít arra, hogy a rendőri hivatásban a stressz nem kivétel, hanem állandó tényező, amely rendkívüli események során extrém szintre emelkedik.

A stressz szerepe a rendőri intézkedésekben

A stressz a rendőri munkában kettős természetű jelenség. Egyrészt szükséges, mert aktiválja a szervezet készenléti állapotát, gyorsítja a reakcióidőt és növeli a fókuszt. Másrészt azonban túlzott mértékben romboló hatású, és olyan fiziológiai, érzelmi és kognitív tüneteket idéz elő, amelyek akadályozhatják az intézkedés szakszerű végrehajtását.

A szakirodalom két alapvető stressztípust különböztet meg:

Eustressz – a teljesítményt fokozó stressz

Ez az a pozitív stresszforma, amely segíti a rendőrt a gyors, határozott cselekvésben. A dokumentum is utal arra, hogy a rendőrök gyakran „készenléti állapotban” működnek, ami a szolgálat természetes velejárója.

[3] (ORFK, Közrendvédelmi statisztikai adatok, 2024)

Distressz – a túlterhelésből fakadó káros stressz

A distressz már a teljesítmény romlásával jár. Tünetei lehetnek:

– beszűkült figyelem, remegés, izzadás, irracionális félelem, érzelmi elárasztottság, döntési bizonytalanság.

A tudományos munkámban szereplő személyes reflexió szerint *„**a rendkívüli események folyamatának minden részletét és a pszichés tüneteit átélve azt szeretném elérni, hogy más rendvédelmi személy ne menjen végig azon az úton, amit 2020 és 2022 között tapostam”***[4]**.** Ez a mondat jól mutatja, hogy a distressz hosszú távon súlyos következményekkel járhat.

A trauma és a poszttraumás tünetek megjelenése

A rendkívüli események során átélt trauma nem csupán egy pillanatnyi sokkhatás, hanem olyan élmény, amely mélyen beépül a rendőr idegrendszeri működésébe.

A tudományos munkában szerepel: ***„a traumás szituációban stresszbetegség fog kialakulni, amelynek következő lépése, hogy a test megbetegszik”***. Ez a gondolat összhangban áll a modern pszichotraumatológia megállapításaival.

A trauma tünetei lehetnek:

- visszatérő képek, emlékbetörések,
- alvászavar, rémálmok,
- fokozott éberség,
- elkerülő magatartás,
- érzelmi kiüresedés,
- indokolatlan dühkitörések.

A rendőrök gyakran nem ismerik fel ezeket a jeleket, vagy szégyellik megélni őket. A tudományos munkám is hangsúlyozza: ***„a harcedzett katonák és rendőrök szégyellik, és nem mernek segítséget kérni”.***

A C-PTSD sajátosságai a rendőri hivatásban

A Komplex Poszttraumás Stressz Zavar (C-PTSD) akkor alakul ki, amikor a trauma nem egyszeri, hanem ismétlődő, tartós vagy extrém intenzitású. A rendőri hivatásban ez különösen gyakori, hiszen a szolgálat során a rendőr:

- rendszeresen találkozik halálesetekkel,
- erőszakos cselekményekkel,
- kiszámíthatatlan helyzetekkel,
- életveszélyes szituációkkal.

[4] (Nagy János r. százados BRFK, 2024)

A tudományos munkában szereplő személyes mondat: ***„Komplex Poszttraumás Stressz Zavart szenvedtem el, és ennek a sötét oldalának a szenvedése késztetett arra, hogy a rendkívüli eseményekkel foglalkozzak”*** – pontosan leírja a C-PTSD lényegét: a trauma nem ér véget az eseménnyel, hanem hosszú időn át jelen marad.

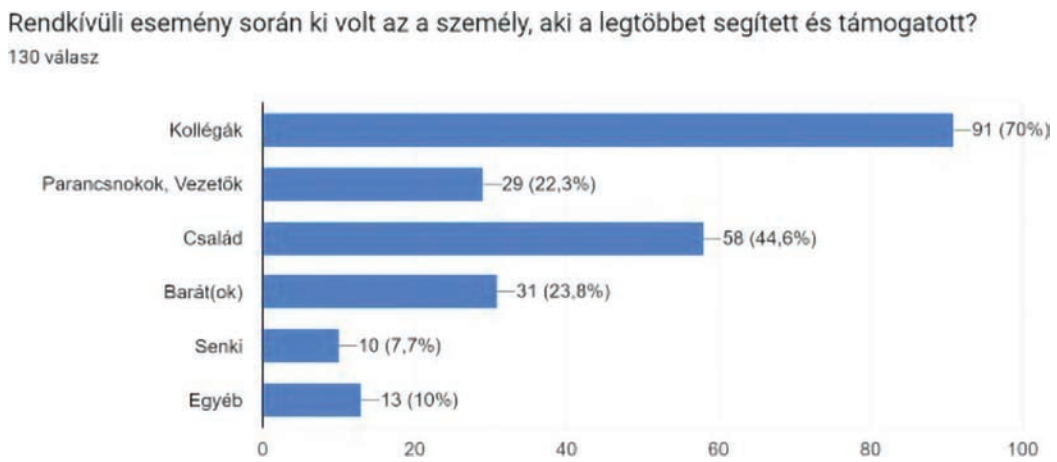
A trauma hatása a családi és társas kapcsolatokra

A rendőrök gyakran nincsenek tudatában annak, hogy a trauma nemcsak őket érinti, hanem a környezetüket is.

A tudományos munkámban szerepel: ***„a traumát hazavisszük, és a szeretteink is elszenvedik”***. Ez a jelenség a szakirodalomban „másodlagos traumatizációnak” nevezett folyamat. A családtagok gyakran tapasztalják:

- a rendőr érzelmi visszahúzódását,
- ingerlékenységet,
- alvászavarokat,
- túlzott éberséget,
- kommunikációs nehézségeket.

A trauma tehát nem egyéni, hanem **családi rendszerben megjelenő** probléma, amely a következő reprezantív felmérésem is megmutat. A vezetők a rendkívüli események utáni támogatásban vagy segítségben CSAK 22.3%-ban történik meg! Úgy gondolom, ennek 100% -nak kell lenni!



1. kép
Forrás: Nagy János, TDK 2024[5]

[5] (Nagy János r. százados BRFK, 2024)

Rövidített esettanulmány – 2020. december 24-én Budapest IV. kerület Kassai utca 19. szám alatt történt rendkívüli esemény szakmai tanulságai.

A rendkívüli események elemzése a rendőri intézkedéstaktika és a mentálhigiénés támogatás szempontjából egyaránt kiemelt jelentőségű.

A 2020. december 24-én, Budapest IV. kerületében történt Kassai utcai eset olyan komplex helyzetet teremtett, amely egyszerre érintette a rendőri intézkedés taktikai, kommunikációs, parancsnoki és pszichés dimenzióit.



2. kép
Forrás: (Police.hu, 2020)

A bejelentés egy zavartan viselkedő férfiról szólt, aki egy lakóépület bejáratát és ablakait ütötte. A helyszínre irányított járőrpár néhány percen belül életveszélyes támadás áldozatává vált: az egyik rendőr több szúrt sérülést szenvedett, a másik pedig sokkos állapotba került.

A tudományos munkában szereplő leírás szerint ***„a helyszínen szembesülni azzal a helyzettel, amikor a halál szele fogadott, a mai napig nem tudom szavakkal kifejezni”*** – ez jól érzékelteti a helyzet extrém pszichés terhelését.

A szolgálatparancsnok elsőként érkezett a helyszínre, ahol a súlyosan sérült rendőr ellátása, a járőrtárs felkutatása és az elkövető lokalizálása párhuzamosan, rendkívül gyors döntéshozatalt igényelt. A helyszíni körülmények – korlátozott információ, bizonytalan elkövetői helyzet, sérült kolléga életveszélyes állapota – olyan komplex stresszhelyzetet teremtettek, amely a rendőri intézkedések egyik legkritikusabb típusa.

Az eset több intézkedéstaktikai tanulságot is hordoz:

- **A Tevékenység Irányító Központ (TIK) által adott információk minősége és részletessége** alapvetően befolyásolja a helyszínre érkező állomány felkészültségét.
- **A lövedékálló mellény viselése** ilyen helyzetekben nem lehet mérlegelés tárgya.
- **A rádióforgalmazás korlátozása** a helyszínen lévőkre és a TIK-re elengedhetetlen a zavartalan koordinációhoz.
- **A járőrpárok pszichés felkészítése** kulcsfontosságú, hiszen a sokkreakciók (pl. megdermedés, beszűkült tudatállapot) valós kockázatot jelentenek.

A Tevékenységirányító Központ (TIK) feladatáról egy rövid ismertetést szeretnék írni, mivel a magyar rendőrség központosított ügyeleti rendszere, amely a vármegyei rendőr-főkapitányságok és a rendőrkapitányságok ügyeleti feladatait egységes szervezetben látja el. A jogszabályi meghatározás szerint a TIK **állandó ügyeleti szolgálati forma**, amely 24 órában biztosítja a rendőri szolgálat folyamatosságát a bejelentések fogadását az elsődleges intézkedések irányítását és a szolgálati erők koordinációját.

Folytatva az intézkedés tanulságait a rendkívüli esemény pszichés következményei hosszú távon is jelentkeztek. A tudományos munkában szerepel: ***„Komplex Poszttraumás Stressz Zavart szenvedtem el, és ennek a sötét oldalának a szenvedése késztetett arra, hogy a rendkívüli eseményekkel foglalkozzak."*** Ez a mondat rávilágít arra, hogy a trauma nem csupán az esemény pillanatában hat, hanem a későbbi életvezetésre, a szolgálatkészségre és a családi kapcsolatokra is.

Az esettanulmány tanulsága, hogy a rendkívüli események kezelése nem ér véget az intézkedéssel. A parancsnoki támogatás, a pszichológiai ellátás, a krízisintervenció és a mentálhigiénés utógondozás ugyanolyan fontos része a folyamatnak, mint az intézkedéstaktikai végrehajtás. A rendőri kultúrában ezért elengedhetetlen a szemléletváltás: a mentális egészség megőrzése a szolgálatbiztonság része.

Empirikus eredmények – A kérdőív elemzése

A rendkívüli események rendőri kezelésének vizsgálatához elengedhetetlen a gyakorló állomány tapasztalatainak és megéléseinek feltárása.

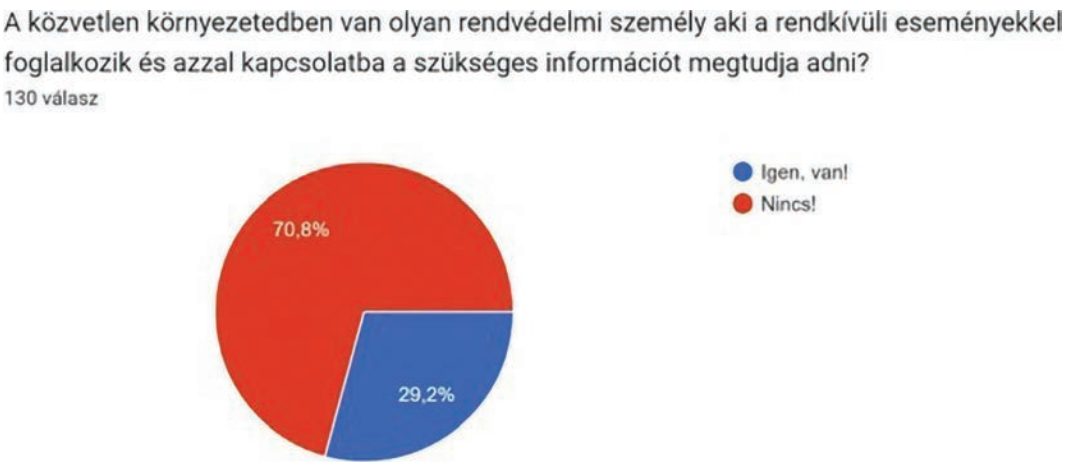
A kutatás célja az volt, hogy feltérképezze, milyen mértékben érinti a rendőröket a szolgálat során átélt trauma, milyen támogatást kapnak a feldolgozáshoz, és hogyan látják a jelenlegi intézkedéstaktikai, parancsnoki és mentálhigiénés rendszert.

A kérdőíves vizsgálat anonim módon zajlott, amely különösen fontos, hiszen a dokumentumban is szerepel: ***„a harcedzett katonák és rendőrök szégyellik, és nem mernek segítséget kérni***[6]***"***. Az anonimitás lehetővé tette, hogy a válaszadók őszintén számoljanak be tapasztalataikról, félelmeikről és a rendszer hiányosságairól.

[6] (Nagy János r. százados BRFK, 2024)

Kiemelten fontos hangsúlyozni, hogy a kollégák sok esetben nincsenek tisztában azzal, hogyan és kitől kérhetnek segítséget, illetve milyen módon és milyen keretek között kell a hozzátartozókat tájékoztatni. A rendkívüli esemény ugyanis nem ér véget azzal, hogy a szolgálati helyen megírjuk a jelentést. A megélt terhelést – akár tudatosan, akár akaratlanul – hazavisszük magunkkal, és a mentális állapotunk hatással van a szeretteinkre is.

Ezért elengedhetetlen, hogy a segítségkérés útjai, a támogatási formák és a családokkal való kommunikáció is egyértelmű, tanulható és elérhető legyen mindenki számára. Az alábbi elszomorító felmérésem eredménye is tükrözi.



3. kép
Forrás: Nagy János, TDK 2024[7]

A kutatás módszertana

A kérdőív több témakört érintett:

- rendkívüli események gyakorisága,
- pszichés tünetek megjelenése,
- parancsnoki támogatás megítélése,
- intézkedéstaktikai felkészültség,
- mentálhigiénés ellátáshoz való hozzáférés,
- a trauma hatása a magánéletre.

A válaszadók többsége közterületi szolgálatot teljesítő rendőr volt, akik rendszeresen találkoznak olyan helyzetekkel, amelyek potenciálisan traumát válthatnak ki.

[7] (Nagy János r. százados BRFK, 2024)

A rendkívüli események gyakorisága

A válaszok alapján a rendőrök jelentős része **havonta vagy hetente** kerül olyan helyzetbe, amely fokozott stresszel vagy traumával jár. Ez összhangban áll a dokumentumban szereplő megállapítással: *„a közterületi szolgálatot teljesítő állomány minden egyes szolgálatban találkozik valamilyen formában traumás szituációval”*.

A leggyakoribb eseménytípusok:

- agresszív, ittas vagy kábítószer hatása alatt álló személyekkel való intézkedés,
- öngyilkossági kísérletek,
- családon belüli erőszak,
- fegyveres vagy eszközös támadás veszélye,
- halálesetek kezelése.

A pszichés tünetek megjelenése

A válaszadók több mint fele számolt be olyan tünetekről, amelyek a trauma feldolgozatlanságára utalnak:

- alvászavar, visszatérő képek, fokozott éberség, ingerlékenység, érzelmi kiüresedés, elkerülő magatartás.

A tudományos munkában szereplő személyes reflexió – ***„a traumát hazavisszük, és a szeretteink is elszenvedik”*** – a kutatás eredményeiben is visszaköszön: a válaszadók jelentős része jelezte, hogy a szolgálat során átélt események a családi életükre is hatással vannak.

Parancsnoki támogatás és intézkedéstaktikai felkészültség

A kutatás egyik legfontosabb megállapítása, hogy a rendőrök többsége **nem érzi megfelelőnek a parancsnoki támogatást** rendkívüli esemény után. A tudományos munkám reprezantív felmérésében is szerepel: ***„a mai napig nincs erre semmilyen intézkedés vagy parancsnoki támogatás”*** – ezt a kérdőív eredményeim is alátámasztják.

A válaszadók szerint:

- a parancsnokok ritkán érdeklődnek a pszichés állapotuk felől,
- nincs egységes protokoll a traumás események utáni teendőkre,
- a krízisintervenció gyakran elmarad,
- a szolgálatba való visszatérés nem mindig fokozatos.

Az intézkedéstaktikai felkészültség megítélése vegyes volt: sokan jelezték, hogy a képzések elméleti jellegűek, és kevés a valós helyzeteket szimuláló gyakorlat.

Mentálhigiénés ellátáshoz való hozzáférés

A válaszadók többsége szerint a pszichológiai segítség:

- nehezen elérhető,
- nem rendszeres,
- nem kötelező,
- és sokan félnek igénybe venni a stigmatizáció miatt.

Ez összhangban áll a dokumentumban szereplő megállapítással: ***„nem mertünk segítséget kérni!”.***

A kutatás fő következtetései

A kérdőív eredményei alapján egyértelmű, hogy:

- A rendőrök rendszeresen találkoznak traumás helyzetekkel.
- A pszichés tünetek gyakoriak, de ritkán kerülnek kezelésre.
- A parancsnoki támogatás rendszere hiányos.
- A mentálhigiénés ellátás nem megfelelően hozzáférhető.
- A trauma hatása a magánéletben is megjelenik.

A kutatás tehát megerősíti, hogy a rendkívüli események kezelése nem csupán intézkedéstaktikai, hanem **komplex mentálhigiénés és szervezeti kérdés.**

Innovációs javaslatok – A rendkívüli események kezelésének fejlesztése

A kutatás eredményei, a személyes tapasztalatok és a nemzetközi gyakorlatok egyaránt azt mutatják, hogy a rendkívüli események kezelése csak akkor lehet hatékony, ha a rendőrség egyszerre fejleszti az intézkedéstaktikai, a parancsnoki és a mentálhigiénés rendszereit. A tudományos munkában szereplő megállapítás – ***„a magyar rendőrség minél gyorsabban a pszichológiai innovációs területre rá kell találjon”*** – pontosan kijelöli a fejlesztés irányát.

Az alábbi javaslatok rendszerszintű változtatásokat céloznak, amelyek hosszú távon növelik a rendőrök biztonságát, a szolgálat minőségét és a szervezet mentális ellenállóképességét.

Intézkedéstaktikai innovációk

A rendkívüli események kezelésének hatékonysága nagymértékben függ attól, hogy a rendőrök milyen felkészültséggel, milyen eszközökkel és milyen parancsnoki támogatással rendelkeznek.

A jelenlegi képzési rendszer túlnyomórészt elméleti jellegű, miközben a rendkívüli helyzetek valóságában másodpercek alatt kell döntést hozni, gyakran extrém stressz alatt. Ennek megfelelően elengedhetetlen a valós helyzeteket szimuláló gyakorlati képzések bevezetése. Ide tartoznak az életszerű szituációs gyakorlatok – például fegyveres vagy felfegyverkezve történő támadás, pszichésen zavart személy kezelése lépcsőházban vagy tömegközlekedési eszközön korlátozott látási viszonyok között –, valamint az éjszakai intézkedéstaktikai tréningek és a stressztesztelt intézkedéstaktikai feladatokra nagyon hangsúlyt fektetni. A kommunikációs lánc hatékonyságát TIK-szimulációk segíthetik, amelyek a valós idejű együttműködést gyakoroltatják.

A rendőrök fizikai biztonságának alapvető eleme a lövedékálló mellény viselése, amely nem lehet választási lehetőség, hanem szigorúan ellenőrzött kötelezettség.

A szolgálatparancsnokoknak kiemelt szerepük van abban, hogy a mellényviselést következetesen ellenőrizzék, miközben a rendszerben modern, könnyített védőfelszerelések bevezetése is indokolt. A helyszíni kommunikáció biztonsága érdekében szükség van a rádióforgalmazás protokolljának szigorítására is. Rendkívüli események során célszerű „csendes csatorna" protokollt alkalmazni, amelyben kizárólag a helyszíni egységek és a TIK kommunikálhatnak, minden más rádióforgalmazás automatikusan tiltásra kerül.

A parancsnoki felelősség megerősítése nélkülözhetetlen eleme a rendkívüli események utókezelésének.

A parancsnoknak kötelessége lenne minden ilyen eseményt követően személyes beszélgetést kezdeményezni, felmérni a beosztott pszichés állapotát, szükség esetén pszichológushoz irányítani, valamint dokumentálni a tapasztaltakat. A trauma utáni azonnali teljes terhelés gyakran kontraproduktív, ezért indokolt a fokozatos visszatérés rendszere: az első 1–2 szolgálat könnyített feladatokkal történjen, majd fokozatosan épüljön vissza a rendőr a teljes szolgálati terhelésbe.

A vezetők többsége nem rendelkezik megfelelő ismeretekkel a pszichés tünetek felismerésében, ezért elengedhetetlen a parancsnoki állomány kötelező képzése a PTSD, a komplex PTSD és a sokkreakciók felismerésére. A képzésnek gyakorlati példákat és esettanulmányokat is tartalmaznia kell, hogy a vezetők valós helyzetekben is magabiztosan tudjanak reagálni.

Mentálhigiénés rendszer innoválása

A tudományos munkában szerepel: ***„Krizisintervenció, pszichológiai konzultáció, csoportos terápiák sem voltak számomra a rendkívüli eseményt követően."*** Ez jól mutatja, hogy a jelenlegi rendszer nem jól működik.

1. Kötelező pszichológiai debriefing rendkívüli esemény után

Nem opcionális, nem kérdés – **kötelező.**

Javaslat:

- 24–72 órán belüli pszichológusi beszélgetés,
- 30 nap múlva kontroll,
- szükség esetén terápiás irányítás.

2. Anonim segítségkérési csatorna

A dokumentum is hangsúlyozza: ***„a rendőrök szégyellik, és nem mernek segítséget kérni”***.

Javaslat:

- anonim online felület (PTSD.hu vagy PTSD-Magyar Rendvédelemben zárt facebook csoport)
- 0–24 órás pszichológusi ügyelet,
- chat-alapú támogatás.

3. Családtámogató programok

A trauma a családot is érinti.

Javaslat:

- családi konzultációs lehetőség,
- rendőr-család edukációs programok,
- krízishelyzetben családtagok bevonása,
- ZoNa alapítvány bevonása.[8]

Szervezeti kultúra és szemléletváltás

A tudományos munkában szerepel: ***„a 90-es évek rendvédelmében szégyen volt, ha valaki gyengének mutatkozott”.*** Ez a szemlélet máig sok esetben jelen van.

1. A „gyengeség” helyett a „professzionalizmus” kultúrája

A segítségkérés nem gyengeség, hanem szakmai érettség.

2. A trauma normalizálása

A rendőröknek tudniuk kell, hogy a trauma természetes reakció.

[8] (ZoNa alapítvány, 2023)

3. A bajtársi támogatás erősítése (peer suport)

A PTSD-csoport (PTSD – A Magyar Rendvédelemben zárt facebook csoport) [9] kiváló példa arra, hogy a bajtársi közösség képes megtartó erőt adni.

A *peer support* olyan strukturált, szervezeti keretek között működő támogatási forma, amelyben azonos beosztású vagy hasonló szolgálati tapasztalattal rendelkező rendvédelmi dolgozók nyújtanak egymásnak pszichés és érzelmi segítséget. Lényege a tapasztalati tudásra épülő, bizalmi alapú támogatás, amely elősegíti a traumák korai felismerését, csökkenti a stigmatizációt, és hidat képez a szakmai mentálhigiénés ellátás felé.

Magyarországon elsőként kezdtem meg a kortársi támogatás azza a peer support tevékenységet és a visszajelzések alapján megállapítható, hogy a rendőrök gyakran nem mernek szakemberhez fordulni, viszont egy bajtárs előtt könnyebben megnyílnak.

A peer support munkám során csökkent a stigmatizáció, erősítette a közösséget és hozzájárult a mentális egészség hosszú távú megőrzéséhez és számomra az egyik legfontosabb egyik eleme, hogy csökkent a kiégés (burnout) a kollégáknál vagy pedig már mernek és tudnak segítséget kérni és kapni.

Összegzés

A rendkívüli események kezelése a rendőri hivatás egyik legösszetettebb és legnagyobb felelősséggel járó területe. A tanulmány eredményei egyértelműen rámutatnak arra, hogy a rendőrök szolgálatuk során rendszeresen találkoznak olyan helyzetekkel, amelyek túlmutatnak a hétköznapi intézkedéseken és amelyek egyszerre jelentenek fizikai, pszichés és mentális terhelést.

A tudományos munkában szereplő megállapítás – miszerint ***„a közterületi szolgálatot teljesítő állomány minden egyes szolgálatban találkozik valamilyen formában traumás szituációval***[10]***”*** – nemcsak személyes tapasztalat, hanem a kutatás eredményei által is alátámasztott tény.

A pszichológiai háttér bemutatása egyértelművé teszi, hogy a trauma nem csupán egy pillanatnyi sokkhatás, hanem hosszú távú, mélyen beépülő élmény, amely hatással van a rendőr személyiségére, döntéshozatalára, szolgálatkészségére és családi életére is.

A tudományos munkában szereplő mondat – ***„a traumát hazavisszük, és a szeretteink is elszenvedik”*** – pontosan összefoglalja a rendvédelmi trauma egyik legfontosabb sajátosságát: a hatása nem korlátozódik a szolgálatra.

Az empirikus kutatás eredményei megerősítik, hogy a rendőrök jelentős része nem kap megfelelő parancsnoki vagy pszichológiai támogatást egy rendkívüli eseményt követően.

[9] (PTSD-Magyar Rendvédelemben, 2022)
[10] (PTSD.hu Nem vagy egyedül, 2026)

A válaszadók többsége úgy érzi, hogy a jelenlegi rendszer nem biztosít elegendő mentálhigiénés ellátást, és a segítségkérés továbbra is stigmatizált. Ez a hiányosság nemcsak a rendőrök jólétét veszélyezteti, hanem a szolgálatbiztonságot is.

A tanulmányban megfogalmazott innovációs javaslatok – az intézkedéstaktikai képzések fejlesztése, a parancsnoki felelősség erősítése, a pszichológiai ellátás rendszerbe szervezése és a szervezeti kultúra átalakítása – olyan irányokat jelölnek ki, amelyek hosszú távon hozzájárulhatnak a rendőri állomány mentális ellenállóképességének növeléséhez.

A dokumentumban szereplő gondolat – ***„a magyar rendőrség minél gyorsabban a pszichológiai innovációs területre rá kell találjon***[11]***”*** – a tanulmány egyik legfontosabb üzenete.

A rendkívüli események kezelése tehát nem csupán szakmai feladat, hanem emberi felelősség is. A rendőrök mentális egészségének megőrzése a szolgálatbiztonság alapfeltétele, és olyan terület, amelyben a szervezet minden szintjének – a járőrtől a parancsnokig – szerepe és felelőssége van.

A tanulmány célja, hogy hozzájáruljon egy olyan rendőri kultúra kialakításához, amelyben a trauma felismerése, kezelése és megelőzése természetes része a hivatásnak.

Zárógondolat

A rendkívüli események kezelése a rendőri intézkedések során nem csupán szakmai felkészültséget, hanem magas szintű emberi érzékenységet, felelősségvállalást és a társadalmi bizalom folyamatos építését is megköveteli.

Az elmúlt évek tapasztalatai egyértelművé tették, hogy a rendvédelmi szervek hatékony működéséhez elengedhetetlen a traumák felismerése, a pszichés terhelés kezelése, valamint a gyermekekkel és más sérülékeny csoportokkal kapcsolatos ügyekben a különösen körültekintő, értékalapú megközelítés.

A „Gyermekek mindenek felett” program szerepe

E szemlélet egyik legmeghatározóbb hazai példája Illés Zoltán rendőr ezredes, a Hajdú-Bihar Vármegyei Rendőr-főkapitányság vezetője által kezdeményezett és működőképessé formált **„Gyermekek mindenek felett” program**. A program célja, hogy a gyermekekkel kapcsolatos rendőri intézkedések minden körülmények között a gyermek legfőbb érdekét helyezzék előtérbe. Ennek érdekében a rendőrök olyan módszertani, kommunikációs és pszichológiai támogatást kapnak, amely segíti őket a traumatizált, bántalmazott vagy veszélyeztetett gyermekekkel való megfelelő, biztonságos és érzékeny bánásmódban.

A program jelentősége messze túlmutat a gyermekvédelem keretein:

[11] (Nagy János r. százados BRFK, 2024)

- erősíti a rendőri állomány érzékenységét,
- támogatja a másodlagos traumatizáció megelőzését,
- javítja a rendőri intézkedések minőségét,
- hosszú távon pedig hozzájárul a társadalmi bizalom növeléséhez.

Illés Zoltán ezredes kezdeményezése mára országos szakmai figyelmet kapott és példát mutat arra, hogyan lehet a rendőri hivatást a humánum, a gyermekvédelem és a traumaérzékenység irányába továbbfejleszteni.

A ZoNa Alapítvány szerepe a rendvédelemben

A rendkívüli események kezelése során a rendőrök gyakran találkoznak olyan helyzetekkel, amelyek mély és tartós pszichés terhelést jelentenek. A traumák feldolgozása, a segítségkérés kultúrájának erősítése és a kortársi támogatás fejlesztése nélkülözhetetlen ahhoz, hogy a rendvédelmi dolgozók hosszú távon is egészségesen, stabilan és magas szakmai színvonalon tudjanak szolgálatot teljesíteni.

Ebben a munkában kiemelkedő szerepet tölt be a **ZoNa Alapítvány**, amely országos szinten támogatja a gyermekvédelem, a traumaérzékeny szemlélet és a rendvédelmi közösségek mentális egészségének erősítését.

Az alapítvány:

- érzékenyítő és edukációs programokat szervez,
- szakmai együttműködéseket épít a rendőrséggel,
- támogatja a traumát átélt gyermekeket és családokat,
- aktívan részt vesz a rendvédelmi dolgozók mentális támogatásában és a stigma csökkentésében.

A ZoNa Alapítvány tevékenysége azért bír kiemelt jelentőséggel, mert hidat képez a civil szféra, a gyermekvédelem és a rendőrség között. Munkája hozzájárul ahhoz, hogy a rendőrök ne csupán jogi és szakmai, hanem emberi, pszichológiai és társadalmi szempontból is felkészültebbek legyenek a rendkívüli események kezelésére.

A rendőri hivatás lelki terhei és a kultúraváltás szükségessége

A rendőri hivatás sajátossága, hogy a szolgálatot teljesítők nap mint nap olyan helyzetekkel találkoznak, amelyek egyszerre próbára teszik szakmai tudásukat, fizikai felkészültségüket és lelki teherbírásukat. A rendkívüli események nem csupán intézkedéstaktikai kihívást jelentenek, hanem mély, sokszor láthatatlan nyomot hagynak a rendőrök életében.

A tanulmány egyik alapvető felismerése – **miszerint *„a pszichés háttér minden egyes rendkívüli eseménynél megjelenik, ha akarjuk, ha nem”*** – pontosan összefoglalja a probléma lényegét.

A rendőri kultúra átalakulása, a mentálhigiénés támogatás megerősítése és a parancsnoki felelősség újragondolása nem csupán szakmai szükségszerűség, hanem emberi kötelesség is. A rendőrök mentális egészsége a szolgálatbiztonság része, és olyan érték, amelyet a szervezet minden szintjén védeni kell. A cél nem csupán a traumák kezelése, hanem egy olyan támogató környezet kialakítása, amelyben a rendőrök biztonságban érzik magukat – a szolgálatban és azon kívül is.

Szemléletváltás és közösségi kezdeményezések

A tanulmány üzenete egyszerű, mégis alapvető: **A rendőr is ember, és a rendkívüli események feldolgozása nem gyengeség, hanem a hivatás része.** A jövő rendőrsége akkor lesz erős, ha tagjai és hozzátartozói lelkileg is támogatást kapnak. Ez a szemléletváltás nemcsak a rendőrök, hanem a társadalom biztonságát is szolgálja.

A saját tapasztalataim és a szolgálat során átélt traumák hatására **kortársi támogatásként** – Magyarországon elsőként – létrehoztam a rendvédelmi dolgozók számára a **„PTSD – Magyar Rendvédelemben"** zárt online közösséget, valamint a civil lakosság számára a **„PTSD.hu – Nem vagy egyedül"** ingyenes webfelületet. Ezek a platformok információt, közösséget és kortársi támogatást nyújtanak mindazoknak, akik érintettek a traumák feldolgozásában.

Irodalomjegyzék:

1. Máté, G. (2022). *A test lázadása – A stresszbetegségek rejtett okai.*
2. U.S. Department of Veterans Affairs (1989). *PTSD: National Center for PTSD – Guidelines and Resources.*
3. Magyar Rendőrség ORFK (2024). *Statisztikai adatok a rendőrök elleni erőszakos cselekményekről.*
4. PTSD – Magyar Rendvédelemben | Facebook[12]
5. Kapcsolat – PTSD.hu | Nem vagy egyedül...[13]

Egyéb források:

- Nagy János (2024). Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Határrendészeti szakirány, *TDK munkája: A rendkívüli események kezelése a rendőri intézkedések során.*
- PTSD – A Magyar Rendvédelemben (2023–2024). Zárt szakmai közösség tapasztalatai és esettanulmányai.

[12] (PTSD-Magyar Rendvédelemben, 2022)
[13] (PTSD.hu Nem vagy egyedül, 2026)

Bakai Levente[1]

Új kihívás a tűzvédelmi tervezésben, az építményinformációs modellezés (BIM), mint munkamódszer

Abszrakt:

A BIM, mint építészeti, tervezési módszer, az utóbbi évtizedben kezdett hazánkban igazán kibontakozni. Az ezt megelőző időszakban az épületek modellezése a háromdimenziós ábrázolásra fókuszált, mely a látványtervek és egyéb részlettervek *megjelenítésére korlátozódtak. Az építményinformációs modellezés (Building Information Modelling – BIM) számos előnnyel jár a korábbi tervezési folyamatokhoz képest. Ennek felismerésével a BIM, mint tervezési módszer egyre elterjedtebbé vált, mígnem az MSZ EN ISO 19650 szabvány megjelenésével nemzetközi szinten is egységes keretrendszerbe foglalták* (Magyar Szabványügyi Testület, 2019a, 2019b)*. Egy épület tervezése több szakág együttműködésével történik. A keretrendszer azonban nem határoz meg konkrétumokat, nem jelöli ki a pontos útvonalat a hatékony tervezési folyamatra vonatkozóan, így a tűzvédelmi tervezésre vonatkozóan sem. Bár a tűzvédelmi tervezés részét képezik a beépített tűzjelző és beépített tűzoltó berendezések tervezése is, ezek az épületbe helyezett kézzel fogható elemekből állnak, így modellezésük nem jelent sokkal nagyobb kihívást az egyszerű „nem BIM" tervezési módszerekhez képest. Nem így az építészeti tűzvédelmi tervezés, amely nem konkrét elemek modellezését jelenti, hanem követelmények megjelenítését egy modellhez – általában építész modellhez – kapcsolódóan. Több hazai értekezés mutat rá ennek nehézségeire és annak leküzdésére vonatkozó lehetőségekre, ám ezek nem, vagy csak minimális mértékben foglalkoznak az úgynevezett* closedBIM *környezetben történő tűzvédelmi tervezéssel (Hajdu, 2023).*

Kulcsszavak: BIM, tűzvédelem, tervezés, IFC, closedBIM, tűzvédelmi modell, 3D, generál tervezés, Revit, paraméter, szoftverkörnyezet,

Abstract:

BIM, as an architectural and design method, has really begun to take off in Hungary over the last decade. Prior to this, building modelling focused on three-di-

[1] gépészmérnök, tűzvédelmi tervező szakmérnök, beépített tűzoltó berendezés tervező TUO, építészeti tűzvédelmi tervező TUÉ, Studio In-Ex Zrt, tűzvédelem stúdióvezető, MMK tűzvédelmi tagozat BIM szakmai kollégium, TvMI oltóberendezések munkacsoport

mensional representation, which was limited to the visualisation of renderings and other detailed drawings. Building Information Modelling (BIM) offers numerous advantages over previous design processes. As this has been recognised, BIM as a design method has become ever more widespread, with the publication of the MSZ EN ISO 19650 standard establishing a unified framework for it at an international level as well. The design of a building involves collaboration between several disciplines. However, the framework does not specify details nor does it set out a precise path for an efficient design process, including fire protection design. Although fire protection design includes the design of built-in fire alarm and fire-fighting systems, these consist of physical elements installed within the building; consequently, modelling them does not present a significantly greater challenge than simple 'non-BIM' design methods. This is not the case with architectural fire safety design, which does not involve the modelling of specific components, but rather the representation of requirements in relation to a model – usually an architectural model. Several Hungarian dissertations highlight the difficulties involved and the possibilities for overcoming them, but these do not, or only to a very limited extent, deal with fire safety design within the so-called closedBIM environment.

Keywords: BIM, fire protection, planning, IFC, closedBIM, fire safety modell, 3D, general planning, Revit, parameter, software environment

Bevezetés

Tervezőtársaimmal több, mint tíz éve elköteleződtünk a legmodernebb generáltervezési technológia mellett. Azóta számos újításon, felmerült problémán, a tervezőprogram korlátainak megismerésén, számos saját fejlesztésű Revit beépülőn túl, továbbra is kitartunk a kitűzött irány mellett. Anélkül, hogy mélyebben belemennénk a BIM, mint módszer elméleti hátterébe, az alábbiakban bemutatásra kerül, hogyan integráltuk a tűzvédelmi tervezést a closedBIM környezetbe.

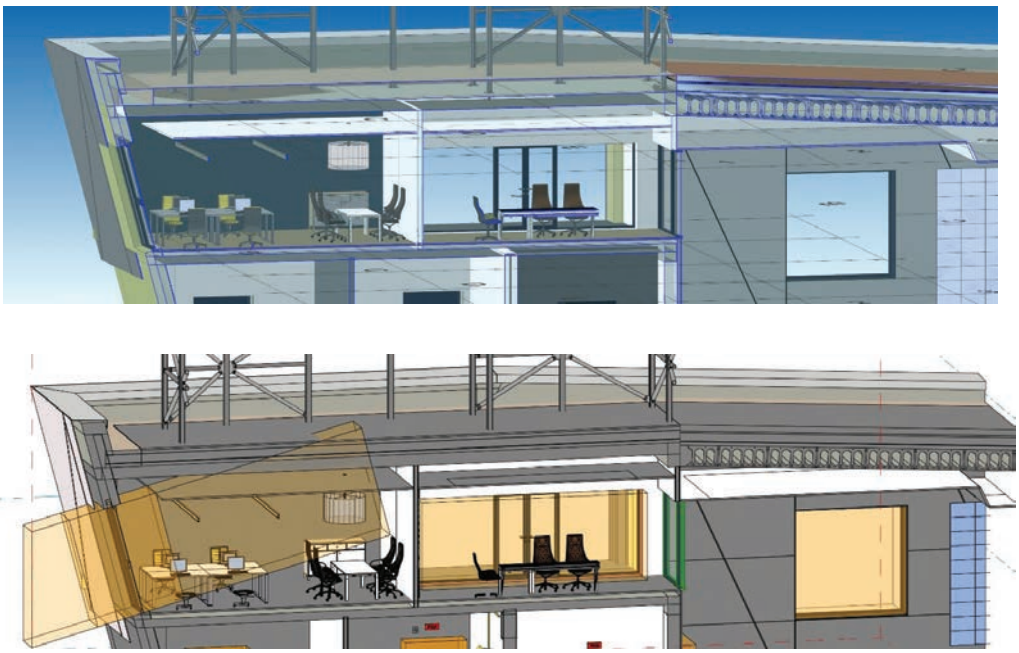
A teljes írás saját tervezőcsapatunk gyakorlati tapasztalatain alapul, nem hivatott a BIM olyan elméleti mélységeibe elkalauzolni az olvasót, melyekről számos írás rendelkezésre áll és egy egyszerű kereséssel fellelhető az Interneten.

Alapvető különbség closedBIM és openBIM között a gyakorlatban, röviden

Számos cikk született már a tűzvédelmi tervezés és a BIM kapcsolatáról, ám ezek a publikációk javarészt, az *openBIM* környezetben való eligazodást segítették. Érthető, hiszen Magyarországon ez a legelterjedtebb munkamódszer, ha BIM-ről van szó. Ezen túl azonban mi egy más, szorosabb együttműködést lehetővé tevő BIM módszert alkalmazunk, amelyet *closedBIM*-nek nevezünk.

Az openBIM lehetővé teszi, hogy a különböző szakágak különböző szoftverkörnyezetben készítsék el saját szakági modelljeiket. OpenBIM tervezési folyamatban egy adott szakág előzetes megállapodások alapján bizonyos időintervallumonként az aktuális modelljének állapotát átkonvertálja IFC formátumba, majd az összes szakág modelljét összegyűjtik egy fájlmegosztó rendszer felületre, ahonnan minden résztvevő letölti a számára szükségeset és jó esetben néhány óra – vagy akár egy teljes nap – elteltével meg tudja nyitni azt a saját szoftverkörnyezetében. Könnyen belátható, hogy a konvertálások és mentések között eltelt időben történt módosításokról akár hetekkel később jelennek meg a tervezési folyamatot befolyásoló változások, amik nem kevés meglepetést tartalmazhatnak. Nem beszélve azokról az IFC exportálás vagy eltérő megjelenítő szoftver miatt elveszett információkról, amiknek bizony IFC használata esetén búcsút inthetünk (Boeykens, 2023). Mindezt tetézi az a mérhetetlen mennyiségű idő, amennyit mind az adatszoláltatás, mind az adat felhasználási oldalon a konvertálások, beillesztések, frissítések felemésztenek. Az idő pedig ma már az egyik kulcsfontosságú eleme a tervezésnek is. Az openBIM technológiát alkalmazva nem támaszkodhatunk csupán a modellre, mindenképpen szükséges kiegészíteni szakági rajzokkal.

Véleményem szerint kiegészítő információnak kiváló, ami segít értelmezni a 2D-ben készült terveket, de közel sem nyújt kielégítő megoldást a tervezés egészére nézve.



1. ábra: Az IFC és IFC közötti különbségekről eltérő megjelenítőben ugyanazon modellrészletről[2]

[2] saját kép IFC képkivágás, tervezési projekt részlet

A closedBIM hátránya az előnye is egyben. Egyetlen szoftverkörnyezetet határoz meg minden szakági tervező számára, ezáltal biztosítva, hogy saját modelljüket szinkronizálják a többi szakág aktuális modelljével. És ez a lényege, a közös platform, a zökkenőmentes átjárhatóság a különböző tervezési területek modelljei között, amely adatokat minden résztvevő egyértelműen és egyformán tud értelmezni. A modelleken történt változások folyamatosan nyomon követhetők a tervezésben részt vevő többi szakág számára is adatvesztés és időveszteség nélkül. Egyetlen „szinkronizálás" gomb megnyomásával már frissül is a modell bármely résztvevő számára.

Röviden: ha pl. az építész tervezők egy ajtót elhelyeztek az építész modellben és elmentették a változást, akkor a többi szakág számára gyakorlatilag azonnal megjeleníthető ez az új ajtó.

A szűk keresztmetszetet az openBIM, illetve closedBIM közötti választásnak általában egyetlen fő szakág megszokott tervezési módszere/szoftverkörnyezete adja, akkor is, ha adott esetben a tervezés résztvevőinek rangsorában második, harmadik helyet elfoglaló épületgépészet és elektromos szakágak egyazon, de a fő szakághoz képest eltérő tervezőplatformra rendezkedtek be.

Miért látjuk mi előnyösebbnek a closedBIM tervezési módszert a magunk szempontjából?

Generáltervező csapatunk 140 fő állandó tervezőmérnökből áll. Nálunk tehát adott a lehetőség, hogy egyetlen platformon dolgozzon mind a 140 mérnök, legyen az építész, szerkezettervező, épületgépész, erősáramú, vagy gyengeáramú tervező, vagy éppen tűzvédelmi tervező. Több, mint 10 évvel ezelőtt az építészeink is átálltak a Revit platformra, innen kezdve minden akadály elhárult a closedBIM-ben történő tervezés elől. Létrehoztuk saját BIM szakmai csapatunkat, akik fejlesztőmérnökeinkkel folyamatos támogatást nyújtanak a BIM kihívásainak leküzdésében, emellett egy úgynevezett BIM Technician Team is felállításra került, akik az egyes szakágspecifikus BIM relevanciájú problémák megoldásában segédkeznek. Ez utóbbi csapat tagjai a különböző szakágak tervezőmérnökeiből tevődik össze, akik a mindennapi tervezés mellett végzik áldásos tevékenységüket.

Tűzvédelmi tervezés BIM környezetben… Az útkeresés

Habár tervezőtársaimmal a tűzvédelem teljes spektrumát lefedjük, azaz építészeti tűzvédelmi tervezésen és annak kiegészítő szolgáltatásain kívül beépített tűzoltó berendezések tervezése és gyengeáramú rendszerek tervezése is portfóliónk részét képezi, jelen írásomban mégis csak az építészeti tűzvédelemre fókuszálnék.

Ennek legfőbb oka, hogy meglátásom szerint a beépített tűzoltó berendezések tervezése és a tűzjelző rendszerek tervezése már több éve elindult a „BIM útján" ezért talán ezeknek a fejlődési iránya lassan, de biztosan egy egyenes mentén halad,

az építészeti tűzvédelemben viszont még nagyon homályos, merre is kellene, vagy lehet haladni, egyáltalán milyen lehetőségek állnak azon kollégák előtt, akik komolyabban érdeklődnek a BIM módszerek iránt (Singh, 2024).

Nagyjából 5 éve fogalmazódott meg a gondolat, hogy ha már a csapatban mindenki Revit-ben dolgozik, mi lenne, ha mi tűzvédelmi tervezők is felhagynánk a hagyományosnak tekinthető tervezési módszerekkel, és elkezdenénk „BIM-esen" dolgozni.

A kiindulópont

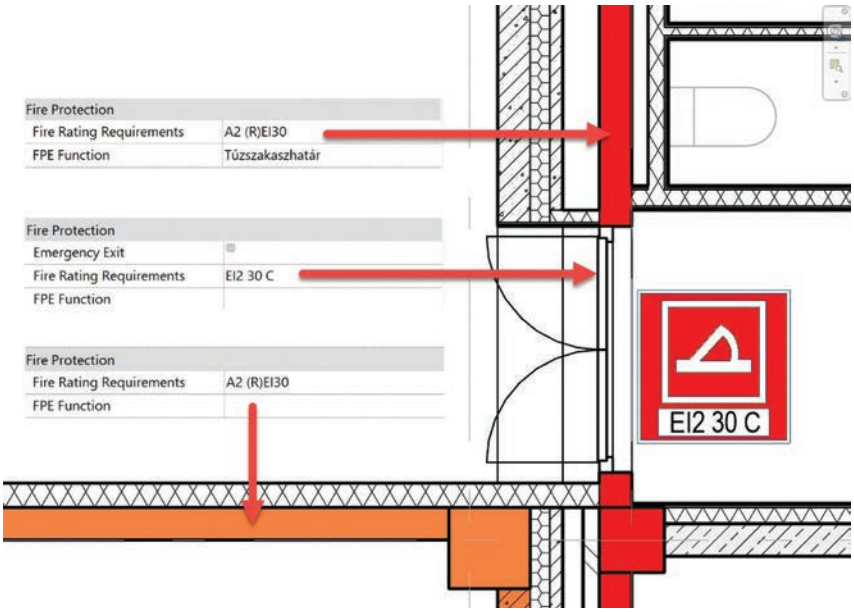
Első változatban a tűzvédelmi tervezés még AutoCAD-ben történt, de a többi releváns szakág Revitben készítette a modelleket, terveket.

A tervezés előrehaladtával a tűzvédelmi tervezéshez szükség volt alaprajzokra, metszetekre. Ezeket az adatszolgáltatásokat az építész szakág biztosította számunkra jellemzően az ő alaprajzuk, metszetük .dwg-be történő exportálásával. A .dwg rajzra jelöltük a tűzvédelmi követelményeket, majd az építész szakág a tűzvédelmi rajzos mellékletnek megfelelően saját modelljében megfelelő paraméterekkel látta el azon építményszerkezeteket, amelyekre tűzvédelmi követelmény került megfogalmazásra. Ez egy hagyományos módszernek mondható, viszont lehetőségünk volt 3D-ben ellenőrizni a modellt olyan esetekben, ahol nem volt egyértelmű számunkra az építészeti kialakítás. Mivel „házon belül" dolgozunk, bármikor, bármilyen épületrészre ráláttunk.

Ahogy egyre inkább elmélyedtünk a BIM rejtelmeiben, mint építészeti tűzvédelmi szakág, szerettünk volna még hatékonyabban eljárni a tervezés folyamán. Elindultunk abba az irányba, hogy nem külön exportált rajzon jelöljük a tűzvédelem relevanciájú követelményeket, hanem közvetlenül Revitben a vonatkozó szakági modellben, ezzel megtakarítjuk azt az időt, amit exportálással kell tölteni. Ha már eleve van rálátásunk az építész és egyéb szakági modellekre, úgy gondoltuk kézen fekvő, hogy ezeket használjuk is.

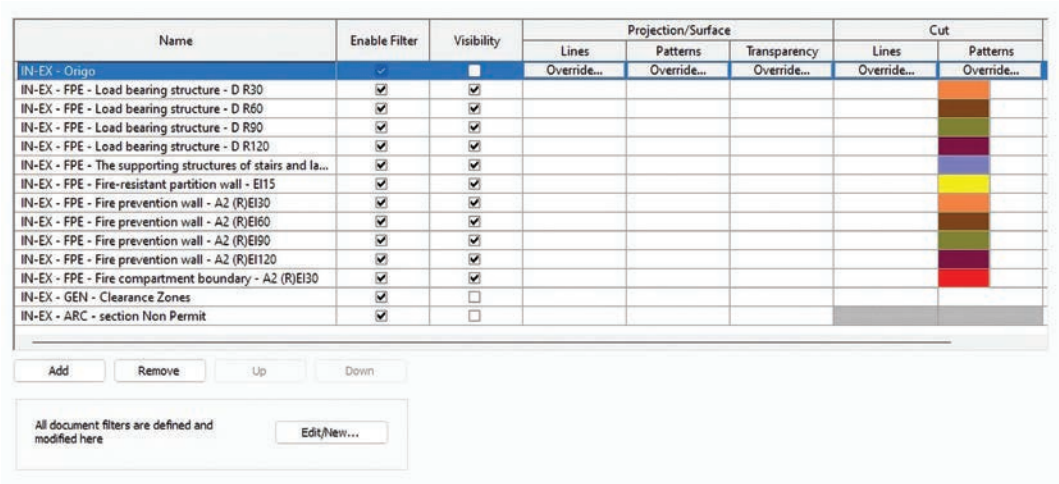
Szintet léptünk

Teljes hozzáférésünk volt minden szakág modelljéhez, melyek közül számunkra az építészet és a statika volt a legfontosabb. Az egyes modellelemek paraméterei közé ezekben a szakági modellekben felvettünk olyanokat, amelyekben megjelenítettük a tűzvédelmi követelményeket. Például egy általános építményszerkezeti elembe bekerült a „fire rating requirement" (tűzvédelmi követelmény), egy ajtó elembe ezen felül bekerült „required clear width" (szükséges szabad szélesség), valamint a room (helyiség) elembe bekerültek a „fire compartmanet" (tűzszakasz), „heat and smoke extraction" (hő- és füstelvezetés), „fire suppression system" (beépített oltóberendezés) ez utóbbiak yes/no paraméterként is értelmezhetők, gyakorlatilag jelöljük, hogy lesz az adott helyiségben, vagy nem.



2. ábra: Építményszerkezetek paraméterei az építész és statika modellben[3]

A paraméterek megléte és kitöltése a Revit-ben lehetőséget adott a színekkel történő megkülönböztetésre, különböző szűrőkhöz való szín rendeléssel. Az azonos értékkel rendelkező paramétereket azonos színnel/mintázattal tudtuk jelölni, mindössze annyit kellett tennünk, hogy meghatároztuk, mely értéknek milyen színe/mintázata legyen és a szűrőt alkalmaztuk.



3. ábra: Paraméterek szűrése lehetőséget ad az azonos követelmények azonos színnel történő megkülönböztetésére[4]

[3] saját kép, képkivágás egy tervezési projektből
[4] saját kép, képkivágás, beállított szűrők egy tervezési projekten

Az egyes elemek tűzvédelmi követelményeit ún. TAG-ek segítségével jelenítettük meg, így a feliratozásuk, szimbólumokkal történő ellátásuk a beírt paraméterek alapján automatikusan megtörténhetett. Egy ajtó esetében ezt úgy lehet elképzelni, hogy ha a „fire rating requirements" paraméterbe felvettük az „EI2 30 C3" szöveget, a TAG megjelenített egy tűzgátló ajtó szimbólumot, rajta a beírt felirattal, amint az ajtót kiválasztottuk.

Ez nagyon egyszerűnek tűnik első ránézésre, de ennek a módszernek is megvannak a maga hátrányai.

Minden modellt, (építészet, statika) külön meg kell nyitni ahhoz, hogy a paraméterek értékeit kitöltsük. Egy nagy méretű, több tízezer négyzetméter összesített alapterületű épület esetén az egyes szakági modellek megnyitása még egy erre felkészült IT hálózattal és munkaállomással rendelkező tervező türelmét is próbára teszi, több percnyi várakozást kikényszerítve a felhasználóból.

Amivel eddig a pontig nem találkoztunk, az az egy adott falra vonatkozó eltérő követelmények kezelésének szükségessége. Gondoljunk csak bele, ha van egy folyosó, amiről nyílik egy gépészeti helyiség, egy elektromos helyiség, egy tűzoltási beavatkozási központ, vagy egyéb, rendeltetéstől függően tűzvédelmi követelménnyel rendelkező falszakaszt igénylő helyiség, a folyosónak a helyiséggel azonos szakasza tűzvédelmi követelményt „kap", de a további falszakaszra nem határoz meg jogszabály követelményt. Lehet, hogy a fal szerkezete teljes folyosó hosszban rendelkezik ugyanazzal a tűzvédelmi teljesítménnyel, de követelmény még sincs rá.

Ennek kiküszöbölésére a falakat követelmény szerinti szegmensekre kellett osztanunk, ami az építészeti szakágnak nem jelentett túl nagy problémát, de figyelmetlenségből így is előfordult, hogy egy fal magasságát átállítva a falnak csak egy része került változtatásra. Alaprajzi nézeten az eltérés nem érzékelhető, így előfordulhat, hogy végül az eltérés észrevétlen marad és további problémákat generál akár a tervezői mennyiségi kiírásban. A falak felosztása jelentősebb problémát a statika szakági modellekben okozott. Tervezési folyamatunkban a vasbeton elemek vasalási tervei is Revit-ben készülnek, ezért egy ilyen feldarabolás, különösen, ha ez egy utólag érkezett késői információ miatt szükséges, a beton vasalási tervekre erősen rányomta a bélyegét.

Ezen felül észrevettük, hogy a tervezés előrehaladtával egyes tűzvédelmi paraméterekkel rendelkező elemek a modellekben véletlenszerű helyeken „bukkantak fel". Később rájöttünk, hogy ennek oka, a már megmodellezett elemek gyorsabb munkavégzés reményében történő másolása több helyre. A másolással természetesen a már beállított tűzvédelmi követelmény is másolásra került. Ezek a hibák váratlanul, az előzőleg beállított szűrők futtatásakor kerültek csak felszínre.

Revitben dolgoztunk az építész modellben, már minden szakágnak adott volt a lehetőség, hogy egyes dedikált nézeteket, amelyeken megjelenítettük a tűzvédelmi követelményeket élőben nyomon kövessenek, akár különösebb előkészület nélkül behivatkozzák a saját nézetük alá (mintha AutoCAD-ben xref-elnénk). De a modell

többi részén, ami nem szerepelt nézeten, nem láthatták a követelményeket (pl. födémek, speciális, tűzszakaszhatárok, álmennyezetek helyiségenként).

Olyan megoldást kerestünk, ami egyben adatszolgáltatásként és tervszintű kiadásra is megállja a helyét, ezért a fejlesztést a 3D tűzvédelmi terv irányába fordítottuk.

Míg az eddigiekben rendre megtartottunk bizonyos módszereket a hagyományos tervezésből, ezúttal teljesen új irányba fordultunk.

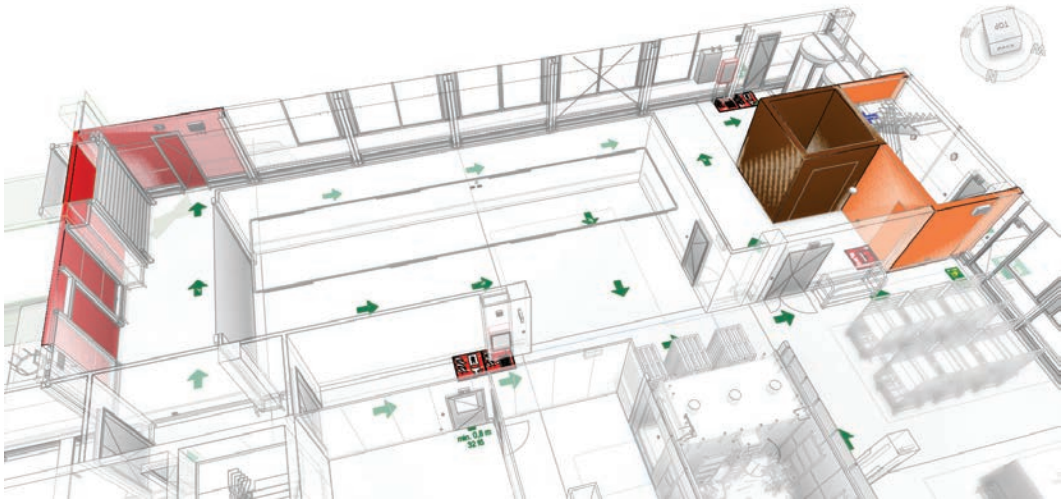
Létrehoztuk a tűzvédelmi modellt…

A tűzvédelmi modell elképzeléseink szerint olyan egyedi elemekkel kerül felépítésre, amelyek képesek a tűzvédelmi követelményeket az épület bármely területére egyértelműen megmutatni. Ez csakis 3D-s jelekkel tűnt lehetségesnek. Létrehoztunk új szimbólumokat, amelyek 3D elemként jelennek meg minden szakág számára, továbbá 3D feliratokat, saját fal elemeket, melyek színe a követelményeknek megfelelően változtatható. A kiürítési útvonalakat 3D nyilakkal jelöltük, a kiürítési szimbólumokat is 3D elemként helyeztük el a modellünkben, amely állandó összeköttetésben áll minden egyéb szakág modelljével.



4. ábra: 3D-s szimbólumokat alkalmazunk, amely a 3D modell bármely részén bármely szakág számára egyértelmű adatszolgáltatást jelent.[5]

[5] saját kép, képkivágás az elkészített 3D szimbólumokról



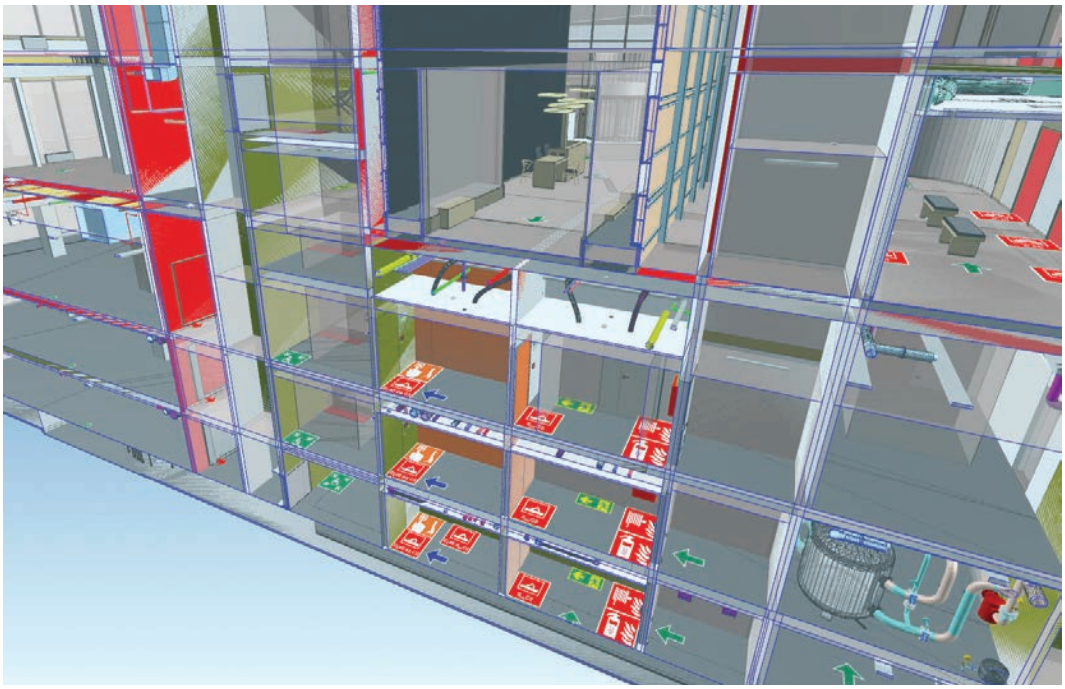
5. ábra: 3D tűzvédelmi modell Revitben egy általános tervezési feladatban. Egyértelműen kivehetők a követelmények.[6]

A 3D modellelemek alkalmazása nem igényel jelentősebb energiabefektetést, hiszen például egy fal elem követelményeinek meghatározásánál ugyanúgy egy vonalként megrajzolt fal elemet helyezünk le, azzal a különbséggel, hogy ennek immár az alsó és felső síkját is be kell állítanunk. Ennek következtében azonban olyan, geometriailag összetettebb helyzetekkel is szembesülünk, melyeket csupán az alaprajzra hagyatkozva nem éreznénk megoldandónak. A megoldandó problémával ezáltal nem a kivitelezési fázisban, hanem már a tervezőasztalon találkozunk, így a felmerült problémára várhatóan sokkal jobb, átgondoltabb tűzvédelmi megoldásokat találhatunk.

Azon túl, hogy 3D elemeket alkalmazunk, az általunk elhelyezett szimbólumok és jelölések szintén rendelkeznek a megfelelő paraméterekkel, így amennyiben egy tervező kolléga, legyen bármely szakág képviselője kijelöli valamelyiket, további releváns információkat is talál. Többek között rögzítjük a modellelemben a követelményt előíró jogszabály, szabvány, vagy megrendelői hivatkozásokat (The Vertex Companies, 2023). Ezzel a későbbiekben is tudjuk, miért azt a követelményt határoztuk meg, ami a modellbe került.

A módszer további előnye, hogy akár egy minimális rendszerigényű IFC modellben a tűzvédelem is megjeleníthetővé válik, hiszen nem csak bizonyos tervlapokon, vagy bizonyos dedikált nézeteken jelennek meg a követelmények, hanem a teljes modellben, így akár egy ingyenes IFC megjelenítő segítségével bárki meg tudja jeleníteni és értékelni a tűzvédelmet, akár magán az építkezés helyszínén is.

[6] saját kép, képkivágás, 3D nézet egy tervezési projekten



6. ábra: Modell megjelenítése BIMCollab Zoom (free version) programban. Tetszőleges metszet.[7]

A 3D tűzvédelmi modell lehetőséget ad bizonyos automatizmusok létrehozására is. A jövőben ezek az automatizmusok tovább egyszerűsítik a munkánkat és minimalizálják a hibalehetőségeket. Jelenlegi fejlesztésünk kapcsán olyan megoldást dolgozunk ki, amely megteremti a tűzvédelmi modell és az egyéb szakági modell közötti kommunikációs kapcsolatot. Amennyiben a tűzvédelmi modellben egy szimbólumot elhelyezünk, az összekapcsolható legyen az egyéb szakági modellekkel és egyes paraméterek automatikusan átemelésre kerüljenek a tűzvédelmi modellből, így a követelményeket egyetlen modellben lesz szükséges kezelni, minimalizálva a hibázás lehetőségét. Ilyen lehet akár egy nyílászáró bármely tűzvédelmi paramétere, amely releváns a konszignáció során.

A jövőben egyre hangsúlyosabb szerep jut majd a BIM modelleknek, nem csak a tervezés, hanem az építmény teljes életpályája alatt. Ezekből pontosabb információk nyerhetők ki karbantartás, átalakítás, vagy bővítés során, melyekhez a tűzvédelmi követelmények és berendezések pontos ismerete elengedhetetlen.

Konklúzió

Ahogy a fentiekből is látszik a BIM-ben történő tűzvédelmi tervezés nem összehasonlítható a jelölővonalak rajzolásával egy alaprajzra. Igen, sokkal összetettebb

[7] saját kép, képkivágás egy tervezési projekten

és több befektetett munkát igénylő folyamat, de a beruházó és a kivitelező számára átadott információ mélysége is egészen más. Arról nem is beszélve, hogy a tervezés résztvevői közötti gyors és félreérthetetlen információáramlás előrevetíti, hogy a folyamat végén átgondolt, mindenki számára azonosan értelmezett tervek szülessenek kiegészítve egy átlátható 3D BIM modellel, amely tényezők összessége ma már elengedhetetlen a beruházás költségének lehető legpontosabb meghatározásához és a kivitelezés alatt felmerülő utólagos költségek minimalizálásához.

Irodalomjegyzék / References

1. Boeykens, S. (2026. június 23.). *Is a fire compartment supported in IFC? Yes and no…* LinkedIn. https://www.linkedin.com/pulse/fire-compartment-supported-ifc-yes-stefan-boeykens-sgnae
2. Érces, G. (2019. június 17.). Épületinformációs modellezés és tűzvédelem. *Védelem Online*. https://www.vedelem.hu/hirek/0/2760-epuletinformacios-modellezes-es-tuzvedelem
3. Hajdu, Sz. (2023). Tűzvédelmi mérnöki módszerek és a BIM modellezés kapcsolata. *Védelemtudomány, 8*(2), 45–62. https://vedelemtudomany.hu/
4. Magyar Szabványügyi Testület. (2019a). *Információk rendszerezése és digitalizációja az épületek és a mérnöki létesítmények esetében, beleértve az építményinformációs modellezést (BIM). Információmenedzsment építményinformációs modellezés felhasználásával. 1. rész: Fogalmak és alapelvek* (MSZ EN ISO 19650-1:2019).
5. Magyar Szabványügyi Testület. (2019b). *Információk rendszerezése és digitalizációja az épületek és a mérnöki létesítmények esetében, beleértve az építményinformációs modellezést (BIM). Információmenedzsment építményinformációs modellezés felhasználásával. 2. rész: Létesítmények megvalósítási fázisa* (MSZ EN ISO 19650-2:2019).
6. Singh, P. (2024. február 15.). *Leveraging BIM for Enhanced Fire Protection Engineering.* LinkedIn. https://www.linkedin.com/pulse/leveraging-bim-enhanced-fire-protection-engineering-prachi-singh-5s2wf
7. The Vertex Companies. (2023, augusztus 21). *Fire Protection Design and BIM.* Vertex Engineering Insights. https://vertexeng.com/insights/fire-protection-design-and-bim/

Tartalom

Drónok, világűr, digitalizáció

Varga Attila:
Geoinformatikai referenciaadatokon alapuló GNSS-független lokalizáció lehetőségei pilóta nélküli légi járműveken 3

Ladányi Éva:
Űrdivat: a védelmi-ipari paradigmától a bioadaptív textíliákig 37

Kassai Károly:
Kiberbiztonsági összetevők – a felelősség 55

Tóth Dávid:
Az uniós jog nem büntetőjogi válaszai a digitális megszemélyesítésre 72

Rendészettudomány

Mogyoródi Gergely–Sallai János:
A lengyel-magyar rendőri kapcsolat és a lengyel rendőrtisztképzés 89

Hottó István:
A svájci rendőrség szervezeti felépítése, képzési rendszere és technológiai eszközei a fenntartható közbiztonság kontextusában 108

Tarkó Áron:
A magánnyomozás szabályozása az USA-ban (Kalifornia) 116

Nagy János:
A rendkívüli események kezelése a rendőri intézkedések során 128

Építészet

Bakai Levente
Új kihívás a tűzvédelmi tervezésben, az építményinformációs modellezés (BIM), mint munkamódszer 145