2019
1.

BELÜGYI SZEMLE

A BELÜGYMINISZTÉRIUM SZAKMAI, TUDOMÁNYOS FOLYÓIRATA

67.
évfolyam

TARTALOM 2019/1.

SZERZŐK 2019/1.

BALLA ZOLTÁN nemzetbiztonsági ezredes, főosztályvezető,
Nemzetbiztonsági Szakszolgálat Szakértői Intézet

DR. BARNÓCZKI LÁSZLÓ nemzetbiztonsági ezredes, igazgató,
Nemzetbiztonsági Szakszolgálat

DR BENCSIK BALÁZS nemzetbiztonsági ezredes, igazgató,
Nemzetbiztonsági Szakszolgálat

DR. DANKÓ GÁBOR c. nemzetbiztonsági alezredes, kiemelt főelőadó,
Nemzetbiztonsági Szakszolgálat

GÉCZI GERGELY nemzetbiztonsági alezredes, osztályvezető,
Nemzetbiztonsági Szakszolgálat
projektmanagement osztály

HAZAI LÁSZLÓNÉ DR. nemzetbiztonsági dandártábornok,
a főigazgató technikai és támogató helyettese,
Nemzetbiztonsági Szakszolgálat

DR. HORVÁTH FERENC nemzetbiztonsági alezredes,
Nemzetbiztonsági Szakszolgálat

JAROLIN JÓZSEF Nemzetbiztonsági Szakszolgálat

MAGYAR MÓNIKA nemzetbiztonsági alezredes, osztályvezető,
Nemzetbiztonsági Szakszolgálat

MORBER SZILÁRD KRISZTIÁN igazságügyi informatikai szakértő,
kiemelt főreferens, NBSZ Szakértői Intézet

NÉMETH ATTILA nemzetbiztonsági ezredes, igazgató,
Nemzetbiztonsági Szakszolgálat

OSZTERTÁG JÁNOS fotó-videotechnikai szakértő, kiemelt szakreferens,
NBSZ Szakértői Intézet

DR. SOLTI ISTVÁN jogász, PhD, a hadtudományok doktora

DR. TARJÁN GÁBORNÉ nemzetbiztonsági ezredes, gazdasági vezető

TATÁR ZOLTÁN hangtechnikai szakértő, kiemelt főelőadó,
NBSZ Szakértői Intézet

TÓTH GERGELY nemzetbiztonsági zászlós, szakreferens,
Nemzetbiztonsági Szakszolgálat

TÓTH TAMÁS nemzetbiztonsági főhadnagy, kiemelt főelőadó,
Főigazgatói Kabinet

ZUBEK GABRIELLA nemzetbiztonsági alezredes, osztályvezető
Nemzetbiztonsági Szakszolgálat

SUMMARY

Zubek, Gabriella
The place of national security services in law enforcement administration [5–17]
The author provides an overview of the historical development and current position of the national security services in the law enforcement structure in Hungary.

Barnóczki, László – Magyar, Mónika
Resolving the paradox of a transparent secret service [18–33]
The author provides an overview of the recent audit of the National Authority for Data Protection and Freedom of Information at the national security services in Hungary.

Horváth, Ferenc
Public service ethics at the national security services [34–52]
The author provides an overview of the ethical and integrity guidelines at the Hungarian Special Service for National Security.

Tóth, Tamás
Recruitment at the national security services [53–67]
The author provides an overview of the recruitment procedures and principles at the SSNS in Hungary.

Tarján, Gáborné – Dankó, Gábor
Budget and asset management of the national security services [68–81]
The authors provide an overview of the tasks, development and budget and asset management of the national security services in Hungary.

Géczi, Gergely
Applied IT project-management instruments and methodologies in the national security services [82–92]
The author provides an overview of IT project management tools and methods as in the practice of the Hungarian Special Service for National Security.

Bencsik, Balázs
Cyber security in the light of EU legislation [93–107]
The author provides an overview of the European Union's complex cyber security program enhancing cyber security for EU citizens and businesses.

SUMMARY

Tatár, Zoltán – Osztertág, János – Morber, Szilárd Krisztián
The development of the national security expert services [108–117]
The authors provide an overview of the tasks and development of the Hungarian Institute for Expert Services of the Special Service for National Security.

Hazai, Lászlóné dr.
Biometric facial recognition [118–126]
The author provides an overview of the development of biometric identification and verification technology.

Németh, Attila – Tóth, Gergely
Applying facial recognition technologies [127–136]
The authors provide an overview of the development of facial recognition technologies.

Jarolin, József
Detecting drones [137–146]
The author provides an overview of the potential and risks in using drones, as well as detection and protection methods for UAS misuse.

Balla, Zoltán
Developing passports since the political transition [147–153]
This author provides an overview of how passport security and technology developed in Hungary since 1990.

Solti, István
The consequences of the Szabó-Vissy-case
on national security covert information gathering [154–166]
The author investigates the options of the Hungarian legislator to meet the demands of an 18 months old European Court of Human Rights ruling on national security information gathering.

DOI: 10.38146/BSZ.2019.1.1

ZUBEK GABRIELLA

A Nemzetbiztonsági Szakszolgálat helye a rendészeti igazgatásban

A Nemzetbiztonsági Szakszolgálat rendkívül sajátos szervezet. Nézzük, miben is rejlik ez a sajátosság!

A rendészeti igazgatás középpontja a közrend és közbiztonság kettőse, ilyenformán alá tartoznak a rendvédelmi, honvédelmi, nemzetbiztonsági szereplők csakúgy, mint bármely, közigazgatási tevékenység keretében eljáró hatóság. Így tehát a magyarországi rendészeti igazgatás – szervezeti felépítését tekintve – rendkívül fragmentált. Ezért ez a tanulmány kizárólag a Nemzetbiztonsági Szakszolgálat szorosan vett működési környezetével, a rendvédelmi és a nemzetbiztonsági szervekkel foglalkozik.

Egy kis történelem

1990 januárjában fideszes és SZDSZ-es országgyűlési képviselők tettek feljelentést a Fővárosi Főügyészségnél, mivel okirati bizonyítékaik szerint a III/III. csoportfőnökség – az 1989. október 23-án hatályba lépő új alkotmány értelmében immár alkotmányellenesen – ellenzéki képviselők titkos megfigyelését végezte.

A Dunagate néven elhíresült titkosszolgálati botrány lendületet adott a titkos információgyűjtés jogi és szervezeti szabályozásának, elodázhatatlanná tette egy (eredetileg rövid időszakra tervezett) átfogó jellegű, az alapvető garanciákat tartalmazó jogszabály megalkotását és elfogadását. E folyamat eredményeként születhetett meg a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról szóló 1990. évi X. törvény, amely az érintett személy tudomása nélkül folytatott, a magánéletet és a személyes adatok védelméhez fűződő jogokat súlyosan sértő eszközök és módszerek – részletes indoklás alapján történő – alkalmazását az igazságügy-miniszter írásos engedélyéhez kötötte.

Látni kell, hogy a rendszerváltozás idején, az akkori politikai helyzetben olyan egyértelmű jogi megoldásokkal kellett szolgálni, amelyek az állampolgárok számára garantálták, hogy nem kerülhet sor még egyszer politikai

okokból folytatott ellenőrzésre. Ennek érdekében a szolgálatokat szervezetileg leválasztották a Belügyminisztériumról, a rendőrségtől pedig elvonták a nyomozati és intézkedési jogkört.

Az 1990. évi országgyűlési választások után egy megosztott szervezeti és irányítási struktúra kialakítására került sor:

– a honvédelmi miniszter felügyelete alá került a Katonai Felderítő Hivatal és a Katonai Biztonsági Hivatal; valamint
– a kijelölt tárca nélküli miniszter felügyelete alá az Információs Hivatal és a Nemzetbiztonsági Hivatal (a Nemzetbiztonsági Hivatal egyik szervezeti elemeként a Nemzetbiztonsági Szakszolgálat jogelőd szerve) kezdte meg működését.

Az „átmeneti törvény" taxatíve felsorolja, hogy a különleges eszközöket a titkosszolgálatok (és a rendőrség) milyen feladatok ellátása érdekében alkalmazhatják, ezzel tulajdonképpen megtörtént a szolgálatok feladatrendszerének meghatározása is, noha ezek részletes szabályozását a törvény nem tartalmazta.

A felosztás – a korábbi (főcsoportfőnökségi) struktúrára támaszkodva – rendkívül egyszerű elveket követve, a tevékenység irányultsága (belföld–külföld) és célja (hírszerzés–elhárítás) alapján határozta meg a szolgálatokat.

Az 1994. évi választások után új összetételű parlament alakult, amelyben a koalíciós kormánynak minősített többsége volt; ez a helyzet már kedvezett a rendészeti tárgyú törvények elfogadásának.

A Nemzetbiztonsági Szakszolgálatot önálló költségvetési szervként a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény hívta életre, elsősorban abból a célból, hogy operatív-technikai szolgálatot hozzon létre titkos információgyűjtésre, illetve titkos adatszerzésre/leplezett eszközalkalmazásra[1] (a továbbiakban mind együtt: titkos információszerzés) feljogosított szervezetek számára.

Ez a nemzetközi szinten is egyedülálló gyakorlat – miszerint a titkos információszerzést tevőlegesen nem az arra feljogosított, hanem egy tőle teljesen független szerv hajtja végre – híven tükrözi a kor támasztotta kívánalmakat: a Nemzetbiztonsági Szakszolgálat létrehozásának indoka és működésének alapelve az alkotmányos jogok érvényesülésének garantálása.

1 A 2018. július 1-jétől hatályos, a büntetőeljárásról szóló 2017. évi XC. törvény szerinti fogalomhasználat.

A szolgálatnak a nemzetbiztonsági szervezetek rendszerében történő önállósítására kizárólag a történelmi múltjára tekintettel került sor, de nem kapott felhatalmazást klasszikus titkosszolgálati feladatok ellátására: sem hírszerző, sem elhárító jogköre nincs. Elnevezése („nemzetbiztonsági") is megtévesztő – különös figyelemmel folyamatosan bővülő szerepkörére –, hiszen olyan egyedülálló szervezetről van szó, amely a rendelkezésére álló titkosszolgálati eszközöket, módszereket és műveleti erőket valamennyi bűnüldöző és nemzetbiztonsági szerv érdekeinek érvényre juttatása érdekében, azonos feltételek alapján alkalmazza.

Hovatovább, a megrendelők összetételéből fakadóan a Nemzetbiztonsági Szakszolgálat feladatellátása sokkal inkább bűnüldözési, mint nemzetbiztonsági jellegű. Szolgáltatói szerepkörben végzett tevékenységének irányultságát és célját a megrendelők érdekei határozzák meg, miközben soha nem áll fenn érdekközössége a megrendelővel, ami az objektív munkavégzés záloga.

Irányítás, koordináció

1990-től 2010-ig a polgári szolgálatok egységes kormányzati irányítás alatt álltak (1990-től 2002-ig a kijelölt tárca nélküli miniszter[2], 2002 és 2007 között a Miniszterelnöki Hivatal, 2007-től a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter).

Az állam szuverenitásának megóvásáért, belső biztonságának garantálásáért a belügyminiszter tehát nem felelős; ez a megoldás szintén a békés átmenet korszaka által megkövetelt jogi garanciák közé sorolandó. Éppen a jogi garanciákra hivatkozva (függetlenül a szolgálatok reformjára vonatkozó szakmai elképzelésektől) 2010-ig a titkosszolgálat nem is tartozott újra belügyminisztériumi irányítás alá, noha a rendszerbe az előzőeken is túlmutató garanciális szabályokat építettek be a visszaélések elkerülése érdekében, így különösen: a rendvédelmi szervek működését az Országgyűlés bizottsági úton[3] felügyeli, a titkosszolgálatok tevékenységét felügyelő bizottság elnöki posztját minden esetben ellenzéki képviselő tölti be, a titkos információgyűjtést engedélyező igazságügyért felelős miniszter nem lehet felelős a polgári szolgálatok irányításáért.

2 1990-től az Nbtv. hatálybalépéséig a polgári nemzetbiztonsági szolgálatok működését „felügyelő", a törvény hatálybalépésével „irányító" miniszter.

3 Honvédelmi és rendészeti bizottság, nemzetbiztonsági bizottság.

A 2010-ben kétharmados többséggel megalakuló kormány ezen az egységes irányításon változtatva az Információs Hivatalt a külügyminiszter, a Nemzetbiztonsági Hivatal jogutódjaként létrejött (újragondolt) Alkotmányvédelmi Hivatalt és a Nemzetbiztonsági Szakszolgálatot – az „átmeneti" törvény megalkotásának huszadik évfordulóján – ismét az állam belső rendjének fenntartásáért, a kapcsolódó ellenérdekelt törekvések felderítéséért felelős belügyminiszter alá helyezte, így az öt szolgálat kormányzati irányítása három miniszter[4] között oszlott meg.

Ahogy arra korábban már többször utaltunk, a Nemzetbiztonsági Szakszolgálat önállóságának megteremtése annak érdekében volt szükséges, hogy a mindenkori kormányzat ne használhassa a szervezet eszközrendszerét aktuális bel- és pártpolitikai célokra. A területen 1996 óta végbemenő decentralizálás, illetve ezzel párhuzamosan a műveleti erők, eszközök egy szervezethez való telepítése ugyanezt a célt szolgálja.

A szolgálatoknak – amelyek működésének alapvető célja az ország függetlenségének és törvényes rendjének védelme – ebben a rendkívül osztott irányítási struktúrában kell elősegíteniük a megalapozott kormányzati (stratégiai) döntések meghozatalát, a különböző forrásokban fellelhető és exponenciálisan növekvő mennyiségű információ megszerzésével, elemzésével, a szinergiák feltárásával és értékelésével.

Az Nbtv.-ben rögzített, együttműködésre vonatkozó rendelkezések önmagukban nem voltak képesek a rendszer hatékony működtetésére, márpedig a megváltozott biztonsági környezetben elemi fontosságú a pontos információk időbeni rendelkezésre állása.[5]

Ebben a helyzetben természetszerűen értékelődött fel a tárcákon átívelő koordinációs mechanizmusok működésének hatékonysága. A kormányzati döntés-előkészítő tevékenység szempontjából ezért kiemelt szerep hárult a speciális hatáskörrel felruházott politikai döntéshozó fórumokra, esetünkben a miniszterelnök által vezetett és a szaktárcák vezetőiből álló Nemzetbiztonsági Kabinetre, valamint a kabinet döntéseinek szakmai előkészítéséért 2011 óta felelős, a honvédelmi és a belügyminiszter által elnökölt Nemzetbiztonsági Munkacsoportra.

A fórumok működése a hatékonyságuk ellenére sem váltja ki a napi operatív együttműködés szükségességét, mindamellett vezetésük és összetételük

4 A katonai szolgálatok 1990-től folyamatosan a honvédelmi miniszter felügyelete/irányítása alatt álltak.
5 Hetesy Zsolt: A titkos felderítés. PhD-értekezés. Pécs, 2011

természetszerűleg garantálja az azonos tárgykörben keletkezett információk értékelését és célirányos felhasználását.

A szervezeti struktúrán végrehajtott, 2012-es szerkezeti változtatás – a Nemzetbiztonsági Szakszolgálat 1995-ös megalakítását leszámítva – a nemzetbiztonsági szektor reformjának(?) eddigi egyetlen materializálódott elemeként a Katonai Biztonsági Hivatal Katonai Felderítő Hivatalba integrálása volt.

Az információfúziós – vagyis a nemzetbiztonsági együttműködésen túlmutató, a teljes nemzeti szervezeti rendszert átfogó[6] koordinációs – szervezet életre hívásának gondolata ezért felerősödött, az ezzel kapcsolatos politikai konszenzus azonban csak a 2016-os párizsi és brüsszeli terrorcselekmények után alakult ki, ennek nyomán pedig intézményesült a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK).

A TIBEK létrehozása korántsem tekinthető előzmény nélkülinek. A Szervezett Bűnözés Elleni Koordinációs Központ 2001. január 1-jei megalakításának egyik célja éppen a rendvédelmi és a nemzetbiztonsági szervek közti információmegosztás előmozdítása volt. A koordinációs központ működési elveinek korlátait (a szervezett bűnözésre vonatkozó jogi szabályozás, az átadott adatok időszerűsége), illetve a nemzeti szintű együttműködési hajlandóság hiányát a 2008-as romagyilkosságok világították meg leginkább, ennek nyomán azonban mégsem az információfúziós szerv (Nemzeti Információs és Bűnügyi Elemzési Központ) létrehozását, hanem a koordinációs központ irányítás alá vonását, illetve – az információk időbeni továbbítása és hatékony felhasználása érdekében – a Belügyminisztériumon belül működő Rendészeti Információs Iroda életre hívását könyvelhetjük el.

A TIBEK nemzetbiztonsági szolgálatként történő megalakítása az információszerzésen túl egyértelművé tette a különböző helyeken (rendvédelmi, nemzetbiztonsági szerveknél) rendelkezésre álló információk szintetizálására és értékelésére, a kormányzati döntés-előkészítést taktikai és stratégiai elemzéssel támogató képesség kialakítására, valamint a rendészeti igazgatás rendszerének kooperatív irányba történő elmozdítására irányuló kormányzati igényt[7].

6 A horizontális együttműködésre korábbi példa 2003 óta működő Terrorellenes Koordinációs Bizottság.

7 Kovács Zoltán András – Dobák Imre: Korszakváltások a magyar nemzetbiztonsági intézményrendszerben (1990-2016). In: Finszter Géza – Sabjanics István (szerk.): Biztonsági kihívások a 21. században. Dialóg Campus, Budapest, 2017

Feladatrendszer, és az együttműködés egyes speciális területei

A hagyományos nemzetbiztonsági szolgálatok feladatai a megalakításuktól 2010-ig fogaskerekekként simultak egymásba. A nemzetbiztonsági tevékenység fókuszát a nemzeti érdekeket veszélyeztető (belső/külső) törekvések felderítése, megelőzése és megszakítása jelenti. Az érdekérvényesítést elősegítő információk megszerzése nélkülözhetetlen a kormány stratégiai döntéseinek meghozatalához. Az alapvető nemzeti érdekeket – és így a hazai nemzetbiztonsági szolgálatok tevékenységrendszerét – a következők szerint oszthatjuk fel:

- külföldi titkosszolgálatok információszerző/befolyásoló tevékenységének gátlása;
- szervezett bűnözés elleni küzdelem (ideértve a terrorszervezeteket, a kábítószer-bűnözést, az illegális fegyverkereskedelmet és az illegális migrációt);
- gazdaságbiztonság;
- alkotmányos berendezkedés védelme;
- tömegpusztító fegyverek elterjedésének akadályozása;
- környezeti biztonság védelme;
- kiberbiztonság feltételrendszerének megteremtése.

Ahogy a felsorolásból is kitetszik, a nemzetbiztonsági szolgálatok tevékenységi köre számos ponton metszi a rendvédelmi szervezetekét, így különösen a kábítószer-kereskedelem, az illegális migráció, a környezeti biztonság és a kibervédelem területén.

Hasonló kapcsolódási pontokat a honvédelem és rendvédelem között is találhatunk; a honvédelem – szakmaspecifikus feladatain túl – részt vesz a terrorizmus elleni küzdelem katonai feladataiban, támogatja a szervezett bűnözés és a kábítószer-csempészet elleni fellépést, tevékeny részt vállal a tömegpusztító fegyverek terjedésének megakadályozásában, valamint környezetbiztonsági (katasztrófavédelmi) feladatokat lát el[8].

A 2010-ben megalakuló kormány nemcsak az irányítási rendszeren módosított, hanem új szereplőket is hozott a rendészeti igazgatás területére: a rendőrségről szóló 1994. évi XXXIV. törvény módosításával a rendőrség szerveként létrejött a belső bűnmegelőzési és bűnfelderítési feladatok ellátásáért felelős Nemzeti Védelmi Szolgálat, az egykor klasszikus polgári elhárítási

8 Lakatos László: Honvédelmi igazgatás. Egyetemi e-jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2011. http://docplayer.hu/940133-Dr-habil-lakatos-laszlo-honvedelmi-igazgatas.html

feladatkörnek számító terrorelhárításért pedig a továbbiakban a Terrorelhárítási Központ (TEK) felel.

A szervezeti struktúrán végrehajtott változtatások – nevezetesen a TEK létrehozása és a Katonai Nemzetbiztonsági Szolgálat megalakításának előző fejezetben jelzett módja – azt az előfeltevést erősítik, hogy a mai kor biztonsági környezetében a kormányzat a hangsúlyt a hírszerzésre helyezi az elhárítással szemben[9].

És hogy hol kapcsolódik ebbe a rendszerbe a Nemzetbiztonsági Szakszolgálat? Ahogyan azt már tárgyaltuk, e speciális szervezet elsődleges feladata, hogy a törvényben feljogosított szervezeteket technikai szolgáltatások nyújtásával segítse a szükséges információk titokban történő megszerzésében.

A rohamosan növekvő információmennyiség elérhetőségét és/vagy megszerzését, a megrendelő számára releváns adatok felhasználhatóságát a Nemzetbiztonsági Szakszolgálat biztosítja technikai hírszerző eszközeivel (és kiterjedt kapcsolati rendszerével). Nyilvánvaló, hogy az ilyen technikai rendszerek fejlesztéséhez rendkívüli, esetenként többmilliárdos forrás rendelkezésre állása szükséges, ezért össznemzeti szinten, gazdasági szempontból feltétlen előnyöket hordoz e kapacitások egy szervezetnél történő koncentrálása.

Azon titkosszolgálati eszközök vonatkozásában, amelyek nem rendeltetésszerű használatából fakadó károkozás mértéke jelentős volna (lehallgatás, magánlakásba történő behatolás), szükséges és indokolt a kapacitások különálló szervezethez történő kiszervezése *(outsourcing);* ez a megoldás egyben elősegítheti a karhatalmi szervek iránt fennálló negatív érzések lebontását is.

Az Nemzetbiztonsági Szakszolgálat kizárólagosságát deklaráló jogi normák a következők:

– az elektronikus hírközlésről szóló 2003. évi C. törvény végrehajtási rendelete [180/2004. (V. 26.) kormányrendelet], valamint a postai szolgáltatásokról szóló 2012. évi CLIX. törvény végrehajtási rendelete [9/2005. (I. 19.) kormányrendelet] szerint: a tartalom-ellenőrzés tekintetében;
– a Nemzetbiztonsági Szakszolgálat által nyújtott szolgáltatások igénybevételének és alkalmazásának egységes eljárási rendjéről szóló, a szolgáltatások igénybevételére jogosult szervezeteket irányító miniszterek, illetve a legfőbb ügyész által kiadmányozott (minősített) normák.

9 Szentgáli Gergely: Csendben szolgálni. A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 és 2014 között. Hadtudomány, 2015/1–2.

Nyilvánvaló, hogy a titkosszolgálati eszközök és módszerek Nemzetbiztonsági Szakszolgálat általi alkalmazásával (vagyis a kapacitások szakszolgálatnál történő koncentrálásával) a megszerzett információk is rendkívül koncentráltan találhatók meg a szervezetnél. A visszaélések elkerülése érdekében azonban számos, a jogbiztonság érvényre juttatását elősegítő szabály megfogalmazására került sor az Nbtv.-ben, most ezeket vesszük sorra.

Az Nbtv. 61. § szerint a megrendelő a törvényességért felel, a Nemzetbiztonsági Szakszolgálat pedig a szakszerű végrehajtásért. Nos, az élet ennél kissé bonyolultabb: a törvény szellemében, de a gyakorlatnak megfelelően az állítás így helyes: a titkos információszerzést a Nemzetbiztonsági Szakszolgálat a megrendelő érdekkörében eljárva, a jogbiztonság szem előtt tartásával hajtja végre.

Egyes esetekben ugyanis, illetve bizonyos eszközök és módszerek alkalmazására kifejezetten nem a Nemzetbiztonsági Szakszolgálat által kerül sor. Ennek eklatáns példája a titkos kutatás, amelyet aposztrofáljunk az egyszerűség kedvéért e helyütt klasszikus nyomozati cselekményként – amit a Nemzetbiztonsági Szakszolgálat semmilyen körülmények között nem folytat.

Mindamellett az sem fedi teljes egészében a valóságot, hogy a törvényességért csak a megrendelő felelős, hiszen a szolgáltatások igénybevételére irányuló írásos megkeresések befogadásakor a Nemzetbiztonsági Szakszolgálat végez egyfajta előszűrést/kontrollt, amely a Nemzeti Adatvédelmi és Információszabadság Hatóság által folytatott audit végkövetkeztetései szerint igen fontos garanciális elem a különleges eszközök alkalmazására vonatkozó eljárási rendben.

A Nemzeti Adatvédelmi és Információszabadság Hatóság éves jelentésében[10] megfogalmazottak szerint a Nemzetbiztonsági Szakszolgálat kulcsszereplő a jogszerűség szavatolásában; az Nbtv.-ben meghatározott munkamegosztási és feladatellátási rendben ez a Nemzetbiztonsági Szakszolgálat Nbtv.-ből levezethető feladata, az információszabadság hatóság pedig támogatja ennek a törvényességi kontrollszerepnek az erősítését.

A Nemzetbiztonsági Szakszolgálat szolgáltató feladataival kapcsolatosan nyilvántartást vezet, amely tartalmazza

– a megrendelő szervezet írásbeli megkeresését a szükséges (bírói, miniszteri, ügyészségi) engedéllyel;
– a megkeresésben megjelölt személyek azonosításához szükséges személyes adatokat;

10 https://www.naih.hu/files/NAIH-BESZAMOLO-2017-mid-res.pdf

– az adott ügyben alkalmazott titkos információszerzés eszközeinek és módszereinek leírását, illetve személyes adatnak nem minősülő, műveleti értékkel bíró adatokat;
– a megrendelő szervezet részére továbbított adathordozók jegyzékét.

A felsorolásban jelölteken túl, vagyis a titkos információszerzés nyomán megszerzett adat nem maradhat a Nemzetbiztonsági Szakszolgálatnál, azokat teljeskörűen és kizárólag a megrendelő szervnek továbbítja. Az adattal ez után a megrendelő rendelkezik, a továbbított adatokat a Nemzetbiztonsági Szakszolgálat rendszereiből, nyilvántartásaiból visszafordíthatatlanul törlik [Nbtv. 61. § (2) bek.]. Ezek is a jogbiztonságot erősítő rendelkezések.

Függetlenül azonban a jogszabályokba és az eljárásokba beépített garanciáktól, az eljárásrendi kérdések egyes elemei folyamatosan górcső alatt – és a laikus közvélemény érdeklődésének homlokterében – állnak. Az átmeneti törvény megalkotásakor még rendkívül erős garanciális elemnek számított, hogy a magánéletet leginkább sértő esetekben a különleges eszközök alkalmazására – az állampolgári jogok védelme érdekében – az igazságügyért felelős miniszter engedélyével kerülhet sor.

Jelenleg viszont éppen ez a gyakorlat áll felülvizsgálat alatt, tekintettel az Emberi Jogok Európai Bíróságának (EJEB) a *Szabó és Vissy kontra Magyarország-ügy*ben, a TEK jogalkalmazásával összefüggésben hozott 2016-os ítéletére, amely olyan követelményeket határoz meg, amelyek a nemzetbiztonsági céllal folytatott titkos információszerzés eljárási szabályainak módosítását igénylik.

A Nemzetbiztonsági Szakszolgálat titkos információszerző kapacitásai kapcsán muszáj kiemelni, hogy az „átmeneti törvény" hatálybalépésétől kezdve a különleges eszközök alkalmazására feljogosított szervezetek száma (vagyis a Nemzetbiztonsági Szakszolgálat szolgáltatásainak megrendelésére jogosultak köre) jelentősen kibővült[11], ezt 2016-ig korántsem követte a szervezet (kormányzati) fejlesztési üteme.

A fennálló kapacitáshiány ellensúlyozását a megrendelői önmérséklet, illetve az engedélyezési gyakorlat felülvizsgálata jelentheti; a 2016–2017. évi jogszabályi változásokra (mindenekelőtt a büntetőeljárásról szóló új törvény

11 Jelenleg kilenc, jogszabályban meghatározott szerv veheti igénybe a Nemzetbiztonsági Szakszolgálat rendszeresített szolgáltatásait: az Információs Hivatal, az Alkotmányvédelmi Hivatal, a Katonai Nemzetbiztonsági Szolgálat, a rendőrség, az Nemzeti Védelmi Szolgálat, a Terrorelhárítási Központ, a Nemzeti Adó- és Vámhivatal, az ügyészség, valamint maga a Nemzetbiztonsági Szakszolgálat. Lásd Nbtv. 8. § (3)–(4) bekezdés.

megalkotására, és ezzel az ügyész nyomozás-felügyeleti jogkörének erősödésére) ezért a Nemzetbiztonsági Szakszolgálat reménykedve tekint.

A Nemzetbiztonsági Szakszolgálat egyéb tevékenységei

Nem engedhetjük meg magunknak, hogy ne ejtsünk legalább néhány szót a szakszolgálat feladatrendszerének egyéb elemeiről is.

A Nemzetbiztonsági Szakszolgálat Szakértői Intézete által ellátott tevékenységi körök ugyanis szintén a kezdetektől (a nemzetbiztonsági hivatali időktől) fogva részei a szakszolgálati feladatellátásnak, ennek megfelelően a hatályos jogszabályokban foglalt rendelkezések szerint igazságügyi szakértői tevékenységet lát el, továbbá költségtérítés mellett gondoskodik a nem műveleti nyomda- és okmánytechnikai, valamint szakértői tevékenység körébe tartozó eszközökről, szolgáltatásokról.

Az okmányvédelmi, az okmánytechnikai és a szakértői szakmai ismeretekre építve hatósági jogkört gyakorol a biztonsági okmányok előállításával, védelmével összefüggésben, valamint szakhatósági tevékenységet végez az értékpapírok előállításának, illetve a biztonsági papírok nemzetközi kereskedelmének engedélyezési eljárásában.

A Nemzetbiztonsági Szakszolgálat feladatrendszerének 2013 óta része a kiberbiztonsági tevékenység, amely a szakszolgálat Nemzeti Kibervédelmi Intézetének szervezeti keretei között zajlik.

A 2015-ben megalakított szervezet három jól elkülöníthető szakmai tevékenység ellátásáért felel:

– megelőző jellegű feladatok (a jogszabályi előírások betartásának ellenőrzésével és érvényesítésével foglalkozó hatósági, valamint a tudatosító tevékenység);
– a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási és sérülékenységvizsgálati feladatok;
– a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó informatikaibiztonságiesemény-kezelési feladatok (CERT-funkciók).

A Nemzeti Kibervédelmi Intézet hatósági jogköre, illetve a CERT-funkciók tekintetében a védendő infrastruktúrák köre – a 2018 decemberében elfogadott törvénymódosítások értelmében – 2019. január 1-jétől jelentősen kiszélesedett.

Szintén a 2019. január 1-jei változások eredményeként elkönyvelhető továbbá a Nemzetbiztonsági Szakszolgálat hatósági feladatkörének erősödése, hiszen a jövőben a Nemzetbiztonsági Szakszolgálat szervezeti keretei között végzi tevékenységét a Nemzeti Biztonsági Felügyelet, amelynek feladata a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a telephelyi iparbiztonsági hatósági feladatok ellátása.

Fontos szempontként ki kell emelni, hogy a Nemzetbiztonsági Szakszolgálatnál működő hatóságok e tevékenységük során független szervezetként járnak el, és a feladatkörükbe tartozó hatósági ügyek tekintetében nem utasíthatók.

Merre tovább, nemzetbiztonság?

Szervezeti struktúra átalakítása

Hogyha alapvetésként fogadjuk el, hogy az „új" biztonságpolitikai környezetben, az „új" típusú biztonsági feladatok kezeléséhez új típusú gondolkodásmód szükséges, vajon miért nem tudunk elvonatkoztatni a polgári nemzetbiztonsági szolgálatok tevékenységének területalapú elhatárolásától? Időről időre bebizonyosodik, hogy az osztott irányítási rend, megspékelve a szolgálatok versengésével, nem minden esetben tudja garantálni a rendelkezésre álló információk szintetizálását és optimális felhasználását. Nyilván nem új keletű a polgári szolgálatok összevonásának gondolata, de mindenképp megfontolandó lehet.

Ha az egyébként a feladatellátás szempontjából „tükörszervezetek" tevékenységében átfedés fedezhető fel, akkor e területeken összeütközés is előfordulhat, ami a szakszolgálati kapacitások természetszerű elaprózódásához vezet. Ilyen értelemben, nemzetbiztonsági szakszolgálati szemszögből, támogatható a polgári hírszerzés és elhárítás integrációja, még ha ez szükségszerűen maga után vonná az irányítási struktúra átrendezését is, a túlzott információ- és hatalomkoncentráció megelőzése érdekében.

Információszerzés

A paradigmaváltás szükséges és időszerű: a modern kori biztonsági feladatok közepette a kibervédelem alapvető képességnek számít. Ideje ezért az észle-

lő-követő (tudatosítás, megelőző jellegű védekezés, észlelés, jelzés) szemléletmódot a nagypolitika által is támogatottan aktív védekezésre cserélni.

Ahogyan az Nbtv. szövegéből is látszik, a hatályos szabályozás a személyt helyezi a felderítés középpontjába, ez a szemlélet a hibrid hadviselés korában, amikor az elkövető kiléte nehezen (vagy egyáltalán nem) megállapítható, már meghaladott. (A titkosszolgálati tevékenység fundamentumát tekintve egyébként is nehezen magyarázható.) A titkos felderítést hatékonyabban támogatná egy olyan jogi rendszer, amely lehetővé teszi a Nemzetbiztonsági Szakszolgálatnál kiépített képességek és kapacitások komplex, célorientált – konkrét, nemzetbiztonsági érdeket sértő vagy fenyegető cselekmény megelőzése és elhárítása érdekében történő – alkalmazását.

Elnevezés

Beszéltünk arról, hogy mennyiben tekinthető nemzetbiztonsági szolgálatnak egy klasszikus titkosszolgálati feladatkör nélküli szervezet, és láttuk azt is, hogy a szakszolgálatot speciális feladatkörében eljárva is abszolút körön kívüli. Ezzel együtt mégsem kérdőjelezhető meg, hogy kizárólag a nemzet biztonsága érdekében tevékenykedik. A speciális funkciókra tekintettel meggondolandó a Nemzeti Biztonsági Szakszolgálat elnevezés használata.

Összegzés

A bevezetőben azt ígértem, arra próbálok válasszal szolgálni, hogy mitől is olyan sajátos ez a szervezet. Íme, egy rövid sommázat a leírtakról.

Az 1995. évi outsourcing

A Nemzetbiztonsági Szakszolgálat létrehozásakor Magyarország takarékossági és adatkezelési szempontokra figyelemmel ugyan, de egy korát megelőző kiszervezést hajtott végre a privát szférát leginkább veszélyeztető titkosszolgálati eszközök és módszerek alkalmazásához szükséges humán háttér és eszközrendszer titkos információszerzésre feljogosított szervezetekről való leválasztásával és egy új, az előzőektől jogi-szervezeti értelemben független szervezetben való összevonásával.

Nemzetbiztonsági?

A Nemzetbiztonsági Szakszolgálat nevében bár nemzetbiztonsági, klasszikus titkosszolgálati feladatköre nincs; feladatai ellátásával alapvető jogi garanciákat hivatott szavatolni, illetve puszta létezése elősegíti a közbizalom erősítését.

Kizárólagosság

A privát szférát leginkább sértő eszközök alkalmazására nemcsak az Nbtv. jelöli ki a szakszolgálatot, ennek jogi és technikai feltételeit egyéb, a piaci szereplőkre vonatkozó jogszabályok is rögzítik.

(Kiber-)harcosok klubja

A kibervédelem súlyának növekedése változást hozott a Nemzetbiztonsági Szakszolgálat feladatrendszerében, és kevéssé várt következményeként a szakszolgálatról kialakított képben is, tekintettel arra, hogy a kibervédelmi tevékenység ellátása feltételezi a tudatosító, tájékoztató tevékenység aktivitásának fokozását a különböző konferenciákon és a média irányába is; ennek során a Nemzeti Kibervédelmi Intézet hozzájárul a szakszolgálat mint titkosszolgálat, áttételesen a nemzetbiztonsági szféra iránt fennálló előítéletek lebontásához.

Az információszerzés metodikájának esetleges változásával a kibervédelmi tevékenységek arzenálját aktív védelmi intézkedések megtételére feljogosított és alkalmas erők rendszerbe integrálásával kell bővíteni, ami tovább növelheti a kiberbiztonság Nemzetbiztonsági Szakszolgálaton belüli súlyát.

DOI: 10.38146/BSZ.2019.1.2

BARNÓCZKI LÁSZLÓ – MAGYAR MÓNIKA

A koffeinmentes kávétól az átlátható titkosszolgálatig

A titkosszolgálati munka és az átláthatóság közötti látszólagos ellentmondás feloldása

A posztmodern jóléti, jogállami társadalmakban a korábbi századokban értelmezhetetlen értékek válnak fő jelentőségűvé. Az is gyakran előfordul, hogy a világ dolgaival kapcsolatos társadalmi elvárások új értelmet kapnak, és egyre szélesebb körű érvényesülésre tartanak igényt. Ezek a folyamatok olyan többé-kevésbé kézzelfogható produktumokban, termékekben nyilvánulnak meg, mint az átjárható határok, a koffeinmentes kávé vagy akár a passzívház.

Érezzük, hogy a példaként említett esetekben olyan kívánalmakat támasztunk az életünk, környezetünk jól ismert részei kapcsán, amelyek a korábbi generációk számára nyilván abszurdnak, szürreálisnak tűnhettek volna. Az abszurditás abból adódik, hogy az új követelmény látszólag éppen az értelmétől, a lényegétől látszik megfosztani az adott dolgot. A hagyományos gondolkodás szerint a határ lényege a kontroll, a rosszhiszemű vagy spontán határátlépések megakadályozása; a kávéra kifejezetten a koffein jótékonynak tartott hatásai okán szokott rá az emberiség; és egy háztartás is olyan dolog, amelynek működtetéséhez ilyen vagy olyan formában energiafelhasználás szükséges.

Gyakorlati, kézzelfogható tapasztalataink alapján aztán mégis vívmányként tekintünk az említettekre. Felismerjük ugyanis, hogy a legális határátlépések könnyítése nem zárja ki a korszerű és hatékony határellenőrzést, a koffeinmentes kávénak jó esetben kávéíze van, ráadásul fogyasztásával száz százalékig rekonstruálható a kávézás szertartása; korszerű anyagok és technológiák felhasználásával pedig egy passzívházban is hasonló komfortszint érhető el, mint egy hagyományos otthonban, mégpedig a felhasznált energiamennyiség radikális csökkentése mellett. Valahogy így tekint a szakszolgálat az átláthatóság követelményére.

Edward De Bono szavai szerint *„kreativitás nélkül csak ismétlés és rutin van; mindkettő nagyon értékes a maga helyén, és viselkedésünk jórészt ebből áll, de a fejlődéshez, a változáshoz és az új irányokhoz kreativitás kell”*[1].

1 Edward De Bono: A kreatív elme – 62 gyakorlat a kreativitás növelésére. HVG Könyvek Kiadó, Budapest, 2009

Másként, a változtatáshoz mindig szükséges egyfajta formabontó, rendhagyó gondolkodás, amely képes a jól megszokott, biztonságos mozgásteret nyújtó határainkat, vagy akár a szakmai komfortzónáinkat is – észszerű és szükségszerű módon – átlépni, netán esetenként áttörni. Erre a fajta rugalmasságra és szemléletváltásra volt szükség részünkről, amíg eljutottunk odáig, hogy meghaladjuk a klasszikus titkosszolgálati szocializáció jelentette eddigi kereteket és persze nagyon precízen, körültekintően kialakított játékszabályok mellett a Nemzeti Adatvédelmi és Információszabadság Hatósággal együttműködésben kísérletet tegyünk legféltettebb eljárásaink átvilágítására.

Persze a változtatni meréshez a belső motiváción túl mindig jól jön egy kis külső kényszer.

A figyelmes olvasó első ízben 2014-ben, majd 2015 nyarán a médiában számos alkalommal találkozhatott olyan cikkekkel, amelyek eleinte a Gamma International, majd később a Hacking Team elnevezésű cégek szervereinek feltöréséről tudósítottak. A jelzett adatbázisokból ismeretlen hackerek (vagy netán sértett/ellenérdekelt alkalmazottak) elképesztő mennyiségű – csak a Hacking Team esetében például közel négyszáz gigabájtnyi – adatot tulajdonítottak el és tették bárki számára szabadon elérhetővé, különféle internetes fájlmegosztó oldalakon.

A sajtóba, illetve a világhálóra kiszivárogtatott adatállomány érzékenysége, az abban szereplő konkrétumok első olvasatra sokkoltak minket. Olyan szalagcímeket lehetett olvasni a sajtóban, hogy *A magyar titkosszolgálatnak még a kémprogram telepítése sem sikerült…*[2] vagy *Kicsengő kémhívás és követésnél megjelenő GPS-jel – ilyen egy állami kémprogram…*[3], ez mindannyiunk számára nagy traumát okozott. Minden összedőlni látszott, ami eddig a világunk alapjait képezte.

Az első meglepetésből és sokkból felocsúdva egy magára valamit adó szolgálatnak azonban ilyenkor intézkednie, értékelnie és reagálnia kell, mégpedig nem pusztán a döntéshozók, illetve a szakmai közvélemény, hanem a „laikus közönség" számára is értelmezhető és megnyugtató módon.

Intézkedtünk hát, mégpedig gyorsan és rendkívül hatékonyan.

E helyütt érthető okokból nem részletezett intézkedéseink nyomán a szivárogtatások az egyes konkrét műveleteink, eszközalkalmazásaink, illetve a mögöttük álló szolgálatok viszonylatában nem okoztak műveleti érdeksérelmet. A szakszolgálat pajzsfunkciója érvényesült, az alkalmazások konkrét

2 https://index.hu/tech/2014/08/12/a_magyar_titkosszolgalatnak_nem_sikerult_a_kemprogram_telepitese/

3 Uo.

iránya, az azokat megrendelő szervezetek és célok árnyékban maradtak, az incidens megállt a szakszolgálat kapuinál.

A kapukon belül azonban a lavinát már nem lehetett feltartóztatni; a történtek kapcsán haladéktalanul vizsgálódni kezdtek az arra feljogosított szervek.

Mindez alig egy évvel az *Edward Snowden* által kirobbantott lehallgatási botrány után történt, amelynek során a CIA számítógépes szakembere olyan, szigorúan titkos NSA-dokumentumokat hozott nyilvánosságra, amelyekből kiderült, hogy az amerikai titkosszolgálatok széles körben figyelik az emberek mobiltelefon-hívásait, valamint internetes tevékenységét az Egyesült Államokban és világszerte. Snowden egyebek között olyan kémprogramok létezését és működési részleteit szivárogtatta ki, amilyen a PRISM, az NSA telefonhívás-adatbázisa és a Boudless Informant, vagy éppen a Tempra, a brit titkosszolgálat által alkalmazott, számítógépes ellenőrző rendszer.

A nemzetközi és a hazai közhangulat az előzmények nyomán pattanásig feszültté vált tehát minden olyan „titkos dolog" iránt, amely nem átlátható vagy nem törvényes. Ebben a helyzetben kaptuk meg 2014 őszén a Nemzeti Adatvédelmi és Információszabadság Hatóságtól azt a kérdéssort, amellyel a kémprogramok állami alkalmazásának részleteire irányuló hatósági vizsgálatot kezdték el.

Emlékezetes, és – titkosszolgálati szakemberként – megdöbbentő volt egy nem rendvédelmi profilú állami szerv részéről olyan precizitással, illetve célirányos, minőségi szaktudással szembesülni, amellyel a hatóság a kémprogramok alkalmazásának jogi, műszaki és technikai részleteit „feszegette".

Hangsúlyoznunk kell azonban azt is, hogy a feltett kérdések között egyetlenegy sem volt olyan, amely meghaladta volna a Nemzeti Adatvédelmi és Információszabadság Hatóság hatáskörét, illetve amelynek megválaszolása alól valamilyen törvényi rendelkezés felmentést adott volna számunkra.

A kérdéssor megválaszolása után, 2014 októberében helyszíni ellenőrzésre is sor került a Nemzetbiztonsági Szakszolgálatnál, amikor is az Országgyűlés nemzetbiztonsági bizottságának tagjai és a Nemzeti Adatvédelmi és Információszabadság Hatóság kijelölt szakértője immár mélységében azt vizsgálta, hogy összhangban van-e az úgynevezett kémprogramok szakszolgálat általi alkalmazása a személyes adatok védelmére és az adatkezelésre, valamint a titkos információgyűjtésre vonatkozó szabályokkal.

A kihelyezett ülés előtt a sajtónak kiszivárogtatott információk kapcsán, így a FinFisher, illetve a FinSpy elnevezésű kémprogramok állami szervek általi alkalmazására irányulóan a nemzetbiztonsági bizottság zárt ülésének

összehívására került sor, amelyen a szakszolgálat – újonnan kinevezett – főigazgatóját is meghallgatták.

A zárt ülés utáni sajtónyilatkozatokból egyértelműen megállapítható, hogy a tudomásukra jutott információk alapján a bizottság tagjai pártállástól függetlenül úgy ítélték meg, hogy Magyarországon a kémprogramok alkalmazása a vonatkozó törvényi előírások betartásával történik, amit a következő sajtóközlemények[4] egyöntetűen alátámasztanak:

– A bizottság szocialista elnöke szerint nincs ok az aggodalomra. *„Aggódni legfeljebb abból a szempontból lehetne, hogy ezeknek a használata annyira rejtett, hogy még egy telefonlehallgatáshoz képest is nehezebben tetten érhető, de valóban, ha a törvényeket betartják, a nemzetbiztonsági törvényben lévő garanciákat például, akkor nem lehet visszaélésszerűen használni ezeket, tehát azt gondolom, hogy pánikkeltésre nincs ok"* – mondta *Molnár Zsolt.*
– *„Világossá tették előttünk a szolgálatok azt is, illetve az igazgató asszony, hogy amióta használták ezt a szoftvert, úgy jártak el, ahogy azt a nemzetbiztonsági törvény előírja. Vagy a mindenkori igazságügyi miniszter, vagy pedig a bűncselekményeket felderítő eljárásokban pedig a bíró adott arra engedélyt, hogy ezt a szoftvert használják"* – közölte Németh Szilárd, a nemzetbiztonsági bizottság fideszes alelnöke.
– *„Az egyik kérdésem direkt arra irányult, hogy tömeges alkalmazásról szó van-e vagy nincs, és egyértelmű választ kaptam arra vonatkozóan, hogy a törvény betűjét és szellemét betartva itt egyedi alkalmazásról van szó, amin erős külső kontroll van"* – mondta Szél Bernadett, az LMP képviselője, aki az ülés összehívását kezdeményezte.

A Nemzeti Adatvédelmi és Információszabadság Hatóság a Nemzetvédelmi Szakszolgálat írásbeli válaszának elemzése, valamint a kihelyezett bizottsági ülésen megismert információk kiértékelése után a következő értékelést hozta nyilvánosságra a honlapján[5]: *„A NAIH által végzett vizsgálat során megismert tényekből az a következtetés adódik, hogy a Nemzetbiztonsági Szakszolgálat a kémprogram alkalmazásával kapcsolatban a törvényi előírásokat maradéktalanul betartva hajtja végre az Nbtv.[6] 8 § (1) bekezdés a) pontjában meghatározott feladatait. A vizsgálat során jogsértésre utaló információ nem merült fel…"*

4 https://hirtv.hu/ahirtvhirei/kemprogram-a torveny-betujet-betartva-alkalmazzak-1243587

5 Bíró János: Jelentés a kémprogramok magyar nemzetbiztonsági célú alkalmazásáról. Adatvédelmi állásfoglalások, jelentések. 2015. 01. 08. https://www.naih.hu/files/adatvedelmi-jelentes-1904-6-2014-T_kemprogram.pdf

6 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.

A vizsgálatok során tehát több szempontból is egyértelműen bebizonyosodott, hogy a szakszolgálat a rendelkezésére álló ellenőrző eszközök alkalmazásakor minden esetben a törvények maximális betartásával járt el.

A modern tömegdemokráciákban az állampolgárok általános tájékozottsági szintjének drasztikus növekedésével az átláthatóság, azaz a transzparencia követelménye egyre markánsabban jelenik meg úgy általában az állam, illetve konkrétabban az állami szervek működése kapcsán is.

A titkosszolgálatok működése tekintetében ennek az igénynek a megfogalmazása első hallásra életszerűtlennek, bizonyos fokig a dolgok természetes rendjével ellentmondásban állónak tűnik.

Az átláthatóság kritériumának való megfelelés a szakszolgálat számára azonban magában hordozza saját szerepértelmezése tökéletesítésének, a hagyományos titkosszolgálati szervezeti szemlélet korszerűsítésének, illetve tevékenységeink új szempontú elemzésének lehetőségét.

Ezek a lehetőségek kellő belső hajtóerőt jelentettek a szakszolgálat számára, hogy innovatív módon gondolkozzon arról, kell-e, lehet-e a működésének átláthatóságát javítania. Ahogy említettük, ehhez sajátos külső motivációt hozott az élet, a 2014-es és 2015-ös szivárogtatások és következményeinek kényszerű kezelése formájában. Ilyen értelemben tehát szerencsés időszakra estek ezek az események. Ráadásul a kémprogramok alkalmazásával kapcsolatos hatósági eljárás rávilágított arra, hogy a nagyfokú szakmai felkészültséget mutató, szinte a „szőrszálhasogatásig" aprólékos, egyszersmind a saját eljárásainak, megállapításainak súlyával és lehetséges következményeivel tisztában lévő, felelős gondolkodású Nemzeti Adatvédelmi és Információszabadság Hatóságban remek partnerre találtunk az audit lefolytatásához.

Az immár közös gondolkodás eredményeként a szakszolgálatnál a titkosszolgálati eszközök alkalmazásával kapcsolatos szolgáltató tevékenység tekintetében a Nemzeti Adatvédelmi és Információszabadság Hatóság munkatársai egy olyan átfogó adatvédelmi auditot folytattak le, amely valamennyi, adatvédelmi szempontból releváns műveleti eljárásunkra kiterjedt. Az audit filozófiájának speciális játékszabályai pedig lehetővé tették, hogy a szakszolgálat úgy feleljen meg az átláthatóság követelményének, hogy közben a működése során érvényesülő szakmai elvek és szabályok, mindenekelőtt a titkosság kritériuma semmilyen módon nem sérült.

A Nemzetbiztonsági Szakszolgálat és a Nemzeti Adatvédelmi és Információszabadság Hatóság szerepkörének tisztázása

Magyarországon a nemzetbiztonsági ágazat és tevékenység transzparens szabályozására a rendszerváltás folyamatában, a demokratikus és jogállami feltételek megteremtődésével kerülhetett sor.

Az 1990. évi X. – úgynevezett ideiglenes – törvény volt az első nyílt, minden állampolgár számára hozzáférhető jogszabály, amelyben megjelentek a titkosszolgálati eszközök és módszerek alkalmazásának, illetve az állampolgári jogok védelmének fontosabb garanciális elemei, feltételei, egyebek között a nemzetbiztonsági tevékenység célirányosságának és arányosságának alapelve is, a szolgálatok tevékenységének részletes szabályait azonban nem állapította meg.

A szolgálatok működésének teljes – európai színvonalú – törvényi szabályozására az Országgyűlés 1995 decemberében kétharmados többséggel alkotta meg a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényt (Nbtv.).

A hatályos Nbtv. jelenleg is a magyar nemzetbiztonsági szolgálatok működésének fő jogi bázisa. Átfogóan szabályozza a szolgálatok működését, felsorolja az egyes nemzetbiztonsági szolgálatokat és feladataikat, meghatározza irányítási rendszerüket, továbbá rögzíti a titkos információgyűjtés eszközeit és módszereit.

A jogszabály a Nemzetbiztonsági Hivatalról leválasztotta a titkos információgyűjtéshez technikai hátteret nyújtó Nemzetbiztonsági Szakszolgálatot, amelynek kormányzati irányítását – hasonlóan a polgári hírszerzéshez és elhárításhoz – 1996 és 2002, valamint 2007 és 2010 között tárca nélküli miniszter, 2002 és 2007 között a Miniszterelnöki Hivatalt vezető miniszter látta el.

2010 nyarától – az Nbtv. módosítása után – a szakszolgálat a belügyminiszter irányítása alá került, amelyet rendészeti államtitkár útján gyakorol; a kormány irányítása alatt álló, az ország egész területére kiterjedő illetékességgel felruházott, önállóan működő és gazdálkodó közhatalmi költségvetési szerv.

A Nemzetbiztonsági Szakszolgálatnak – az ágazati jogszabályokban meghatározottaknak megfelelően – kizárólagos hatásköre van a titkos információgyűjtés külső engedélyhez kötött azon szegmensére vonatkozóan, ahol műszaki-technikai szempontból egyedülálló, komplex, ebből adódóan jelen-

tős anyagi ráfordítást, különleges szakértelmet és tapasztalatot igénylő rendszerek kiépítése vagy speciális szaktudással felvértezett humán erőforrás megléte szükséges.

A fejlesztéseknek és kapacitásoknak a szakszolgálatnál történő koncentrált megjelenítése gazdasági és szakmai előnyöket hordoz, illetve jogi garanciát jelent.

Gazdasági előnyök:

– a rendelkezésre álló költségvetési források nem aprózódnak fel;
– a „megrendelői kör" (partnereink) valamennyi szereplője egyaránt részesül a rendszer által nyújtott fejlesztésekből.

Szakmai előnyök:

– a megrendelői igényekhez alkalmazkodó koncentrált fejlesztés, illetve országos lefedettség;
– folyamatos, huszonnégy órás igénykielégítő, illetve azonnalos reagálási kapacitás;
– hatásköri összeütközések esetén koordinációs képesség;
– a nem azonos elvek alapján megvalósuló eszközalkalmazások okozta dekonspirációs veszély kiküszöbölése.

Jogi garanciák:

– a szakszolgálat a tudomására jutott információkkal semmilyen módon nem rendelkezik, azokat a törvényi szabályozók alapján reprodukálhatatlanul törli a saját nyilvántartásából;
– nincs lehetőség a „készletező" adatgyűjtésre;
– a megrendelő és végrehajtó elkülönülése a társadalmi közbizalmat erősíti;
– független végrehajtó szervként kizárt a külső engedélytől eltérő, vagy azon túlterjeszkedő eszközalkalmazás.

A szakszolgálat nem hagyományos értelemben vett rendvédelmi szerv, és nem is klasszikus titkosszolgálat. A Nemzetbiztonsági Szakszolgálatnak nincsenek saját ügyei, nem tartozik a hatáskörünkbe a különböző bűncselekmények felderítése, ellenérdekelt titkosszolgálati törekvések kipuhatolása, vagy az eredeti, hírszerzői tevékenység[7].

7 Kivételnek számítanak a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 8. § (1) bekezdés f) pontja alapján ellátandó feladatok. *„Ellátja az objektumai műveleti védelmének és személyi állománya, valamint a hatáskörébe tartozó más személyek nemzetbiztonsági ellenőrzésének feladatait."*

A szakszolgálat küldetése, hogy az elképzelhető legspeciálisabb és legtitkosabb eszközök alkalmazásával támogassa mindazon bűnüldöző szerveket és nemzetbiztonsági szolgálatokat, amelyeknek az említett értelemben vett felderítő tevékenység a hatáskörükbe tartozik.

A Nemzetbiztonsági Szakszolgálat számára – központi szolgáltató szervezetként – létkérdés annak a bizonyos mértékben ambivalensnek nevezhető egyensúlyi helyzetnek a fenntartása, amelyben maximális módon bírja a szolgáltatásai igénybevételére jogosult szervezetek bizalmát, miközben nem veszíti el a civil társadalom előtti megbecsültségét sem.

A Nemzeti Adatvédelmi és Információszabadság Hatóság a jogosultságaiból, szerepköréből és pozíciójából adódóan az említettekkel kapcsolatos, tudatos véleményformálásban egyfajta szövetségese – s egyben ellenőre is – tudott/tud lenni a szakszolgálatnak, hiszen a vonatkozó törvényi felhatalmazás alapján gyakorlatilag ugyanúgy ellenőrizheti a nemzetbiztonsági szolgálatok adatkezelését, mint bármelyik civil szervezetét. Ez a független, külső ellenőrzési szerepkör az alapvető jogok szempontjából azért kiemelkedően fontos, mert még egy demokratikus rendszerben sem tud a civil közvélemény közvetlen tapasztalás útján ismereteket szerezni egy titkosszolgálat tevékenységének jogszerűségéről, tekintettel annak minden téren megnyilvánuló konspiráltságára.

A Nemzeti Adatvédelmi és Információszabadság Hatóság küldetését, illetve annak súlyát az alaptörvény[8] VI. cikk (4) bekezdése határozza meg, amely szerint: *„A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi."* Az alaptörvény[9] alapvetéseket tartalmazó, B) cikk (1) bekezdéséből pedig, ami független, demokratikus jogállamként határozza meg hazánkat, egyértelműen levezethető, hogy az állam alapjogvédelmi ellenőrző intézményrendszerének hatásköre minden egyes állami szervre, így a nemzetbiztonsági szolgálatokra is ki kell hogy terjedjen.

A hazánkban 2012 januárja óta működő új adatvédelmi intézmény rendkívül autonóm államigazgatási szervnek tekinthető, amely – a korábbi ombudsmani modellel viszonylagos ellentétben – akár igen erős hatósági eszközökkel tudja az álláspontját érvényesíteni. Az előbbieken túl pedig törvény tiltja a hatóság működésébe való bárminemű beavatkozást.

8 Magyarország Alaptörvénye (hetedik módosításának) VI. cikk (4) bekezdése.
9 Magyarország Alaptörvénye B. cikk (1) bekezdés.

Az auditról általában – speciális játékszabályok alkalmazása

A szakszolgálat titkos információgyűjtő tevékenységének, valamint a kapcsolódó adatkezelési folyamatok átfogó adatvédelmi ellenőrzésének megtervezésénél a Nemzeti Adatvédelmi és Információszabadság Hatóság egyfajta módszertani referenciaként vette figyelembe annak a vizsgálatnak az eredményeit, amelyet *Péterfalvi Attila* még adatvédelmi biztosként folytatott le a szakszolgálatnál. A 2003-as ellenőrzés alapvetően az adatkezelés rendjének vizsgálatára irányult, de a végkövetkeztetése, miszerint az adatkezelésünk példaértékű, számottevő mértékben hozzájárult az öntudatunk és a szakmai, valamint a civil közvélemény irányába mutatott nyitottságunk fejlődéséhez.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke és a szakszolgálat főigazgatója közötti egyetértésnek megfelelően, a Nemzetbiztonsági Szakszolgálat főigazgatója – a bevezetőben tárgyalt események után, 2015-ben – felkérte a Nemzeti Adatvédelmi és Információszabadság Hatóság elnökét egy olyan átfogó vizsgálat lefolytatására, amelynek deklarált célja a titkos információgyűjtés során alkalmazott teljes eszközrendszer vizsgálata volt, az adatvédelmi aspektusból fontos sarokpontok sérülékenységeinek tekintetében. Az ellenőrzés abszolút precedensjellegű volt, hiszen korábban sem hazai, sem pedig nemzetközi szinten nem került sor arra, hogy egy adatvédelmi hatóság egy titkosszolgálat adatkezelését ilyen minőségben és mélységben ellenőrizze.

A vizsgálatra történő felkészülés és egyeztetések során már a tervezésnél körvonalazódott, hogy a titkos információgyűjtés olyannyira eltér a Nemzeti Adatvédelmi és Információszabadság Hatóság által korábban folytatott vizsgálatok tárgyától, hogy egy teljesen új módszertan kidolgozására van szükség. A koordinációs folyamat során a két szervezet megállapodott abban, hogy egy gyakorlatorientált, rendkívül komplex ellenőrzésre kerül sor annak érdekében, hogy ne csak az adatkezelési szint esetleges problémáit lehessen feltárni, hanem az eszközalkalmazások gyakorlati működésének adatvédelmi vetületeit is.

Az Infotv. által meghatározott eljárástípusok közül (adatvédelmi hatósági eljárás, vizsgálati eljárás, titokfelügyeleti hatósági eljárás, adatvédelmi audit) a Nemzeti Adatvédelmi és Információszabadság Hatóság szakértői a tudomásukra jutott, igen bonyolult szempontrendszer értékelése után a legkevésbé formakényszeres, szolgáltató jellegű eljárást, az adatvédelmi auditot választották ki. Figyelembe vették azt is, hogy az újszerű metodika kialakításához

– és akár menet közbeni formálásához – kifejezetten rugalmas, folyamatos konszenzuson alapuló együttműködés szükséges az ellenőrizni kívánt szervezettel, amit leginkább az auditálás képes nyújtani.

A törvényességnek való teljes megfelelés, valamint a szakszolgálat titkos információgyűjtéshez kötődő szolgáltatásainak igénybevételére jogosult szervezetek bizalmának megőrzése érdekében értelemszerűen arra nem kerülhetett sor, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóság szakértői az adatvédelmi audit során úgynevezett éles adatokat vagy folyamatban lévő ügyeket, esetleg célszemélyeket ismerhessenek meg. Ezen túl bizonyos esetekben még a szakszolgálat – vizsgálatban részt vevő – személyi állománya kilétének konspiráltságára is figyelmet kellett fordítanunk.

Fontos volt annak előzetes rögzítése is, hogy az auditálás során ne az egyes szakszolgálati munkatársak egyedi, szakmai teljesítményét vizsgálják, hanem a szakszolgálat működésének rendszerét, legyen szó akár a fiktív megkeresések érkeztetési folyamatáról, vagy éppen a titkos megfigyelés végrehajtásáról. Ebből adódóan a vizsgálat fókuszpontjában a titkos információgyűjtéssel kapcsolatos – jogi, módszertani, technikai – rendszer(ek) funkciójának, tevékenységének megfelelősége állt.

A Nemzeti Adatvédelmi és Információszabadság Hatóság munkatársai mindvégig kifinomult tapintattal, egyúttal az objektív megismerésre való törekvéssel jártak el az ellenőrzés során. Ezzel összhangban – a szakszolgálat által alkalmazott különleges eszközök és módszerek védelme érdekében – néhány eszközcselekményt „back office" működési kereteken belül hajtottunk végre, ezek megmutatására azonban magától értődő módon nem került sor. Ilyenek voltak például az online kutatás (kémprogram alkalmazása) technikai részleteinek egyes elemei, a küldemény-ellenőrzések során a speciális bontási technikák szakmai finomságai vagy éppen a titkos kutatás során alkalmazott zárnyitási eljárások.

Az audit végrehajtása, eredményének bemutatása

Az előbbiekben részletesen tárgyalt vizsgálati módszer kiválasztását, valamint a speciális „játékszabályok" mindkét részről történő elfogadását, illetve a megfelelő előkészítést követően azután megkezdődhetett az adatvédelmi audit. Csaknem két éven át, összesen harmincnégy modellesemény végrehajtására került sor a gyakorlatban.

Az auditálás során a Nemzeti Adatvédelmi és Információszabadság Hatóság kijelölt szakértői – mint egy fiktív megrendelő szervezet munkatársai – a titkos információgyűjtés modellfolyamatát a következő tárgykörökre bontva, közvetlenül vizsgálták:

– a szakszolgálat szolgáltató szerepkörében – Nbtv. 8. § (1) bekezdés szerinti – (fiktív) megkeresések érkeztetése, ellenőrzése, illetve a (fiktív) megrendelő szervezettel történő kapcsolattartás;
– a szolgáltatás végrehajtása;
– a beszerzett adatok – szükség szerinti – feldolgozása és a keletkezett információk továbbítása a (fiktív) megrendelőnek.

Az audit a titkos információgyűjtés adatvédelmi szempontból érzékeny eszközeire és módszereire fókuszált, illetve kiterjedt a szolgáltató tevékenység minden munkafázisára; ezen belül jelentősebb hangsúlyt kaptak – a statisztikai adatokat alapul véve – azok a szolgáltatások, amelyekből a Nemzetbiztonsági Szakszolgálat rendszeresen a legtöbbet teljesíti.

A Nemzeti Adatvédelmi és Információszabadság Hatóság kijelölt szakértői – akik értelemszerűen átestek nemzetbiztonsági ellenőrzésen, volt személyi biztonsági tanúsítványuk, valamint felhasználói engedélyük és titoktartási nyilatkozatot írtak alá – a modellesemények precíz megtervezése érdekében előzetesen, átfogó módon tanulmányozták a vonatkozó joganyagokat; a külső és belső normákat egyaránt.

A gyakorlatorientált ellenőrzés megvalósítása érdekében a Nemzeti Adatvédelmi és Információszabadság Hatóság – a rendkívül alapos felkészülést követően – a szakszolgálat kijelölt munkatársaival együttműködve kialakított tehát harmincnégy olyan, előzetesen meghatározott fiktív szituációt (modellesemény), amelynek végrehajtása során a szakszolgálat minden alkalommal választási helyzetbe került egy adatvédelmi szempontból releváns kérdésben.

A tesztek terveit előzetesen csak a szakszolgálat kijelölt kapcsolattartói ismerhették meg, akik a Nemzeti Adatvédelmi és Információszabadság Hatóság elvárásának megfelelően, írásban vállaltak titoktartási kötelezettséget.

A tesztek között számos olyan „stresszteszt” jellegű modellesemény kialakítására és végrehajtására is sor került, amelyek nem – a titkos információgyűjtés során – tipikusan előforduló helyzeteket modelleztek, hanem olyanokat, amelyek valós körülmények között, csekély gyakorisággal megjelenő, igen bonyolult jogi megítélésű szituációk. Ezek esetében a szakszolgálat számára nem volt opció a mindennapi rutinnak megfelelő, jól bevált, szinte ref-

lexszerű válasz, hanem a jogértelmezési finomságok terén kellett állást foglalnia egyes adatvédelmi kérdéskörökben.

A szervezeteink közötti folyamatos egyeztetések általi mozgásteret használva, a Nemzeti Adatvédelmi és Információszabadság Hatóság szakértői az adatvédelmi audit során az auditálás eszközrendszerének szinte teljes körű repertoárját felvonultatták, illetve alkalmazták, hiszen sor került a tevékenységet szabályozó normakörnyezet tanulmányozására, előzetes konzultációkra, prezentációk megtekintésére, szó- és írásbeli felvilágosításkérésre, helyszíni, közvetlen megfigyelésekre, strukturált interjúkra, gyakorlatorientált tesztekre, hang- és képrögzítéssel járó dokumentálásra stb.

A tesztek technikai hátterének megteremtése érdekében a hatóság egyes esetekben például preparált csomag- vagy levélküldeményeket készített elő, illetve a telefonlehallgatások ellenőrzéséhez egy tökéletesen szeparált elektronikus hírközlési tesztkörnyezetet alakított ki, amelyen az ellenőrizendő kommunikáció zajlott. Az audit módszertanának részletes bemutatása a Nemzeti Adatvédelmi és Információszabadság Hatóság 2016. évi országgyűlési beszámolójában olvasható[10].

Utólag már mókásnak tekinthető pillanatok is fűszerezték a tesztek végrehajtását.

Talán a legjobb példa erre, amikor a küldemény-ellenőrzést vizsgáló egyik modellesemény végrehajtása során munkatársaink két hosszú, barna, feltehetően női hajszálat találtak egy csomagküldemény konspirált bontásakor. Bár az ellenőrzés iránya nyilvánvalóan nem az ilyen praktikus értelemben vett konspirált végrehajtás vizsgálata volt, körültekintő, és érthető szakmai okokból „kellően paranoid" munkatársaink nyilván arra gondoltak, hogy a hajszálak, illetve azok felfedezése hozzátartozik a teszt eredményes teljesítéséhez. Természetesen később kiderült, hogy az agyafúrt preparátumnak gondolt hajszálak teljesen véletlenül kerültek a csomagra, nem a Nemzeti Adatvédelmi és Információszabadság Hatóság szakértőinek rafináltsága folytán. Az életszerűség eddig azért nem terjedt, mint ahogy az audit scope-ja sem terjedt túl az adatvédelmi relevanciájú szabályok és alapelvek érvényesülésének vizsgálatán.

Az ellenőrzési cselekmények tapasztalatainak részletes kiértékelését a Nemzeti Adatvédelmi és Információszabadság Hatóság egy terjedelmes összefoglaló jelentésben, egy kiemelkedő szakmai színvonalú és igen hasznos

10 A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2016. évi tevékenységéről. Budapest, 2017. https://www.naih.hu/files/NAIH-BESZ-MOL- – 2016_MID-res.pdf

dokumentációban rögzítette, majd adta át a szakszolgálat számára; az abban található érzékenyadat-tartalom miatt – ellentétben a szokásos eljárással – nem tettük közzé a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján.

A következő idézetek mindegyike az adatvédelmi audit vezetője és szakértői által készített jegyzőkönyvből[11] való:

– *„az összefoglaló értékelésben rögzített tények visszaigazolják azt, hogy az NBSZ magas szakmai színvonalon és a jogszerű adatkezelés iránt elkötelezetten hajtja végre a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatait…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság);
– az Nbtv. szabályozási rendszerében a *„megrendelő szervezet – szolgáltató szervezet” szerepkörök elválasztása törvényességi kontrollfunkciót ruházott az NBSZ-re azáltal, hogy a szolgáltatónak ellenőriznie kell azt, fennállnak-e a szolgáltatás teljesítésének jogi feltételei, vagyis az NBSZ előzetesen ellenőrzi és visszautasítja vagy kijavíttatja a törvénysértő megrendeléseket…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság);
– *„indokolt, hogy egy szervezetben koncentrálódik a titkos megfigyeléshez szükséges speciális technika és szakértelem… az audit alapján megállapítható, hogy a végrehajtás törvényességének biztosítása a Szakszolgálatnál olyan fontos szempont, amelyet a szervezet akár a megrendelő szervezettel szemben is érvényesít…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság)
– *„a Hatóság az NBSZ szakértőivel együttműködve kidolgozta azt a módszert, amely a jogszabályi előírások maradéktalan betartása mellett alkalmas a titkos információgyűjtő tevékenység komplex adatvédelmi ellenőrzésére…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság)
– *„az NBSZ minden esetben figyelembe vette az alkotmányos/adatvédelmi követelményeket és megtagadta a fiktív megrendelő szerv próbálkozásait a törvény kijátszására…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság);
– *„az NBSZ által követett jogértelmezés és joggyakorlat az Nbtv. által meghatározott keretek közé esik, ezért adatvédelmi szempontból nem kifogásolandó…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság);
– *„az NBSZ belső normái olyan feladat ellátási és eljárási rendet írnak elő, amelyek a személyes adatok védelmének követelményeivel konform módon töltik be a törvényi szabályozás kisebb hézagait és szabályozzák a szervezet tevékenységét…”* (Nemzeti Adatvédelmi és Információszabadság Hatóság).

11 Péterfalvi Attila – Bíró János: A Nemzetbiztonsági Szakszolgálat adatvédelmi auditjának értékelése. Budapest, 2017. december. Nem publikált kiadvány.

Tanulságok, következtetések, nyomon követés

Az eddig teljesen járatlannak tűnő út – az egyedülálló módszertan – az auditálási folyamat során mindkét szervezet számára fokozatosan egyre biztonságosabbá és megnyugtatóvá vált, hiszen a Nemzeti Adatvédelmi és Információszabadság Hatóság szakértői közvetlen, „kézzelfogható" ismeretszerzés útján szerezhettek tapasztalatokat a Nemzetbiztonsági Szakszolgálat gyakorlati működésének jogszerűségéről és adatvédelmi megfelelőségéről. A szakszolgálat munkatársai pedig számukra újszerű, kifejezetten friss, esetenként az általuk megszokottól teljesen eltérő szempontok szerinti megközelítéssel tekinthettek az ellenőrzési cselekmények végrehajtásakor a mindennapi, rutinszerű tevékenységükkel kapcsolatos, potenciális adatvédelmi sérülékenységekre.

Az eredmények alapján a Nemzeti Adatvédelmi és Információszabadság Hatóság véleménye[12] szerint *„az audit messzemenően visszaigazolta az NBSZ elkötelezettségét az adatkezelés törvényességét illetően, ugyanakkor a tesztek a titkos információgyűjtéssel kapcsolatos tevékenységek néhány olyan részletét is feltárták, amelyekkel kapcsolatban a Hatóság az adatvédelmi követelmények magas szintű érvényesítése érdekében észrevételekkel és javaslatokkal élt".*

Az audit rendelkezésre álló dokumentumai hihetetlen gazdag ismeretanyagot jelentenek a szakszolgálati tevékenység adatvédelmi aspektusai iránt érdeklődő, és persze egyidejűleg ilyen szempontból arra illetékesek számára. Mégis, az auditot röviden, majdhogynem statisztikai szemlélettel összefoglalva a következők állapíthatók meg.

A Nemzeti Adatvédelmi és Információszabadság Hatóság a szakszolgálat hathatós közreműködésével az audit során a szolgáltatási kínálatunk adatkezelési szempontból legérzékenyebb elemeinek átvilágítása érdekében harmincnégy, a megrendelést, a teljesítést (eszközalkalmazást), a közbenső és utólagos adatkezelési folyamatokat hűen és teljeskörűen utánzó modellesetményt hajtott/hajtatott velünk végre, amelyeket negyvenegy ellenőrzési cselekményben vizsgált és rögzített. Az ellenőrzési cselekmények, illetve azok kiértékelése nem tárt fel jogellenes adatkezelési gyakorlatot.

– Harmincegy ellenőrzési cselekmény esetében a konklúzió az adatvédelmi követelményeknek való teljes megfelelés volt.

12 Uo.

– Nyolc esetben fogalmazott meg a Nemzeti Adatvédelmi és Információszabadság Hatóság magas szintű adatvédelemre irányuló javaslatot a jelenleg is jogszerű adatkezeléssel kapcsolatban.
– Ezen kívül két ellenőrzési cselekmény kapcsán jelzett a hatóság olyan korrekciós javaslatot, amely jövőbeli, potenciálisan jogsértő adatkezelési szituáció megelőzésére vonatkozott.

Az audit tapasztalatairól készült jegyzőkönyv[13] ajánlásait és észrevételeit feldolgoztuk, kiértékeltük és bár a tevékenységünk jelenleg is jogszerűen zajlik, a magasabb szintű adatvédelem elérése érdekében teendő feladatok megvalósítására intézkedési tervet készítettünk, amelynek ütemezett végrehajtása napjainkban is tart.

A konkrét esetekre vonatkozó javaslatok alapján a kötődő munkafolyamatainkat átvizsgáltuk, ezek korrigálása ütemezetten folyamatban van; az adatvédelmi változásmenedzsment-keretrendszert azonban már kidolgoztuk, amelyet a Nemzeti Adatvédelmi és Információszabadság Hatóság a technikai vonatkozású szolgáltatásokkal összefüggő jogértelmezési kérdések bonyolultságára, valamint a technikai környezet folyamatos változékonyságára tekintettel javasolt kialakítani és mielőbb bevezetni.

Az adatvédelmi audit tehát számos ponton hagyott nyomot a szakszolgálat életében. Felülvizsgáltunk több munkafolyamatot, tökéletesítgettünk bizonyos mozzanatokat, pontosítottunk egyes belső szabályzatainkon, vagy éppen finomhangoljuk technikai eszközeink, rendszereink működését. A legfontosabb hatás azonban nem ilyen kézzelfogható, ugyanis a szervezeti kultúra egészen más szegmensében következett be. Ez pedig a közös tudások és hivatkozások területe, mégpedig egy olyan íratlan ismeretanyagra vonatkozóan, amely csak az adott szervezet, jelen esetben a szakszolgálat sajátja.

Nos, véleményünk szerint nincs az a továbbképzés vagy érzékenyítő tréning, amely annyit adna, annyira közel hozná, izgalmassá és átélhetővé tenné az adatkezelés elvi és gyakorlati kérdéseit, mint amennyire az audit, illetve az abban való közreműködés tette. Az ellenőrzési cselekményekben való tevőleges közreműködés körülbelül annyival izgalmasabb az adatkezelésre vonatkozó jogszabályok tanulmányozásánál, mint amennyire egy joghallgató számára egy érdekfeszítő, borzongató thriller megtekintése vonzóbb perspektíva a büntetőeljárási kódex átmeneti rendelkezéseinek bebiflázásánál.

13 Uo.

Végezetül legyen szabad megosztani az olvasóval egy sajátos életérzést. A szakszolgálat unikális rendeltetésű, különleges szolgáltató szervezet, amely immár két évtizede folyamatosan csiszolja, finomítja azokat a képességeit, érzékeit, amelyek elengedhetetlenek a környezetünk, illetve a saját magunk által támasztott követelményeknek való megfeleléshez.

E kompetenciák sorában jelentős helyet foglal el egyfajta jogtudatosság, illetve érzékenység, ami egy nagyon komoly jogalkalmazói jogértelmezési munka keretében él és fejlődik. Túl az auditon, immár mondhatjuk, hogy ehhez a fejlődéshez (is) találtunk olyan partnerra, a Nemzeti Adatvédelmi és Információszabadság Hatóságra, amely szervezet az autonómiájából adódóan képes kellő távolságtartással, higgadtan és elfogulatlanul visszajelzést adni a tevékenységünkről.

Nehéz visszaadni azt a jóleső érzést, amely akkor töltött el minket, amikor a hatóság – alapos vizsgálódás után – visszaigazolta egy-egy saját bázisú jogértelmezésünk, illetve azon alapuló gyakorlatunk helyességét. Azt gondoljuk, ilyesmit érezhet egy tudományos-fantasztikus filmben, a távoli galaxisban magányosan bolyongó asztronauta, amikor más civilizáció nyomára bukkan: „Nem vagyok egyedül!”

DOI: 10.38146/BSZ.2019.1.3

HORVÁTH FERENC

A közszolgálati etika alapvető kérdéskörei a Nemzetbiztonsági Szakszolgálatnál

A Nemzetbiztonsági Szakszolgálat speciális szerepet tölt be a magyar rendvédelem szervezetrendszerében, így működése a közszolgálati etika terén is vet fel sajátos kérdéseket. Jelen tanulmány fő célkitűzése körülhatárolni, így átláthatóvá tenni a polgári nemzetbiztonsági szolgálatok működésének közszolgálati etika szempontjából leginkább érzékeny kérdésköreit, amelyek a költségvetési források felhasználásával kapcsolatos klasszikus anomáliák, korrupciós kockázatok, a minősített adatok kezelésével, a titkosság és konspiráció illetéktelenek előtti fenntartásával kapcsolatos feladat, illetve a titkos információgyűjtés eszközei és módszerei alkalmazásának etikai vonatkozásai köré csoportosíthatók.

E kérdéskörök feltárása segítheti a belső ellenőrzést, a belső bűnmegelőzési és bűnfelderítési feladatokat végző szervek, a civil kontrollt biztosító és a törvényességi ellenőrzést végző szervek energiáinak hatékonyabb összpontosítását a közbizalmat leginkább megalapozni, illetve megrendíteni képes témakörökre.

Jog és etika

Azért fontos mindezeknek a kérdésköröknek az etikai oldalával foglalkozni, mert a jogszabályok megalkotása önmagában nem vezet olajozottan működő együttéléshez, rendhez. A jogkövetés végső formája szubjektív lélektani folyamatokon keresztül bontakozik ki. A jog tiszta, objektív kategóriákban, leegyszerűsített helyzetekben gondolkodik, nem térhet ki az élet sokszínűségének megfelelő minden helyzetre. A büntető törvénykönyv különös része csak az elkerülendő végállapotokat írja le tényállásként, de nem részletezi az oda vezető, lelki szempontból kockázati tényezőként kezelendő lépéseket.

Költségvetési források felhasználása

A Nemzetbiztonsági Szakszolgálat önállóan működő és gazdálkodó költségvetési szerv, és mint ilyen, társadalmi funkciójának ellátása során köteles ha-

tékonyan és átláthatóan gazdálkodni az adófizetők pénzével. Beszerzései, beruházásai, fejlesztései, eszközgazdálkodása, bérgazdálkodása – a vonatkozó jogszabályoknak és közjogi szervezetszabályozó eszközöknek megfelelően – szigorú előírások, többszörös ellenőrzések, megosztott jogosultságok mellett zajlik, annak közérdekből nyilvános gazdálkodási adatai a honlapon bárki számára hozzáférhetők.[1]

A szervezeti gazdálkodás nem légüres térben zajlik. A lehetséges szolgáltatók, beszállítók köre a gyakorlatban rendszerint véges, hiszen Magyarország „kicsi". A piaci környezetben minden szereplőnek megvan a maga imázsa, híre, stílusa, a felek ismerik egymást, ajánlásaik, személyes kapcsolataik vannak. A költségvetési szerv gazdálkodásért felelős munkatársai is jól működő kapcsolatrendszert építenek ki az évek alatt, tudják, milyen ügyben kihez fordulhatnak, más szervezetek beszerzői milyen tapasztalatokat szereztek a piaci szereplőkről. Alapvető kérdés, hogy például a hatékonyságot szolgáló meghívásos közbeszerzési eljárások során az ajánlattételi szakaszban kiket hívunk meg, melyek azok a partnerek, amelyektől jó színvonalú szolgáltatást várhat a szervezet a célok megvalósulása érdekében. Nagyon fontos, hogy ilyenkor szigorúan csak szakmai szempontok érvényesüljenek.

A döntések pártatlanságát szolgálja, ha mindenki komolyan veszi a kormánytisztviselői hivatásetikai kódex[2] ajánlásait, és megőrzi elfogulatlanságát, nem fogad el ajándékokat, visszautasítja a felkínált jogtalan előnyöket, nem kerül mások befolyása alá, illetve nem él vissza hivatali helyzetével. Az ajándékok például a cégekkel való kapcsolattartás során udvariassági, figyelmességi gesztusnak, ártatlan „reklámfogásnak" tűnhetnek, visszautasításuk szociális szempontból kellemetlen, miközben alkalmasak lehetnek arra, hogy a szociálpszichológiai csereelmélet[3] elvei alapján – a jó kapcsolat fenntartása érdekében – lélektanilag viszonzásra sarkallják a kedvezményezettet, ami jelen esetben etikai, súlyosabb esetben akár jogi vonzattal is együtt járhat. Az ajándékok, előnyök a fokozatosság elve alapján idővel egyre nagyobb értékűek lehetnek, miközben a kedvezményezett érzékenysége csökken, sőt idővel elvárttá is válhat a figyelmesség, különösen, ha mindenki más is kap a környezetében a partnerektől hasonlókat. Így válhat az eredetileg egyedi, egyszeri esetből csoportnorma, megszokott hétköznapi jelenség, az apró fi-

1 http://nbsz.hu/?mid=6

2 http://korrupciomegelozes.kormany.hu/download/b/df/70000/Kormánytisztviselői%20Hivatásetikai%20Kódex.pdf

3 Bővebben Lőrincz László: A vonzás szabályai – hogyan választanak társat az emberek? Szociológiai Szemle, 2006/2., 96–110. o.

gyelmességből pedig integritássértés. Hiába határozza el a szakterületre érkező, tiszta lelkű munkatárs, hogy nem vesz részt ilyesmiben, adott esetben már egy jól működő rendszer részeként kell megtalálnia a saját helyét, alkalmazkodnia kell a „játékszabályokhoz", az „értelmezési kerethez", ahol minden külső szereplő ilyen attitűddel áll az üzlethez.

Ugyancsak kardinális kérdés, hogy mekkora összeg kerül a papírokra. A piacon az ár általában bizonyos mértékig relatív, a keresleti-kínálati viszonyoktól függ. Különösen az olyan áruknál, szolgáltatásoknál tud változékony lenni, amelyek esetében nincs bevett piaci szokásrendszer, mert egyediek, ritkák – és a nemzetbiztonsági szolgálatok beszerzései némely esetben ilyenek. Ilyenkor az eladó vagy eladók szabnak árat, és nehéz elkerülni közöttük az egyeztetés, összejátszás lehetőségét, az árak tudatos felsrófolását, ahol még az olcsóbb is drága. A közbeszerzési eljárásoknál nem feltétlenül mutatnak normális statisztikai eloszlást az ajánlatok, nem ritkán a piacinál magasabb végső beszerzési érték tapasztalható, illetve a várhatónál sűrűbben fordulnak elő az éppen értékhatár alatt megszabott árak. A pályázat elbírálóinak szaktudása különösen fontos szerepet kap, hiszen végül nem minden esetben kapnak reális, felelősséggel elfogadható ajánlatot. Az alkupozíció kialakításánál úgy kell eljárni, hogy ne legyen nyilvánvaló a megrendelő kiszolgáltatottsága, ha mindenáron vennie kell. A beszerzési eljárások során tehát a szervezeti szereplőknek szigorúan be kell tartaniuk az eljárásra vonatkozó titoktartási kötelezettséget, nem szabad információkat szivárogtatniuk a piaci szereplők irányába, bármilyen jó is a kapcsolatuk egyébként.

Az árszabásoknál külön figyelmet érdemlő kategória a lehetséges „zsebalkuk" köre, amikor a szervezet képviselője információt ad az „elfogadható" árról, kardinális szempontokról, a konkurencia ajánlatairól, „titkos közvetítői háladíjért" cserébe. A kapcsolattartás során szükség van a személyes jó kapcsolatra, rugalmasságra a főbb beszállítókkal, de nem lehet erősebb a lojalitás kifelé, mint a szervezet irányába, ezért kerülni kell a személyes, magánjellegű kapcsolattartást és bármi olyan befolyást, ami anyagi, érzelmi lekötelezettséget válthat ki az irányukba.

A beszerzési folyamat végén, a teljesítésigazolásokkal kapcsolatban a feltárt hiányosságok súlyának megítélésén jelentős pénzösszegek múlhatnak, további munkanapok elrendelése, kötbér kifizetése válhat szükségessé. A beruházónak anyagi érdeke kedvező döntést kicsikarni az illetékes szakemberből. Amennyiben például a korábbi munkafázisokban a megrendelő szervezet műszaki munkakörben dolgozó képviselője elmulasztott valamilyen ellenőrzést, utólag már nagyon nehéz ezzel kapcsolatos észrevételt tennie, hiszen az felve-

ti a saját felelősségét is a hiányosság kialakulásában, kezeletlen voltában. Fontos tehát mindent szigorúan a szabályzókban foglaltaknak megfelelően végrehajtani még jelentős időnyomás és túlterheltség mellett is, illetve lehetőség szerint külön szakemberekre bízni a kivitelezés folyamatába épített időközi ellenőrzéseket és a végső munka átvételt. Ha a kivitelező bármilyen módon nyomást kísérel meg gyakorolni a döntéshozó(k)ra, azt azonnal jelenteni kell a vezetésnek, hogy a sérült pártatlanságra tekintettel másra szabhassák a feladatot.

A közvagyonnal való gazdálkodás másik jelentős kérdésköre a meglévő eszközök és készletek felelősségteljes kezelése, meglétének, megfelelő állapotának fenntartása, magáncélra való felhasználásának elkerülése. Ezek azok a témakörök, amelyekben büntetőjogi tényállás megvalósulása esetén nehéz nem szándékosságot feltételezni. Az eszközök és készletek eltulajdonításának megelőzése rendszeres vezetői ellenőrzések, leltári ellenőrzések és hatékony objektumvédelem kérdése.

Ha már csökkenő mértékben is, de mégis tapasztalható egy hátrányos szemléletbeli sajátosság, ami talán még a rendszerváltozás előtti Magyarország „minden a dolgozó népé" attitűdjének a maradványa. Még harminc év után is társadalmi szinten tapasztalható egyfajta tolerancia az olyan viselkedésformák kapcsán, amelyek a közös erőforrások magáncélból való önkényes felhasználására irányulnak, sőt, néha még szimpátia is övezi a hatóságokkal szembeszálló, lázadó egyént.[4] A mai napig bocsánatos bűnként tekintenek az emberek a hivatali eszközön való magáncélú fénymásolásra, a szolgálati autóval való hazakanyarodásra, az irodai fogyóeszközök otthoni felhasználására vagy a táppénz indokolatlan igénybevételére.

A központi költségvetésből kapott erőforrásokkal való gazdálkodás során tehát kiemelten fontos betartani az előírásokat, de emellett figyelmet kell fordítani arra is, hogy az egész szemlélet- és gondolkodásmód is a „jó gazda" elvét kövesse, még olyan kérdésekben is, amelyekre nem terjed ki szabályozás, ellenőrzés vagy objektív mérce.

Titkok védelme

Ahogy az előző témakörnél, a titok témakörének is van egy jogi meghatározása, illetve a jogalkalmazás során megnyilvánul egy sor olyan lélektani fo-

4 A Budapesti Közlekedési Központ (BKK) ellenőrei és a bliccelők, a traffipax mellett álló rendőrök és a gyorshajtók harcában máig nem egyértelmű, hogy a jogkövetést támogatná a közhangulat, pedig a közfeladatot ellátók már régen nem egy elnyomó állam képviselői, hanem a demokratikus jogrend őrzői.

lyamat, amelyek árnyalják, módosítják a jogkövetés szubjektív lehetőségeit. Az adatok kiszivárogtatásának több elméleti fajtája is létezhet aszerint, hogy kinek milyen motiváció bázisán történik információátadás, például:

1. bizalmi kapcsolatban információ önkéntes megosztása belső lelki igény alapján
   a) kötődési igény,
   b) a személyes fontosság hangsúlyozása (hencegés);
2. nem bizalmi kapcsolatban információ önkéntes megosztása óvatlanságból (például alkohol);
3. nem bizalmi kapcsolatban információ önkéntes megosztása haszonszerzés céljából;
4. nem bizalmi kapcsolatban információ kényszerű megosztása (például zsarolás).

A közérdekű és közérdekből nyilvános adatok hozzáférhetőségének lehetővé tétele a szabad véleménynyilvánításhoz való jog gyakorolhatóságának fontos előfeltétele, mindamellett a *minősített adat védelméről szóló 2009. évi CLV. törvény* lehetőséget ad arra, hogy az állam a minősítéssel védhető közérdek körébe tartozó adatokhoz való hozzáférést korlátozza azokra, akik az előírt követelményeknek megfelelnek.

Az állam érdeke (titkosítani) és az állampolgár érdeke (megismerni) egyensúlyára kell törekedni. Az adatok védelmével kapcsolatban fontos alapelv lett tehát a szükségesség és arányosság elve, azaz csak a minősítés szükségességét megalapozó indokok fennállása esetén, csak a feltétlenül szükséges mértékben és időtartamra lehet minősítést alkalmazni. Ez azonban differenciált és tudatos, jogi szemléletű gondolkodást, a minősítés funkciójának és korlátainak alapos ismeretét feltételezi minden olyan munkatárs részéről, aki munkája során minősített vagy minősítést érdemlő adatokkal kerül kapcsolatba, illetve minősítésre javaslatot tesz.

Mindennek van azonban lélektani vonatkozása is. A titok teher, a titoktartásnak súlyos érzelmi ára van, hiszen elszigetel azoktól, akikhez az ember legszívesebben őszintén és korlátozások nélkül kapcsolódna, az elhallgatás óhatatlanul falat emel a titok birtokosa és a családi kapcsolatok, barátok közé, amit meg kell szokni és tudni kell kezelni. Ha valaki úgy lép e pályára, hogy már meghatározott szabályok szerint működő párkapcsolatban él, nem minden esetben könnyű elfogadtatni a társsal az új helyzethez kapcsolódó szigorú és speciális szabályokat, a titkolódzást, amikor korábban mindent meg tudtak osztani egymással. Erős bizalom kell ahhoz, hogy a társ vakon el-

higgye, hogy a másik már megint egy szolgálati feladat miatt kell hogy elmenjen otthonról az éjszaka közepén, amiről többet nem mondhat. Ha feltétel nélkül megbíznánk is a társunkban, fontos tudatában lenni, hogy egy második személy már nem annyira motivált megőrizni a titkot, így erősebbek lehetnek számára a további titokmegosztás előnyei (bizalom, figyelem elnyerése), mint a hátrányai.

Személyiségfüggő, ki mennyire igényli mindenáron megélni az önfeltárás mélyebb szintjeit, de a nemzetbiztonsági pályán az alkalmasság korlátja lehet, ha valaki nem képes pontosan érzékelni és megvédeni az énhatárait. Különösen igaz ez arra az esetre, amikor a titokbirtokos a különleges munkakörére való nyílt hivatkozással próbál figyelmet és elismerést szerezni magának civil társaságban, és elejt olyan információkat, amelyek felkelthetik mások érdeklődését.

A titok védelmének megvannak a képzések során elsajátítható kommunikációs fogásai, amelyeket meg kell tanulni tudatosan alkalmazni. A legjobb, ha a külvilág nem tudja, hogy egyáltalán van a birtokunkban titok. Ha ugyanis ez kiderül, beindul a természetes kíváncsiság, motiváció ébredhet a titok, az információ megszerzésére. Ezért is fontos, hogy a szükséges ismeret elve alapján törekedjünk arra, hogy az egyes minősített adatokat csak azok ismerhessék meg, akiknek munkájuk során ez feltétlenül szükséges, így a munkatársak nem tudnak többet a kelleténél. Ez a fajta „belső konspiráció", a saját munkakörben megtapasztaltak megosztásának szervezeten belüli tilalma csökkenti a titokkezeléssel kapcsolatos terhelést.

Elvárás munkatársainktól, hogy lehetőség szerint ne hirdessék nyíltan munkahelyüket, és különösen ne pontos munkakörüket, feladataikat.

Laikusoktól könnyebb megvédeni a titkokat, hiszen nincsen kifinomult eszköztáruk, helyzeti hatalmuk a titok birtokosa kapcsán, és a motivációik is esetlegesebbek, nem fektetnek túl sok energiát a feltárásba, ha nehézségekbe ütköznek. Kifejezetten ellenérdekelt felek (például hírszerzők, bűnözői körök) azonban megkísérelhetnek közel férkőzni titokbirtokoshoz, emellett motiváltak sok energiát (időt és pénzt) fektetni egy olyan kapcsolat kiépítésébe, amely végül a titkok megszerzéséhez vezethet. Az integritássértésekbe való bevonás során az ellenérdekelt csoportok tulajdonképpen a beszervezés logikáját használva igyekeznek eltéríteni a munkatársat a „rendeltetésszerű" munkahelyi működéstől, ezáltal jogosulatlanul hozzáférve információkhoz, illetve befolyásolva a pártatlan, objektív működést. Ezért fontos szempont a nemzetbiztonsági pályán dolgozók kifogástalan életvitele, biztonságtudatos magatartása, az anyagi függetlenség. A szokatlan megkeresésekkel, gyanús élethelyzetek-

kel kapcsolatban a munkatársakban ki kell alakítani egyfajta egészséges gyanakvást, tudatosítani kell, hogy érdemes adott esetben a belső biztonságért felelős szervezeti elem szakembereinek a segítségét is igénybe venni.

E témakörhöz tartozik a leszerelés utáni titokvédelem, a munka során megszerzett szaktudás felhasználásával kapcsolatos kérdések köre is. A speciális nemzetbiztonsági munkakörökben megszerzett tudás sok esetben annyira egyedi, hogy az csak a munkaerőpiac egy nagyon szűk szeletén belül számít értékesnek és keresettnek. Máshoz viszont adott esetben nem ért a pályaelhagyó, így megélhetési kényszerhelyzetben kell élete végéig elkötelezettnek maradnia az integritásnak megfelelő megoldások iránt, egy olyan közegben, ahol sokan szívesen fizetnének az általa birtokolt tudásért. Ez a probléma rávilágít arra, hogy a munkáltatónak kötelessége és érdeke is egyben tudatos életpálya-tervezés és korrekt eljárásrendek, illetve versenyképes javadalmazás révén az egész karrierívre nézve gondoskodni munkavállalóiról, miközben a munkavállaló hűsége, elkötelezettsége, hivatástudata jelentős biztonsági vonatkozásokkal is bír.

Titkos információgyűjtés, leplezett eszközalkalmazás

A közszolgálati etika harmadik, egyben legspeciálisabb kérdésköre magával a nemzetbiztonsági szolgálatok társadalmi alapfunkciójával kapcsolatos.[5] A fő probléma, hogy jelenleg nincsenek egyértelműen megfogalmazva a nemzetbiztonsági szolgálatok részére a társadalmi rendeltetésük, működésük erkölcsi legitimációját adó keretek, nem világos, hogy a nemzetbiztonsági szolgálatok mint a közhatalom gyakorlásának sajátos eszközei milyen végső célt szolgálnak, és mi teszi e célokat erkölcsi szempontból védhetővé. Márpedig a nemzetbiztonsági szolgálatok társadalmi funkciójának megértése, elfogadása nemcsak a közvélemény viszonyulása és a közbizalom, hanem a munkavállalók elkötelezettsége szempontjából is alapvető kérdés.

A nemzetbiztonsági szolgálatok társadalmi felhatalmazás alapján, szigorú jogszabályi keretek között végzett munkájuk során a nemzeti, társadalmi szintű biztonság igénye és a személyes alapjogok[6] adta szabadság korlátozá-

5 Bővebben Horváth Ferenc: A közszolgálati etika elméleti és gyakorlati kérdései a Nemzetbiztonsági Szakszolgálatnál. Doktori értekezés. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, Budapest, 2018.

6 A nemzetbiztonsági szolgálatok tevékenysége a magánlakás, a magántitok és a levéltitok, illetve a személyes adatok védelméhez, információs önrendelkezéshez, valamint a birtokvédelemhez fűződő alapvető jogok korlátozásával járhat együtt.

sának szükségessége, illetve az ezek közötti helyes arány megtalálása, egyensúlyuk megteremtése keletkeztet etikai dilemmát.

Szükséges tehát egy olyan erkölcsi alap kialakítása a nemzetbiztonsági tevékenység vonatkozásában, ami megnyugtató választ ad arra a kérdésre, hogy arányban áll-e, időtálló, univerzális emberi értékeket jelentő célt szolgál-e az a jogkorlátozási gyakorlat, amelyet a nemzetbiztonsági szolgálatok társadalmi funkciójuknál fogva folytatnak, egyre bővülő technikai lehetőségek birtokában.

Az igazságos hírszerzés elmélete

A nemzetbiztonsági etika nemzetközi szakirodalmának egyik jellegzetes alakja *Ross W. Bellaby,* akinek – az Amerikai Egyesült Államok hírszerző szerveinek működését meghatározó hivatalos doktrínákkal összhangban álló[7] – álláspontja szerint az állami hírszerző szolgálatok célja az állam és a társadalom védelme, eszköze pedig a titkos műveletek végrehajtása, ami nemhogy szükségtelenné és lehetetlenné tenné az etikai követelmények fokozott érvényesítését, hanem éppen ellenkezőleg: indokolja. Bellaby az igazságos háború elméletén[8] belül kezeli a nemzetbiztonsági etikát, annak kiterjesztése révén az igazságos hírszerzés elméletét dolgozta ki.[9] Ennek alapelvei a következők:

- *Igazságos ok:* a titkos információgyűjtés eszközeinek és módszereinek alkalmazásával járó kárt elégséges fenyegetés kell, hogy igazolja.
- *Legitim autoritás:* a politikai közösség akaratát legitim módon képviselő hatalom hajthatja végre.
- *Helyes szándék:* az eszközöket csakis az azokat megalapozó fenyegetések elhárítására lehet alkalmazni, sosem más (például politikai, gazdasági, szociális) céllal.
- *Végső esetben való alkalmazás:* előbb a lehető legkisebb sérelemmel járó eszközöket kell alkalmazni, mielőtt a komolyabbakhoz fordulnánk.
- *Arányosság:* az eszközök okozta kár egyensúlyban kell hogy álljon a várható eredménnyel.
- *Diszkrimináció:* különbséget kell tenni a jogos (potenciálisan veszélyes) és a nem jogos (járulékos) célszemélyek között.

7 Lásd John B. Chomeau – Anne C. Rudolph: Ethical 'Need to Knows' for Intelligence Officers. CIA. 1987. http://isme.tamu.edu/JSCOPE87/ChomeauRudolph87.pdf

8 Erről bővebben Boda Mihály: A katonai vezetés erkölcsi és morális elemei. http://mhtt.eu/hadtudomany/2015/2015_elektronikus/18_BODA_MIHALY.pdf

9 Ross W. Bellaby: Ethics of Intelligence: A New Framework. Routledge, London–New York, 2014

Bellaby alapvetése, hogy a nemzetbiztonsági szolgálatok által az állampolgároknak való morális kár okozásának tilalma nem abszolút, hiszen az állam és a társadalom ellen irányuló fenyegetést el kell hárítani, akár a szabadságjogok, alapvető egyéni érdekek ellenében is. Az állampolgárok alapvető érdekeik érvényesítése révén válhatnak képessé saját jóllétük önmaguk által választott módon való megvalósítására. Ha azonban az állam megtalálja a morális károkozás igazságos célját, és képes beazonosítani azoknak a körét, akikkel szemben a morális károkozásnak helye van, akkor a morális károkozás tilalma – a felvetődő kockázattal arányos mértékben – felülírhatóvá válik.

Bellaby tehát a lehetséges következmények (elhárítandó konkrét veszélyek) oldaláról közelíti meg a nemzetbiztonsági etika kérdéskörét, az állam érdekeinek szempontjából. Elmélete hasznos szempontokkal szolgálhat a gyakorlati alkalmazáshoz, részletesen kifejti azokat a tényezőket, amelyek alapján súlyozni lehet a különböző fenyegetések komolyságát és ezzel párhuzamosan az alkalmazható titkosszolgálati eszközök mélységét. Vannak azonban az elméletnek fontos hiányosságai is. Idekapcsolódik, hogy a jogos és nem jogos célszemélyek kiválasztása – mint az igazságos hírszerzés egyik alapelve – ugyanilyen logika alapján nehezen érvényesíthető szűrő-kutató munka nélkül, ami viszont az „igazságos ok" és a „helyes szándék" alapelveivel nem fér össze. Ugyancsak kritika fogalmazható meg azzal kapcsolatban, hogy a feltételezett fenyegetésnagyság becslésének módszertana tudományos szempontból kevéssé tűnik kidolgozottnak. Az igazságos háború és hírszerzés elméletének alapvető problémája, hogy partikuláris érdekek szerint határozza meg adott fél konfliktusban betöltött szerepét, így más nézőpontból, más értékeket valló szociális közeg szemszögéből már más tűnik igazságnak és igazságosnak.

Az említett kritikai pontok miatt vált szükségessé egy olyan nemzetbiztonsági etikai alap kidolgozása, amellyel szemben a következő tartalmi követelmények fogalmazhatók meg:

– tegye egyértelművé a követendő végső célokat, irányokat;
– univerzális értéket, és nem partikuláris (állam-) érdeket állítson fókuszba;
– proaktív módon a cselekvés szándékát helyezze előtérbe (valaminek a megteremtésére irányuló törekvés magának az ügynek a megvalósulása érdekében) és ne reaktív módon a cselekedet következményét (észlelt veszély elhárítása).

A nemzetbiztonsági etika deontologikus[10] megközelítése

Ahhoz, hogy az igazságos hírszerzés modelljével szemben univerzálisan érvényes és elfogadható célokat találjunk a titkos információgyűjtés, leplezett eszközalkalmazás etikai alátámasztásához, *Kant* kategorikus imperatívusza[11] szolgáltathat alapot, amely szerint akkor etikus egy cselekedet, ha annak végrehajtója jó szívvel venné, ha a saját cselekedete hátterében álló megfontolás általánossá válna a világban, és vele szemben is e szerint cselekednének.[12]

Az „aranyszabály", a kategorikus imperatívusz általános megfogalmazása jót tesz ugyan az elméleti érvényességének, ám megnehezíti a gyakorlati alkalmazhatóságát. E probléma kiküszöbölése érdekében a gyakorlati szempontból kiválóan tesztelhető, és a matematika eszközeivel tudományosan elemezhető játékelmélet kontextusába helyeztem a kategorikus imperatívuszt.

A játékelmélet olyan életszerű modellhelyzetekkel foglalkozik, amelyekben a részt vevő felek reakciói kölcsönösen meghatározzák egymás nyerési lehetőségeit, kihatnak egymás jövőbeli viselkedésére, így visszahatnak a felek további saját nyerési esélyeire is. A legismertebb játékelméleti alaphelyzet, a „fogolydilemma", amelynek elnevezése *Albert W. Tucker*től származik.[13] A történet szerint – leegyszerűsítve – egy bűnügy két feltételezett elkövetőjét elfogják, de nincs ellenük közvetlen bizonyíték, így a vallomásaikra van szükség az ítélethez. Külön cellában vannak, nem beszélhetnek egymással. Ha egyikük sem vall, mindketten egy-egy évet kapnak, ha csak az egyikük vall a másikra, akkor a vallomást tevőt elengedik, a másik tíz évet kap. Ha viszont mindketten egymás ellen vallanak, öt-öt évre kerülnek börtönbe. Az általánosítható erkölcsi kérdés itt az, hogy egy kialakult kölcsönös bizalmi, függési helyzetben mit tesznek a felek. Hogyan helyes, illetve hogyan célszerű viselkedni ebben a helyzetben?

10 Általános érvényű parancsokat, kötelességeket vagy törvényeket előtérbe helyező etikai elmélet, szemben például a következményeket hangsúlyozó konzekvencionalista, illetve a hasznot előtérbe helyező utilitarista szemlélettel.

11 „Cselekedj úgy, hogy akaratod maximája mindenkor egyszersmind általános törvényhozás elveként érvényesülhessen." Immanuel Kant: Az erkölcsök metafizikájának alapvetése. A gyakorlati ész kritikája. Az erkölcsök metafizikája. Gondolat Kiadó, Budapest, 1991, 138. o.

12 Egy tolvaj például nem kívánhatja, hogy őt is meglopják, illetve a lopás általános gyakorlattá váljon, hiszen akkor megszűnne a magántulajdon, és maga a lopás is értelmetlenné válna.

13 Mérő László: Mindenki másképp egyforma. A játékelmélet és a racionalitás pszichológiája. Tercium Kiadó, Budapest,1996, 46. o.

A többmenetes fogolydilemma bizonyítottan leghatékonyabb részvételi stratégiáját a Tit for Tat[14] (TFT) jelenti, ami két egyszerű szabályból épül fel:

1. az első lépésben kooperál;
2. ezután azt lépi, amit a partnere az előző lépésben.

Ez a stratégia egyszerre barátságos (nem kezdeményez versengést), megbocsátó (egyszer büntet, majd visszaáll kooperációra), provokálható (versengés viszonzása), reakcióképes (figyelembe veszi a másik fél lépéseit) és kiismerhető (egyszerű, átlátható működés).[15]

Minden konfliktushelyzetben egy rendszer részei vagyunk, viselkedésünkkel kihatunk a másik fél viselkedésére, „bűnünk" visszaszáll a saját fejünkre. Ha tehát nem az egyéni rövid távú érdekek alapján, hanem a másik félre gyakorolt hatásunkat figyelembe véve, együttműködő légkör megteremtésére törekedve veszünk részt az ilyen morális töltéssel bíró konfliktushelyzetekben, akkor tulajdonképpen életre keltjük Kant kategorikus imperatívuszát, amit ő az ideális társadalomfejlődés zálogának tart. Ha mindenki a partneri hozzáállás következetes alkalmazásával venne részt e helyzetekben, a közös nyereség is maximalizálhatóvá válna.

Ahhoz, hogy a játékelméleti tanulságokat sokszereplős társadalmi folyamatok szintjére terjeszthessük ki, *Garrett Hardin Közlegelők tragédiája* elnevezésű elméleti modelljét[16] hívjuk segítségül: ha egy zárt közösség minden tagja egyformán, egy-egy tehénnel terheli a közös legelőt – figyelembe véve a közös erőforrások végességét, a legelő eltartóképességét –, akkor egyensúlyi helyzetben mindenki egyformán részesedik a közös jóból. Ha azonban vannak, akik titokban nagyobb arányban terhelik a közös erőforrást, és több tehenet is legeltetnek (versengő stratégia), akkor rontják a többiekre jutó hasznot (egy-egy tehén súlya csökken a kevesebb rá jutó fű miatt), míg ők jobban járnak a többieknél, hiszen két kicsit sovány tehén is több, mint egy normál súlyú. Minél többen választják azonban – felbátorodva vagy feldühödve a versengők példáján – ezt a versengő stratégiát, annál kisebb lesz egy-egy tehén súlya, így annál kevesebb haszon jut egy tehénre. Idővel az aránytalanul sok tehén olyan sovány lesz, hogy már a két tehén súlya sem éri el az egy normál tehén súlyát, végül pedig minden tehén éhen hal. A való életben

14 Magyarul: Kölcsönkenyér visszajár!

15 Mérő László: i. m. 59–65. o.

16 Részletesen elemzi Hankiss Elemér: Társadalmi csapdák – diagnózisok. Magvető Kiadó, Budapest, 1985, 11–68. o.

társadalmi szinten az adófizetés elkerülése, a környezetszennyezés és egy sor más bűncselekmény is hasonlóképpen működik.

Czibor Andrea[17] laboratóriumi körülmények között, valódi téttel bíró közjavak elrendezésben, csoportszintű társas dilemmahelyzetekben vizsgálta, hogy milyen eszközök és tényezők segítik elő a csoportszintű együttműködés fenntartását, a kollektív racionalitás érvényesülését az individuális racionalitással szemben. Négy-öt fős „közhasznú javak tragédiája" játékban a kísérleti személyek arról döntöttek, hogy a kísérletvezető által rendelkezésükre bocsátott pénzösszegből mennyit kínálnak fel a csoport közös számlájára. Alaphelyzetben az egyéni számlán felgyűlt összeget a kísérlet végén mindenki megkapta, úgy, hogy a felajánlott összeget a kísérletvezető megtöbbszörözte és egyenlő mértékben szétosztotta a résztvevők között, függetlenül attól, ki mennyit tett be a közösbe. A kezdeti negyven–hatvan százalékos átlagos hozzájárulás a körök során jellemzően egyre apad, hatvan kör után nullához közelít, miközben társas feszültségek keletkeznek a csoporton belül. Az ok az, hogy a játékosok egy része „free-rider" (potyautas) stratégiát folytat, azaz nem fizet be, csak részesedik. A többség „feltételes együttműködő" módon viselkedik, azaz konformista módon a mások részéről tapasztalt együttműködési hajlandóság függvényében járulnak hozzá a közös terhekhez. A harmadik stratégia az „altruista", mindentől függetlenül folyamatosan együttműködik. A tapasztalatok szerint a „feltételes együttműködők" sokaságát a „free-riderek" tevékenysége demoralizálja, így jelenlétük nélkül a csoportok sokkal inkább képesek az együttműködés fenntartására, különösen olyan, a versengést erősíteni hivatott feltételek mellett, amikor csak a „győztes" kapta meg az egyéni számláján felhalmozott összeget.

Érdemes tehát olyan feltételeket teremteni, amelyek az együttműködésnek kedveznek, és szigorúan fel kell lépni azokkal szemben, akik megszegik az együttműködés szabályait, hiszen tevékenységük nemcsak az általuk kisajátított erőforrások révén okoz kárt a közösségnek, hanem az általuk gerjesztett további versengéssel is.

A modern, demokratikus jogállamok alaptörvényeiben mindenhol nagy hangsúlyt kap az állampolgárok alapvető jogai és kötelezettségei között fennálló egyensúly. A stabil társadalmakban a választópolgárok túlnyomó része igazságosnak érzi és a közjó érdekében valóként el tudja fogadni ezeket az

17 Czibor Andrea: Döntések társas dilemmahelyzetekben: Személyiségjellemzők és szituációs faktorok hatása. Doktori értekezés. Pécsi Tudományegyetem Bölcsészettudományi Kar Pszichológia Doktori Iskola, Pécs, 2014

alapelveket. *Robert Merton*[18] anómiaelmélete szerint a társadalmi együttélés mindenki által elfogadott céljai (például stabilitás, család, életszínvonal, fogyasztás stb.) és eszközei (például munkába járás, adófizetés, jogkövetés stb.) összhangban kell hogy álljanak. Sajnos azonban nem mindenki működik együtt a közjó érdekében. Az állampolgárok bizonyos része egyetért ugyan a társadalmi célokkal, de nem fogadja el magára nézve kötelező érvényűnek azok megszerzésének társadalmilag elfogadott eszközeit. Ha egy közösségben a többség a közjót szem előtt tartva együttműködő stratégiát folytat, önérdekeit képes korlátozni a közérdek érvényesülése kedvéért, akkor az a néhány fő, aki megfelelő ellenőrzés hiányában, titokban megszegi a közösségi normákat[19], azaz versengő stratégiára vált és bűnelkövetés formájában az önérdekét helyezi előtérbe, az óriási profitot képes felhalmozni a többiek rovására. Ha a közösség nem elég éber, és nem szankcionálja idejében ezt a viselkedést, az erősen demoralizáló hatásúvá válhat. Ahogy egyre többen váltanak versengő stratégiára, egyre nehezebb lesz hozzáférni a megfogyatkozó közös erőforrásokhoz, egyre több terhet visel az egész közösség, a végén már maguk a versengők is, míg végül mindenki rosszul jár, ahogy azt Hardinnál is láthattuk.

Amíg nem erősödik meg egy társadalomban a tagok, közösségek erkölcsi nívója, illetve nem alakul ki az együttműködésen alapuló közösségi normák dominanciája, addig a versengő stratégiák kiszűrése érdekében – a TFT, illetve a kategorikus imperatívusz szellemében – mindenképpen szükség van ellenőrzésre és restriktív, represszív eszközökre az állam részéről, de csak a feltétlenül szükséges mértékben, máskülönben beszűkülnek az egyéni fejlődés, az autonóm önmegvalósítás lehetőségei.

Álláspontom szerint tehát a nemzetbiztonsági szolgálatok általánosan megfogalmazható végső rendeltetése hozzájárulni egy olyan társadalmi környezet megteremtéséhez, amelyben a demokrácia mint a társadalmi fejlődés alapiránya[20] zavartalanul kibontakozhat és működhet. A szolgálni kívánt univerzális érték ehhez kapcsolódóan az egyéni fejlődések és autonómiák ösztönzése és harmonizálása a közösségi kooperáció maximalizálása a kategorikus imperatívusz elvének minél szélesebb körű érvényesítése révén. A rendvédelem és ezen belül a polgári nemzetbiztonsági szolgálatok fő célkitűzése tehát

18 Robert K. Merton: Társadalomelmélet és társadalmi struktúra. VI. fejezet: Társadalmi struktúra és anómia. Osiris Kiadó, Budapest, 2002

19 Azaz nem teljesíti saját társadalmi kötelezettségeit, miközben önkényesen korlátozza mások alapvető jogait (például lopás = magántulajdonhoz való jog önkényes korlátozása).

20 Bővebben Horváth Ferenc: i. m.

a bűnüldözés terén: *a titkos információgyűjtés, leplezett eszközalkalmazás eszközeinek és módszereinek alkalmazása révén olyan közeget teremteni és fenntartani, amely segít kibontakoztatni az állampolgárok alapvető jogainak, érdekeinek érvényesülését, kiszűrni azokat, akik saját érdekükben illegitim módon korlátozni kívánják ennek lehetőségeit (például bűnözők), kedvező feltételeket teremtve ezzel az együttműködésen alapuló, demokratikus társadalmi fejlődés számára.*

Az általam javasolt nemzetbiztonsági etika tehát a kategorikus imperatívuszon alapuló, deontologikus megközelítést képvisel, amely szerint a nemzetbiztonsági szolgálatoknak nem pusztán utólag, passzívan kell etikai elveiket hozzáigazítaniuk a tőlük függetlenül kibontakozó társadalmi-politikai változásokhoz, hanem tevékenységük révén nekik maguknak kell biztosítaniuk, hogy a társadalmi fejlődés folyamatai szabadon, illetéktelen külső befolyás nélkül kibontakozhassanak a demokrácia irányába.

A leírtak alapján a nemzetbiztonsági szolgálatok tevékenysége demokratikus viszonyok között akkor tekinthető etikusnak, ha ezen elvek alapján folyik, e cél kibontakozását szolgálja és nem igazolható, ha ettől eltérő, parciális érdekek szolgálatában áll. Hipotetikus szinten értelmezve a kérdést tehát legitim cél lehet a társadalom demokratikus működési rendje ellen fellépők nemzetbiztonsági kontrollja, de erkölcsileg nem védhető az, ha egy demokráciában a titkos információgyűjtés eszközeit és módszereit például a következők szerint használják fel:

– jogszabályi kereteken kívüli dokumentálatlan eszközalkalmazás, szóbeli utasítás alapján;
– közérdek helyett magánérdeket szolgáló eszközalkalmazás;
– állampolgárok alapjogainak a saját hatalom fenntartását célzó korlátozása;
– nem célszemélyekkel kapcsolatos készletező adatgyűjtés, a célhoz kötöttség alapelvét sértő szűrő-kutató munka;
– a megszerzett terhelő információk igazságszolgáltatás előli visszatartása, készletezése az érintettekre való nyomásgyakorlás, befolyásszerzés céljából;
– fiktív veszély alapján megindított eszközalkalmazás;
– az eszközalkalmazás idején a célszemély természetes életvitelének manipulálása provokációval.

A fejlett demokratikus országok államrendje az imént ismertetett alapelveket támogató értékrendet feltételez, a leírt törvényi garanciák is ez irányba mutatnak. Fontos azonban, hogy a deklarált értékek és a ténylegesen megnyilvá-

nuló viselkedésmódok összhangban álljanak egymással, máskülönben a társadalmat belső meghasonulás, értékválság hatja át, a demokrácia egésze válik hiteltelenné. Ezzel összhangban fontos, hogy az önmagukat demokratikusnak valló országok lehetőleg ne törekedjenek direkt módon gazdasági és katonai potenciáljuk aránytalan felfejlesztésére más kultúrák, régiók, országok rovására, illetve ne hagyják figyelmen kívül más régiók problémáit, nehézségeit, érdekeit, azaz a globális, nemzetközi gazdasági térben ne alapértelmezetten versengő, rövid távon felhalmozandó nyereségre törekvő, másokat tudatosan kedvezőtlenebb pozícióba taszító stratégiával szálljanak játékba. Mindezek a viselkedésformák, illetve az ezeket kiszolgáló nemzetbiztonsági tevékenységek etikai szempontból ugyanis nehezen védhetők, nem állnak összhangban a demokrácia szellemével és negatív módon vissza is hatnak az adott társadalmak (kultúrák) belső viszonyaira.

A nemzetbiztonsági etika lehetőségei a gyakorlatban

„Az etika még a legszerencsésebb esetben is csak úgy funkcionál, mint az eltévedt hajós távcsövében halványan fölsejlő világítótorony. Ha megpillantja, sem biztos, hogy partot ér, de nélküle odaveszne biztosan."[21]

Ebben a szakaszban támpontokat adtam a nemzetbiztonsági szolgálatok etikus működéséhez azáltal, hogy összegyűjtöttem a kapcsolódó elméleteket és feltártam a gyakorlati lehetőségeket, amelyek erkölcsi keretet kínálnak e speciális tevékenységekhez. A hazai és a nemzetközi helyzet realitása talán frusztrálón elérhetetlennek tűnővé teszi a megfogalmazott szigorú, tisztán racionális, már-már idealista mércét nemzetbiztonsági szolgálataink számára. Mégis szükséges időtálló alapelveket megfogalmazni, hiszen e keretek vázolása mozdíthatja elő a titkos információgyűjtés eszközeit és módszereit törvényi felhatalmazás alapján végző szervezetek tudatos erkölcsi felelősségvállalását a társadalom irányába.

A nemzetbiztonság kérdései átívelnek az egyes kormányciklusokon, az e pályát választók Magyarország érdekeit szolgálják.[22] A társadalmi rendszerek igyekeznek folyamatosan adaptálódni a világban zajló változásokhoz, így

21 Himmer Péter: Etikai jellegű töredékek. Erkölcsről, etikáról, az értékekről és az emberről. Underground Kiadó, Budapest, 2011, 112. töredék

22 Izsa Jenő: Erkölcsi aspektusok, dilemmák, konfliktusok a titkosszolgálati szakmai tevékenységben, avagy a szakmai etika kérdései. HVK Hadtudományi Tájékoztató, 2001, 37–56. o.

hosszabb távon nem maradhatnak éppen aktuális formájukban tökéletesek, előbb-utóbb feszültségekkel telítődnek, változnak, átalakulnak. A fennmaradás érdekében mindig is szükség volt a társadalom folyamatos önellenőrzésére, amelynek egyik eszköze a titkos információgyűjtési tevékenység, ám ez minden korban más színezetet kapott. A történelem fordulatai során egy-egy rezsim leköszönése, vagy létrehozása kapcsán a titkosszolgálati munkatársaknak állást kellett foglalniuk, erkölcsi és/vagy jogi felelősséget kellett vállalniuk együttműködésükért. Mennyiben felelősek a szolgálatok, ha korábbi vezető politikusok, akiket elláttak a döntéseikhez szükséges információkkal, tévedtek, rossz nyomon jártak, rossz következtetéseket vontak le az információkból, illetve rosszra használták őket?

Speciális, kiszolgáló szerepkörénél fogva a Nemzetbiztonsági Szakszolgálat részt vesz a nemzetbiztonsági munkában, ám annak csak bizonyos részfeladatait látja el.[23] Ez etikai szempontból egyfelől könnyebbség, hiszen a szakszolgálat munkatársai csak a titkos információgyűjtés technikai kérdéseiben érintettek. Másfelől viszont kiszolgáltatott helyzetben is vannak, nem látják ugyanis a nemzetbiztonsági munka elindításának kiváltó körülményeit, ahogy a megszerzett és a megrendelőnek maradéktalanul átadott adatok további hasznosulását sem, miközben érzik, hogy e speciális feladatkör milyen súlyos etikai vonatkozásokat vet fel, milyen hatalmas felelősséggel jár. A Nemzetbiztonsági Szakszolgálat végrehajtó állományának tehát nincs közvetlen és teljes rálátása a nemzetbiztonság és a nemzeti érdek stratégiai kérdéseire, ez a szint kénytelen beérni a hittel, hogy a döntéshozók és saját vezetőik pártatlanul, önérdekmentesen, elhivatottan és kompetensen szolgálják a közérdeket, így az ennek esetlegesen ellentmondó információk súlyos erkölcsi, érzelmi, motivációs válságot idézhetnek elő a nemzetbiztonsági pályát betöltőkben. Akkor várhatunk hosszú távú elkötelezettséget, lelki egészséget és motivált munkavégzést, ha munkatársaink önbecsülését, hivatásukra való büszkeségét nem csökkentik bűntudati-lelkiismereti gátak. Ezt elsősorban úgy kell elérni, hogy kikezdhetetlen erkölcsi bázison állva végezzük munkánkat, egyértelmű visszajelzést kapunk céljaink helyességéről, munkánk társadalmilag pozitív eredményéről.

A téma érzékenységénél fogva még a jól működő demokráciában biztosított jogi garanciák mellett is fontos, hogy a jogszabályokban foglaltak teljes

23 Nincs önálló hírszerzői, elhárítási vagy nyomozati jogköre, de komplex eszközrendszerével és speciálisan felkészült személyi állományával biztosítja az arra jogosult megrendelő szervezeteknek a titkos információgyűjtéshez, leplezett eszközalkalmazáshoz szükséges műveleti, technikai eszközöket, anyagokat és szolgáltatásokat.

körű betartásán túl a megrendelői és végrehajtói oldal munkatársai egyaránt szilárd és egységes erkölcsi bázison állva lássák el feladataikat. Fontos, hogy megbízhassanak egymásban, emellett élvezzék a társadalom, az adófizetők bizalmát is, akiknek érdekében e tevékenység végső soron megvalósul.

A megrendelés jogszerűségéért, az adatok felhasználásáért a megrendelő felel, a Nemzetbiztonsági Szakszolgálat munkatársainak felelőssége alapvetően a titkos információgyűjtés és adatszerzés eszközei, módszerei alkalmazásának szakszerűségére vonatkozik. A Nemzetbiztonsági Szakszolgálat jogszerűséggel kapcsolatos felelőssége kiterjed azonban a megrendelések fogadásának és teljesítésének körülményeire. Ezzel kapcsolatban a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) a szakszolgálat főigazgatójának felkérésére speciális, gyakorlatias ellenőrzési módszertant alkalmazó átfogó vizsgálatot végzett el[24] 2016 áprilisa és 2017 februárja között, ami 34 tesztmegrendelés alapján vizsgálta a szakszolgálat adatkezelési gyakorlatát. A tapasztalatok alapvetően pozitívak voltak: *„…az audit messzemenően visszaigazolta az NBSZ elkötelezettségét az adatkezelés törvényességét illetően, ugyanakkor a tesztek a titkos információgyűjtéssel kapcsolatos tevékenységek néhány olyan részletét is feltárták, amelyekkel kapcsolatban a Hatóság az adatvédelmi követelmények magas szintű érvényesítése érdekében észrevételekkel és javaslatokkal élt”*[25].

A titkos felderítés hazai szabályozásának legújabb fejezetét nyitotta meg a büntetőeljárásról szóló, 2018. július 1-jén hatályba lépő 2017. évi XC. törvény. A témakör néhány régi nagy adósságát rendezte ugyan az új törvény, de még mindig maradtak hiányosságok.[26]

Mindenképpen pozitív eredmény, hogy a már folyamatban lévő esetek *bűnügyi* felderítésével kapcsolatos eszközalkalmazás egységes szabályozást kapott, szoros ügyészi kontroll mellett zajlik, és az eljárási garanciák fokozott érvényesülése javítja a megszerzett információk felhasználásának esélyeit a bíróságon. Továbbra is túl tágan értelmezhetők azonban a titkos információgyűjtés alkalmazhatóságának céljai, így lehetőség van titkos felderítésre tisztán prevenciós érdekből, ami nem felel meg a szükségesség és arányosság elvének, különösen, hogy a magánszférát legmélyebben érintő, külső engedélyhez kö-

24 A Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója a 2016. évi tevékenységéről B/13846. Budapest, 2017, 104–109. o. https://www.naih.hu/files/NAIH-BESZ-MOL—2016_Mid-Res.pdf

25 Uo. 109. o.

26 Bárándy Gergely – Enyedi Krisztián: Leplezett eszközök és titkos információgyűjtés, avagy az új büntetőeljárási törvény margójára. http://ujbtk.hu/dr-barandy-gergely-dr-enyedi-krisztian-leplezett-eszkozok-es-titkos-informaciogyujtes-avagy-az-uj-buntetoeljarasi-torveny-margojara/

tött eszközök és módszerek alkalmazására is lehetősége nyílik bármely jogosult szervezetnek, amennyiben megalapozottan feltehető, hogy attól szervezett bűnözéssel kapcsolatos információk megszerzése várható. A kérdés, hogy az engedélyt aláíró bírók mennyire fogják megkövetelni ennek alátámasztását a gyakorlatban. Az is képlékeny maradt, hogy az úgynevezett „előkészítő eljárást" illetően – ahol azt kell megtudni, fennáll-e a bűncselekmény gyanúja (tehát konkrét gyanúok nélkül, a gyanú gyanújára indul a leplezett eszközalkalmazás) – mi indítja el a folyamatot, mi ad erre erkölcsi felhatalmazást. Végül a titkos felderítés újraszabályozása kapcsán a legszembeötlőbb hiányosság az, hogy az Emberi Jogok Európai Bírósága elmarasztaló ítélete ellenére a Terrorelhárítási Központ a kifejezetten terrorelhárítással kapcsolatos felderítői feladatait továbbra is az Nbtv. és nem az Rtv. alapján végzi, így a külső engedélyköteles eszközök és módszerek nem bírói, hanem igazságügy-miniszteri engedéllyel folynak, ami sérti az Emberi jogok európai egyezményének 8. cikkét (magánélet védelme).

Mindenképpen szükség van tehát minden résztvevő (megrendelők, végrehajtók, ügyészek, bírók) demokratikus értékek mellett elkötelezett, etikus hozzáállására, ugyanis már a jogi szabályozás szintjén megjelennek nem egyértelmű, objektíven alá nem támasztható mozzanatok, amelyek értelmezése a jogalkalmazás során ad némi mozgásteret. Nehezen ellenőrizhető például, hogy mindenképpen szükség van-e titkos felderítésre, valóban esélytelen-e más forrásból megszerezni a szükséges információt, valóban súlyos bűncselekmény gyanújáról van-e szó, mikor indokolt eredménytelenség okán megszüntetni az eljárást stb. Gyakorlati oldalról fontos tehát garantálni, hogy a gépezet ne indulhasson be nem kellően alátámasztott indoklással.

Konklúzió

Mindennek van egy látható, megragadható, ellenőrizhető jogi és egy háttérben meghúzódó etikai oldala. Utóbbi sokkal nagyobb odafigyelést igényel, hiszen képlékenyebb, sokszínűbb, lélektani és közösségi aspektusokkal sokkal inkább átitatott, emellett sokkal kevésbé tudatos, mint a jogi oldal. A motivációt, elkötelezettséget és a tényleges tisztaságot ugyanakkor ez utóbbi szabja meg, hiszen a jogalkalmazás, jogkövetés során az emberi lélek hangszerén kel életre a jog kottája.

A közszolgálati etika kérdésköreinek lehatárolása, kulcskérdéseik beazonosítása segít tisztán látni a lényeget a Nemzetbiztonsági Szakszolgálat tevé-

kenységével kapcsolatban, ami egyfelől a közbizalom megteremtése érdekében fontos, másfelől pedig munkatársaink motivációit, elkötelezettségét, valamint biztonságtudatosságát is erősíti, ha megértik, tudatosítják a főbb erkölcsi mozzanatokat.

A szakszolgálatnak fontos társadalmi funkciója és felelőssége van. Mivel a társadalom civil kontrollja nem láthat bele olyan szabadon a tevékenységünkbe, mint a közszolgálat más szegmenseiben, különösen fontos, hogy a ránk nehezedő erkölcsi felelősség tudatában, a törvényes és igazságos működésmódok iránt elkötelezetten, még a más szervezetek által elvártnál is magasabb szintű etikai normáknak feleljünk meg, belülről fakadó igény alapján.

DOI: 10.38146/BSZ.2019.1.4

TÓTH TAMÁS

A Nemzetbiztonsági Szakszolgálat felvételi eljárási rendszere[1]

A Nemzetbiztonsági Szakszolgálat – akárcsak más nemzetbiztonsági szolgálatok, rendvédelmi szervek – jogszabályok, belső normák alapján, meghatározott eljárásrend szerint hajtja végre felvételi eljárását. Személyi állományát *hivatásos szolgálati jogviszony*ban[2] álló személyek, közalkalmazottak, valamint köztisztviselők alkotják.

A tanulmány a szakszolgálat felvételi eljárását, annak szakaszait, az egészségi, pszichológiai, biztonsági kritériumrendszer megfeleléséhez szükséges kompetenciák mérésének, ellenőrzésének folyamatát ismerteti, valamint bemutatja a leggyakoribb humán kiválasztási módszereket. Továbbá figyelmet fordít a kiválasztás új nehézségeire az információs társadalom függvényében.

A Nemzetbiztonsági Szakszolgálat felvételi eljárásának folyamata

A szakszolgálat tevékenységének és működésének csak nyílt jogforrásokban szereplő elemei nyilvános adatok, minden más a szervezetre, tevékenységre utaló információ a minősítéssel védhető közérdekek körébe tartozó *minősített adat.*[3] Ez azt a helyzetet idézi elő, hogy a szolgálatról külső személyek nehezen szereznek tudomást, hiszen a titkosság alapvető tényező egy nemzetbiztonsági szolgálat működésében. Adott időszakban vizsgálva a szakszolgálathoz jelentkezők 67 százaléka hagyományosan, azaz ismerősök, közeli hozzátartozók útján szerzett tudomást az álláslehetőségről, míg többletinformációja a

1 A tanulmány elkészítésében nyújtott önzetlen és lelkiismeretes közreműködéséért szeretném köszönetemet nyilvánítani Csákány Edina kisasszonynak, akinek támogatása, a téma iránti szilárd elkötelezettsége, valamint kiemelkedő tudományos alapossággal elkészített kutatása nélkül e tanulmány nem jöhetett volna létre.

2 A rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény 13. § (1) bek.

3 A minősített adat védelméről szóló 2009. évi CLV. törvény 3. § (1) bek. 1.

vizsgált halmaz 41 százalékának nem volt, másik 41 százaléka a szakszolgálat honlapján informálódott.[4]

A felvételi eljárás minden jelentkező esetében azonos protokoll alapján zajlik, azonban az általános feltételeken túl, a szakterületek elvárásainak megfelelően mérik a jelentkezők képességeit. Az eljárás menete szakterületenként eltérhet. A felvételi eljárás a jogszabályok által támasztott normarendszer alapján viszonylag hosszadalmas, három-négy hónap, egymásra épülő, többlépcsős eljárás, hiszen igazolnia kell, hogy a jelentkező megfelel a pszichológiai, egészségi kritériumoknak.

A vizsgálatsorozat először egy pszichológiai előszűrés keretében azt kívánja mérni, hogy a pályázó birtokában van-e a munkakör betöltéséhez szükséges pszichés kompetenciáknak.

A szakszolgálatnál a pszichológiai alkalmassági vizsgálatot egységesen, a szervezet pszichológusai által meghatározott és elfogadott vizsgálati módszerek alapján kell elvégezni. A vezető pszichológus a pszichológiai alkalmassági vizsgálaton részt vevő személlyel ismerteti a vizsgálat célját, lefolytatásának menetét, továbbá tájékoztatást ad az eljárások típusairól, mérési tartományukról. A pszichológiai alkalmasságot személyiségtesztek, intelligencia- és figyelemtesztek, műszeres vizsgálatok, az exploráció komplex értékelése alapján, valamint kiegészítő vizsgálatok elvégzésével a vizsgálatot végző pszichológus minősíti.

Az egyes feladatkörökhöz rendelt kompetenciák mérésén túl fontos lehet a prediktorok monitorozása is. A prediktorok segítségével mérhetők a képességek, személyiségvonások, kompetenciák, míg a pályázóval szemben támasztott kritériumok meghatározása a tervezett munkakörhöz rendelhető prediktorok kiválasztásában segíthet. Csoportosításuk történhet az egyes munkakörök meghatározása alapján. Ebben az esetben kétfajta munkakör különböztethető meg, az úgynevezett *knowing,* illetve *doing* típusú beosztások. A *knowing* típusú munkakörök elemzése során a meglévő tudás és annak megfelelő alkalmazása a kritériumrendszer alapja, idesorolandók a szellemi tevékenységre épülő feladatok, ennek mérésére a személyiség-, képesség-, illetve teljesítménytesztek alkalmasak. A *doing* típusú munkaköröknél, amelyek közé a fizikai vagy operatív feladatok sorolandók, a gyakorlati készségek mérésére helyeződik a hangsúly.

4 Zalai Noémi: A pályaalkalmasság vizsgálatának elemei és alkalmazható kiválasztási, szakmai felkészítési modellek a Nemzetbiztonsági Szakszolgálatnál. Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem Humán Tudományok Doktori Iskola, Budapest, 2012, 82–83. o. http://docplayer.hu/24639898-Doktori-phd-ertekezes.html

A jelentkező abban az esetben kap *Pszichikailag alkalmas* minősítést, ha megfelel a hivatásos szolgálat ellátásának és a tervezett beosztásának megfelelő képesség- és személyiségbeli követelményeknek.

A teljes körű pszichológiai alkalmassági vizsgálat után egy a szolgálatra való alkalmasság különleges feltételeként tartott kritériumnak is meg kell felelnie a jelentkezőnek, mégpedig az érintett hozzájárulásával, a felvételi eljárás keretében poligráfos vizsgálatot kell lefolytatni.

A vizsgálat a felkészüléssel veszi kezdetét, amelynek során az interjúztató meggyőződik arról, hogy az alany alkalmas-e a vizsgálatban való részvételre, valamint tájékoztatja a vizsgálat során elhangzó kérdésekről. Ez után következnek az ellenőrző kérdések, amikor is az interjúztató alapméréseket végez eldöntendő kérdések alapján. A következő szakasz a valós méréshez szükséges kérdések tesztje, amelynek során a kérdéseket meghatározott, strukturált kérdéssorba rendezve teszi fel a vizsgáló. E teszteknek két típusa van, az összehasonlító vagy kontroll-, valamint a releváns–irreleváns kérdések tesztje. Egy kérdéssor hét–tizennégy kérdést tartalmaz, így húsz-huszonöt másodperces kérdésközökkel legfeljebb öt percig tart. A poligráfos vizsgálat alatt a jelentkezőnek mozdulatlanul kell ülnie.[5]

Abban az esetben, ha a felvételiző a pszichológiai alkalmassági vizsgálat során *Pszichikailag alkalmas,* valamint *Pszichikailag feltételesen alkalmas* minősítést szerez, illetve a poligráfos vizsgálat nem detektál kockázati tényezőt, hazugságot, kezdetét veheti a következő szűrési szint az egészségi alkalmasság megállapítása céljából.

Az egészségi alkalmassági vizsgálat lefolytatása után a pályázó négyféle minősítési szintre válik besorolhatóvá:

a) egészségileg alkalmas;
b) egészségileg korlátozással alkalmas;
c) egészségileg alkalmatlan;
d) egészségileg ideiglenesen alkalmatlan.

Egészségileg alkalmas minősítést akkor szerez a vizsgált személy, ha egészséges, vagy csak olyan szervi, szervrendszeri-működési elváltozása van, amely az élettani tűréshatárokat nem haladja meg, illetve egészségi állapota megfelelő kezeléssel tartósan egyensúlyban tartható, az elváltozás a szolgálat teljesítésében nem korlátozza.

5 Budaházi Árpád: A műszeres vallomásellenőrzés, különös tekintettel a poligráfos vizsgálatra. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2012, 131–142. o. http://ajk.pte.hu/files/file/doktori-iskola/budahazi-arpad/budahazi-arpad-muhelyvita-ertekezes.pdf

Abban az esetben, ha a pályázó az egészségi alkalmassági vizsgálat nyomán *Egészségileg alkalmas,* valamint *Egészségileg korlátozással alkalmas* minősítést szerez, a jogszabály alapján[6] megfelelt a szolgálati beosztásának és életkorának megfelelő egészségi, pszichikai és fizikai alkalmassági követelményeknek, így továbbléphet a felvételi eljárás következő szintjére, a szakmai interjúra.

A szakmai interjú után a pályázót tervezett beosztásának szervezeti egységétől tájékoztatják az eljárás eddigi eredményeiről, illetve, ha a tervezett szolgálati hely igényt tart rá, újabb szakmai interjút kezdeményeznek vele.

Az előbbiek alapján kijelenthető, hogy indokolt a felvételi eljárás viszonylag hosszabb időintervalluma.

Az általános és speciális alkalmassági követelmények

A szakterületek eltérő, összetett feladatrendszere és profilja differenciált szakmai, egészségi, pszichológiai követelményrendszert támaszt a felvételizővel szemben. A jelentkezőknek azonban a hivatásos szolgálati jogviszony létesítéséhez – a speciális feltételrendszerből adódó többlépcsős vizsgálatok előtt – meg kell felelniük a jogszabályok által meghatározott alapvető jogi követelményrendszernek is.

A jogszabály alapján a szakszolgálat hivatásos állományú tagja bizonyos alkotmányos jogaiban korlátozott, vagy korlátozható, ha azt a szolgálati érdek úgy kívánja. Ezt a követelményt a pályázónak vállalnia kell a hivatásos jogviszony teljes ideje alatt. Az említett jogszabályi előírásokon túl, a jelentkezőnek meg kell felelnie egyéb, a hivatásos szféra, a konspirált és szakmaspecifikus feladat-végrehajtás, valamint a szervezet által támasztott etikai normarendszernek, mind személyiségében, mind kognitív képességeiben egyaránt. Tudományos kutatások, vezetői és humánpolitikai állásfoglalások alapján, a Nemzetbiztonsági Szakszolgálat állományába jelentkező vonatkozásában az alapvető pszichológiai, egészségi kritériumok mellett követelmény a teherbírás, a megfelelő szintű stressztűrő képesség, a szorgalom, a kiemelkedő színvonalú munkavégzés, a koncentrálókészség és az elhivatottság.

A hivatásos szféra, valamint a jelentős hagyományokkal és szakmai tradíciókkal büszkélkedő Nemzetbiztonsági Szakszolgálat értékrendje alapján morális kívánalom a felvételizőktől a szolgálati fegyelem, az elkötelezettség,

6 2015. évi XLII. tv. 106. § (1) bek.

az elhivatottság, a hivatástudat, a megbízhatóság, a stabil értékrend, a józan értékítélet, a szakmai alázat, az innováció és önképzés iránti hajlandóság, az alkalmazkodási készség, összességében tehát az integrációs hajlam. Az integritás, a megvesztegethetetlenség követelménye magában foglal olyan értékeket is, mint a szakmai felkészültség, a pártatlanság, az elfogulatlanság, a jogszabályok megtartása, a közösségi érdekek előtérbe helyezése az egyéni érdekekkel szemben, az erkölcsi feddhetetlenség, a becsületesség, az őszinteség, a közvetlenség, a semlegesség, a megfontoltság, a megbízhatóság, az ügyfélközpontúság, a tisztelet, az objektivitás és az illemtudás.

Ha a pályázó megfelel az említett kritériumoknak, tudomásul veszi a rá vonatkozó jogszabályi előírásokat azzal, hogy a Nemzetbiztonsági Szakszolgálat hivatásos állományába került, három, a további szolgálati tevékenységét alapvetően meghatározó kötelezettséget vállal: a szolgálati beosztásában meghatározott feladatait a törvényes előírásoknak megfelelően teljesíti, elöljárója utasításának – bűncselekmény kivételével – engedelmeskedik, továbbá *Magyarország nemzetbiztonsági érdekeit* minden törvényes eszközzel érvényesíti és – *ha kell, élete árán is – megvédi.*[7]

Kiválasztási módszerek és validációs mutatóik

A környezet változásával a szakszolgálat szervezete és ezzel együtt a rendszeresített munkakörök kritériumai is folyamatosan változnak. Ez elengedhetetlen a biztonsági környezet változásai által támasztott feladatoknak történő optimális megfeleléshez, ezért fontos perzisztens jelleggel nyomon követni és mérni az egyes kiválasztási módszerek érvényességét, aktualitását. A módszereket különböző értékelő standardokkal mérik, amelyek alapján jellemezni lehet őket. A legfontosabb ilyen mutatók a validitás, a megbízhatóság, a korrektség, a használhatóság, a költség, a hozzáférhetőség, a felhasználó képesítése, képzettsége, az elfogadás, az elméleti háttér, a jelöltekre gyakorolt hatás, valamint a módszer prognosztizációs képessége.[8] Az említettek közül költséghatékonysági és kiválasztásoptimalizációs szempontból négy mutató összehasonlítását érdemes elvégezni *(táblázat)*.

A *táblázat*ban szereplő módszereket továbbá érdemes besorolni a már korábban említett prediktorok csoportosítása alapján, hiszen a vizsgált alany

7 1995. évi CXXV. törvény 22. § (2) bek.

8 Mike Smith – Ivan T. Robertson: Advances in Selection and Assessment. J. Wiley & Sons Ltd., New Jersey, 1989, p. 142.

Módszere	Validitás	Korrektség	Használhatóság	Költség
Értékelő-/fejlesztőközpontok	magas	magas	alacsony	magas
Munkapróbateszt	magas	magas	alacsony	magas
Biodata kérdőív	magas	mérsékelt	magas	alacsony
Egymás értékelése	magas	mérsékelt	alacsony	alacsony
Személyiség-kérdőív	mérsékelt	magas	alacsony	mérsékelt
Képességteszt	mérsékelt	magas	mérsékelt	alacsony
Intelligenciateszt	mérsékelt	mérsékelt	magas	alacsony
Szituációs gyakorlat	mérsékelt	nem ismert	alacsony	mérsékelt
Önértékelés	alacsony	magas	mérsékelt	alacsony
Interjú	alacsony	mérsékelt	magas	mérsékelt
Referencialevél	alacsony	nem ismert	magas	alacsony

Szerkesztette a szerző. Forrás: Juhász Márta: A kiválasztás és a munkaköri alkalmasság pszichológiája II. rész. Munkaügyi Szemle, 2006/2., 25. o.
http://www.munkaugyiszemle.hu/sites/default/files/Juhasz_Marta_2.pdf

múlt- és jelenbeli viselkedéséből következtetni lehet a jövőbeli magatartására. Abban az esetben, ha a prediktorok osztályozására az előrejelzésre való következtetés levonása szempontjából kerül sor, megkülönböztethetők az analitikus és analóg tesztek.

Az analitikus, azaz az előrejelzésen alapuló prediktorokat az individuális különbségek detektálására alkalmazzák, ezek eredményeiből az egyén jövőbeli teljesítményére lehet következtetni. A megszerzett tesztpontszámok alapján előre kell jelezni a jelölt munkahelyi teljesítményét, viselkedését. Ilyen prediktorok az általános és specifikus képességmérő tesztek, úgymint a különböző intelligenciatesztek, a specifikus képességmérő eljárások, a személyiség- és érdeklődés-kérdőívek, a motivációs kérdőívek, valamint a kreativitástesztek.

Az analóg, azaz a mintaalapú kiválasztási módszereknél a prediktor azonos azzal a kritériummal, amelyet a munkakörben a munkatevékenység során kell elvégezni. Ilyen prediktor a munkapróba, amikor a pályázó a tervezett beosztásban elvégzendő feladatot hajt végre a vizsgálat során. Idesorolandók még a szituációs gyakorlatok, amelyeket nehéz elkülöníteni a munkapróbatesztektől. Míg a munkapróbateszt általában szenzomotoros képességeket vizsgál, amit különböző eszközök felhasználásával kell elvégezni, addig a szituációs gyakorlatok az egyének döntéshozatali és együttműködési képességét hivatott értékelni. Méri az egyének problémaérzékenységét, problémamegoldási stratégiáit, kommunikációs képességeit, meggyőző képességeit. Ezek főként csoportos helyzetekben zajlanak. Hátrányuk, hogy igen költséges az összeállítá-

suk és levezetésük, viszont egyszerre több személy megfigyelése és kiválasztása is lehetséges.[9]

A kutatások eredményei alapján kijelenthető, hogy a legjelentősebb validitási és hatékonysági mutatókkal az értékelő-/fejlesztőközpont (Assessment/Development-Center; AC/DC) büszkélkedhet, így igazolható, hogy ez a fajta eljárás hozhatja talán a legszélesebb, legsokoldalúbb és legrelevánsabb adathalmazt a kiválasztási eljárás során, azonban érdemes megvizsgálni az egyéb tesztek egyedi jellemzőit is.

Önéletrajz

Az önéletrajz a kiválasztási folyamat első lépése. A szakszolgálat állományába pályázóknak is ezt kell először elektronikus formában eljuttatniuk a szolgálat humánutánpótlásért felelős területére. Az önéletrajzok kritériumrendszere régióként, országonként eltérő, azonban az esetek nagy részében tartalmazzák a pályázó aktuális fényképét, személyes adatait, tanulmányai és korábbi munkahelyei idejének és helyének fordított sorrendű, kronologikus felsorolását.

Munkapróbateszt

Az adott munkatevékenységhez szükséges képességek mérésére használják. Elsősorban olyan munkaköröknél vált be, amelyek komplex végrehajtást igényelnek. Célja, hogy a pályázó szenzomotoros képességeinek elemzésével megvizsgálja a tervezett munkakör betöltéséhez szükséges kompetenciák meglétét. A munkapróba megfigyelési szempontjai közé tartozik az utasítás és a feladat felfogása, a különleges megnyilvánulások az utasítás alatt, a látenciaidő, a feladatkezelés és -befejezés jellegzetességei, az általános munkamagatartás, valamint az igényszint mérése. A legmagasabb validitási mutatókkal jellemezhető eljárás.[10] Nemzetbiztonsági szolgálatok kiválasztási rendszerében való alkalmazása azonban kétségeket vet fel, hiszen a munkafolyamatok titkosságának megőrzése érdekében nincs lehetőség azok próbafeladatként való alkalmazására.

9 Hegyi Hella: Személy(iség) a kompetenciák mögött. Doktori értekezés. Pécsi Tudományegyetem Alkalmazott Pszichológia Doktori Program, Pécs, 2012, 22. o. http://pea.lib.pte.hu/bitstream/handle/pea/15201/hegyi-hella-phd-2012.pdf?sequence=1&isAllowed=y

10 Csirszka János: A személyiség munkatevékenységének pszichológiája. Akadémiai Kiadó, Budapest, 1985, 179. o.

Biodata (életrajzi) kérdőív

A módszerrel viszonylag gyorsan és egyszerűen hajtható végre a jelentkezők szűrése. A biodata kérdőív összeállítását munkakörelemzésnek kell megelőznie, mivel csak így nyílik lehetőség a munkakör kritériumainak megfelelő kérdéssor összeállítására. *„A munkakörelemzés tehát az a folyamat, amely feltárja és meghatározza a munkakör tartalmát (célját és funkcióját, a munkakörbe tartozó feladatokat, a kapcsolódó hatáskört és felelősséget), kapcsolatrendszerét, valamint a munkakör sikeres ellátásához szükséges kompetenciákat (képességeket és készségeket, elvárt magatartást, tudást és tapasztalatot).”*[11] A teszt alapvetően objektív, jól vissza-ellenőrizhető kérdéseket tartalmaz, azonban lehetséges szubjektív, nehezen ellenőrizhető elemek használata is. A tesztet hivatali munkakörök esetében magasabb prediktív validitás jellemzi, mint az operatív tevékenység vonatkozásában. Az eljárást főleg előszelekciós céllal, egy hosszabb kiválasztási folyamat részeként alkalmazzák.[12]

360 fokos visszajelzés

A vizsgálat egy több szempontú teljesítményértékelési rendszer. A teszt során több vélemény alapján elemzik a résztvevő teljesítményét, mivel ugyanazon szempontok alapján értékeli a jelöltet önmaga, a beosztott, a vezető, az azonos munkakörben dolgozó munkavállaló, valamint akár külső értékelő is. Előnye, hogy több álláspont alapján kap visszajelzést a pályázó, hátránya, hogy a szervezetek nehezen tudják használni a 360 fokos visszajelzés eredményeit. Előfordul, hogy az adatok felvétele nem megfelelő módon történik, illetve nem elég hatékony az eredmények visszajelzése. A módszer validitási mutatója mérsékelt, hiszen az önértékelés alacsony, míg a társak értékelése magas mutatóval bír, így a két eljárás átlaga a mérvadó.[13]

11 Szakács Gábor – Bokodi Márta: Munkavégzési rendszerek. Munkavégzési rendszerek a közszolgálatban. ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel. Nemzeti Közszolgálati Egyetem, Budapest, 2014, 30. o. https://cmsadmin-pub.uni-nke.hu/document/vtkk-uni-nke-hu/munkavegzesi-rendszerek-a-kozszolgalatban.original.pdf

12 Tarnóczi Richárd: A határainkon túl szolgálatot teljesítő katonai állomány kiválasztási rendszerének kialakítása. Az Értékelő Központ alkalmazásának lehetséges aspektusai a Magyar Honvédség személyzeti kiválasztása során. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, Budapest, 2007, 27–43. o. http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/tarnoczi_richard.pdf

13 Sándor Tímea: Az AC/DC módszer és a 360°-os visszajelzés használatának szempontjai. Humán Innovációs Szemle, 2014/1–2., 20–21. o. http://humanexchange.hu/site/uploads/HISZ_V_18-33.pdf

Személyiségteszt

A jelölt személyiségéről többféle módon szerezhető információ, napi tevékenységének megfigyelése során értékelhetővé válik különböző személyiségdimenziók alapján, tesztelhető egy speciálisan, előre megtervezett helyzetben, valamint a vizsgált személyt felkérhetjük, hogy értékelje magát differenciált személyiségskálákon. A vizsgálat lehet írásbeli és szóbeli is.[14] A személyiségtesztek a következő két fő csoportba sorolhatók:

Projektív eljárások: strukturálatlan, vagy kevésbé strukturált, általában képi eszközök, amelyekkel a személyek rejtett motivációit, érzelmeit vizsgálják. Idesorolható a Rorschach-, a Lüscher-, továbbá a Szondi-teszt.

Kérdőívek: a kérdőív előnye, hogy a vizsgálni kívánt érzelmi faktorok előtérbe helyezhetők, azonban hátránya, hogy az egyszerű emberek számára a kérdés megértése bonyolult lehet, valamint előfordulhat, hogy a pályázó a számára legmegfelelőbb választ adja.[15]

Képességteszt

Főleg szenzomotoros képességek vizsgálatára használják, például a mélységészlelés, térbeli látás, mozgásérzékelés mérése során. Ezek egyfajta szakszerű előkészítést igénylő szűrővizsgálatok, amelyek önmagukban nem adnak teljes képet az egyén alkalmasságáról. A képességvizsgálatok a teljesítménytesztek csoportjába sorolhatók, hiszen meghatározott időkereten belül kell a feladatokat a legmagasabb szinten elvégezni, illetve a vizsgált személyt az adott állapotában, az adott készségszintjén elemzik. A vizsgálatok felhasználhatóságuk és korrektségük tekintetében limitáltak, mivel bizonyos specifikus képességek eltérően jellemzők a férfi- és a női csoportokra, például a térlátás, a verbalitás és az aritmetika területén. Érvényesség szempontjából is csak mérsékelt értéket mutatnak.[16]

14 Maesen de Sombreff – Willem K. B. Hostfee: Assessment and selection in organizations. John Wiley & Sons Ltd., New York, 1994, p. 356.

15 Csirszka János: Munka- és pályaalkalmasság pszichológiája. Tankönyvkiadó, Budapest, 1977, 213. o.

16 Juhász Márta: A kiválasztás pszichológiai alapjai, oktatási segédlet. BME, Budapest, 2002, 22. o. https://doksi.hu/get.php?lid=6754

Intelligenciateszt

Az intelligencia mérésére szolgáló eljárások a vizsgált alany logikai, eduktív képességeit, valamint az információ tárolására és előhívására utaló reproduktív képességeket hivatottak vizsgálni. Az eduktív mentális képességek főleg nonverbálisak, magukban foglalják az új belátásokat, a jelentésteli rendezőelvek felismerésének képességét, továbbá olyan összefüggések azonosítását, amelyek felismerése bonyolultabb szellemi folyamatot feltételez. A reproduktív képességek azonban többnyire verbálisak, az információ tárolásán és előhívásán, illetve az ezekkel végzett műveletek explicit tudásán, verbalizálásán alapulnak.[17] Az intelligenciatesztek érvényességi mutatói mérsékeltek, azonban magas használhatósági érték jellemzi őket.[18]

Szituációs gyakorlat

A szituációs gyakorlatokat nehezen lehet elkülöníteni a munkapróbatesztektől. A munkapróba alapvetően a vizsgált személy szenzomotoros képességeit vizsgálja, míg a szituációs gyakorlat a pályázó döntéshozatali mechanizmusát hivatott monitorozni. Képes mérni a problémamegoldó képességet, a problémaérzékenységet, a kommunikációs készséget, valamint a meggyőzőkészséget. Egy rendkívül fontos mutató az operatív munkakörök betöltésénél, hiszen az önálló döntéskészség elengedhetetlen a feladat-végrehajtás során.[19]

Interjú

„Az interjú személyes beszélgetésen alapuló információszerző eljárás."[20] Célja felmérni a jelentkező készségeit, képességeit, valamint alkalmasságát úgy, hogy az írásbeli vizsgálatokkal nem mérhető tulajdonságok értékelhetők.

A módszerek validitása és hatékonysága nagyban függ a külső környezet változása által támasztott új kritériumoktól. Ilyen befolyásoló tényező a biztonsági környezet, a szervezetet irányító testület, a szövetségesi rendszerek

17 Nagybányai Nagy Olivér – Rózsa Sándor: A mentális képességek tesztelése. In: Rózsa Sándor – Nagybányai Nagy Olivér – Oláh Attila: A pszichológiai mérés alapjai. Elmélet, módszer és gyakorlati alkalmazás. Bölcsész Konzorcium, 2006, 195. o. http://mek.niif.hu/05500/05536/05536.pdf

18 Tóth László: Intelligencia. Debrecen, 2009, 6. o. http://www.mateh.hu/tehetsegkonyvtar/Dr_Toth_tanulmanyok/Intelligencia.pdf

19 Juhász Márta: i. m. 30. o.

20 Gyökér Irén: Humánerőforrás-menedzsment. Műszaki Könyvkiadó, Budapest, 2001, 155. o.

által támasztott új elvárások és feladatok, valamint a társadalmi átalakulás során bekövetkezett munkaerőpiaci változások.

A kiválasztás új nehézségei az információs társadalom tükrében

A társadalmi, környezeti változások hatással vannak a szakszolgálathoz jelentkezőkre, az 1995 és 2009 között születettek, azaz a Z generáció tagjai már a globális információs térben szocializálódtak, így a digitális eszközök, a felhasználók és az információk által létrehozott *kibertérben*[21] élik mindennapjaikat. *„A tömegesen terjedő infokommunikációs eszközök a kommunikáció jellegét is megváltoztatják."*[22] A generáció tagjai a kibertérben kommunikálnak, tartanak kapcsolatokat egymással, szocializációjuk során interakcióik megszokott dimenziójává vált, így a komfortzónájuk része.

További probléma, hogy a jelentkezők körében egyre nagyobb arányban tapasztalható a dizájnerdrogok kipróbálása, alkalmi fogyasztása, ez bizonyos mennyiségi korlátok után szintén felvételi eljárásból kizáró ok.

Az előbbiek alapján megállapítható, hogy a Z generáció integrációs készsége igen alacsony, miközben ez a hivatásos szolgálat és a teljes közszolgálat egyik legfontosabb követelménye. A korosztályból kikerülő pályázók jelentős hányada csak munkahelyet keres, amit a kíváncsiság, kalandvágy, önmegvalósítás motiválhat, nem pedig élethivatást – e felfogás nélkül nem lehet felelősen és teljeskörűen gyakorolni a köz szolgálatát. Saját vágyaik beteljesítése a fő motivációjuk, amit a szervezeti, társadalmi érdek elé helyeznek, így nehezen tudnak egy integritásalapú szervezet részeként tevékenykedni. Ez a szakszolgálat vonatkozásában biztonsági kockázatot is magában hordoz.

Igen erőteljesen detektálható, hogy az információs társadalom fiatalabb generációira és a tradicionális, hagyományos értékrendre épülő, integritásalapú nemzetbiztonsági szolgálatokra, mint a szakszolgálat, egyre kevésbé összeegyeztethető elvárások a jellemzők. A szolgálat részéről felértékelődött a kiegyensúlyozott, stabil értékrend, a megbízhatóság, a józan értékítélet kívánalma.

21 Simon László – Magyar Sándor: A terrorizmus és indirekt hatása a kibertérben. Nemzetbiztonsági Szemle, 2017/3., 96–97. o. http://archiv.uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2017-3-1.original.pdf

22 Kováts Ildikó: Információs társadalom, emberi tényező, civil társadalom, média. Adalékok a magyarországi digitális műsorszórás előrejelzéséhez. Jel-kép, 2006/2., 20–21. o. http://real-j.mtak.hu/5612/2/JelKep_2006_2.pdf

Az integritáshajlambeli hiányosságokon túl jelentős probléma, hogy a Z generációhoz tartozó pályázók egészségi, pszichológiai, mentális szempontból kevésbé tudnak megfelelni a szakszolgálat által meghatározott kiemelkedő követelményrendszernek, amely nélkülözhetetlen a fokozott veszélyeztetettségben végzett nemzetbiztonsági tevékenységhez.

Egy másik jelentős probléma a nemzetbiztonsági szolgálatok működését jellemző titkosság szempontja, valamint az információalapú társadalom tagjai közötti igen jelentős információigény ellentéte. A szakszolgálat jogszabály alapján *titkos információgyűjtés*[23] végrehajtása, valamint *leplezett eszközök*[24] alkalmazása során, jogszabály alapján jogosult a tevékenységével érintett személyek bizonyos alkotmányos jogainak korlátozására, nemzetbiztonsági, bűnüldözési, valamint bűnfelderítési célból, természetesen csak az elérendő céllal arányos mértékben, a törvényesség és szakszerűség figyelembevétele mellett. A tevékenység például együtt járhat a magán- és levéltitok, a magánlakás, a személyes adatok védelméhez, illetve a birtokvédelemhez fűződő alapvető jogok korlátozásával is.[25]

Véleményem szerint négy nagyobb csoportba sorolhatók az információs társadalom hatására kialakuló, a kiválasztást nehezítő tényezők, ennek okán nélkülözhetetlen lesz egyfajta paradigmaváltás a nemzetbiztonsági szolgálatok humán utánpótlásának tekintetében.

a) pszichológiai, egészségi alkalmasság tényezők hiánya;
b) alacsony egyéni integritáshajlam;
c) biztonságtudatosság hiánya;
d) titkosság–információs igény ellentét okozta feszültség.

Megoldási javaslatok

A Nemzetbiztonsági Szakszolgálat hivatásos jogviszony betöltéséhez kötött beosztásainál indokolt lehet a hivatásos előképzettség megléte, hiszen ez egyfajta előszűrő a pályázók mentális és egészségi, valamint szervezetszociológiai kompetenciáinak, tulajdonságainak tekintetében, azonban jelenleg erre csak és kizárólag a társszervektől átszerelt, vagy újra felszerelt állomány vonatkozásában van lehetőség.

23 1995. évi CXXV. törvény 53–62. §
24 A büntetőeljárásról szóló 2017. évi XC. törvény 214–255. §.
25 Hazel R. Markus – Paula Nuris: Possible Selves. American Psychologist, vol. 41, no. 9, 1986, p. 959. https://www.researchgate.net/publication/232565363_Possible_Selves

Véleményem szerint továbbá indokolt lehet a kiválasztási rendszer olyan jellegű átalakítása, amely lehetővé tenné a jelöltek képességeinek teljes körű vizsgálatát, egy komplex kompetenciaprofil kialakításával. A generációs sajátosságokhoz igazítva érdemes lenne vizsgálni és optimalizálni a meglévő kiválasztási eljárásokat. Eredményesebb lenne minél több gyakorlati jellegű feladat bevezetése, amelyek konkrét helyzetben vizsgálják a jelöltek reakcióit, képességeit, készségeit. A felvételi eljárások során a kompetenciák szélesebb körű vizsgálatára alkalmas lehet az értékelő-/fejlesztőközpont bevezetése, alkalmazásával ugyanis jelentős eredményeket sikerült elérni a belügyi vezető-kiválasztási rendszerben.[26] A kiemelkedő stressztűrő képesség is fontos szerepet játszik az eredményes feladat-végrehajtás során, ennek széles körű mérése is indokolt lehet. A legújabb tudományos kutatások is alátámasztják, hogy a kognitív rugalmasság képessége kapcsolatban áll a stresszhatást követő kortizolszint-változással, azaz a kortizolszint méréséből következtetni lehet a pályázó stressztűrő képességére.[27] Ezen felül az egyes munkakörök differenciált követelményrendszerének figyelembevételével specifikusan, akár technikai, informatikai, operatív, funkcionális jellegű feladatok bevezetése is indokolt lehet, ugyanis minél komplexebb és testre szabottabb a kiválasztási rendszer, annál magasabb a felvett pályázók beválási aránya.[28]

A Nemzetbiztonsági Szakszolgálat számára rendkívül fontos az integritásalapú szervezeti modell fenntartása és fejlesztése, hiszen csak a szigorú értékrenddel, magas hivatástudattal felvértezett állomány tudja a közhatalom által ráruházott rendvédelmi, nemzetbiztonsági, közszolgálati feladatait pártatlanul, a tőle elvárható legjobb minőségben ellátni. Azonban a humán utánpótlás folyamatossága érdekében elengedhetetlen olyan új értékek meghonosítása a szervezeti kultúrában, amik megfelelnek az újabb generációk követelményeinek, természetesen a szervezet alapértékeivel összhangban, nem pedig azok háttérbe szorításával, lecserélésével. Érdemes lehet az önmegvalósítási vágy, a kreativitás, továbbá az innovációs hajlandóság, az

26 Zalai Noémi: A vezető-kiválasztás jelenlegi gyakorlata a polgári nemzetbiztonsági szolgálatoknál, a Terrorelhárítási Központnál és a külföldi nemzetbiztonsági szolgálatoknál. In: Hegedűs Judit: Tanulmánykötet a belügyi-vezetői kiválasztási eljárásról. Belügyminisztérium, Budapest, 2014, 31–99. o. http://real.mtak.hu/28656/1/14_TANULMANYKOTET.pdf

27 Papp Katalin: Fejlődéspszichológiai műhelymunka, Viselkedéselemző Portfólió. Szakdolgozat, ELTE Pedagógiai és Pszichológiai Kar, 2018, 25–40. o.

28 Zalai Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál. Nemzetbiztonsági Szemle, 2016/1., 40–41. o. http://epa.oszk.hu/02500/02538/00013/pdf/EPA02538_nemzetbiztonsagi_szemle_2016_01_034-044.pdf

egyéni kompetenciák folyamatos fejlesztése, a tudás, tanulás iránti igény integrálása a szervezeti értékrendbe. Természetesen a reform nem lehet egyoldalú, a pályázók kiemelkedő alkalmazkodási képessége elengedhetetlen, hiszen először nekik kell illeszkedniük a szervezeti normákhoz, értékrendhez, elvárásokhoz.

E folyamatok megtervezése, kialakítása és végrehajtása csak megfelelő integritásmenedzsment során lehetséges, amelyre a szakszolgálat kiemelt figyelmet fordít. A szervezeti struktúrában létrehozták az integritás munkacsoportot, valamint kijelölték az integritásfelelősöket. Fő feladataik közé tartozik az integritásmenedzsment kézikönyv elkészítése, amelynek elsődleges funkciója a szervezeti értékrend aktualizálása a tradicionális közszolgálati értékek és kívánalmak, valamint az információs társadalom igényeinek figyelembevételével. A Nemzetbiztonsági Szakszolgálat állományának feladatvégrehajtása során nagyon nagy figyelmet kell fordítani a kellő biztonságtudatosságra. Abban az esetben, ha a pályázók nincsenek birtokában az informatikai eszközök biztonságos kezeléséhez szükséges ismereteknek, akár gondatlanul is megoszthatnak jogosulatlan személyekkel védett információkat. A biztonságtudatos magatartás hiánya nem szakszolgálat-specifikus jelenség, hanem globális társadalmi jellemző, amely az információalapú társadalom egyik jelentős problémája. Ezt az állítást hivatott alátámasztani az Európai Bizottság 2017-ben kiadott hatástanulmánya, amely szerint az infokommunikációs eszközök végfelhasználói körét nem jellemzi kellő biztonságtudatosság az alkalmazásuk területén, ez hozzájárul az információs aszimmetria növekedéséhez.[29] A nemzetbiztonsági szolgálatok működését jellemző kiemelkedő szintű információvédelem, azaz a titkosság gátolja a munkaerőpiacon elhelyezkedni kívánók rendkívüli információigényét a leendő munkahelyük kiválasztását célzó piackutatás során. A szervezet működésével, tevékenységi körével kapcsolatos védett információk fókuszban tartása mellett szükséges a munkaerő-kínálat információigényének optimális kielégítése. Tudomást kell szerezniük a szakszolgálat létezéséről, úgy kell bemutatni nekik a szervezetet, a képviselt értékrendet, a feladatkört, a lehetőségeket, elvárásokat, hogy azok vonzóvá váljanak számukra. A választásban további motiváló tényezők lehetnek a kiszámítható életpályamodell nyújtotta

29 European Commission: Commission Staff Working Document Impact Assessment, Accompanying the document proposal for a regulation of the european parliament and of the counciL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 4/6, Brussels, 2017, pp. 10–13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2017%3A500%3AFIN

lehetőségek és a biztonság, az illetmény és egyéb, az illetményen kívüli juttatások bemutatása, valamint a szakszolgálat állományához tartozás elitségének, kiváltságának hangsúlyozása. Az intenzív toborzási tevékenység szélesebb spektrumú kiterjesztése a digitális térben további eredményeket hozhat a jelentkezők számának növelésében.

Az előbbiek alapján jól látható, milyen, az információs társadalom támasztotta, új típusú nehézségekkel kell megküzdenie a Nemzetbiztonsági Szakszolgálatnak a humán utánpótlási, kiválasztási tevékenységében. Ezek alapján konstatálható, hogy elengedhetetlen a szervezet paradigmaváltása, és alkalmazkodása az utánpótlási bázist jelentő társadalmi csoportok igényeihez, a hierarchikus, tradicionális nemzetbiztonsági szolgálatra jellemző egyedi értékek és elvárások szem előtt tartása mellett.

DOI: 10.38146/BSZ.2019.1.5

TARJÁN GÁBORNÉ – DANKÓ GÁBOR

A polgári nemzetbiztonsági szolgálatok speciális költségvetési és vagyongazdálkodásának legfontosabb szabályai

A Nemzetbiztonsági Szakszolgálat mint polgári nemzetbiztonsági szolgálat költségvetési és vagyongazdálkodása tekintetében egyfajta kettősség figyelhető meg, amely adódik egyrészt abból, hogy a Nemzetbiztonsági Szakszolgálatra mint az Országgyűlés által létrehozott, önállóan működő és gazdálkodó központi költségvetési szervre az általános, minden költségvetési szervre irányadó költségvetési és vagyongazdálkodási előírások vonatkoznak. Másrészt azonban a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) szerinti alaptevékenység[1] ellátásával összefüggésben elengedhetetlen a speciális gazdálkodási szabályok alkalmazása.

Míg az első esetkörben a költségvetési és vagyongazdálkodással kapcsolatos információk, adatok alapvetően nyíltak, bárki számára megismerhetők lennének, addig a kifejezetten nemzetbiztonsági tevékenység gazdálkodási adatai „zártak", azokat csak az arra feljogosított szervek és személyek ismerhetik meg, éppen az alaptevékenység leplezése, a műveleti feladatok, módszerek és az állomány védelme, valamint a szolgálatok törvényes érdekeinek sértetlensége érdekében. Kiemelendő azonban – a későbbiekben részletezettek alapján –, hogy a szolgálatok törvényes érdekeinek védelmére kibocsátott törvényben és annak felhatalmazása alapján kiadott jogszabályban meghatározott módon korlátozzák az általános, költségvetési szervként kezelt adatokat is.

E tanulmányban a polgári nemzetbiztonsági szolgálatok (a továbbiakban: szolgálatok) speciális költségvetési és vagyongazdálkodása legfontosabb szabályainak – a minősített adatok védelme okán alapvetően a jogszabályok – bemutatására és elemzésére törekszünk annak érdekében, hogy képet adjunk a „titkosszolgálati gazdálkodás" jogszabályokon alapuló, sajátos tevékenységé-

1 A 8. § (1) bekezdés alapján, különösen annak a) és b) pontja szerint: a jogszabályok keretei között eszközeivel és módszereivel – írásbeli megkeresésre – szolgáltatást végez a titkos információgyűjtés, illetve a büntetőeljárásról szóló törvény szerinti leplezett eszközök alkalmazásának végrehajtásához a titkos információgyűjtés folytatására, valamint a leplezett eszközök alkalmazására feljogosított szervek részére, illetve e szervek igényei alapján biztosítja az e tevékenységhez szükséges különleges technikai eszközöket és anyagokat.

ről. A tanulmány alapvetően a Nemzetbiztonsági Szakszolgálat szemszögéből mutatja be e sajátos tevékenységet, jelentős elvi jellegű eltérés a szolgálatok tekintetében – a vonatkozó egzakt jogszabályi előírásokból adódóan – nem lehet, azonban a gyakorlati végrehajtás során, jogszabály keretei között, a belső normatív szabályozásban lehetnek különbségek.

Ezek tekintetében elöljáróban is feltétlenül hangsúlyozandó, hogy bár az e körbe tartozó információk nem nyíltak, azok esetében is megvalósulnak a nyílt gazdálkodás kritériumai, vagyis különösen a törvényesség, ellenőrizhetőség, dokumentáltság és egyéni felelősség előírásai. A szolgálatok e tevékenységüket is külső kontroll alatt, fokozott vezetői ellenőrzés keretében, mindenre kiterjedő nyilvántartás vezetése mellett végzik.

A sajátos költségvetési gazdálkodás szabályainak bemutatása

Az általános szabályoktól történő eltérést lehetővé tevő sarkalatos törvény a már hivatkozott Nbtv., amelynek 63–66. §-ai az alaptevékenység ellátása érdekében sajátos gazdálkodási szabályokat állapítanak meg.

Az Nbtv. 63. § (1) és (2) bekezdése az alaptevékenységgel összefüggő sajátos költségvetési források tekintetében összesítő elnevezésként a „speciális működési kiadások" fogalmat vezeti be és alkalmazza, amelynek tekintetében lehetővé teszi, hogy azokat felhasználásuktól/jellegüktől (dologi, beruházási, személyi kiemelt előirányzatok) függetlenül, eltérően a számviteli jogszabályokban meghatározottaktól, egységesen és összevontan egy összegben, elkülönített előirányzatként kell szerepeltetni.

Az Nbtv. valamennyi a szolgálatok *„titkosszolgálati tevékenységéhez, a titkos információgyűjtés eszközeinek és módszereinek alkalmazásához"* közvetlenül kapcsolódó személyi és tárgyi vonatkozású kiadást ebbe a körbe sorol, függetlenül attól, hogy azokat a számviteli szabályok alapján mely kiemelt előirányzaton kellene elszámolni, ha az adott kiadás „nyílt" jellegű lenne.

Ezeknek a megengedő-kötelező szabályoknak a jelentősége abban rejlik, hogy a szolgálatok kiemelt előirányzatait a mindenkori költségvetési törvény tartalmazza, ezáltal az ez irányú források egyfajta „bekeverése" a kiemelt előirányzatok közé már megteremti annak a lehetőségét, hogy a speciális kiadásoknak sem a mértékét, sem pedig jellegét (a felhasználás célját) arra illetéktelenek ne ismerhessék meg. E szabály nyomán még következtetéseket sem lehet arra vonatkozóan levonni, hogy az adott szolgálat ezt az előirány-

zatát milyen célra kívánja felhasználni. Példaként: ha egy konspirált objektumként használandó épület megvalósítása lenne a cél, a példa kedvéért egymilliárd forint tervezett összegben és ennek érdekében a szolgálat beruházási kiadását ezzel az összeggel megemelnék, valamint ha ehhez nyílt módon nyújtana forrást a pénzügyi kormányzat (jogszabály, nyílt kormányhatározat), akkor az egyértelműen az objektum látókörbe kerülését okozná (legrosszabb esetben már a létesítésekor dekonspirálódhatna).

Az előbbieken túlmenően a speciális eljárási részletszabályokat (nyílt jogszabályként) a polgári nemzetbiztonsági szolgálatok költségvetésének és gazdálkodásának egyes speciális szabályairól szóló 130/2011. (VII. 18.) kormányrendelet (a továbbiakban: 130/2011. kormányrendelet) tartalmazza. Ez a jogszabály nemcsak a „speciális", hanem a nyílt költségvetési források tekintetében is lehetővé teszi, hogy azokat a szolgálatok a törvényes érdekeik védelmében, zártan kezeljék, a költségvetési gazdálkodási feladatokat, nyilvántartást saját hatáskörben vezessék, abból adatot korlátozottan szolgáltassanak.

Részletek

E körben a 130/2011. kormányrendelet lehetővé teszi – az „általános" költségvetési gazdálkodást folytató szervekkel ellentétben –, hogy a szolgálatok *„saját gazdasági szervezeteik útján a tervezéssel, előirányzat-felhasználással, a hatáskörükbe tartozó előirányzat-módosítással, az üzemeltetéssel, fenntartással, működtetéssel, beruházással, a vagyon használatával, hasznosításával és nyilvántartásával, a munkaerő-gazdálkodással, a készpénzkezeléssel, a könyvvezetéssel, valamint a beszámolási kötelezettséggel, adatszolgáltatással és a belső kontrollrendszer működtetésével kapcsolatos feladatokat"* sajátos szabályok szerint, saját maguk láthassák el.

Kifejezetten a Magyar Államkincstárral összefüggően, *„ezen szervnél vezetett fizetési számlát érintő kiadások és bevételek teljesítése során a fejezeti elosztási számlára és a fejezeti maradvány-elszámolási számlára történő utalásra, a lakástámogatásra és a dolgozók lakásépítésének, lakásvásárlásának munkáltatói támogatására szolgáló számla, az európai uniós forrásokra az »Azonosítás alatt álló kiadások«-ra és az »Azonosítás alatt álló bevételek«-re vonatkozó Egységes Rovat Azonosító Kódokat használhatják".* Ez azt jelenti a szolgálatok esetében, hogy az átutalások teljesítése – az illetményjellegű kiadásokon kívül – a Magyar Államkincstárnál vezetett pénzforgalmi számlához kapcsolódóan elektronikus formában a GIRO rendszerén, egy tit-

kosított vonalon, szűkített adattartalommal történik. Így azok jellegét – a személyi, üzemeltetési vagy eszközbeszerzési kiadás – a Magyar Államkincstár nem tudja, nem tudhatja, csak minden esetben a számlán lévő összeg (fedezet meglétét) ellenőrzi, a rendelkezésre álló likviditási fedezetet vizsgálja meg. A Magyar Államkincstár a 130/2011. kormányrendelet értelmében a kiadások és bevételek kiemelt előirányzatokon történő könyvelését mindig a szolgálatok által, szűkített formában megadott pénzforgalmi jelentés alapján hajtja végre.

A jogszabály szintén az általánosságban már megjelenített indokok alapján lehetővé teszi továbbá a szolgálatok számláinak forgalmáról történő *adatszolgáltatás* korlátozását, arról csak külön meghatározott, alapvetően az *ellenőrzés*t végző szervek, célhoz kötötten kaphatnak adatot azzal, hogy a Magyar Államkincstáron belül is korlátozott az adatszolgáltatás, illetve a hozzáférés. A gyakorlatban ezekhez az adatokhoz mind a Magyar Államkincstár, mind az érintett szervek érvényes nemzetbiztonsági ellenőrzésen átesett munkatársai férhetnek hozzá.

Szintén jogszabályon alapuló, kiemelt jelentőségű előírás a szolgálatok kötelezettségvállalásainak saját hatáskörben történő vezetése. Ez szinkronban van az Nbtv. 51. § (1) bekezdésével, amelynek alapján csak az irányító miniszter, illetve a főigazgató hozzájárulásával hozhatók nyilvánosságra a szolgálatok eszközbeszerzéseivel és egyéb szerződéseivel kapcsolatos adatok. E szabály jelentőségéhez nem férhet kétség, belátható, milyen jelentős kockázatot hordozna magában, ha az adott szolgálat teljes kötelezettségvállalási rendszere „publikussá" válna. A kötelezettségvállalások – általánosan – tartalmazzák a szerződő felet, az adott szerződést/kötelezettségvállalási alapdokumentumot, a konkrét összeget, a terhelendő előirányzatot, ezek összességéből egyértelműen megállapíthatók a szolgálatok fejlesztési/együttműködési irányai, a beszerzendő eszköz(kör), az érintett partneri kör, a rendelkezésre álló pénzügyi forrás. Mindezek nyilvánosságra kerülése már súlyos kockázatot hordoz magában, a szolgálatok tevékenységét, működésének rendjét sérti.

A szolgálatok a jogszabályokban meghatározott egyes adatszolgáltatásokat kétféle módon készítik el, részletes változatban minősített formában, és összevont adattartalommal, nyílt módon. Ezeknek az adatszolgáltatásoknak a körét és azt, hogy kinek kell megküldeni, melyik szervnek, szintén a 130/2011. kormányrendelet előírásai tartalmazzák. Természetesen konspirációs megfontolásból ezekben az adatszolgáltatásokban a szolgálatok létszámára vonatkozóan sem lehet részletesebb bontású adat, mint hogy „hivatásos", „rendvédelmi igazgatási alkalmazott" és „munkavállaló".

A szolgálatok speciális működési kiadásai felhasználásának külső szerv által történő ellenőrzése vonatkozásában az Nbtv. 66. §-a tartalmaz jelentősen korlátozó (szigorító) rendelkezéseket, meghatározza, hogy arra kizárólag törvényességi szempontból kerülhet sor. Célszerűségi és eredményességi szempont szerinti ellenőrzést külső szerv nem folytathat le, arra kizárólag a szolgálatokat irányító miniszter jogosult. A miniszter, mint a szolgálatok irányítására felhatalmazott vezető e tevékenysége körében eleve ismeri a titkos információgyűjtés eszközeit és módszereit, így jogosult a gazdálkodás célszerűségi és eredményességi szempont szerinti ellenőrzésére.

A törvény továbbá tilalmazza a gazdálkodás külső szerv által történő ellenőrzése során a titkos információgyűjtés közben keletkezett információra, forrására, illetve az alkalmazott titkos információgyűjtő módszer konkrét jellegére utaló adatok megismerését. E szabályok kidolgozására kifejezetten a titkosszolgálatok törvényes érdekeinek, az alaptevékenységük ellátásához használt eszközök, módszerek védelme érdekében került sor. A külső szerv ellenőrzést végző munkatársai annak ellenére sem ismerhetik meg ezeket az adatokat, információkat, hogy – a Nemzetbiztonsági Szakszolgálat gyakorlata/tapasztalata alapján – érvényes, „kockázatmentes" nemzetbiztonsági ellenőrzéssel bírnak és a minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) szerinti személyi biztonsági tanúsítványuk, felhasználói engedélyük és titoktartási nyilatkozatuk van. Nem vonható kétségbe, hogy milyen jelentős károkat okozhatna egy a Nemzetbiztonsági Szakszolgálat által fejlesztett, beszerzett, kifejezetten titkosszolgálati speciális eszközrendszer létének, tulajdonságainak illetéktelenek (különösen bűnözői körök, ellenérdekű titkosszolgálatok) általi megismerése. Vagy a szolgálatokkal együttműködő személyek kilétének (kapcsolati háló feltárása) megismerése, ami e személyek életét is veszélybe sodorhatná. Természetesen nem vonjuk kétségbe és nem kételkedünk abban, hogy a külső ellenőrzést végző személyek eleget tesznek titoktartási kötelezettségüknek, azonban a minősített adatok kezelése során a „klasszikus" bizalmi elv nem érvényesül. A „Megosztom veled a titkot, de tartod a szádat, ugye?" jellegű kérdéseknek nem lehet létjogosultságuk a minősítettadat-kezelés körében. Ugyanez az elv „hatványozottan" igaz a szolgálatok műveleti tevékenységének, eszközeinek, módszereinek, adatszerzési forrásainak tekintetében is azzal, hogy ebben az esetben – a törvényi előírások alapján – eleve korlátozott ezek megismerhetősége.

Mindezek alapján látható, hogy *a szolgálatok ellenőrzése garantált,* azonban azt részletesen körülírt és tételesen meghatározott – különösen a speciális gazdálkodási tevékenységét érintően –, *célhoz kötött módon végezhetik* a

kijelölt ellenőrző szervek. Kiemelendő, hogy a Nemzetbiztonsági Szakszolgálat esetében is függetlenített belső ellenőrzés működik, amely – a külső ellenőrzésen és a folyamatba épített vezetői ellenőrzésen túlmenően – ellátja e tevékenység rendszeres és tételes kontrollját is.

A kapcsolódó feladatok részletes szabályozását külön együttműködési megállapodás(ok) tartalmazzák, tekintettel azok szenzitív, illetve az Mavtv. szerinti minősítettadat-tartalmára, az abban foglaltak elemzésére jelen anyagban nincs lehetőség. Ugyanez igaz a speciális működési kiadásokra és bevételekre vonatkozó felhasználás, bizonylatolás, elszámolás és ellenőrzés részletes szabályaira vonatkozó külön miniszteri utasításban megfogalmazott szabályokra, amelyek minősített jellegük okán szintén nem jeleníthetők meg.

Az előbbiekben részletezett, speciális gazdálkodási szabályok mellett minden esetben érvényesülnek, érvényesülniük kell – a nyílt és speciális gazdálkodást is érintően – a következő *alapelvek*nek:

– törvényesség: a kiadás és bevétel kezelése, felhasználása, nyilvántartása és ellenőrzése a vonatkozó jogszabályok (különösen: a számvitelről, a személyi jövedelemadóról szóló törvény, az Nbtv.), valamint közjogi szervezetszabályozó eszközökben meghatározott előírások figyelembevételével és betartása útján valósul meg;
– egyéni felelősség megállapíthatósága;
– konspiráció megvalósítása a vonatkozó előírások szerint az érintett gazdálkodási adatok védelme érdekében;
– dokumentáltság a gazdasági eseményekkel összefüggésben;
– ellenőrzöttség és ellenőrizhetőség megvalósítása és védelme;
– tervszerűség: a szükséges kiadások pénzügyi fedezetének megteremtése és felhasználása a jóváhagyott éves elemi költségvetésében foglaltak szerint;
– valódiság elve: a felvetődő kiadással és a keletkező bevétellel kapcsolatos, dokumentált gazdasági eseményeknek a valóságban is megtalálhatóknak, bizonyíthatóknak, kívülállók által is megállapíthatóknak (a leírt ellenőrzési korlátozásokkal) kell lenniük. A kapcsolódó számviteli bizonylatok adatainak tartalmilag hiteleseknek, megbízhatóknak és helytállóknak kell lenniük.

A vagyongazdálkodás szabályainak bemutatása, különös tekintettel a szolgálatok ez irányú sajátosságaira

Tekintettel a bevezetőben foglaltakra, a Nemzetbiztonsági Szakszolgálat „dualisztikus” szervi jellege (költségvetési/titkosszolgálati szerv) okán az in-

gó- és ingatlanvagyon-gazdálkodás tekintetében is egyértelműen kettős működés tapasztalható mind a jogszabályi előírások, mind pedig azok gyakorlati végrehajtása tekintetében. Teljes egészében kettéválik a nyílt és a speciális működési kiadásból finanszírozott vagyonelemek kezelésének rendje azzal, hogy a szolgálatok nyílt, vagyonkezelésben lévő vagyona tekintetében is eltérő, a szolgálatok konspiratív érdekét védő szabályok irányadók.

Általános vagyongazdálkodási szabályok

Az állami vagyonra, vagyongazdálkodásra vonatkozó jogszabályok[2] alapján a szakszolgálat által kezelt, illetve kezelésébe kerülő *ingó- és ingatlanvagyon-elemek állami vagyonnak minősülnek,* amelyek esetében az állam tulajdonosi jogait a magyar állam nevében az állami vagyon felügyeletéért felelős miniszter gyakorolja, feladatait a Magyar Nemzeti Vagyonkezelő (MNV) Zrt. útján látja el. A vonatkozó előírásokból megállapítható, hogy fő szabály szerint a központi költségvetési szervnek nincs önálló tulajdonjoga, tulajdonjogot, vagyoni értékű jogot a magyar állam javára szerez meg, amely azt maga kezeli, illetve szerződés – így különösen vagyonkezelés, bérlet, haszonbérlet stb. – alapján a vagyonkezelő szerveknek átengedi. A gyakorlatban a költségvetési szervek/szolgálatok a vonatkozó jogszabályi előírások és a vagyonkezelői szerződés szabályai alapján az általuk kezelt „nyílt" ingó- és ingatlanvagyon-elemek *vagyonkezelői,* annak tulajdonosi joggyakorlója pedig az MNV Zrt.

A vagyonkezelt vagyon tekintetében a szolgálatok is vagyonkezelési szerződést kötnek az MNV Zrt.-vel, amely – a Nemzetbiztonsági Szakszolgálat ez irányú szerződésének alapulvételével – számos korlátozó, illetve az általános költségvetési szervektől eltérő rendelkezést tartalmaz éppen a szolgálatok érdekeinek védelmében, amelyek közül a leglényegesebbek

– a kezelt vagyonról az MNV Zrt. részére történő (szűkített) korlátozott tartalmú adtaszolgáltatás előírásai;
– a saját hatáskörben megvalósuló nyilvántartás vezetése;
– a speciális működési kiadásból finanszírozott ingatlan és ingók tekintetében a szakszolgálat elkülönített nyilvántartást vezet, arról adatot az MNV Zrt. részére nem szolgáltat;
– a speciális ingatlanokra vonatkozó további előírások (saját hatáskörben, miniszteri hozzájárulással történő átminősítés, saját hatáskörben történő

2 Az állami vagyonról szóló 2007. évi CVI. törvény; a nemzeti vagyonról szóló 2011. évi CXCVI. törvény (Nvt.); illetve az állami vagyonnal való gazdálkodásról szóló 254/2007. (X. 4.) kormányrendelet.

nyilvántartás, értékesítés, abból befolyó vételár saját hatáskörben történő felhasználása);
– titkos információgyűjtő, titkos adatszerző tevékenységhez szükséges különleges technikai eszközök, anyagok térítésmentes, saját hatáskörben megvalósuló átadása;
– korlátozott külső ellenőrzés végrehajtásának szabályozása és egyben korlátozása.

Az előbbiekkel összefüggésben célszerű részletesen bemutatni a szolgálatok speciális vagyongazdálkodását.

Speciális vagyongazdálkodási jogszabályok

Az Nbtv. 63. § (5) bekezdése[3] alapján – a törvény ez irányú módosításával – 2015. január 1-jével az MNV Zrt. tulajdonosi joggyakorlásából kikerült *a titkosszolgálati tevékenységéhez,* valamint a *titkos információgyűjtés* eszközeinek és módszereinek alkalmazásához *közvetlenül kötődő,* e célra beszerzett és használt *vagyon,* amelynek – a Nemzetbiztonsági Szakszolgálat vagyonkezelési szerződésében is deklarált módon – *a Nemzetbiztonsági Szakszolgálat a tulajdonosijog-gyakorlója.*

Tehát a szolgálatok mindazon vagyon tekintetében tulajdonosijog-gyakorlónak minősülnek, amelyet az alaptevékenységükkel összefüggően használnak fel és külön szabály szerint azzá minősítenek. Álláspontunk szerint az e körbe tartozó vagyon gyakorlatilag minden, a speciális működési kiadásból finanszírozott vagyont magában foglalja, de azon túl is mutat, figyelemmel arra, hogy az Nbtv. vonatkozó szabálya nem forrás/finanszírozottság szempontjából, hanem az alaptevékenységgel közvetlenül összefüggő felhasználás oldaláról sorolja ebbe a körbe a vagyont. Vagyis lehetséges, hogy egy vagyontárgyat a szolgálat „nyílt" költségvetési forrásból (köz)beszerzési eljárás nyomán nyíltan (a Nemzetbiztonsági Szakszolgálat jelenik meg szerződő félként) szerez be, azonban a felhasználása már közvetlenül összefügg

3 (5) A nemzetbiztonsági szolgálatok titkosszolgálati tevékenységéhez, valamint a titkos információgyűjtés eszközeinek és módszereinek alkalmazásához közvetlenül kötődő, e célra *beszerzett és használt vagyon felett* az államot megillető *tulajdonosi jogok és kötelezettségek* összességét a *nemzetbiztonsági szolgálatok gyakorolják.*
(6) A nemzetbiztonsági szolgálatok titkosszolgálati tevékenységéhez, valamint a titkos információgyűjtés eszközeinek és módszereinek alkalmazásához közvetlenül kötődő *vagyonértékesítésből származó bevétel* a nemzetbiztonsági szolgálatok *speciális bevétele,* amelyet az e tevékenységhez szükséges *ingatlan és egyéb eszközök vételére, felújítására, felszerelésére,* illetve *bővítésére* használhatnak fel.

a titkosszolgálati tevékenységgel. Erre tipikus és egyben klasszikus példa a *Mások élete* című film egyik jelenete, amelyben a célszemély(ek) lakásában található villanykapcsolót cserélik ki/preparálják technikai eszközzel ellátottra. Vagyis – elvonatkoztatva a konkrét filmbeli jelenettől – egy közforgalomban kapható eszköz nyílt módon történő megvásárlása után (ami önmagában nem teremt dekonspirációt) annak titkos információgyűjtéshez történő közvetlen felhasználása okán az már a tulajdonosi körbe tartozó módon kezelendő. A helyzetet még jobban érzékeltető egyéb példa a szakszolgálat érdekeinek védelme miatt jelen tanulmányban nem jeleníthető meg.

További részletszabályokat tartalmaz a 130/2011. kormányrendelet, amelynek alapján a szolgálatok a használatukban, hasznosításukban, vagyonkezelésükben vagy tulajdonosi joggyakorlásuk alatt álló állami vagyonról *saját hatáskörben* vezetnek részletes *nyilvántartást,* azzal, hogy *a vagyonról* az államháztartás számviteléről szóló 4/2013. (I. 11.) kormányrendelet 5. mellékletének adataiból az *Eszközök* alcím betűvel és római számmal jelölt sorainak megfelelő adattartalommal küldenek adatot az MNV Zrt.-nek, illetve a vonatkozó jogszabályok alapján adatkérésre felhatalmazott szerveknek. Vagyis e jogszabály nemcsak a tulajdonosijog-gyakorlás körébe tartozó, hanem jogcímtől függetlenül, valamennyi a szolgálatok által kezelt vagyonelemre kiterjedően lehetővé teszi a saját hatáskörben történő részletes nyilvántartás vezetését és a *korlátozott, szűkített adattartalmú adatszolgáltatás*t.

Célszerű röviden bemutatni, hogy az adott ingó- vagy ingatlanvagyontárgy a jogszabályi feltételek – a titkos információgyűjtés eszközeinek és módszereinek alkalmazásához közvetlenül kötődő, e célra beszerzett és használt vagyon – teljesülésén túlmenően a *gyakorlatban hogyan kerül „a tulajdonosijog-gyakorlás",* illetve „a speciális működési kiadásból finanszírozási" *körbe.* E tekintetben az ingó- és ingatlanvagyon-elemek kezelése kettéválik. *Az ingatlanok esetében* a vonatkozó előírást a 130/2011. kormányrendelet 6. § (1) bekezdése tartalmazza, miszerint a „Szolgálatok főigazgatói *az Nbtv. 63. § (2) bekezdése alapján* a miniszter jóváhagyásával meghatározzák *azon ingatlanok körét, amelyek speciális működési kiadásból finanszírozott ingatlannak minősülnek".* Vagyis a főigazgató kezdeményezése alapján – minden esetben a szolgálat érdekének védelmében, minősített tartalmú dokumentum alapján – miniszteri döntéssel történik meg a „speciálissá" minősítés. A finanszírozás fogalmát a jogszabályok nem definiálják, azonban a kifejezés hétköznapi értelemben is az ingatlan létesítésével, fenntartásával (üzemeltetésével) összefüggő költségeket foglalhatja magában. Az ingatlan-

nyilvántartásban (a szolgálatok érdekeinek védelmében) fő szabály szerint az adott ingatlan bejegyzésére a szolgálathoz nem köthető módon kerül sor.

Ingóságok esetében – mivel a jogszabály csak a már ismertetett szabályokat tartalmazza – a *„speciális" körbe kerülés főigazgatói,* illetve a Nemzetbiztonsági Szakszolgálat belső normája alapján leadott hatáskörben az érintett szakterület vezetőjének *döntési kompetenciájába tartozik.* Ha az adott vagyontárgy beszerzése eleve speciális működési kiadásból történik, vagy annak felhasználása a titkosszolgálati tevékenységgel közvetlenül összefügg, e körbe tartozóan kezelendő.

Az értékesítés vonatkozásában a szolgálatoknak további sajátos jogosultságaik vannak az Nbtv. és a 130/2011. kormányrendelet szabályai alapján. Az „általános" költségvetési szervektől eltérően a szolgálatok jogosultak a titkosszolgálati tevékenységéhez, valamint a titkos információgyűjtés eszközeinek és módszereinek alkalmazásához közvetlenül kötődő *vagyont (ingó és ingatlan is) saját hatáskörben értékesíteni,* az értékesítésből származó bevétel a szolgálatok speciális bevétele, amelyet az e tevékenységhez szükséges ingatlan és egyéb eszközök vételére, felújítására, felszerelésére, illetve bővítésére használhatnak fel.

Célszerű bemutatni, hogy ezek az előírások hogyan érvényesülnek a gyakorlatban a Nemzetbiztonsági Szakszolgálatnál. A részletes, saját hatáskörű nyilvántartás a „nyílt" és a „speciális" ingó- és ingatlanvagyon-elemek külön-külön adatbázisban (a Mavtv. előírásaira is figyelemmel) feltüntetett, a számviteli törvény szerinti részletes, dokumentálását foglalja magában, sajátos és részletes belső előírások alapján. A „speciális" vagyonelemek nyilvántartása, az abba való betekintés és az adatok kezelése a Nemzetbiztonsági Szakszolgálaton belül is korlátozott, vagyis csak az arra kifejezett felhatalmazással bíró munkatársak férhetnek hozzá ezekhez az adatokhoz, garantálva ezzel a belső konspirációs előírások érvényre juttatását. A szűkített adatszolgáltatás pedig annyit takar, hogy a vagyonelemek összességéről (a gyakorlatban a speciális ingatlanok kivételével) kizárólag összevontan egysoros adatszolgáltatás történik nyílt formában (például Eszközök/Tárgyi eszközök/Ingatlanok és kapcsolódó vagyoni értékű jogok x forint). Így szavatolható a Nemzetbiztonsági Szakszolgálat alaptevékenységéhez is használt eszközeinek védelme, hiszen egy összevont nyilvántartási értékből sem az eszközök darabszáma, értéke, sem pedig a felhasználás célja nem megállapítható illetéktelenek által.

A Nemzetbiztonsági Szakszolgálat vagyonkezelési szerződése és az MNV Zrt.-vel kialakított ez irányú partneri együttműködés a gyakorlatban garantál-

ja az Nbtv. 63. § (5) bekezdése szerinti, a Nemzetbiztonsági Szakszolgálat tulajdonosijog-gyakorlásába tartozó ingatlan- és ingóvagyon-elemek konspirált használatát és védelmét. A szerződés az iménti előírásokat erősíti meg, kiemelendő, hogy a gyakorlatban a speciális működési kiadásból finanszírozott és a közhiteles ingatlan-nyilvántartásban a szakszolgálathoz nem köthető, valamint külön, „speciális" módon használt/hasznosított ingatlanról – konspirációs-műveleti okok és a minősített adatok védelme okán – a Nemzetbiztonsági Szakszolgálat nem szolgáltat adatot. Erre vonatkozóan a hatályos vagyonkezelői szerződés is analóg előírásokat tartalmaz, például a *Feladatellátás érdekében igénybe vett ingatlanok kimutatása (ingatlanhoz kapcsolódó jogosultságok kimutatása)* és az *Ingatlanokhoz kötődő vagyoni értékű jogok kimutatása* részek nem nyilvános/minősített adatok védelme okán kitételeket tartalmazza.

Az állami vagyon kezelésének ellenőrzése a szolgálatok tekintetében, az általános ellenőrzési előírásokhoz képest – a nemzetbiztonsági szolgálatok tevékenységének sajátosságai és az ellenőrzési korlátok széles körére figyelemmel, a már hivatkozott Nbtv. 66. §-a alapján – eltérő. Az MNV Zrt. – a vagyonkezelési szerződés alapján – a jogszabály szerinti ellenőrzési jogosítványait *a szolgálatokat irányító miniszter által kijelölt szerven keresztül gyakorolja,* így a titokvédelmi és konspirációs szempontok garantálása érdekében az MNV Zrt. nem végezhet közvetlen ellenőrzést.

Az említett kérdéskörökben az állami vagyon kezelésére vonatkozó „általános érvényű" jogszabályok és a szolgálatok tekintetében irányadó, a tevékenység jellegéből adódóan speciális jogszabályok közti részbeni ellentmondás figyelhető meg. Ez alapvetően abból ered, hogy a vagyonkezelési általános előírások alapján alapvetően a „közvagyon" kezeléséhez kapcsolódó adatok nyilvánosak, bárki számára megismerhetők, az ezekről történő adatszolgáltatás nem korlátozható. Ezzel szemben, figyelemmel egyebek közt a már hivatkozott Nbtv. 51. § (1) bekezdésében foglaltakra is, amely szerint a minősített adatokon túlmenően csak az irányító miniszter vagy a főigazgató engedélyével hozhatók nyilvánosságra a többi között a szolgálatok objektumaival, eszközbeszerzéseivel és egyéb szerződéseivel összefüggő adatok. A gyakorlati végrehajtás során a Nemzetbiztonsági Szakszolgálat a tulajdonosijog-gyakorlása körébe tartozó vagyonelemek tekintetében a saját hatáskörben vezetett részletes nyilvántartása a Mavtv. alapján minősített adatnak minősül, így e nyilvántartás mind a Mavtv., mind az Nvt. 10. § (1) bekezdésében foglaltakra figyelemmel nyilvánosságra nem hozható. A vagyonkezelésre vonatkozó jogszabályok a kivételi köröket nem tartalmazzák

a gyakorlati végrehajtás tekintetében egzakt módon, így az ellentmondások az MNV Zrt.-vel kötött szerződésben tárgyalt és szükség szerint külön minősített tartalmú megállapodásban rendezhetők.

A sajátos beszerzési szabályok bemutatása

A szolgálatok (köz)beszerzései vonatkozásában is a gazdálkodással összefüggésben már megjelenített kettősség tapasztalható. Egyrészről a közbeszerzési szabályok alkalmazása mint közpénzből gazdálkodó szervezetek számára kötelező, másrészről a minősített adatok védelme és a titkosszolgálati tevékenységgel összefüggő tevékenység okán külön jogszabályok szerinti eljárás keretében lehetőség van speciális beszerzési eljárások lefolytatására, sőt egyes esetekben közvetlen szerződéskötésre is.
A Nemzetbiztonsági Szakszolgálat ez irányú gyakorlata és tapasztalatai – természetesen a titokvédelmi szabályok miatt részletek ismertetése nélkül – a következőképpen összegezhetők.

A Nemzetbiztonsági Szakszolgálat köteles *a közbeszerzésekről szóló 2015. évi CXLIII. törvény* (Kbt.), illetve minősített adatot érintő beszerzések esetében a védelmi és biztonsági célú beszerzésekről szóló 2016. évi XXX. törvény *(védelmi törvény)* alkalmazására, azonban az alaptevékenységéből adódó sajátosságai okán – a Kbt., illetve a *védelmi törvény* szerinti kivételi körökbe tartozóan – sok esetben nem lehetséges a nyilvánosság bevonásával, illetve e jogszabályok alkalmazásával megvalósuló köz-/beszerzések lefolytatása, alapvetően a tevékenység ellátásához szükséges eszközök, szolgáltatások igénybevételének „titokban" maradása érdekében. Egyes esetekben már az eszköz elnevezésének, jellegének, vagy az igénybevétellel érintett szolgáltatás jellegének nyilvánosságra kerülése is jelentős károkat okozhatna a szolgálatok számára.

Mindezen okok alapján a külön eljárási jogszabályok[4] szerint a Nemzetbiztonsági Szakszolgálat a Belügyminisztériumon keresztül kezdeményezi a Kbt., illetve a *védelmi* törvény alkalmazása alól *az adott feladat (projekt) mentesítését az Országgyűlés nemzetbiztonsági bizottságánál.* A bizottság a Kbt.,

4 Az alapvető biztonsági érdeket érintő beszerzések Országgyűlés általi mentesítésének kezdeményezésére vonatkozó feltételekről és eljárásról, valamint az ilyen beszerzések megvalósításakor az ajánlatkérő által érvényesítendő követelményekről szóló 225/2016. (VII. 29.) kormányrendelet, illetve a minősített beszerzések Országgyűlés általi mentesítésének kezdeményezésére vonatkozó feltételekről és eljárásról, valamint az ilyen beszerzések megvalósításakor az ajánlatkérő által érvényesítendő követelményekről szóló 492/2015. (XII. 30.) kormányrendelet.

illetve a *védelmi törvény* alkalmazásának kizárására vonatkozó döntése (határozata) alapján a Nemzetbiztonsági Szakszolgálat a „nemzetbiztonsági" feladatokkal közvetlenül összefüggő beszerzések tekintetében a következők szerint folytatja le a beszerzéseket.

Belső eljárásrend szerinti beszerzési eljárás alkalmazására, kifejezetten a Kbt., illetve a védelmi törvény felhatalmazása alapján (törvényi kivételi körök), a nemzetbiztonsági bizottság mentesítése alapján azon beszerzések tekintetében van lehetőség különösen:

– amelyek esetében a törvény alkalmazása olyan információk átadására kötelezné Magyarországot, amelyek felfedése ellentétes az ország biztonságához fűződő alapvető érdekeivel (védelmi törvény);
– amelyek esetében a közbeszerzési szabályok alkalmazása olyan információ átadására kötelezné Magyarországot, amelyek felfedése ellentétes az állam biztonságához fűződő alapvető érdekeivel (Kbt.); illetve
– amelyek esetében Magyarország alapvető biztonsági, nemzetbiztonsági érdekei, a minősített adatok védelme vagy a szükséges különleges biztonsági intézkedések a közbeszerzési eljárásban előírható biztonsági intézkedésekkel nem garantálhatók (Kbt.).

Ezekben az esetekben részletesen a beszerzési eljárás a vonatkozó törvényi előírásokkal analóg módon, azok alapelveinek betartásával, részletes dokumentáltsággal valósul meg, egyetlen alapvető eltérés, hogy a beszerzési eljárás semmilyen módon nem nyilvános.

Speciális esetekben *a hírszerző és elhárító* tevékenység körébe tartozó, úgynevezett *védelmi irányelv*[5] alapján lehetőség van speciális beszerzési eljárás lefolytatására, rendkívül indokolt, egyedi esetekben, amikor a beszerzés jellege egyáltalán nem teszi lehetővé eljárás lefolytatását. Ezen körben gyakorlatilag a Nemzetbiztonsági Szakszolgálat (nyíltan, vagy fedésben) köt közvetlenül szerződést a partnerrel. E beszerzések a védelmi irányelv alapján eleve nem tartoznak sem a Kbt., sem pedig a védelmi törvény hatálya alá, ezért ezek a beszerzések a nemzetbiztonsági bizottsági mentesítés nélkül hajthatók végre.

5 A közbeszerzésekről és a 2004/18/EK irányelv hatályon kívül helyezéséről szóló, az Európai Parlament és a tanács 2014. február 26-i 2014/24/EU irányelve 15. cikk (1) bekezdése és a honvédelem és biztonság területén egyes építési beruházásra, árubeszerzésre és szolgáltatásnyújtásra irányuló, ajánlatkérő szervek vagy ajánlatkérők által odaítélt szerződések odaítélési eljárásainak összehangolásáról, valamint a 2004/17/EK és 2004/18/EK irányelv módosításáról szóló, az Európai Parlament és a tanács 2009. július 13-i 2009/81/EK irányelve.

Összegzés

A polgári nemzetbiztonsági szolgálatok sajátos költségvetési és vagyongazdálkodása a jogszabályban meghatározott alapfeladataik, speciális tevékenységük konspiratív módon történő végrehajtását szolgálja, elősegítve a bűnmegelőzés és bűnfelderítés hatékony végrehajtását.

Hangsúlyozandó, hogy a „titkosszolgálati gazdálkodás" csak és kizárólag a vonatkozó jogszabályokban meghatározott feltételekkel és módon folytatható, a végrehajtást pedig az arra kijelölt szervek ellenőrzik, ezáltal garantálva a törvényes végrehajtást.

DOI: 10.38146/BSZ.2019.1.6

GÉCZI GERGELY

Alkalmazott IT projektmenedzsment-eszközök és -módszerek a Nemzetbiztonsági Szakszolgálat gyakorlatában

A tanulmányban azt szeretném bemutatni, hogy a Nemzetbiztonsági Szakszolgálatnál az elmúlt évtizedek tapasztalatai alapján, a sikereket és a kudarcokat is figyelembe véve, mely IT projektmenedzsment-eszközök és -módszerek alkalmazását tartjuk a leghatékonyabbnak. Hangsúlyozandó, hogy tapasztalataink kizárólag a Nemzetbiztonsági Szakszolgálatra vonatkoznak, vagyis más szervezeti kultúrájú szervezetnél – különösen az üzleti vállalkozásoknál – nyilvánvalóan más módszerek működnek megfelelően. Az alkalmazandó módszereket a mindenkori projektmenedzser szerepét betöltő munkatársnak kell tudnia kiválasztani.

Még mielőtt belekezdenék a mélyebb ismertetésbe, szükséges tisztázni, hogy mit nevezünk projektnek, hogyan ismerjük fel, mely ismérvek alapján kell és lehet megkülönböztetni az üzemeltetési tevékenységektől. Általánosan elfogadott definíció, hogy egy projekt olyan ideiglenes tevékenység, amelyet egy egyedi termék, szolgáltatás vagy egyéb eredmény létrehozása (például építmény) érdekében végeznek. A projekt ismérve, hogy a napi munkavégzéshez képest nagyobb kockázatú, amelyre jellemzők a határidő-, költség- és erőforráskorlátok, valamint a minőségre vonatkozó kívánalmak. Tehát a projekt egy időben jól körülhatárolt feladat, amely a kijelölt világos céloknak megfelelő tevékenységek és a rendelkezésre álló erőforrások összehangolt felhasználásával valósítható meg. A végrehajtás során a számításba vett feltételek, erőforrások megfelelő időben és mennyiségben való rendelkezésre állása szükséges a tervszerű végrehajtáshoz, ha ezek hiányoznak, szükségessé válhat a projekt újratervezése. Előállhat olyan eset is, hogy egy korábban még „projektnek" minősülő tevékenység a napi rutin részévé válik (például egy számítógépes hálózat elemeinek első körös letelepítése még egy projekt része, de annak üzemszerű bővítése, karbantartása már nem). Hasonlóan a know-how, vagy esetleg valamilyen erőforráshiány miatt egy tevékenység inkább lesz projekt, mint üzemeltetési feladat (például számítógépes hálózat bővítése egy új telephellyel).

A Nemzetbiztonsági Szakszolgálatnál a 2000-es években már világossá vált, hogy a projektek megvalósítása során a műszaki kiválóság mellett a

megvalósítás körülményeivel is foglalkozni kell, így egyre szélesebb körben használták a projekt kifejezést. Kezdetben még nem különült el tisztán az üzemeltetési (a projektek utókezelése automatikusan az üzemeltetéssel folytatódott) és a projekt tevékenység, mindez konfliktus forrása volt az üzemeltetői és a fejlesztői területek között.

Tekintettel arra, hogy a szakszolgálat tipikusan lineáris-funkcionális szervezet, ennek megfelelően a tervezési, döntési, vezetési, szervezési, irányítási és ellenőrzési tevékenységek a szervezeten belül – a funkciók szerint –, szakterületenként oszlanak meg. A felső vezetés gyakorolja a döntési jogköröket és állapítja meg a döntési szintek delegálásának módját. A kommunikáció alapvetően vertikális irányú, a horizontális kommunikációt alapvetően az informális kapcsolatok határozzák meg.

A projektek megvalósítását tipikusan keresztfunkcionális csoportok segítségével lehet a legeredményesebben elvégezni, így a horizontális kapcsolatok a projektek megvalósítása során felértékelődnek. A szakirodalom szerint a projektmenedzser szerepe ebben a szervezeti formában elsősorban információgyűjtésből, elemzésből, tanácsadásból és persze adminisztrációból áll, amiből következik, hogy a projektmenedzser befolyása a döntéshozatalra és a döntések végrehajtására a projekt sikeressége szempontjából meghatározó jelentőségű. A másik tipikus szervezeti struktúrából adódó probléma, hogy a projektre delegált munkatársak kétfelé dolgoznak, hiszen a projektmunka mellett a szokásos munkájukat is el kell látniuk. A szakirodalom szerint az említett problémák folyamatosan megszűntek, amint a szervezet (vagy esetünkben annak egy kijelölt része) egyre inkább projektközpontúvá vált. Így jött létre a funkcionális szervezeti struktúrában egy a projektmegvalósítás tevékenységeit különállóan irányító egység a projektekre kijelölt projektmenedzserekkel, mindemellett megtartva az egyéb IT-projektek megvalósítása során fontos funkcionális tevékenységeket (például hálózattervezés, üzleti elemzés, tesztelés). A szervezet alapvető funkcionális struktúrája miatt képes elkerülni, hogy az érdekek ütközésekor a projektérdek háttérbe szorítsa a szakszolgálat által képviselt szakmai érdekeket.

A projektszervezet szerepkörei

A Nemzetbiztonsági Szakszolgálatnál a következőkben bemutatott szerepkörök különböztethetők meg. Kiemelt projekt esetében szükség lehet az adott szerepkör bővítésére, illetve egyes szerepkörökben helyettes kinevezésére.

Kisebb vagy egyszerűbb projekt esetében viszont lehetővé kell tenni bizonyos szerepkörök összevonását. A szerepkörök meghatározására az adott személy hatáskörének és felelősségének egyértelmű beazonosítása céljából került sor.

A stratégiai szintű döntéshozó testület a projektek kiemelkedő szintű monitorozása mellett elősegíti a projektek előrehaladásához szükséges stratégiai döntéseket, kezeli az erőforrásokat, az alacsonyabb szinten felvetődő és nem megoldható nézeteltéréseket.

A projektigazgató képviseli a projektet a szakszolgálaton belül, felel a projekt szakmai végrehajtásáért, a kitűzött célok megadott keretkövetelmények betartásával való eléréséért. Saját hatáskörben intézkedik a felső szintek által meghozott elvi döntések érvényre juttatásáért. A projektigazgatónak teljes felelőssége és hatásköre van a projekt keretén belüli döntések (határidő, erőforrások, hatókör) meghozatalára. Figyelemmel kíséri a projekt előrehaladását, szükség esetén haladéktalanul intézkedik a projekttervekben rögzített feladatok akadályoztatásának felszámolásáról.

A szakszolgálaton belül a projekt által érintett felhasználói terület vezetője (ha van ilyen) képviseli elsősorban a projektben a felhasználói igényeket, kijelöli a szakmai csoportok kulcsfelhasználóit, jóváhagyja a projekttermék éles üzembe állítását, kezdeményezi a felhasználói funkciókat érintő változások végrehajtását.

A projekttámogató Nemzetbiztonsági Szakszolgálaton kívüli gazdasági társaság vezető képviselője a projekt céljait figyelembe véve képviseli a gazdasági társaság érdekeit és jelzi a kockázatokat.

A munkacsoport szakmailag illetékes személyekből álló csoport, tagjai a projektmenedzser, a projektkoordinátor, a kulcsfelhasználók és a szakszolgálaton kívüli gazdasági társaság szakértője. Vezetését a szakszolgálat részéről a projektigazgató által kijelölt projektmenedzser látja el. A munkacsoport ülésezésének a rendjét a projektmenedzser alakítja ki a munkacsoport tagjaival egyeztetve.

A projektmenedzser napi szinten együttműködik a projekt résztvevőivel, összehangolja a munkájukat és megszerzi a szükséges erőforrásokat. A projektigazgató felhatalmazása és a vele való egyeztetés alapján a projektmenedzser felelős a projekt mindennapi irányításáért.

Jogköre és feladatai:

– irányítja a munkacsoportok tevékenységét;
– vélemények alapján intézi a folyó fejlesztéseket;

– ellátja a projekthez kapcsolódó általános adminisztratív feladatokat (időszakos és eseti jelentések, zárójelentés);
– folyamatos kapcsolattartás a munkacsoport tagjaival;
– részletesen megtervezi és ellenőrzi a projektet a célok megvalósulásának érdekében;
– elkészíti és naprakészen tartja a különböző jelentéseket és projekt dokumentumokat (projektterv, ütemterv);
– gondoskodik a kifizetési kérelmek megfelelő időben és tartalommal történő elkészítéséről;
– gondoskodik a projektszintű pénzügyi nyilvántartásról;
– összefogja és szervezi a projekt résztevékenységeit;
– kezeli a projektszintű változásokat (akadályok és lehetőségek skálázása).

A projektkoordinátor napi szinten együttműködik a projektmenedzserrel, és segíti őt az adminisztratív feladatainak ellátásában. Projektkoordinátor szerepkörre akkor van szükség, ha a projektmenedzser a projekt méretéből adódóan önállóan nem képes ellátni a projekt adminisztrálását, vagy az a munkaideje aránytalanul nagy részét tenné ki.
Jogköre és feladatai:
– projektmenedzser helyettesítése annak távollétében;
– a projekthez kapcsolódó általános adminisztrációs, dokumentációs feladatok ellátása (időszakos és eseti jelentések készítése, zárójelentés, kifizetési igénylés);
– folyamatos kapcsolattartás a munkacsoport tagjaival;
– a projekt részletes tervezése, ellenőrzése, a célok megvalósításának érdekében;
– különböző jelentések és projekt dokumentumok elkészítése és naprakészen tartása (például: projektterv, ütemterv);
– kifizetési kérelmek megfelelő időben és tartalommal történő elkészítése;
– projektszintű pénzügyi nyilvántartás karbantartása;
– a rábízott résztevékenységek összefogása és szervezése.

A kulcsfelhasználó a Nemzetbiztonsági Szakszolgálat érintett felhasználói szervezeti egységéből kijelölt személy, aki képviseli a részletekbe menő felhasználói igényeket, részt vesz a kijelölt munkacsoport munkájában és felhasználói szempontból értékeli az elkészült dokumentumokat (például követelményrendszer, átvételi kritérium).

Projektfolyamatok és kapcsolódó dokumentumok

A projektfolyamatok és dokumentumok kialakítása során leginkább a PRINCE2 *(Projects in controlled environments)* ismereteinkre hagyatkoztunk. Egy projekt élettartamának négy fő ciklusa különböztethető meg: előkészítés, tervezés, végrehajtás és zárás. Az életciklus különböző fázisában specifikus dokumentáció elkészítése szükséges. A következőkben bemutatom a projekt-életciklusokat és az azokban elkészítendő dokumentumokat.

Projekt-előkészítési fázis, amelyben felvetődik az igény egy új szoftver megvalósítására vagy egy már meglévőnek a továbbfejlesztésére. Célja az ötlet javaslatként való kidolgozása és az igény pontosítása. A projekt indításának fázisában még nem kerül sor a projektszervezet meghatározására. A Nemzetbiztonsági Szakszolgálat szervezetén belül a felső vezetés által kijelölt személyek a kapott megbízásuk alapján elkészítik a megvalósítási tanulmányt, amely meghatározza a projekt hatókörét *(scope).* Annak jóváhagyása után amennyiben a projekt életképes, azaz az elvárt projekttermék az adott határidőre és a rendelkezésre álló erőforrások alapján megvalósítható, elkészül a projektindító javaslat. Részei a projekttel kapcsolatos műszaki és adminisztratív előírások és a hozzájuk kapcsolódó dokumentációk. A javaslatban meg kell határozni az elérendő eredményeket, a becsült megvalósítási időtartamot, a költségkeretet és az erőforrásigényt. A projektindító javaslat elfogadásával döntés születik a projekt indításáról, és megtörténik a projekt menedzserének megbízása is. A projektindító javaslat jóváhagyása után kezdődik a kapcsolódó beszerzési eljárás.

Az előkészítési fázis a kapcsolódó beszerzési eljárás megkezdésével ér véget, amely magában foglalja a vállalkozási szerződés kötését. A vállalkozási szerződés a projekt során a projekttervvel párhuzamosan kezelendő dokumentum, amely a Nemzetbiztonsági Szakszolgálat és a vállalkozó együttműködésének az alapja.

A tervezési fázis központi irányelve a projektműködés szabályozása, a projektterv elkészítése és a projektszervezet kialakítása. Fő jellemzője a tevékenységek, erőforrások tervezése-ütemezése, integrálása minőségi, illetve biztonsági előírásokkal, adminisztrációval. Lehetőség adódik életciklusellőrehaladás-ellenőrzési tervek készítésére. A sikeres vállalkozási szerződéskötés után a beszerzési eljárás során véglegesített műszaki tartalom alapján lehetséges a végleges projektszervezet kialakítása a szakszolgálaton kívüli gazdasági társasággal. A projektszervezetet a szerződéskötés után lehetőleg harminc napon belül fel kell állítani (ennek elhúzódása esetén ad hoc jellegű lehet a munkavégzés). A projekt kezdetén készül el a projektszervezet műkö-

dését részleteiben szabályozó projektalapító dokumentáció (a projekt során nem vagy ritkán változó elemeket tartalmaz), illetve a projektterv (a projekt során folyamatosan felülvizsgált elemeket tartalmaz). A különböző partnerekkel való együttműködés során a projektalapító dokumentációt és a projekttervet közös dokumentumban hozzuk létre.

A megvalósítási fázis a projektterv megléte, illetve a projektszervezet megalakulása után kezdődhet el. A projekt végrehajtási (implementációs) fázisában történik meg a tervek megvalósítása.

Elengedhetetlen a tevékenységek figyelemmel kísérése és irányítása, valamint az előrehaladás (periodikus) vizsgálata. A projekt legalább egy végrehajtási ciklust tartalmaz, egy ciklus ajánlott maximális hossza három–hat hónap. Kiterjedtebb projektek esetében szükség lehet több párhuzamos végrehajtási ciklus létrehozására is. Kellő figyelmet kell fordítani a projekten belüli változások menedzselésére és a kommunikációs feladatok tervezett végrehajtására.

A felső vezetőket a projekt végrehajtásáról, annak várható befejezéséről a végrehajtási ciklusok lezárásakor, periodikusan (alapértelmezésben havonta), illetve kivételes esetek alkalmával szükséges projekt-előreheladási jelentésben tájékoztatni (értékeli a projekt készültségének fokát, predikciót tartalmaz a várható befejezésre vonatkozóan). A tájékoztatás további formái elsősorban a döntéshozatal elősegítése érdekében:

– emlékeztető;
– tájékoztató jegyzet (elektronikus formában);
– szóbeli tájékoztató;
– egyéb (kivételes jelentés).

A végrehajtási folyamat a projekt zárásának megkezdéséig tart, feltétele a kifejlesztett projekttermék migrációs és implementációs tervek elfogadása, az átadás-átvétel lebonyolítása, továbbá döntés a bevezetésről.

A projekt lezáró fázisában kerül sor az elkészült termék átadására és a végfelhasználók általi elfogadására, a projekt kiértékelésére és a nyomon követési feladatok elvégzésére. A projekt zárására akkor kerülhet sor, ha minden projekttermék elkészült, vagy ha a projekt korai zárása vált szükségessé.

Agilis szemlélet a szoftverfejlesztési projektekben

Egyedi szoftverfejlesztés esetében a végrehajtás fázisában az agilis szoftverfejlesztési módszertanok (elsősorban Scrum és Kanban), valamint a meglévő

tapasztalatok alapján kialakított módszertan szerint történik a munkavégzés. Más természetű projektekkel szemben (például infrastrukturális vagy építési beruházás) napjainkban már kerülendő a vízesésmodell szerinti projektmegvalósítás a szoftverfejlesztésben, tekintve hogy a szoftverekkel kapcsolatos elvárások kevésbé jól követelményesíthetők, mint a több felhasználói visszajelzést lehetővé tevő agilis módszerek esetében.

A fejlesztés résztvevői elfogadják, hogy a követelmények teljes körű, előzetes feltárása és azok „egy lépésben" való megvalósítása (vízesésmodell) helyett hatékonyabb az implementációs fázist előbbre hozni, és a követelmények finomításának részévé tenni.

A fejlesztésben részt vevők ehhez az alapelvhez tartják magukat mindaddig, míg a megadott projekt scope-ját a megadott határokon belül képesek tartani. A költségek és határidők rögzítettek, továbbá a készítendő termékkel kapcsolatos minőségi elvárások is rögzítettek kell hogy maradjanak.

A scope-hoz képesti toleranción túli eltéréseket (például nem megvalósuló funkciók, vagy azok cseréje) mindig adminisztratív síkon dokumentált változáskezeléssel (például szerződésmódosítás) szükséges jóváhagyni, azaz az új scope-ot meghatározni.

A projektet több, rögzített időtartamú iterációra bontjuk fel, amelyeken lehetőleg állandó összetételű csapat dolgozik (vállalkozó és a Nemzetbiztonsági Szakszolgálat), fejlesztési ciklusonként mindenképpen rögzített a határidő és a költségkeret is.

A vállalkozóval kapcsolatos legfontosabb kívánalom, hogy minden fejlesztési ciklus végén tesztelt, működő, az átvételi kritériumoknak megfelelő, dokumentált terméket szállítson le. A minőség tehát a költség- és határidőkényszerekkel együtt rögzített paramétere a projekteknek.

A funkcionális követelmények további finomításával a vállalkozó a szakszolgálat jóváhagyásával készíti el a rendszertervet, és határozza meg a feladatokat. A fejlesztés megkezdése előtt a szakszolgálat témánként fontossági sorrendbe állítja a műszakikövetelmény-rendszerben megfogalmazott feladatokat, a vállalkozó a funkcionális követelmények alapján megbecsüli a feladatok költségét (például munkanapokban). Az így előálló dokumentum *(product backlog)* már tartalmazza az egyes funkciók fejlesztésiidő-becslését is, annak érdekében, hogy a későbbi megvalósítás során az előrehaladás százalékosan mérhető legyen, illetve hogy az esetleges igénymódosítások egyértelműen elszámolhatók legyenek.

A *product backlog*ban szereplő funkciókat lebontják oly módon, hogy egy-egy feladat *(user story)* előzetesen becsült fejlesztésiidő-szükséglete lehetőleg ne legyen több tíz „embernapnál", azaz nyolcvan óránál.

A fejlesztés kéthetes ciklusban *(sprint)* történik. Cél, hogy egy *sprint* alatt a fejlesztőcsapat egy vagy több működő szoftveregységet tudjon létrehozni. A megvalósítandó funkciók kiválasztására a kidolgozott *user story*k közül kerül sor. A *sprint* elején mindig kijelölik azokat a feladatokat, amelyeket a *sprint* során megvalósítanak, annak érdekében, hogy elkerüljük az esetleges üresjáratokat a *sprint*ek kezdetére, így legalább kétsprintnyi fejlesztési időre elegendő funkció kidolgozására kerül sor. A *sprint*ek végén történik annak áttekintése, hogy mely *user story*k készültek el, és melyek nem. Szabály, hogy a *sprint* során az elvégzendő feladatokon nem lehet, nem illik változtatnia egyik félnek sem.

További szabály, hogy ha egy új funkció jelenik meg igényként, akkor annak bekerülése a *product backlog*ba ugyanannyi költségű (fejlesztési idejű) funkció kivételét vonja maga után. Ha egy *sprint* során egy vállalt feladat nem készülne el, akkor azt a következő *sprint*ben újra lehet ütemezi, de ennek nem lehet költségnövekedési vonzata. A sikertelen teljesítésekből fakadó többletköltség a vállalkozót terheli. Amennyiben egy *sprint* során elkészült feladat megfelel az előzetes sikerkritériumoknak, de valamiért mégsem teljesíti az eredeti igényt, akkor azt a feladatot teljesítettnek kell tekinteni, a hozzárendelt költséget el kell számolni, a módosított igényt leíró feladatot új feladatként fel lehet venni, költséget kell rendelni hozzá, és be kell ütemezni a lehető legkorábbi *sprint*be.

Minden *sprint* végén bemutatott és elfogadott feladatok alapján látható, hogyan halad a teljes projekt megvalósítása.

Ha egy projekt hat hónapnál tovább tart, akkor érdemes több fejlesztési ciklusra bontani. A fejlesztési ciklus több *sprint*ből áll, a ciklusok végén kötelezően kell lennie egy integrációs *sprint*ciklusnak is. Minden fejlesztési ciklusban több, funkcionálisan összefüggő, használatba vehető feladat megvalósítására kerül sor.

Az agilis fejlesztések során kiemelt fontosságú a fejlesztő munkacsoportok gördülékeny működése, a munkacsoport tagjai a szakszolgálat és a vállalkozó delegáltjai. Egy projekten belül több munkacsoport is működhet, de kisebb projektek esetében a projekttagok egyben a munkacsoport tagjai is. A szerepkörök elnevezései és funkciói alapvetően a Scrum módszerből kerültek át.

A Product Owner (termékmenedzser) feladata, hogy megfogalmazza azokat a célokat, amelyek eléréséért a fejlesztőcsapat dolgozik. Az ő felelőssége

a termékvízió és a termékjellemzők megfogalmazása és ezek világos, érthető közvetítése a fejlesztő csapatnak. A termékmenedzser végzi a termékfunkciók specifikációját, az ő feladata továbbá a fontossági listán vezetni azokat a *user story*kat, amelyeket a fejlesztői csapatnak meg kell oldania a *sprint*ek alatt. A termékmenedzser egyetlen személy, nem testület. Nagyobb projektekben több termékmenedzser is szerepelhet, de a feladataik között minimális lehet az átfedés. Függetlenül attól, hogy a termék fejlesztése több érdekelt céljait is szolgálja, ezek megértése és az ezek közötti összhang megteremtése, valamint azok konkrét célkitűzésekké alakítása a termékmenedzser mint egyetlen személy felelőssége.

A *Scrum Master* (agilis folyamatot felügyelő személy) szerepét általában a vállalkozói oldal képviselője látja el. Feladata, hogy a csapaton belül mindenki megértse, elfogadja és betartsa az agilis fejlesztés szabályait. A csapat és a csapatot körülvevő szervezet előtt is képviseli a *scrum* alapelveit, figyeli a csapatot érő hatásokat és igyekszik ezeket úgy befolyásolni, hogy azok a csapat hatékony működését szolgálják.

A fejlesztőcsapatot (tesztelők és fejlesztők) azok a szakemberek alkotják, akik előállítják a terméket. A csapat lehetőleg önszerveződő és keresztfunkcionális. A csapaton belül nem szükséges a szerepek megkülönböztetése, mindenki lehet egyszerűen fejlesztő függetlenül attól, hogy valaki gyakrabban, vagy ritkábban végez tesztelési feladatokat. Ideális esetben a csapaton belül nincsenek kisebb csapatok, a csapat egyetlen, oszthatatlan egész.

A projektek során leggyakrabban alkalmazott projektmenedzsment-eszközök

Expert judgement (szakértői vélemény)

Talán a leggyakrabban használt módszer, alapvetően szakértői vélemények összegzését jelenti egy adott témában. Olyan szakértői igény is felvetődhet amely nincs jelen a projektcsapatban, így idesoroljuk a külső cégektől igénybe vett technológiai tanácsadást is. Legnagyobb előnye, hogy segíti a gyors döntéshozatalt, mindamellett érdemes nem csak egy szakértő véleménye alapján megítélni a helyzetet.

Ishikawa-diagram

A más néven halszálkadiagram egy adott probléma ok-okozati összefüggéseit mutatja be. A fő szálakat minden problémához egyedileg definiáljuk. Az Ishikawa-diagram vizuálisan segít megérteni az ok-okozati viszonyokat. A halszálkák meghatározása előtt gyakran egyéb technikák segítségével készül rendszerezetlen lista a lehetséges okokról, ez után ezeket az okokat kategorizálják az Isikawa-diagram segítségével. Felrajzolása gyakran táblára kerül, a megállapított kiváltó okokat dokumentálják.

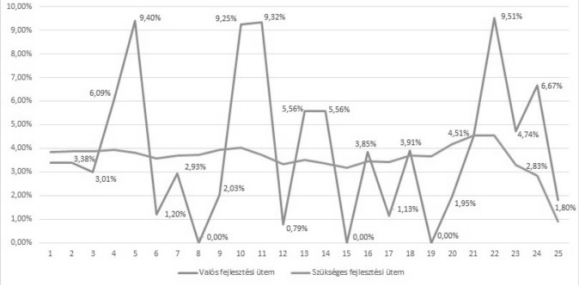
Pareto-diagram

A közismert úgynevezett nyolcvan–húsz szabályon alapszik, amely szerint a problémák nyolcvan százaléka mögött a kiváltó okok húsz százaléka áll. Tehát ez alapján érdemes rangsorolni az okokat, és először a legtöbb problémát okozó húsz százalékkal kell foglalkozni. Az elemzés sikerének kulcsa a „kategóriák" célszerű, szervezetre és tevékenységre jellemző meghatározása. A döntés-előkészítéshez szükséges a grafikus ábrázolás is, a szituációk elemzésekor elégséges az adatok elemzése *(1. számú ábra)*.

A folyamat kiválasztott paramétereinek időbeli (vízszintes tengelyen *sprint*ek sorszáma) alakulását leíró eszköz (például fejlesztés sebessége), amelyet jellemzően vonaldiagram formájában lehet megjeleníteni. Az ábra kiegészíthető egyéb információkkal (például időbeni befejezéshez szükséges fejlesztési sebesség, az elfogadásra és beavatkozásra vonatkozó határok jelö-

1. számú ábra

A fejlesztés sebessége az elvárt fejlesztési sebességhez képest

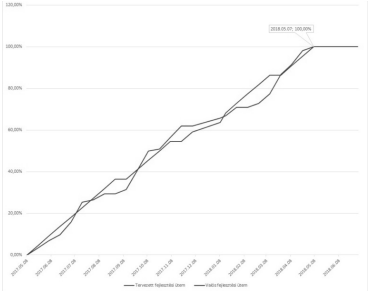


lésével). PMBook* ajánlása szerint hét egymás utáni átlag alatti érték esetén már mindenképpen vizsgálni kell az okokat, tapasztalatunk szerint háromnégy átlag alatt teljesítményű *sprint* esetében (hat-nyolc hét) már érdemes az okokat keresni.

Az agilis fejlesztések során leggyakrabban alkalmazott Burndown diagrammal szemben *(2. számú ábra)* annak fordított (Burnup) ábrázolása, elsősorban a közérthetőség elősegítése miatt. Egyszerre mutatja meg a tervezett (kívánt) és a valós előrehaladást. A vezetői összefoglalók elengedhetetlen kelléke. Segítségével jól ábrázolható a projektek időbeni megvalósulásának alakulása, így az esetleg szükséges beavatkozásokat idejében előre lehet vele jelezni (például erőforráshiány).

2. számú ábra

A fejlesztés valós üteme a tervezetthez képest



Összegzés

Tapasztalatainkat összegezve elmondható, hogy továbbra is igaz a IT projektmenedzsmentben az állítás, hogy leginkább a tervezésen múlik egy projekt sikeressége. Mindamellett a jól megtervezett projektet is működtetni kell (például scope-változások, vagy kockázatok kezelése), mindez pedig akkor lehetséges, ha projektmenedzserek képesek a leghatékonyabb módszerek kiválasztására és használatára.

* http://dinus.ac.id/repository/docs/ajar/PMBOKGuide_5th_Ed.pdf

DOI: 10.38146/BSZ.2019.1.7

BENCSIK BALÁZS

A kiberbiztonsági feladatok kezelése az európai uniós jogalkotás fényében

A XXI. században a társadalom technológiafüggősége, a digitális eszközök és technológia térnyerése olyan jelentős mértékű, hogy mára szinte behálózta az életünk mindennapi tevékenységeit, munkafolyamatait és hivatali ügyintézéseit. A kibertér térnyerésének és a digitális technológia elterjedésének köszönhetően az irodából, otthonról vagy akár útközben is elintézhetjük magán-, illetve munkahelyi feladatainkat. Ha azonban nem megfelelő körültekintéssel, nem tudatosan élünk a technológia adta vívmányokkal, számos veszélyt és fenyegetést is a fejünkre vonhatunk.

Napjainkban egyre elterjedtebbé válik a dolgok internete is (Internet of Things; IoT). Az IoT eszközök képesek kétirányú kommunikációt folytatni más eszközzel, adatokat, információkat továbbítanak nekik, a felhőalapú technológia segítségével eltárolja vagy továbbítani tudja a világ bármely részére. Az IoT technológián alapuló eszközöket okos- vagy smarteszközöknek is nevezzük. Ennek megfelelően IoT eszköz lehet a telefon, számítógép, tablet és a tévé, de ami ennél különlegesebb, hogy már olyan eszközök is felszereltek efféle technológiával, mint például az autó, a villanykörte, a hűtőszekrény vagy akár egyes orvosi eszközök.

Láthatjuk, hogy az életünk minden apró szegmensét behálózzák az okosmegoldások, az IoT technológia, ezért az adataink biztonsága érdekében nagyon fontos, hogy minden eszköz esetében törekedjünk a megfelelő és biztonságos használatra, a biztonsági beállítások körültekintő elvégzésére.

Miután pedig a kibertér az életünk minden apró területén jelen van, ugrásszerűen növekszik a sérülékenységek és támadható eszközök és rendszerek aránya. Egyre gyakoribbak az állami és a civil szektort érő kibertámadások. Világszerte évi négyszázmilliárd dollárra* becsülhető a kiberbűnözők által okozott kár a globális kibertérben.

A 2013-as Ibtv. meghatározása szerint kibertérnek nevezzük a *„globálisan összekapcsolt decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk for-*

* http://www.digitalhungary.hu/interjuk/Teged-is-megloptak/5530/

májában megjelenő társadalmi és gazdasági folyamatok együttesét". Általános jellemzője, hogy globális, folyamatosan bővölő virtuális hálózat, decentralizáltságából fakadóan pedig egyetlen állam által sem szabályozható. Ennek következtében jelentős biztonsági kockázatokat hordoz minden egyes felhasználó számára.

Miért van szükség ilyen átfogó kiberbiztonsági programokra?

A kibertámadásoknak súlyos, a nemzetbiztonság, a gazdaság, illetve a társadalom mindennapi életét veszélyeztető következményei lehetnek. Ezt támasztja alá a Világgazdasági Fórum éves globális kockázati rangsora is, amely szerint a hagyományos veszélyek (háborús konfliktusok, terrorizmus, természeti katasztrófák stb.) mellett a kibertér fenyegetései minden évben egyre előrébb kerülnek.

A probléma olyannyira kritikus, hogy Kanada, Svédország, Norvégia, Finnország, Dánia, Hollandia, Japán, az Egyesült Arab Emírségek, Malajzia és Szingapúr is első helyen említi meg a kibertámadásokat mint amely a legnagyobb veszélyt jelenti a társadalomra és a gazdaságra.

Összetettségét jól jelzi, hogy 2015 óta a kibertámadások két legkiemelkedőbb alkategóriájának tekintjük a kiberkémkedést és az adatlopást, amelyeknek főleg a gazdasági következményei jelentősek.

Globális fenyegetések

Az Europol fenyegetésértékelése szerint megfigyelhető a kiberbűnözés és a „hagyományos" bűnözés közötti határvonal elmosódása, hiszen a bűnözők számára az internet megfelelő felület a tevékenységük kiterjesztésére, illetve további eszközöket kínál a bűncselekmények elkövetéséhez. Az internet nyújtotta anonimitás és személytelenség biztonságot ad és bátorítja a bűnözőket, illetve nagyon megnehezíti, szinte lehetetlenné teszi a nyomon követésüket és az igazságszolgáltatás elé állításukat.

A 2017. májusi zsarolóvírus-hadjárat mutatja igazán a támadás egyes ágazatokra és az országokra gyakorolt valós hatását, hiszen több mint százötven országban, több mint százkilencvenezer rendszert érintett, beleértve például a kórházak feladatait. A korábbiakban jellemző számítógépes kártevők célja

főként az adatlopás vagy a kritikus rendszerek megbénítása, valamint a zombihálózatok bővítése volt, napjainkban viszont az olyan károkozók elterjedése figyelhető meg, amelyek fájlokat tiltanak le, alkalmazásokat zárnak le, a feloldásukért pedig pénzt követelnek a felhasználótól. Az egyik ilyen kiemelkedő támadássorozat volt az elmúlt időszakban a WannaCry zsarolóvírushullám 2017 májusában, amely az elmúlt évek eddigi legnagyobb és legtöbb felhasználót és szervezetet elérő támadássorozata volt.

A vírus gyors terjedésének legfőbb oka egy a Windows minden verziójában megtalálható (az XP-től a Windows 10-ig bezárólag) sebezhetőség volt. Ez önmagában még nem lett volna elég a kártevő térnyeréséhez, ehhez jelentősen hozzájárultak a felhasználók. A Microsoft már március közepén kiadta a sérülékenység javítására szolgáló frissítést, amelynek számítógépére telepítését számos felhasználó nem engedélyezte, elhalasztotta vagy figyelmen kívül hagyta. Ennek következtében több héttel a vírus felbukkanása után még mindig jó néhány olyan Windows-alapú számítógép akadt, amelyre nem került fel a sérülékenységet kijavító és a kártevő elkerüléséhez szükséges frissítés.

A kártevő hihetetlen sebességgel söpört végig az egész világon, felmérhetetlen károkat okozva cégeknek, szervezeteknek és magánszemélyeknek.

2016 folyamán egy trójai típusú káros kód elterjedésének lehettünk tanúi, amely szintén Windows-alapú operációs rendszereket támadott. Az áldozatok bitcoinban fizetendő díj ellenében kapták meg a támadótól a kódot a saját rendszerükhöz. Hasonló támadást észleltek 2017-ben is a WannaCry-hullám után, és ez még a WannaCrynál is gyorsabban terjedt. Kéretlen leveleken keresztül jutott el az áldozatokhoz, titkosította a felhasználó merevlemezének adatait, majd a titkosított jelszót, feloldó kulcsot díj ellenében kínálta a felhasználónak. A Petya elnevezésű kártevő főként Ukrajnát támadta, onnan is indult ki a MEDoc nevű ukrán cég egyik platformjának feltörésével, a cég nevében számtalan fertőzött e-mailt küldtek, valamint a MEDoc gépéről megszerezték a felhasználóik belépési adatait. A MEDoctól így megszerzett adatokat is titkosította, és a helyreállításért, a feloldókulcsért kriptovalutát kért a támadó vírus. Aztán a szakértők gyorsan rájöttek, hogy itt már nem a pénzügyi haszonszerzés volt a cél, inkább a káoszkeltés és a gazdasági károkozás, elsősorban Ukrajnában. A Petya aktívan terjedt világszerte, így további jelentős károkat okozott még Oroszországban, Lengyelországban, Olaszországban és Németországban is.

Megfertőződött egyebek kötött a csernobili atomerőmű állapotát monitorozó rendszer, a kijevi reptér biztonsági rendszere és a kormányzati infrastruktúra is, valamint az orosz Rosznyefty egyik rendszere is. De érintett volt

az Oreót gyártó Mondelez cég, a Mars, a Nivea, valamint az OTP Bank ukrán leányvállalata is. Ekkor már egyértelmű volt, hogy ez már nem kifejezetten a Petya nevű kártevő, inkább egy pusztításra törekvő, törlő fertőzésről van szó *(wiper),* amelynek esetében nem lehet visszaállítani az adatokat, mivel a vírus „eldobja" a feloldókulcsot, az csak álca volt. Ennek a fertőzésnek a hivatalos neve PetrWrap lett.

A felhasználók és a vállalatok

Ma már mindenki tisztában van vele, hogy a kibertér lehet a modern világ új hadszíntere. Nemcsak a bűnözők, hanem egyes nagyhatalmak is egyre gyakrabban nem a hagyományos eszközökkel, hanem diszkrétebb, kibereszközökkel szereznek érvényt akaratuknak és céljaiknak, például a belső demokratikus folyamatokba történő beavatkozás útján. Egyre inkább terjednek a dezinformációs kampányok, álhírek és kritikus infrastruktúrák elleni kiberműveletek, és az eddigi gyakorlatunktól eltérő válaszreakciót igényelnek. Az új technológiák terjedése és ugrásszerű fejlődése tovább fogja gazdagítani a kibertérben rossz szándékúan, támadásra vagy befolyásolásra felhasználható eszközöket és szolgáltatásokat.

Ez is bizonyítja, hogy a digitális átalakulással és fejlődéssel egyidejűleg egyre jelentősebb és változatosabb fenyegetésekkel kell szembenézünk, ezért kiemelkedő fontosságú a megfelelő kiberbiztonsági környezet és szabályok kialakítása. Elengedhetetlen a társadalmunk és gazdaságunk számára kulcsfontosságú hálózatok és szolgáltatások vonatkozásában a megfelelő kiberbiztonsági intézkedések megvalósítása. Az e szolgáltatásokat érő támadások vagy incidensek felmérhetetlen károkat okozhatnak, valamint visszavethetik a fogyasztók új technológiák iránti bizalmát.

A veszélyeztetettséget nemcsak vállalati hálózatok és szabályok, hanem a felhasználók szintjén is szükséges kezelni, hiszen mint minden rendszerben, itt is az ember a leggyengébb láncszem. Az Eurostat 2016-os felmérése szerint az unió polgárainak a hetvenegy százaléka megosztott már online valamilyen személyes adatot. A leggyakrabban megosztott adattípusok a kapcsolattartási adatok voltak (az internethasználók hatvanegy százaléka), majd következnek a személyes adatok, például név, születési idő vagy személyi igazolvány száma (52 százalék) és fizetési adatok, például hitel-/betéti kártya vagy bankszámla száma (40 százalék).

A felmérés kimutatja továbbá, hogy az uniós állampolgárok több mint ötöde (22 százalék) szolgáltatott már ki más személyes adatokat, például fényképeket, vagy az egészségükre, a foglalkozásukra vagy a jövedelmükre vonatkozó információkat különböző online felületeken.

Az említett felmérés eredményei szerint a fiatalabb generációk könnyebben elérhetővé teszik személyes adataikat, ugyanis a 16–24 éves internethasználók több mint háromnegyede (78 százalék) osztott meg valamilyen személyes információt online, szemben a 65 és 74 év közötti felhasználók 57 százalékával.

A felhasználókon túl a vállalatoknak, szervezeteknek is modern, napjaink próbáinak megfelelő információbiztonsági technológiával és szabályrendszerrel kell bírniuk az adataik, rendszerek és dolgozóik biztonsága érdekében. Az Eurostat-felmérés az állampolgárok, azaz a felhasználók szokásain túl megvizsgálta a vállalatok digitális szokásait is. E szerint napjainkban az unióban működő összes vállalkozás (98 százalék) használ számítógépeket, és közülük csak 31 százaléknak van formálisan meghatározott informatikai biztonságpolitikája, belső szabályozása. A felméréshez Magyarországról kapott adatok szerint a kis- és közepes vállalatok mindössze kilenc százalékának volt biztonsági politikája, a nagyvállalatok esetében ez az arány ötven százalék.

Az Eurostat-felmérés eredményeiből kitűnik, hogy a biztonságos és tudatos digitális jelenlét terén még jelentős fejlődésre van szükség az állampolgárok és a vállalatok szintjén egyaránt. E cél elérésének számos módja lehet, a folyamatos oktatástól, tudatosítástól egészen a szigorú jogszabályok és ellenőrzési mechanizmusok kialakításáig.

Az unió válasza a növekvő próbatételekre

Az IKT piaca jellemzői

Jelenleg az Európai Unióban az infokommunikációs szektor alapjai döntő mértékben harmadik országokban fejlesztett és gyártott hardvereszközök, illetve szoftverek, mindez egyes területeken monopolisztikus vagy oligopolisztikus ellátási láncok kialakulásához vezetett. Ezek az infokommunikációs rendszerek ma már csak biztonságtudatos módon fejleszthetők és üzemeltethetők a kibertérben folyamatosan jelen lévő fenyegetettség miatt. A gyártói biztonságtudatosság, a számítógép-biztonsági és -incidenskezelő csoportok *(Computer Security Incident Response Team; CSIRT)* hálózata, illetve a kibervédelmi jogszabályok lehetővé teszik a kibertámadásokból adódó koc-

kázatok bizonyos mértékű kezelését. A legnagyobb probléma az, hogy a kibertérben nem érvényesül az arányosság elve: a kétszer nagyobb tűzfal nem jelent kétszer nagyobb védelmet, sőt egy apró hiba egy teljes infokommunikációs ökoszisztémát tehet ki potenciális támadásoknak a hiba javításáig, amely hónapokig is elhúzódhat.

Az infokommunikációs szektorban a termékek és szolgáltatások kiemelkedően magas innovációs tartalmának, illetve az internet globalitása miatti mobilitásnak köszönhetően kiemelkedő a gyártói koncentráció. Néhány nagyvállalat – sok esetben állami támogatás és összefonódás mellett – oligopolisztikus piacot alakított ki világszerte, ezért gyakorlatilag megkerülhetetlenné váltak az infokommunikációs rendszerek biztonságának garantálása szempontjából. E gyártók és szolgáltatók döntően nem uniós tagállamokban működnek.

Az Európai Bizottság 2017 szeptemberében átfogó, ambiciózus kiberbiztonsági csomagot bocsátott ki, amely a megnövekedett kiberfenyegetésekre, valamint az egységes digitális piac elérésének akadályaira kíván megfelelő válaszokat, mechanizmusokat és jogi garanciákat alkotni.

A kiberbiztonsági csomag magában foglalja a bizottság közleményét a felülvizsgált uniós kiberbiztonsági stratégiáról, egy jogszabályjavaslatot, az úgynevezett kiberbiztonsági jogszabályt *(Cybersecurity Act),* amely az Európai Unió Hálózat- és Információbiztonsági Ügynöksége *(European Union Agency for Network and Information Security; ENISA)* mandátumának felülvizsgálatára vonatkozik, az európai kiberbiztonsági ügynökség létrehozásával, továbbá a kiberbiztonsági tanúsítás kérdéskörével kapcsolatos rendelkezéseket. A csomag része az úgynevezett blueprintre vonatkozó bizottsági ajánlás is, amely ismerteti, hogy a kiberbiztonságot miként illesztik be a meglévő uniós szintű válságkezelési mechanizmusokba, és meghatározza a tagállamok egymás közötti, valamint a tagállamok és az illetékes uniós intézmények, szervezeti egységek, ügynökségek és testületek együttműködésének céljait és módszereit a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre reagálás terén.

Fontos kiemelni, hogy kibertérből érkező fenyegetések az egyes államok számos különböző működési területét érintik, ezért nem lehet meghatározni olyan univerzális védekezési stratégiát, amely egyaránt hatékony az infokommunikációs gyártók hibáiból eredő sérülékenységek, a bűnözői csoportok támadásai, illetve potens állami szereplők által kifejtett offenzív tevékenységek ellen. A fenyegetések potenciális hatásainak felmérése is problematikus terület, mivel nehéz rangsorolni a veszteség súlyossága szempontjából egy milli-

árdos gazdasági kémkedési ügyet, egy emberéleteket követelő ipari kiberszabotázs akciót, illetve a kibertérben a demokratikus választási rendszer befolyásolására tett kísérletet. Sajátos veszélyforrás a szuverén állam polgáraival szemben tömegesen elkövetett illegális adatgyűjtés, ami a személyes adatok megsértéséhez, sőt akár az állampolgárok döntéseinek tömeges manipulációjához, és a demokratikus értékek sérüléséhez is vezethet.

A kiberbiztonsági támadások, fenyegetések nem maradnak országhatárokon belül, ezért törekedni kell arra, hogy olyan szabályozásokat fogalmazzunk meg, amelyek nemzetközi szintűek és a világ minden részén egységesen alkalmazhatók. Ennek megfelelően a határon túli, nemzetközi együttműködés kérdéskörét is elsőrendűként kezeli a kiberbiztonsági csomag, így célkitűzésként fogalmazza meg az EU–NATO-együttműködés elmélyítését, a nemzetközi regionális és bilaterális kapcsolatokban a kiberbiztonság, válságkezelés és -megelőzés terén történő együttműködést, valamint a harmadik országokkal történő együttműködés során a kapacitásépítés támogatását és a jó tapasztalatok megosztását.

A csomag számos javaslatot fogalmaz meg a kiberbűnüldözés terén történő együttműködés, a kibertámadás elhárításának a kidolgozására, az állami és magánszektor együttműködésének elősegítésére, a kutatás-fejlesztés terén megvalósítandó együttműködésre, valamint a kiberkészségbázis létrehozására.
A továbbiakban az itt vázolt kibercsomag egyes témáit és elemeit ismertetem.

Biztonsági tanúsítási keretrendszer

Az informatika gyorsan változó iparág, egyes területein elengedhetetlenül fontos az új technológiákhoz való hozzáférés (például tudományos munkák, programozás stb.). Tagadhatatlan, hogy a kiberbiztonsági csomag egyes javaslataival az unió területén működő szervezetek némi hátrányba és időhátrányba kerülhetnek, például a tanúsítás szükségessége miatt az engedélyeztetési folyamat következtében. Mindamellett nagyon fontos a gyors változások megfelelő és állandó követése, figyelése, az azokra való felkészülés hálózatbiztonsági szempontból, hiszen az egyes biztonsági események, működésben bekövetkező sérülések, meghibásodások, továbbá a támadások jelentős hányada éppen a legújabb fejlesztések és változások miatt következik be, nem kismértékben a nem kellő védelmi felkészültség okán.

A kialakítandó tanúsítási keretrendszer célja, hogy az egységes tanúsítás bevezetésével javuljon a termékek és szolgáltatások biztonsága, tájékoztassa és meggyőzze az állampolgárokat az érintett infokommunikációs termékek

és szolgáltatások biztonsági tulajdonságairól, ezzel növelve a beléjük vetett bizalmat. Hosszú távon ez az uniós piac fellendüléséhez vezethet. A javaslat egyik ambíciója, hogy a biztonsági aspektus már a kezdeti szakaszban, a termékek és szolgáltatások tervezése és fejlesztése során is figyelembe veendő szempont legyen, így megvalósulhasson az úgynevezett „secured by design", azaz a tervezett biztonság elve.

Ezért a kiberbiztonsági csomag javaslatot fogalmaz meg a tanúsítás kérdéskörének uniós szintű szabályozására is.

Ennek megfelelően az Európai Unió egy jogszabályjavaslat keretében létrehozza az európai kiberbiztonsági tanúsítási keretrendszert az infokommunikációs termékekre és szolgáltatásokra vonatkozóan.

Az európai kiberbiztonsági tanúsítási keretrendszer általános célja annak igazolása, hogy a keretrendszer szabályainak megfelelően tanúsított infokommunikációs termékek és szolgáltatások megfelelnek a meghatározott kiberbiztonsági követelményeknek. Ebbe beletartozna például a (tárolt, továbbított vagy más módon feldolgozott) adatok védelmének képessége a véletlen vagy illetéktelen tárolással, feldolgozással, hozzáféréssel, nyilvánosságra hozatallal, megsemmisítéssel, véletlen elvesztéssel vagy módosítással szemben.

A keretrendszer létrehozása lehetővé teszi majd egyfelől, hogy az ilyen rendszerek részeként kiállított tanúsítványok minden tagállamban érvényesek legyenek, illetve minden tagállam elismerje őket, továbbá megfelelő megoldást kínálna a piac jelenlegi széttagoltságának problémáira.

Az unió kiberbiztonsági tanúsítási keretszabályozása a meglévő szabványokra hagyatkozna, azokra a technológiai követelményekre és értékelő eljárásokra, amelyeknek jelenleg minden terméknek meg kell felelnie egyes tagállamokban, és nem egy teljesen új uniós technológiai szabványt dolgoznának ki.

A jogszabály nem vezet be közvetlenül működőképes tanúsítási rendszereket, ehelyett egy úgynevezett keretrendszert alakít ki az infokommunikációs termékekre és szolgáltatásokra vonatkozó egyedi tanúsítási rendszerek (európai kiberbiztonsági tanúsítási rendszerek) létrehozásához. A bizottság felkérésére az európai kiberbiztonsági tanúsítási rendszerek kidolgozása az ENISA feladata az európai kiberbiztonsági tanúsítási csoport segítségével. Az így elkészülő tanúsítási rendszereket a bizottság fogadja el hivatalosan végrehajtási jogi aktusok által.

Az ilyen rendszereknek olyan konkrét elemet kell tartalmazniuk, mint az érintett termékek és szolgáltatások kategóriáinak azonosítása, a kiberbiztonsági követelmények részletes leírása (szabványok vagy műszaki előírások), a

konkrét értékelési kritériumok és módszerek, valamint a biztonság elérendő szintje (alapvető, jelentős vagy magas).

A javaslatban foglaltak szerint a szabályozás ellenőrzési, felügyeleti és végrehajtási feladatai a tagállamokra hárulnak. Ennek érdekében a tagállamoknak létre kell hozniuk egy nemzeti tanúsításfelügyeleti hatóságot, amelynek feladata, hogy felügyelje, a tagállam területén letelepedett megfelelőségértékelő szervezetek és az általuk kiállított tanúsítványok megfelelnek-e a rendelet előírásainak és a vonatkozó európai kiberbiztonsági tanúsítási rendszereknek. A nemzeti tanúsításfelügyeleti hatóságok illetékesek a tagállam területén letelepedett megfelelőségértékelő szervezetek által kiállított tanúsítványokkal kapcsolatos, természetes és jogi személyek által benyújtott panaszok kezelésére egyaránt.

Végül pedig a javaslat létrehozza az európai kiberbiztonsági tanúsítási csoportot, amely az egyes tagállamok nemzeti tanúsításfelügyeleti hatóságaiból áll. A csoport fő feladata, hogy tanácsot adjon a bizottságnak a kiberbiztonsági tanúsítási politikát érintő kérdésekben, és együttműködjön az ENISA-val az európai kiberbiztonsági tanúsítási rendszerek tervezetének kidolgozásában. A jogszabálytervezet szerint az ENISA feladatai közé tartozik majd, hogy ellássa az európai kiberbiztonsági tanúsítási csoport titkársági feladatait, illetve hogy a nyilvánosság számára elérhető, naprakész nyilvántartást vezessen az európai kiberbiztonsági tanúsítási keretrendszer részeként jóváhagyott rendszerekről. Az ENISA a szabványtestületekkel is kapcsolatot tartana, hogy elősegítse a jóváhagyott rendszerekben használt szabványok megfelelőségét, és hogy azonosítsa a kiberbiztonsági szabványokat igénylő területeket.

Kiberdiplomácia

A 2017 júliusában elfogadott, a rossz szándékú kibertevékenységekkel kapcsolatos közös uniós diplomáciai intézkedések uniós kerete (úgynevezett „kiberdiplomáciai eszköztár") létrehoz egy a közös kül- és biztonságpolitika keretébe tartozó intézkedésgyűjteményt, mely intézkedések az EU politikai, biztonsági és gazdasági érdekeit sértő kibertevékenységekre adott reakciók, válaszok erősítését hivatottak megvalósítani. Ez az eszköztár a bilaterális diplomáciai vagy politikai egyeztetéstől egészen a szigorú, akár gazdasági korlátozó intézkedésekig számos különböző erősségű és hatású reagálási lehetőséget fogalmaz meg. A keretrendszer fontos lépés az uniós és tagállami szintű jelző- és reagálási kapacitások fejlesztésében. Az eszköztár hosszú távon hoz-

zájárul a konfliktusok megelőzéséhez, a kiberbiztonságot fenyegető veszélyek mérsékléséhez, illetve a nemzetközi kapcsolatok stabilitásának a növekedéséhez egyaránt. Remélhetőleg az eszközök használata visszatartó erejű lesz a lehetséges agresszorok magatartására, így hosszú távon csökkenteni fogja a támadások és kiberincidenesek számát. Az eszköztár alkalmazása kapcsán kiemelendő, hogy a rossz szándékú kibertevékenységekkel szemben az „arányos reagálás" elvét szükséges betartani. A támadás állami vagy nem állami szereplőknek tulajdonítása a továbbiakban is a minden forrást igénybe vevő hírszerzésre alapított, szuverén politikai döntés marad.

Az EU–NATO-együttműködés fontossága

A kiberbiztonság kérdéskörét és a kibertérbeli stabilitás garantálását elsőrangúként kezeli az EU és a NATO egyaránt. Ennek megfelelően 2016. július 8-án sor került egy közös EU–NATO-nyilatkozat elfogadására a kiberbiztonság, a hibrid fenyegetések és védelem terén történő együttműködési célok megfogalmazására. A stratégia célja az unió és a NATO közötti együttműködés kibővítése, a párhuzamos és összehangolt EU–NATO-gyakorlatok szervezésével, illetve a kiberbiztonsági követelmények és szabványok kölcsönös átjárhatóságának megteremtésével.

A hibrid fenyegetések vonatkozásában a stratégia célja a már korábban létrejött együttműködések és közös erőfeszítések – különösen a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport és a NATO hibrid fenyegetéseket elemző csoportja közötti együttműködés – elmélyítése, élénkítése az ellenálló képesség és a kiberválságokra való reagálás erősítése érdekében.

A kiberbiztonsági vészhelyzet-elhárítási mechanizmus és a kiberbiztonsági vészhelyzet-elhárítási alap

Mivel egyes kiberbiztonsági incidensek jelentős hatással lehetnek akár a gazdaság működésére és az emberek mindennapi életére, ezért fontos megfontolni egy vészhelyzeti válságmechanizmus kidolgozását, illetve a létező biztonságpolitikai válságmechanizmusok kiberbiztonságra történő kiterjesztését.

A kibercsomag része az a tervezet is, amely vázolja a kiberbiztonsági szempontok beillesztését az integrált uniós politikai válságreagálási rendszerébe, illetve az EU általános riasztási rendszereibe.

A kiberbiztonsági aspektus válságmechanizmusokba való hatékony beillesztésén túl fontos lenne egy kiberbiztonsági vészhelyzet-elhárítási alap lét-

rehozása is, a más uniós biztonságpolitikai területeken meglévő hasonló válságmechanizmusokhoz kapcsolódó alapok példája nyomán. Az alap lehetővé tenné, hogy egy jelentősebb és átfogóbb incidens esetén vagy utána a tagállamok támogatást, segítséget kérjenek a gyors reagálás megvalósításához, vagy a vészhelyzeti válaszlépések finanszírozására.

Természetesen az alap felhasználására csak azoknak a tagállamoknak nyílna lehetőségük, amelyek az uniós előírásoknak és szabályoknak megfelelő kiberbiztonsági rendszert alakítottak ki (még az incidens bekövetkezése előtt), megfelelően végrehajtották a hálózati és információs rendszerek biztonságának az egész unióban egységesen kimagasló szintjét biztosító intézkedésekről szóló, az Európai Parlament és a tanács (EU) 2016/1148 irányelve (2016. július 6.) rendelkezéseit, illetve fejlett nemzeti kockázatkezelési és felügyeleti keretrendszerük van.

Kiberbiztonsági kompetenciahálózat
és az európai kiberbiztonsági kutatási és kompetenciaközpont

Az EU-stratégia napirendjére tűzte a kutatás- és kompetenciafejlesztés fellendítésének és uniós szinten történő koordinálásának kérdéskörét is. Alapvető cél, hogy uniós szinten fejlesszék a közösség digitális gazdasága, társadalma és demokráciája biztonsága érdekében kulcsfontosságú kritikus infrastruktúrákat és digitális szolgáltatásokat egyaránt.

Ez a kormányzati és magánszféra együttműködésével, az akadémia és a kutatás-fejlesztési területek bevonásával valósulhat meg a leghatékonyabban. A PPP-együttműködés fontosságát már a korábbi stratégiai dokumentumok is kiemelt célként fogalmazták meg. A bizottság előrejelzése szerint a köz- és magánszféra közötti kiberbiztonsági partnerség 2020-ig várhatóan 1,8 milliárd euró befektetést generál. A világ más területein ezt jelentősen meghaladja az együttműködésbe befektetett összeg. Az Egyesült Államokban például tizenkilencmilliárd dollárt szánnak a kiberkutatás-fejlesztésre a Fehér Ház által kiadott 2016. évi „kiberbiztonsági intézkedési terv" alapján.

Az Európai Unió a kiberbiztonsági képességének megerősítése céljából az uniós tagállamok kiberbiztonsági kompetenciaközpontjainak hálózatba szervezését tervezi, valamint létre szándékozik hozni a hálózat központjául szolgáló úgynevezett európai kiberbiztonsági kutatási és kompetenciaközpontot. Ez a hálózat és annak központja serkentené a kiberbiztonság területén a technológia fejlesztését és bevetését, segítené a kutatás-fejlesztési támogatások hatékony elosztását, uniós és nemzeti szinten kiegészítené a terület kapacitás-

építési erőfeszítéseit, valamint lehetőséget nyújtana nagyobb kutatás-fejlesztési projektek megvalósítására több tagállam kutatóközpontjainak közös kezdeményezéseként.

Első lépésként a bizottság a nemzeti központok hálózatba szervezését szeretné megkezdeni. A pilot projektként funkcionáló első szakaszban a Horizon2020 keretből ötvenmillió eurót fordítana a hálózat kialakítására.

A tervezet szerint a jövőben a kutatási területek a következő generációs digitális technológiák fejlesztésére is fókuszálnának, lefedve így a mesterséges intelligenciát, a kvantum-számítástechnikát, a blokkláncot és a biztonságos digitális személyazonosságot.

Kiberkészségbázis kiépítése

A 2017. évi Global Information Security Workforce tanulmány alapján előrejelzések szerint a kiberbiztonságiszakember-hiány a privát szektorban 2022-re 350 ezer fő lesz, de globális szinten elérheti akár az egymilliót is. E probléma megoldása érdekében fejleszteni kell a kiberbiztonsági oktatást. Szükség van még több kiberbiztonsági szakember képzésére, az infokommunikációs szakemberek kiegészítő kiberbiztonsági képzése, illetve új kiberbiztonsági szakképzések útján.

A szakemberek képzésén túl fontos, hogy a többi szakterület (például mérnöki tevékenység, közoktatási, menedzsment vagy jog) oktatási tervébe is be kell építeni alapvető kiberbiztonsági tananyagot, aminek célja, hogy más specifikus szakterületeken is beépüljön a jövő szakembereinek a gondolkodásába a biztonsági aspektus figyelembevételének fontossága, illetve hogy a munkájuk és mindennapi életük során tudatosan és biztonságosan mozogjanak a kibertérben.

A kiberbiztonság fontosságának megértését, tudatosítását, a kiberbűnözés veszélyeinek ismertetését, az alapvető digitális készségek és tudás elsajátítását már az általános és középiskolai tanulmányok idején meg kell kezdeni. Ez a folyamat segítheti hozzá a tanulókat ahhoz, hogy a későbbiekben tudatosan, biztonságosan és megfontoltan használhassák a digitális szolgáltatásokat és eszközöket a kibertérben.

Az Európai Unió célkitűzései között szerepel, hogy kialakít egy uniós szintű egységes portált, amelyen összegyűjti az összes tudatosításra alkalmas eszközt egy úgynevezett egyablakos rendszerben, tanácsot adva a felhasználóknak az egyes támadások, fertőzések megelőzéséhez, elkerüléséhez és észleléséhez. A portálon javaslatokat, információkat és segítséget találhatnának

a felhasználók arra vonatkozóan, hogy mi a teendő, ha valamilyen informatikai támadás áldozatául esnek, IT-biztonsági incidens elszenvedői lesznek, továbbá a portálon elérhetővé lehetne tenni az ilyen események esetében szükséges bejelentési mechanizmusok elérhetőségeit, linkjeit.

Az állampolgárok oktatása, tudatosítása, képességeinek folyamatos fejlesztése kiemelkedő fontosságú, hiszen az incidensek 95 százalékát valamilyen szándékos vagy nem szándékos emberi tévesztés, hiba vagy figyelmetlenség idézi elő. Ezért fontos felismernünk és minden szervezetben és természetes személyben tudatosítanunk, hogy a kiberbiztonság mindannyiunk felelőssége. Ennek megfelelően a személyes, vállalati és közigazgatási szinten egyaránt egy olyan figyelmes és tudatos magatartásnak (kiberhigiénés szokásrendszernek) kell kialakulnia, amikor is minden résztvevő megérti az aktuális fenyegetéseket, és megfelelő eszközei és képességei vannak a támadások felismerésére és a hatékony védekezésre.

Az uniónak és a tagállamoknak kiemelt fontosságúként kell kezelniük a kiberbiztonsági tudatosítást, a tudatosság fejlesztését. Ezt javasolt megvalósítani kifejezetten az iskolák, az egyetemek, az üzleti közösség és a kutatási szervek számára kidolgozott célzott tudatosító kampányok idején. Az kibercsomag célja az ENISA által 2012 óta minden év októberében tartott kiberbiztonsági hónap kampány (ECSM) folyamatos bővítése és frissítése annak érdekében, hogy a kampány mindig az aktuális trendekre és fenyegetésekre hívhassa fel az állampolgárok figyelmét, illetve hogy minél szélesebb közönséget tudjon hatékonyan megszólítani. A tudatosítás témakör esetében fontos felhívni a figyelmet az online félretájékoztató kampányok és a közösségi médiában megjelenő álhírek káros hatásaira. A tagállamoknak közösen, a meglévő tapasztalataikat egymással megosztva kell szembenézniük ezekkel a nehézségekkel, egyebek között a 2019-es európai parlamenti választásra való felkészülés kapcsán.

Összegzés

A digitális technológia megállíthatatlan fejlődése és a kibertér életünk minden területére történő kiterjedése megállíthatatlan folyamat. Ez a fejlődés számos lehetőséget és egyben veszélyt is hordoz magában.

A fejlődést nem lelassítani vagy megállítani kell, hanem meg kell próbálni ahhoz alkalmazkodni, kihasználni a benne rejlő lehetőségeket és előnyö-

ket. Nagyon fontos, hogy ebben az új, fejlett digitális technológiával teli világban megtanuljunk biztonságosan és magabiztosan mozogni.

Ennek megvalósítása érdekében az államoknak, vállalatoknak, fejlesztőknek, gyártóknak, szolgáltatóknak, állampolgároknak/felhasználóknak, sőt még a nemzetközi szervezeteknek, közösségeknek is fel kell ismerniük a szerepüket és felelősségüket.

Az Európai Bizottság által megfogalmazott kibercsomag-koncepció számos kulcsfontosságú, egymásra épülő és egymást kiegészítő intézkedést azonosított.

Sajnos nem elég a szigorú jogszabályok megalkotása, ellenőrzése és szankcionálása ezen a területen, hiszen a kiberbiztonság megteremtése és fenntartása az információbiztonságban érintett valamennyi szereplő közös felelőssége, és ennek megvalósítása elképzelhetetlen a felek együttműködése nélkül.

IRODALOM

https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

http://www.digitalhungary.hu/interjuk/Teged-is-megloptak/5530/

https://www.enisa.europa.eu/publications/european-cyber-security-month-2017

http://ec.europa.eu/eurostat/cache/infographs/ict/

https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

https://mno.hu/belfold/vilaghodito-utjara-indult-petya-a-zsarolovirus-2405259

https://kiberhonap.hu/

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

https://pcworld.hu/pcwlite/ujabb-durva-zsarolovirus-pusztit-europaban-es-amerikaban-230639.html

http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#hide/fn-1

JOGSZABÁLYOK

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály") szóló rendelettervezet

Ellenálló képesség, elrettentés, védelem: az unió erőteljes kiberbiztonságának kiépítése vonatkozásában. Az Európai Parlament és a tanács közös közleménye.
http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

Az Európai Parlament és a tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről.
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU

A tanács következtetései a kiberdiplomáciáról, 2015.
http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf

A tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről, 2017.
http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

DOI: 10.38146/BSZ.2019.1.8

TATÁR ZOLTÁN – OSZTERTÁG JÁNOS – MORBER SZILÁRD KRISZTIÁN

Technikai szakértői szakterület fejlődése a feladatok tükrében

A Nemzetbiztonsági Szakszolgálat Szakértői Intézet technikai szakértői osztálya – külön jogszabály rendelkezései szerint – országos hatáskörrel igazságügyi szakértői tevékenységet végez a nyomozó hatóságok, bíróságok, egyéb szervek megkeresései alapján. Szakértői feladataink jelentős része kiemelt, országos szinten figyelemmel kísért büntetőügyekhez kapcsolódik.

A kompetenciánkba tartozó tevékenységekre – hangtechnikai szakértés 2003-tól, fotó-, videotechnikai szakértés 2006-tól, informatikai és mobileszköz-szakértés 2011-től – jelentkező igény, illetve a kiadott szakértői vélemények száma nagymértékben növekedett. A szakmai tapasztalat, az alkalmazott módszerek megbízhatóságának folyamatos tesztelése, a legfrissebb tudományos ismeretek és innovatív fejlesztések lehetőségének keresése, a nemzetközi szakértői intézetekkel való rendszeres tapasztalatcsere (ENFSI társult tagság minden szakterületen) országos viszonylatban állandó, kiemelkedő színvonalat garantál. A folyamatosan magas szintű szakmai tevékenység további garanciája a minőségirányítási rendszer valamennyi szakterületre folyamatban lévő kiterjesztése.

Hangtechnikai szakértői terület

A *hangtechnikai szakértés* területén ma már másfél évtizedes szakmai tapasztalata van a szakértői intézetnek. A legkorszerűbb számítógépes technikákkal komplex feladat-végrehajtás folyik a következő feladatkörökben:

– beszélőazonosítás;
– zajszűrés;
– eredetiségvizsgálat;
– szöveges leirat készítése;
– beszélőprofil-készítés.

2002-ben kezdődött a hangszakértők képzése, ebben oroszlánrészük volt a Magyar Tudományos Akadémia Nyelvtudományi Intézet Kempelen Farkas Beszédkutató Laboratórium munkatársainak. Itt akkortájt már évek óta foglalkoztak akusztikai-fonetikai alapú beszélőazonosítással. A kollégák a szükséges fonetikai alapokat és a beszélők összehasonlításának gyakorlati módszerét tanulták meg az ottani kutatóktól. Az elsajátított ismeretek birtokában 2003-ban megkezdőhetett a szakértői intézetben a hangszakértői vélemények készítése. Kezdetben a beszélőazonosítást, az eredetiségvizsgálatot és a beszélőprofil-készítést nyelvész szakértői támogatással végeztük. A nyelvészeti elemzéseknek ma is fontos szerepük van a hangszakértői feladatokban, azonban a digitális beszédelemzési módszerek fejlődésének köszönhetően nagyobb hangsúlyt kapott a fonetikai alapú összehasonlítás. A kezdetektől jelentős anyagi erőforrások bevonásával európai, sőt világviszonylatban is elismert és alkalmazott szakértői hardver-szoftver elemek beszerzésére került sor, valamint megépültek a speciális hangszigeteléssel ellátott laboratóriumaink. A legújabb fejlesztések eredményeként 2017-ben ezen a szakértői területen is bevezettük a minőségirányítási rendszert, és azóta a szakértői intézet hangtechnikai szakértői laboratóriuma a Nemzeti Akkreditáló Hatóság által NAH-1-1206/2015 nyilvántartási számon akkreditált vizsgálólaboratórium. Ez újabb szintet jelentett a szakértői munkában.

A *beszélőazonosítás* módszertanában a hangszintű összehasonlítás lett az elsődleges bizonyíték a beszélők azonosságának vagy különbözőségének megállapításában. Azt vizsgáljuk, hogy az egyes hangokat milyen artikulációs konfigurációval ejtik ki a beszélők, és ezek mennyire hasonlóak. Ezt kiegészítik a prozódiai vizsgálatok, ugyanis a beszéd dallama, a ritmus, a beszédtempó összehasonlítási eredményei is bizonyítékot szolgáltatnak a vélemény megalkotásához. A fonetikai vizsgálatok eredményeinek összehasonlítását korábban a CSL 4400 és CSL 4500 szoftverekkel végeztük, majd 2017-től az ACU Expert nevű szakértői szoftvert használjuk. A nemzetközi trendeket követve 2010-ben sor került a Batvox 3.1 automatikus beszélőazonosító szoftver beszerzésére, amely azóta a szakértőivélemény-alkotást újabb bizonyítékokkal támogatja. Ennek a fejlesztése 2014-ben megtörtént, és azóta a Batvox 4.1-es verziót alkalmazzuk. Az összehasonlítás sikeres elvégzése érdekében, lehetőség szerint, személyesen vesszük fel a gyanúsítottól, a vádlottól vagy a tanútól az összehasonlító hanganyagot. Ehhez rendszeresítettünk egy mobil munkaállomást, amellyel a kirendelő hatóság hivatalos helyiségében tudjuk rögzíteni a szükséges hangmintát az ország egész területén.

Az összehasonlított beszélők (tudniillik a kérdéses és a mintaadó) azonosságának mértékét valószínűségi skála alkalmazásával határozzuk meg. Nem adunk kategorikus véleményeket, mert ha minden bizonyíték arra utal, hogy a két beszélő megegyezik és a szakértőnek nincs kétsége afelől, hogy a beszélők azonosak, akkor is kimutatható minimális matematikai esélye annak, hogy különböző személyekről van szó. Ma kilencfokozatú valószínűségi skálát alkalmazunk a hangtechnikai szakértői véleményekben.

Az automatikus beszélőazonosító módszertan hatékonyságának növelése érdekében az Európai Szakértői Intézetek Hálózatának Beszéd- és Hangelemző Munkacsoportjának találkozóin szerzett tapasztalatok felhasználásával, illetve kutatókkal történő együttműködések segítségével a szakértői intézetben a hangtechnikai szakértői területen folyamatos fejlesztések zajlanak.

A zajos, torzított vagy rosszul érthető beszédet tartalmazó hanganyagokat *zajszűrés*sel, a beszédérthetőség növelésével javítjuk. A hangfelvétel felhasználásától függően különböző módon hajtjuk végre a tisztítást. Ha az elhangzott szöveg leiratozása a cél, akkor a hallgató számára zavaró zajokat csökkentjük és a kérdéses beszélő hangját erősítjük. A másik esetben, amikor automatikus beszélőazonosításhoz használjuk a felvételt, akkor – a beszédhez nem tartozó zajok törlésén túl – csak a háttérzaj csökkentése a cél. Ezt a feladatot 2003-ban a Sound Cleaner nevű szoftverrel kezdtük, majd 2005-től a mai napig a CEDAR Cambridge Forensic System nevű munkaállomást (szoftver és hardver) használjuk. Ez a rendszer modulos felépítésű, és a digitális zajszűrési algoritmusok fejlesztésének köszönhetően újabb és újabb modulok érhetők el, amelyek beszerzésére folyamatosan lehetőségünk van, ezáltal nyújthatjuk a legjobb minőséget. Fontos ismerni azonban a zajszűrés korlátait. A tisztítás mindig kompromisszumok következménye. A modul kiválasztása és a zaj törlésének mértéke határozza meg a végeredményt. A digitális hangrögzítés technológiája következtében a rögzített beszéd és a zaj füllel már nem választható szét olyan hatékonyan, mint élő beszélgetés esetében. Sőt erre a zajszűrő modulok sem mindig képesek. Tehát ha a rögzített beszéd olyan jelentős zajjal fedett, hogy az eredeti hanganyagban sem hallható a beszéd, akkor valószínűleg tisztítás után sem lesz érthető.

Egy kérdéses hanganyag *eredetiségvizsgálat*ára akkor van szükség, ha felvetődik a gyanú, hogy abban utólagos szándékos beavatkozás történt. Ez lehet egy rész kivágása, új rész beillesztése, más formátumra való átalakítás stb. A hangfájl másolása az eredeti formátum megtartásával nem minősül a hanganyag manipulációjának. Egy hangfelvétel eredetiségének megállapításához ideális esetben rendelkezésünkre áll a hangrögzítő eszköz is. Ennek

birtokában van lehetőség a legrészletesebb és legpontosabb vizsgálatok elvégzésére. Szerencsés esetben a rögzítésre használt konkrét eszköz beazonosítása is megtörténhet. Az elemzéseket a kezdetektől a CSL4400, a CSL4500 és az Adobe Audition szoftverekkel végeztük. 2017-től elsősorban az erre a célra is kifejlesztett ACU Expert programot használjuk, amelynek segítségével egyebek között a különböző formátumokból (amr, mp3, wav stb.) eredő sajátosságokat vagy hangszerkesztő program használatának nyomait tudjuk felkutatni. Az ACU Expert legújabb fejlesztése következtében az elektromos hálózat 50 Hz-es frekvenciaingadozása egyedi mintázatának vizsgálatára is lehetőség van. Ezzel a módszerrel sok esetben meghatározható a hangfelvételnek – vagy egyes részeinek – a konkrét rögzítési időpontja. Ennek a vizsgálatnak a módszertanunkba történő bevezetése jelenleg is folyamatban van, és terveink szerint hamarosan alkalmazni tudjuk.

Szöveges leirat készítésére akkor rendelik ki a szakértőket, amikor a kérdéses hanganyagokban elhangzott szövegből tartalmi kivonat vagy összefoglaló nem elegendő a megrendelő számára, hanem szó szerinti leiratra van szüksége. A minőségi eszközökkel és a szakértői gyakorlattal a legrészletesebben rögzítjük az elhangzottakat. A leiratban jelzés szintjén megjelennek a megakadásjelenségek (például újraindítás, dadogás, hezitálás) vagy a nevetések is, amelyek akár pluszinformációval szolgálhatnak a megrendelőnek.

Beszélőprofilt (csoportbehatárolást) a szakterület indulása óta készítünk. Jellemzően – a nyelvi profilkészítéshez hasonlóan – a hangzó szöveg alapján a beszélő személy szociodemográfiai sajátosságainak (nem, életkor, iskolázottság, származási hely) felismerése az elsődleges cél. Ezen túlmenően minden egyéb, a beszélőre jellemző sajátosság megállapítása megkísérelhető, ami hozzájárulhat a nyomozás sikerességéhez. Ilyen lehet például: alkoholos vagy kábítószeres befolyásoltság, dohányzás, betegség, vagy a beszélők viszonya stb. Ezeknek a vizsgálatára jelenleg a szakértői módszerek a legalkalmasabbak; a beszélőazonosításhoz hasonló automatikus profilkészítési módszerek kutatási szinten már elkezdődtek, de alkalmazásuk nem jellemző. A percepciós vizsgálatok jellemzője, hogy a vizsgáló személye nagymértékben meghatározza a végeredmény helyességét. Amikor a nyomozó megvizsgálja az ismeretlen kérdéses beszélőt, akkor megpróbál következtetni arra, hogy milyen társadalmi csoportokba tartozhat, milyen személyiségjegyei vagy fizikai adottságai lehetnek. Ebben segíti őt a saját szakmai és élettapasztalata, ami alapján gyakran jó megállapításokat tesz. A nyomozás sikerességéhez azonban esetenként részletesebb elemzésekre és pontosabb válaszokra van szüksége. Ehhez kirendelheti a hangtechnikai szakértőket, amikor is szakér-

tői gyakorlattal felvértezett nyelvész és fonetikus tudományos alapú módszerek alkalmazásával a lehető legtöbb oldalról vizsgálják meg az ismeretlen beszélőt. Ideális esetben a nyomozó a munkája elején, amikor találkozik az ismeretlen beszélővel, kirendeli a szakértőt egy profil elkészítésére, azonban ez a folyamat hosszadalmas és még költségekkel is jár. Ezért az a jellemző, hogy a szakértői intézet csak abban az esetben kap kirendelést beszélőprofil-készítésre, ha a nyomozó már hosszabb ideje nem jut megfelelő eredményre a nyomozásban. Ebben a gyakorlatban a nyomozás hatékonyságának növelése érdekében rengeteg fejlesztési potenciál van, amihez a hangszakértői területen megvan a szakértelem.

Fotó-, videotechnikai szakértői terület

Kriminalisztikai, illetve igazságszolgáltatási területen jelentősen megnőtt az igény a videó-/képfelvételek komplex elemzésére. Napjainkban egyre nagyobb teret hódítanak a biztonságikamera-rendszerek. Utcán, intézményekben, bankokban, benzinkutaknál elhelyezett kamerák rögzítik az ott történt eseményeket.

Nagy valószínűséggel bennünket is napjában többször rögzít valamilyen kamerarendszer. A kamerák szemtanúi bűncselekményeknek, illetve a bűncselekmény helyszínére tartó vagy az onnan távozó elkövetők mozgásának. A bűnüldöző szervek számára nagy fontosságú a rögzített felvételekből a maximális információtartalom megszerzése. Az információmegszerzés bonyolult folyamat, különleges szakértelmet és eszközrendszert igényel. A 2006-tól működő *fotó-, videotechnikai szakértői terület* tevékenysége – speciális szakértői szoftveres és hardveres támogatással – kiterjed a tárgyak vagy személyek tulajdonságainak, jellemzőinek, sajátosságainak, azonosságának megállapítására (tárgy- vagy személy-összehasonlításra, fotó- és videogrammetriára), a bizonyítás szempontjából releváns események lefolyásának megállapítására (például cselekmény körülményeinek feltárására, történeti folyamatának vizsgálatára), jelenségek ok-okozati összefüggéseinek megállapítására (például felvételi körülmények, képmanipuláció feltárására stb.), rejtett sajátosságok láthatóvá tételére (például konvertálásokra, képjavításra).

A Nemzetbiztonsági Szakszolgálat Szakértői Intézet Fotó-videotechnikai Laboratóriuma a Nemzeti Akkreditáló Hatóság által NAH-1-1206/2015 nyilvántartási számon akkreditált vizsgálólaboratórium. Ennek keretében valamennyi, a megrendelő (kirendelő) szerv által átadott irat, dokumentum stb.

vizsgálatára pontosan körülírt és ellenőrzötten végrehajtott vizsgálati módszereket alkalmazunk. A vizsgálatok során készült, dokumentált feljegyzések, valamint képi illusztrációk felhasználásával történik a szakértői vélemények összeállítása, valamint azok eredményeinek dokumentálása. Az ügyben szakvélemény adására kijelölt szakértő tevékenységét konzultáló szakértő kontrollálja, ezáltal igyekszünk biztosítani a szakvélemények szakmailag korrekt, tévedésektől, illetve hibáktól mentes kialakítását.

Sok esetben már a felvételek megtekintése is gondot okoz, azok speciális tulajdonságai miatt, ezért ezeket feldolgozható formátumba kell konvertálni. A gyártók üzletpolitikai okokból egyedi zárt rendszereket forgalmaznak, illetve biztonságikamera-rendszerekre jellemző a time-lapse technológia, ami általában több kamera hosszú idő alatt rögzített felvétele gyors lejátszási módban. Úgynevezett demultiplexeléssel leválogatható a kérdéses kamera felvétele normál lejátszási módban. A tradicionális technológiákon alapuló fényképezés feldolgozása is a digitalizálással kezdődik, amelynek előfeltétele a maximális képi információ megőrzése. A digitális videók lejátszásához pedig konténerformátumokra és megfelelő kodekekre van szükség. A nem ideális körülmények között készült képi felvételek gyakran zajosak, homályosak, túlzottan vagy kevéssé kontrasztosak, egyenlőtlenül megvilágítottak lehetnek. A paraméterek ismeretében utólag optimalizálhatjuk ezeket a tulajdonságokat. Egyes esetekben lehetőség van jó minőségű képfelkonvertálásra több videoképkockából származó képi információ egyesítésével, az úgynevezett super-resolution technikával. Zajok, bemozdulások esetén előfordul, hogy fontos részletek átvitele sérül, hagyományos módszerekkel a felismerés lehetetlen, azonban van esélye annak, hogy statisztikai eljárásokkal ilyenkor is fel lehessen ismerni az alakzatokat. A szakértői vizsgálat része vagy – azonosításra alkalmas referenciafelvételek hiányában – a célja a képi információtartalom (csoport és egyedi jellemzők) leghatékonyabb kinyerése a képjavítás, lényegkiemelés speciális eszközrendszerével. A képjavításra alkalmazott módszereink az Európai Bizottság által támogatott ENFSI S-FIVE projekt iránymutatásait követi.

Szükséges lehet a felvételi körülmények feltárása, vizsgálhatjuk a fájlinformációkat. Például a digitális fényképezőgépek a fényképezés során, úgynevezett exif adatokat is rögzítenek, amelyek a kép készítésének körülményeit írják le (dátum, idő, gyártó, géptípus, rekesz, záridő, ISO érték, képorientáció).

Eseményelemzés témakörben optimális esetben végigkövethetjük a célszemélyek mozgását, cselekményeit. A felvételek utólagos kiértékelésével meghatározhatjuk a képen látható tárgyak, személyek kiterjedését.

A foto-, illetve videogrammetria a fényképekről, illetve videofelvételekről vett méretekből, illetve beszerezhető referenciaméretekből meghatározhatóvá teszi az azon szereplő tárgyak vagy személyek valós kiterjedését, méretét. Erre több módszer létezik, fotó-, videotechnikai szakértői szempontból a leghatékonyabb a szuperimpozíciós vagy (mozgó felvételek esetében) a videoprojekciós módszer, amelynek elve, hogy a méretarányos felvételek egymásra vetítésével, illetve számítástechnikai alkalmazások segítségével történő összeillesztéssel (amennyiben a kamerarendszer kiépítése és az általa rögzített tér főbb statikus elemei változatlanok) lehetőség nyílik a méretek meghatározására, ezáltal az azonosság valószínűsítésére vagy kizárására.

Az azonosítás célja a vizsgált tárgy vagy személy azonosságának megállapítása vagy kizárása. A tárgyak és személyek egyediek, általános és különös sajátságaik vannak. Besorolhatók osztályokba, csoportokba, ezek az úgynevezett csoportjellemzők, mindamellett csak rájuk jellemző sajátosságokkal is bírnak, ezek az úgynevezett egyedi jellemzők. A módszer célja annak megítélése, hogy a fotókon vagy videófelvételeken ábrázolt tárgyak vagy személyek összehasonlítása során megállapított, megegyező és eltérő ismérvek (azok okainak lehetséges feltárása mellett) mennyiségi és minőségi azonosítási értékei valószínűsítik vagy kizárják az azonosságot.

A biometriai azonosítás során számolni kell azzal, hogy a matematikai módszerek is csak valószínűsítő véleményt fognak eredményezni. A szakvélemény bizonyosságának foka több tényező függvénye. Arc-összehasonlításra alapvetően az Unidas Expertise programot használjuk szuperpozíciós (egymásra vetített) felvételek részletes összehasonlításának elősegítésére.

Az egyes módszereknél erősebb biometrikus eljárást kaphatunk, ha egy rendszerben egyszerre több, egymástól független jellemzőt, vagy ugyanazon jellemző független módszerekkel való feldolgozását vesszük figyelembe.

Ilyen irányú szakértői tevékenység (amely követi a nemzetközi ajánlásokat) Magyarországon kizárólag intézetünkben zajlik. A módszertani kontrollt az Európai Szakértői Intézetek Képalkotó Munkacsoportjával folytatott tapasztalatcsere segíti elő. A munkacsoport éves ülését 2015-ben, Budapesten szerveztük, amelyen európai és ausztrál szakértői intézetek képviselői voltak jelen. Részt vettünk a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalának égisze alatt kiépült állóképes arckép-azonosítási projekt bevezetésében, a szoftverek előzetes tesztelésében, a munkatársak képzésében. Ismereteink jelentősen bővültek az ott megvalósuló antropológiai képzés során. Munkatársunk a Holland Szakértői Intézet szervezésében folyó európai szakértői képzésen vett részt, az Európai Szakértői Intézetek Képalkotó

Munkacsoportja által szervezett éves arc-összehasonlító tesztek, illetve azok értékelése segít tökéletesíteni az arc-összehasonlítási módszertanunkat.

Informatikai szakértői terület

Az informatikai szakértői terület kialakítására 2011-ben került sor a Nemzetbiztonsági Szakszolgálat Szakértői Intézetében. A szakértői tevékenység eleinte kizárólag számítástechnikai eszközökre (azaz elsősorban számítógépekre és adathordozóikra) korlátozódott, majd egyre inkább megfogalmazódott az igény a mobil kommunikációs eszközök (mobiltelefonok, navigációs eszközök) adattartalmának vizsgálatára is.

A modern információtechnológiai eszközök elterjedésével mindkét szakértői ágazat rövid időn belül rohamos fejlődésnek indult. Az elsősorban Microsoft operációs rendszerek vizsgálatára szakosodott informatikai szakértői ágazat az évek során képessé vált már platformfüggetlen módon vizsgálni a digitális nyomokat Windows, Linux, Unix és Mac OS környezetben is. Az eleinte csak a hagyományos mobiltelefonok vizsgálatára szakosodott mobileszköz-szakértői ágazat mára képessé vált a modern okostelefonok, tabletek és egyéb okoseszközök teljes körű vizsgálatára, szintén operációs rendszertől – legyen az Android, iOS, Windows Mobile vagy BlackBerry – függetlenül.

Az információtechnológiai eszközök elterjedésével és az internet mindennapossá, sőt elengedhetetlenné válásával egyre inkább elterjedt a kiberbűnözés is, illetve az annak eszköztárát képező rosszindulatú szoftverek *(malware)*. A 2013-ban még elszórtan jelentkező, majd az évek során egyre gyakoribb malware-fertőzések szükségessé tették egy olyan szakterületi ágazat kifejlesztését is, amely képes a rosszindulatú szoftverek működését vizsgálni, illetve a segítségükkel végrehajtott bűncselekmények eseményeit rekonstruálni. A szakterületen 2016 óta folyik kifejezetten ezt a célt szolgáló rosszindulatú szoftver kimutatására irányuló szakértői tevékenység.

A fejlődés nem lett volna lehetséges az intenzív eszközfejlesztések és -beszerzések, létszámbővítés, nemzetközi oktatás, illetve a saját erejű tudományos kutatómunka nélkül. A szakterületen dolgozók létszáma a kezdeti három főről hét év alatt nyolcra bővült, több mint felük igazságügyi szakértői minőségben tevékenykedik.

A szakértői intézet technikai szakértői tevékenységén belül egyszerűen csak „informatikai szakértésnek” titulált szakterület valójában tehát három – egymást kölcsönösen átfedő – ágazatra oszlik: informatikai szakértésre, mo-

bileszköz-szakértésre és malware-szakértésre. Ez a technikai szakterület a gyakorlatban az igazságügyi szakértői szakterületekről szóló hatályos 9/2006. (II. 27.) IM rendeletben meghatározott informatikai szakterületen túlnyúló – a rendelet szerint inkább a hírközlési szakterülethez tartozó – vizsgálatokat is végez.

Tekintve, hogy a szakértői intézet igazságügyi vonatkozásban elsősorban büntetőügyekben rendelhető ki, ezért tevékenységének erőteljes kriminalisztikai vonulata is van. A miniszteri rendelet által meghatározott informatikai és hírközlési szakterületek azonban kizárólag műszaki értelemben kapcsolódnak az intézet munkájához. A kriminalisztikai ismeretek elsősorban a nyomozó hatóságok információtechnológiai eszközökkel kapcsolatos bűnjelrögzítési tevékenységének elősegítése során bírnak rendkívüli fontossággal.

A kriminalisztika tudománya a nyomon olyan fizikai elváltozást ért, amely a bűncselekmény elkövetésével bármilyen kapcsolatban áll. A digitális nyomok azonban valójában információtechnológiai eszközök (hardverek) és programok (szoftverek) működése közben folyamatosan keletkező, módosuló és megsemmisülő adatok. A digitális bizonyítékok lefoglalását oly módon kell elvégezni, hogy utólag hitelt érdemlően bizonyítani lehessen a rögzített digitális adatok eredetiségét és hitelességét. A digitális nyomok felkutatásához és rögzítéséhez ezért speciális ismeret, szakértői tudás szükséges – ez azonban már túllép egy kriminalisztikai ismeretekkel nem bíró informatikai szakértő szakmai kompetenciáján.

Az előbbiekben körülírt speciális ismeret számítástechnikai szempontból a bűnügyi informatika *(computer forensics),* de tágabb – azaz nemcsak informatikai, hanem minden modern digitális eszközre kiterjeszthető – értelmezésben a bűnügyi információtechnológia *(IT forensics).* A szakértői intézet nem titkolt célja, hogy a *bűnügyi információtechnológia* új szakértői területként legyen bejegyezve a Magyar Igazságügyi Kamara kriminalisztikai szakterületein belül. Ennek megfelelően kidolgozás alatt vannak azok a szakmai módszertanok és eljárások, amelyek nemcsak az új igazságügyi szakterület létrehozásának létjogosultságát indokolják, hanem egyben a szakterület minőségirányítása és akkreditált működése érdekében is szükségesek, e cél megvalósítására várhatóan 2020-ig sor kerül.

A szakértői intézet tevékenységi körét tekintve szabatosan most már bűnügyi IT szakértőinek nevezhető szakterülete 2013 óta társult tagja az Európai Szakértői Intézetek Bűnügyi Információtechnológiai Szakértői Munkacsoportjának. A munkacsoport évente megrendezett értekezletein az európai szakértői intézetekből érkező résztvevők beszámolnak az elmúlt időszak

bűnügyi tudományos fejlődésének eredményeiről az informatikai szakértés és egyéb kapcsolódó témakörökben. A szakterület tagjai 2009 óta rendszeresen részt vesznek az Európai Csalás Elleni Hivatal (OLAF) által támogatott nemzetközi bűnügyi informatikai képzéseken is, valamint az Európai Rendőr-akadémia (Cepol) kiberbűnözés elleni szemináriumain.

Összegzés

Az eddig elért gyors ütemű fejlődés a szakértő munkatársak innovatív hozzáállásának, motiváltságának, a Nemzetbiztonsági Szakszolgálaton belüli szakmai együttműködésnek, az ENFSI-munkacsoportokban folyó munkának, az OLAF, az IACIS (Informatikai Bűnügyi Technikusok és Szakértők Nemzetközi Szervezete), valamint egyéb hazai és nemzetközi szakmai tréningeken és konferenciákon való részvételnek köszönhető, amelyek a jövőben is elsőszámú garanciái a folyamatos szakmai fejlődés fenntartásának.

Az eddigi tapasztalatok alapján a kirendelők részéről egy-egy ügyhöz kapcsolódóan (a feladat teljes körű megoldása szempontjából) fokozott igény a különböző szakértői területek eszközrendszerének felhasználása a komplex elemzések lefolytatása során, amire azok kompetenciái ideális lehetőséget nyújtanak.

DOI: 10.38146/BSZ.2019.1.9

HAZAI LÁSZLÓNÉ DR.

Módszerek, technikák a biometrikus arcfelismerésben, -azonosításban

Az emberek egyedi, tudományosan igazolt, fiziológiai vagy viselkedésalapú jellegzetességeit felhasználó, mérhető, az egyéni azonosítást lehetővé tevő módszert nevezzük biometriának. A biometrikus azonosítás az e megkülönböztethető jellegzetességeken alapuló, napjainkban igen széles körben és területen használt – általában a biztonság megerősítését támogató – módszereket magában foglaló gyűjtőfogalom.

Az ember mérhető adottságai, jellegzetességei például az ujjlenyomat, a tenyérlenyomat, az írisz mintázata, az erek mintázata a retinában, az ujjban, a tenyérben, a hangképzés jellemzői, illetve a testrészek (arc, fül, kéz) geometriája, biológiai, fizikai jellemzői, valamint egyes viselkedésalapú jellemzők, mint például a járás, testtartás stb. Az egyes jellegzetességek, sajátosságok matematikai módszerekkel, algoritmusokkal írhatók le. Az így kapott biometrikus adat *(template)* egy olyan gépi kód, amely lehetővé teszi az összehasonlítást[1].

Egy biometrikus azonosítási módszer hatékonysága egyrészt attól függ, hogy mely biometrikus sajátságokat kívánjuk mérni, a mérést milyen pontossággal tudjuk elvégezni, illetve nagyon nagy mértékben természetesen attól, hogy az adott sajátság mennyire egyedi, mennyire jellemző egy adott személyre, és fontos az is, hogy mennyire állandó. Másrészt meghatározza a módszer eredményességét, hogy milyen algoritmusokat használ a biometrikus minták generálására és milyet az összehasonlításra.

A biometrikus elemek személyazonosításra történő tömeges, illetve automatikus alkalmazása és ezzel összefüggésben a kapott eredmények értékelése sok paraméter, körülmény vizsgálatát, figyelembevételét igényli. A technikai részletek kidolgozását mindig meg kell hogy előzze annak eldöntése, milyen célból, miért van szükség a biometrikus azonosításra, ez után vizsgálni kell a *biztonság kérdését, amely magában foglalja* a szükségesség és az arányosság szempontjait, a biometrikus azonosító hamisíthatóságának kérdését, a mérések pontosságát és megbízhatóságát, az ebből eredő hibák nagysá-

1 ICAO Doc 9303 Machine Readable Travel Documents. 2015, part 9.

gát. Fontos továbbá vizsgálni az *alkalmasság, alkalmazhatóság* aspektusait, amely olyan, a gyakorlatban fontos kérdések elemzését takarja, mint a biometrikus azonosítók mérésének gyorsasága, hitelessége, megismételhetősége, a mérés bonyolultsága, a mérő eszközök bonyolultsága, mérete, költsége, a mérést befolyásoló egyéb tényezők, a kockázatok ismerete, a módszer elfogadottsága stb.

Ezzel párhuzamos, szintén nem kevésbé összetett feladat a *kivitelezés, a további technikai kérdések* (például milyen adat és milyen formátumban tárolódjon, az adat tárolására alkalmas adathordozó típusának kiválasztása), valamint a *biztonsági követelmények* kidolgozása (például a tárolt adatokhoz való hozzáférés, a hitelesítés rendje).

A biometrikus azonosítás irányait, módszereit, ezek fejlődését vizsgálva megállapítható, hogy az elmúlt évtizedben visszatérően igen nagy figyelmet, érdeklődést kapott az arcfelismerés és -azonosítás. Nagyon sok kutató foglalkozik a témával már hosszú ideje, és a mesterséges intelligencia, az okosalkalmazások lehetősége napjainkban újabb lendületet adott a kutatásoknak.

Az ok nyilvánvaló, hiszen ez az úgynevezett passzív azonosítást lehetővé tevő, sokféle területen és célra használható eljárás a leginkább elfogadott biometrikus módszer, mert nem igényli a személy aktív közreműködését, emellett gyors, és tömegeseményeknél távoli azonosításra is alkalmazható. Tény azonban, hogy az elmúlt néhány évtizedben olykor pozitív, máskor negatív vélemények születtek a rendszerek alkalmasságának, használhatóságának a megítélését illetően.

A biometrikus azonosítást végző rendszerek hatékonysága nagymértékben a választott biometrikus jellemző emberenkénti egyediségétől és az adott jellemző mérésének pontosságától függ.

Nem szerencsés olyan biometrikus sajátosságokat választani, amelyek nehezen vagy csak nagy hibával mérhetők.

A biometrikus azonosítók közül az arcazonosítás a kényelmi szempontokat figyelembe véve optimális, de megbízhatósága kimutathatóan elmarad a többi biometrikus azonosító jelentős részétől. Ahhoz, hogy mely tényezők játszanak ebben jelentős szerepet, ismerni szükséges a technológiát, hogy az egyes technológiai lépések, a választott paraméterek, a különböző döntési folyamatok ismeretében megfelelően értékelni tudjuk a kapott eredményeket.

Ha az arcazonosítást összevetjük más biometrikus azonosítással, megállapítható, hogy az arcalapú azonosítás esetében a variabilitás, a pozíciók, a beállítások, a megvilágítás minősége, a gyűjtött, illetve a mintaképek felbontá-

sára, minőségére (zajosságára) való érzékenység nagymértékben befolyásolja a rendszerek eredményességét.

Hibát okozhat számtalan, ma még meg nem magyarázott tényező, például egyes rendszerek jobb eredményt mutathatnak a nők azonosítása esetében, mint a férfiaknál, vagy hasonló probléma állhat elő idősebb, illetve fiatal emberek vonatkozásában, vagy különböző bőrszín esetében. Téves elfogadás történhet, ha az adatbázisban tárolt fotóhoz képest változott a személy hajviselete, a hajszíne. Az ergonómiai tényezők mellett hatással lehet az eredményre az a környezet, amelyben használjuk az adott rendszert, és azoknak az eszközöknek az állapota, amelyeket a rendszer használ. Hibát okozhat, ha alacsony felbontású kamerával készült az összehasonlítás alapjául szolgáló fotó.

Laboratóriumi körülmények között, szigorúan ellenőrzött és kézben tartott paraméterek mellett, elfogadott technológiát, algoritmusokat alkalmazva az arc detektálásának hibája öt és tíz százalék között változik[2]. Érdemes tehát a célokat ennek tudatában meghatározni, dönteni az alkalmazás körülményeiről, értelmezni az azonosság kérdésének – elfogadás vagy elutasítás – biztonságra gyakorolt hatását.

Az arcazonosítás folyamata képfeldolgozás, képanalízis, amelynek első fontos lépése az *arc felismerése a képen (detektálás),* ez az optikai adatfelvételezés – a mozgó (videófolyam) vagy az álló képek rögzítése kamerák segítségével – után különböző, általános (szűrés, szegmentálás stb.) és az arcazonosítást támogató speciális képfeldolgozási módszerekkel (algoritmusokkal) történik. Az arc felismerését támogató, ismert speciális képfeldolgozási eljárások, detektáló módszerek például[3]:

– a bőrszín alapján történő keresés (például RGB[4] alapszínek alapján, a bőrszín homogén színkülönbségi értékeinek segítségével);
– template-illesztés módszerével, ami lehet például egy mintázatalapú felismerés (például világos és sötét régiók, foltok keresése egy adott felületen, ezt nevezik fényességalapú felismerésnek *[brightness based recognition],* vagy kontúr, sziluett alapján, amelyet jellemzőalapú felismerésnek *[feature based recognition]* neveznek); vagy

2 https://www.gemalto.com/govt/inspired/biometrics

3 Távoli személyazonosítási technikák. Budapesti Műszaki és Gazdaságtudományi Egyetem Méréstechnikai és Információs Rendszerek Tanszék–Gardware Systems Kft., 2005. http://oldweb.mit.bme.hu/eng/research/search/downloads/tst/Irodalomkutatas.pdf

4 RGB-színtér (R: vörös, G: zöld, B: kék), az RGB színtér három alapszín keveréséből létrehozott színkocka. Ebben a háromdimenziós színtérben egy szín háromkomponensű *(r, g, b)* vektorként határozható meg, így létrehozva a kétdimenziós színteret, amely már használható az összehasonlításra.

– statisztikai analízis, gépi tanulás módszere segítségével (például neurális háló alkalmazása, amelyhez először manuálisan rögzítik az arckép egyes elemeit, amelyek a neurális háló számításának kiindulási pontjai).

A detektálás során számos nehézséget kell kezelniük a rendszereknek, mint például

– az arc pozíciójának, beállításának variációit – az ideális pozíció természetesen a szembe pozíció, azonban nyilvánvaló, hogy ritkán megvalósítható ez az ideális kép, ezért ennek a problémának a kezelésében ma már nagyszámú felvételezési módszer és algoritmus nyújt segítséget;
– a mérni kívánt sajátosság takarását, rejtését;
– az arckifejezés változásait;
– a különböző kamerák és a környezet kondícióinak hatását a képi paraméterekre.

Az arcnak a képen való megtalálása után – vagy ezzel párhuzamosan – a rendszer soron következő feladata a biometrikus azonosításhoz szükséges *mérendő és összehasonlítható tulajdonságok kivonása,* összegyűjtése. Ezeknek az algoritmusoknak is általában az arc tulajdonságainak detektálásához alkalmas arcazonosító algoritmusok az alapjai.

Az azonosításhoz szükséges műveletek sora általánosságban a következő módon írható le. A választott biometrikus azonosító, ebben az esetben az arckép *optikai adat felvételezését követő digitalizálás* után jön létre az a képpontokból (pixelekből) álló sokdimenziós tér (*N* dimenziós vektortér), amely a képfeldolgozási műveletek alapjául szolgál, és amelyben *meghatározzuk a minta sajátosságparamétereit, vagyis a koordinátáit, az úgynevezett sajátságvektorokat.* A biometrikus rendszerekben ezeknek a sajátságvektoroknak a segítségével történik meg az *összehasonlítás,* a *hasonlósági (távolsági) mutatók kiszámítása,* majd ez után áll elő a *döntés, az azonosság mértékének a megállapítása.* A döntés a sajátságvektorok távolságértékeiből számolt bináris függvény, ami válasz a két minta hasonlóságának kérdésére. Az eredményt pontosítja, ha az egyes sajátosságokhoz tartozó bizonytalansági faktorokat is ismerjük, és az eredményt ezzel korrigáljuk.

Az úgynevezett multimodális rendszereknél – amikor egy ember különböző biometrikus jellegzetességeinek a mérésére is sor kerülhet – a biometrikus-sajátosság-paraméterek együttes használata is ismert, ebben az esetben a paramétereket egyetlen sajátságvektorba integrálják. Azonban a biometrikus azonosítást végző multimodális rendszerek esetén a gyakorlati megvalósítás

nehézségei miatt ekkor is inkább az egyes egyedi sajátosságok összehasonlítására kerül sor[5].

Osztályozásukat tekintve az arcazonosító algoritmusok lehetnek minta- vagy geometriaalapú algoritmusok.

A mintaalapú arcazonosítási módszerek esetében a teljes kép vagy annak egyes kiemelt részleteinek (például szem, orr, száj) összevetése történik a tárolt mintakép(ek) elemeivel különböző algoritmusok segítségével. Ebben az esetben is sajátságvektorok kivonatolására van szükség, de ezeket nem geometriai módszerek, hanem különböző statisztikai eljárások állítják elő (*eigenface,* legközelebbi szomszéd osztályozás stb.).

Ezek a rendszerek érzékenyek a megvilágításra, erőforrás-igényesek. Hibát okozhat a pixelek intenzitásának eltérése az adatbázis képeihez viszonyítva.

A geometriai módszerrel az egyes képi elemek, arcrészletek (például szem, orr, száj) egymáshoz viszonyított pozíciójának, méretének, alakjának vizsgálatával, összevetésével végzik az azonosítást. A hiba csökkentése érdekében fontos tényező a mért sajátosságok számának helyes megválasztása.

Ezek a rendszerek érzékenyebbek lehetnek a pozícióra, beállításokra, mert nem eléggé pontosak a jellemző azonosítási pontok felvételét illetően.

A különböző módszerek különböző érzékenységgel kezelik az egyes körülményeket, beállításokat.

Gyakran egy arcot detektáló, azonosító módszer nem elégséges a megfelelő eredmény eléréséhez, ezért szükség lehet a különböző módszerek kombinálására is. Ezzel a megoldással napjainkban a fejlesztők élnek is, sok kutatás igazolja, hogy hibrid módszerekkel – többféle algoritmus használatával – jobb eredmény érhető el.

Ahhoz, hogy jó döntés szülessen egy biometrikus azonosító, jelen esetben arcfelismerő azonosító rendszer létrehozásánál – mint említettem –, lényeges szempont, hogy konkrétan meghatározzuk a felhasználás célját. Ha *ellenőrzés, vagyis az azonosság megerősítése* a cél, ebben az esetben 1:1 megfeleltetésről beszélünk, amikor a rendszer az *egy* személyről készített digitális képet *egy* ellenőrző mintaképpel hasonlítja össze. Ilyen alkalmazás például a határellenőrzésnél a biometrikus útlevélben lévő digitálisan rögzített kép és a jelenlévő útlevélkép, valamint a szintén jelenlévő személy összehasonlítása vagy ilyen a mobiltelefonokba telepített arcfelismerő alkalmazás. Abban az esetben, ha az *azonosítás, vagyis felismertetés* a feladat, 1:*n* vagy *n:n* azonosításról beszélünk, amikor egy (esetleg több) aktuális képhez keressük az elő-

5 Távoli személyazonosítási technikák… i. m.

re létrehozott adatbázisban lévő leginkább megfeleltethető, illetve azonos mintaképet.

Az ellenőrzés, vagyis az azonosság megerősítése (1:1 megfeleltetés) technikailag egyszerűbb, kevesebb hibával terhelt feladat, míg az azonosítás, felismertetés komplexebb, technikailag a variabilitás okán rendkívül összetett tevékenység. Ennek megfelelően a különböző célra különböző képességű, felépítettségű rendszerek létrehozása szükséges.

Egy biometrikus rendszer megbízhatósága, használhatósága szempontjából fontos tényező, hogy mekkora a használt adatbázis *(n)* mérete. Az, hogy mi az optimális méret, sok tényező függvénye. Függ az adatbázisban lévő felvételek paramétereitől (az általános és a speciális képfeldolgozási paraméterektől), az adatbázist alkotó populáció összetételétől, függ az alkalmazott algoritmusoktól amelyeket a rendszer használ. Fontos tudni, hogy az algoritmusokat optimalizált adatbázisokra tesztelik. Ronthatja az arcazonosítás, az adatbázisban keresés, végső soron a döntés hatékonyságát, eredményességét az, hogy a képfeldolgozási algoritmusok az azonosításhoz több sajátosságparamétert használnak, és ezeket általában egy adott képre optimalizálják, majd ezeket használják az adatbázisban lévő különböző képekre. Ebben az esetben nyilvánvaló, hogy nem a minden képre optimalizált sajátosságparaméterek alapján kerül sor a keresésre. Ezt próbálják kiküszöbölni az optimális paraméter keresésére fejlesztett eljárások.

A különböző biometrikus sajátosságot alkalmazó biometrikus rendszereket összehasonlítva az irodalom megállapítja, hogy az arcazonosításnak a legnagyobb a téves elfogadási *(False Accept Rate; FAR)* és a téves visszautasítási *(False Reject Rate; FRR)* rátája[6]. Ezek a mutatók a rendszer megbízhatóságát jellemzik, azt határozzák meg, hogy például egy adott személy esetén milyen valószínűséggel következik be az, hogy a rendszer tévesen fogad el egy pozitív vagy negatív állítást, tévesen azonosít (FAR), illetve hogy milyen valószínűség esetén következik be, hogy tévesen utasít el egy pozitív vagy negatív azonosság állítást (FRR)[7].

A függvényként értelmezett FAR és FRR görbék metszete az azonos hibaérték *(Equal Error Rate; EER)*. Ez az érték a FAR és az FRR eloszlásfüggvények metszéspontja, vagyis az az állapot, amikor FAR = FRR. A két mutató tehát olyan eloszlásfüggvény, amely csak együttesen értelmezhető. A

6 https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/
7 Távoli személyazonosítási technikák… i. m.

biometrikus rendszerek skálázhatók, ami az jelenti, hogy a mutatók változtathatók, de *ha az egyik mutatót növeljük, akkor a másik csökken.*[8]

Az, hogy egy rendszer tévesen azonosít-e (FAR), attól függ, hogy a rendszert működtető algoritmus hány azonosított sajátosság alapján fogadja el a képet. Vagyis meg kell határozni azt a küszöbértéket, amelynél több azonosított sajátosság esetén a képet a rendszer már azonosnak tekinti, ennél a küszöbértéknél kevesebb azonosított sajátosság esetén a rendszer elutasít. Ez tehát a rendszer működésének egyik fontos eleme.

Mint ahogy az előzőekből is kitűnik, az arcazonosításra különböző módszerek, algoritmusok, eszközök használatosak. Az arcazonosításhoz használt algoritmusok, a választott módszerek és eszközök némelyike jobb, míg más megoldások kevésbé pontos eredményt adnak[9].

A használat során azonosított problémák, mint a megvilágítás, a pozíció, az arckifejezés továbbra is a kutatások, fejlesztések fontos területei, úgyszintén az algoritmusok megfelelőségének, alkalmasságának megkerülhetetlen mutatói (a sajátosságok mérhetősége, a mérés pontossága, a találati arány, a hibaszázalék) és a működést meghatározó lényeges paraméterek, mint

– az azonosítás sebessége;
– a műveletek végrehajtásához szükséges memóriakapacitás;
– az automatizáció szintén a fejlesztések kiemelt területei.

De kutatási terület az úgynevezett multimodális rendszerek alkalmazhatóságának kérdése is, ami a különböző biometrikus megoldások kombinálását jelenti, ami az azonosítás biztonsági szintjének a növelése, az azonosítás során felvetődő hibák csökkentése érdekében kap egyre nagyobb hangsúlyt. Ilyen multimodális rendszerek jönnek létre például az arc/hang, az arc/ujjlenyomat, az ujjlenyomat/írisz[10] biometrikus azonosítók kombinálásával.

Ezeknél az alkalmazásoknál szintén fontos szerepük van a megfelelő megválasztott algoritmusoknak és a használni tervezett eszközöknek.

Fontos eleme a biometrikus azonosításnak az adatbázisban tárolt képek minőségének megfelelősége. Az arcfelismerő minták, algoritmusok gyártónként nem kompatibilisek. Ezen túl fontos figyelembe venni azt is, hogy az egyes fejlesztők, gyártók külön mintaadatbázisokra fejlesztenek, erre optimalizálják a rendszereiket, ennek következtében az egyes rendszerek nem feleltethetők meg egymásnak. Nemzetközi ellenőrzések viszonylatában a kompa-

8 http://www.securinfo.hu/termekek/biometria/1160-arc-alapu-azonositas-a biometriaban.html
9 Proyecto Fin de Carrera: Face Recognition Algorithms, 16 June 2010.
10 https://findbiometrics.com/solutions/multimodal-biometrics/

tibilitás, a hatékonyság, az ellenőrzések eredményessége érdekében cél, hogy minél szabályozottabb, egységesebb képformátumokban tárolják az összehasonlítandó biometrikus adatot. Az arcfelismeréshez a kép tárolása pixelgrafikus formákban (például: *BMP*, 24 bit színmélységű, bittérképes, nem tömöríthető képformátum; *JPEG,* 24 bit színmélységű, veszteségesen vagy veszteségmentesen tömöríthető képformátum; *PNG,* veszteségmentesen tömöríthető RGB képet adó képformátum) történhet, amelyek képpontokból, úgynevezett pixelekből építik fel a képet[11]. A Nemzetközi Polgári Repülési Szervezet *(International Civil Aviation Organization; ICAO)* által preferált, standardizált képi adat a 300 dpi-s színes kép, amely kilencven pixelből áll a szemek között, és a mérete kb. 640 kB, pixelenként 24 bittel. Ez a kép jelentősen tömöríthető JPEG/JPEG2000 technikát alkalmazva, a tömörítési eljárás történhet veszteséggel, illetve veszteségmentesen.

Megjegyzendő, hogy az e-útlevelekben lévő, a chipen tárolt arcképek tömörítésének mértéke 15 és 20 kB közé esik. A megengedett minimum 12 kB[12].

A standardizált képformátum kiküszöbölheti, vagy legalábbis mérsékli a különböző algoritmusokkal működő rendszerek esetében az azonosítási anomáliákat.

Napjainkban az arcazonosítás, ezen belül az automatikus arcazonosítás, adatbázisban való keresés számos biztonsági területen új lendületet adott ennek a biometrikus azonosítási programnak. Lásd az egyesült államokbeli Biometrikus Exit programot[13], amelynek többféle biometrikus azonosítási megoldása volt napirenden évek óta, de a technológia hibái, és esetenként „kísérleti megoldásai" ellenére – a repülőtéri kapuknál végrehajtható tömeges ellenőrzés lehetősége, az arc ellenőrzésének egyszerű kivitelezhetősége miatt – végül az arcazonosítási technológia bevezetésére került sor.

Új eljárások, mint a 3D felismerés[14], amely esetében a 3D szenzorokkal gyűjtött adatok teljesebb körű információt adnak az arc sajátosságairól, mert csökken a megvilágításra, az árnyékolásra és a nem megfelelő pozícióra visszavezethető hiba, vagy az arckifejezés variabilitásának csökkentését célzó módszerek, a bőr textúrájának analízise, a hőképek analízise mesterséges intelligencia segítségével (arcfelismerés sötétben)[15], illetve a különböző módszerek kombinálása napjainkban új irányokat nyithat meg a biztonsági területeken.

11 Távoli személyazonosítási technikák… i. m.

12 ICAO Doc 9303… i. m.

13 Ravi Das: The controversial comeback of facial recognition. Keesing Journal of Documents and Identity, vol. 54, 2017

14 http://www2.mit.bme.hu/services/vimm3241/tanul/beadott/regi/SzigetvariMadai/

15 https://www.sciencedaily.com/releases/2018/04/180416142443.htm

Fontos tehát az azonosítás/felismerés módszereinek, az alkalmazás körülményeinek, a lehetséges hibáknak a pontos, ha nem is teljes körű feltérképezése, a kapcsolódó kockázatoknak az elemzése ahhoz, hogy megfelelő döntés szülessen egy módszer kiválasztásánál vagy egy rendszer létrehozásánál.

Mivel ehhez többnyire csak korlátozott információ áll rendelkezésre, mert a gyártók az egyedi fejlesztésű rendszereikről csak kevés információt osztanak meg, és mert az egyes rendszereket optimális körülményekre tesztelik, általában kisszámú adatbázissal, ezért lényeges a tervezett körülményekre és paraméterekre saját tesztek elvégzése, az eredmények értékelése és a kockázatok megállapítása.

DOI: 10.38146/BSZ.2019.1.10

NÉMETH ATTILA – TÓTH GERGELY

Arcfelismerő rendszerek alkalmazása

Jelen tanulmány az arcfelismeréssel kapcsolatos gyakorlati megvalósítás szempontjából vizsgálódik, az arcfelismerés elméleti kérdéseit nem járja körbe. Az arcfelismerő technológiák és számítástechnikai eszközök fejlődésével egyre megbízhatóbb, kisebb hibaarányú arcfelismerő rendszerek érhetők el. A rendészeti célú felhasználás mellett a polgári célú is egyre elterjedtebbé válik, tekintettel arra, hogy az arcfelismerés érintésmentes azonosítást tesz lehetővé. A továbbiakban bemutatjuk a rendészeti célú arcfelismerés optimális feltételrendszerét.

Arcfelismerés helye a biometrikus azonosítás rendszerében

A biometria szó görög eredetű, amely két részből áll: a 'bios', vagyis élet és a 'metrein', vagyis megmér, összemér szóból. Ebben az értelemben használva egy ember fizikai paramétereinek mérését jelenti. Pontosabban egy személy egy vagy több egyedi fizikai jellemzőjének mérésen alapuló azonosítását.

A biomertikus adatokat általában két klasszikusan nagy csoportra osztják, amelyben a biológiai és a viselkedésalapú paraméterek szerepelnek.[1]
A biológiai alapú biometrikus adatok a következők:

- bőrmintázat: ujjnyomat, ujjlenyomat, ujjnyom, tenyérnyomat, talplenyomat, kézgeometria;
- érhálózat: tenyér-, ujjerezet;
- arc: 2D, 3D, hőkép;
- szem: írisz, retina;
- DNS.

A viselkedésalapú biometrikus adatok a következők:

- kézírás: íráskép, dinamika;

1 Kovács Tibor – Milák Istán – Otti Csaba: A biztonságtudomány biometriai aspektusai. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécs, 2012. [Pécsi Határőr Tudományos Közlemények XIII.] http://www.pecshor.hu/periodika/XIII/kovacsti.pdf

– beszédhang;
– gépelési ritmus;
– mozgás: járásmód, a test helyzetének változásai.

Egzakt mérési, algoritmizálási, értékelési mód kizárólag a biológiai (fiziológiai) csoport tekintetében szolgál egyértelmű, értékelhető eredménnyel.[2]

Arcfelismerés

A biztonságérzet világban tapasztalható csökkenésével párhuzamosan egyre nagyobb az igény a felhasználók hiteles azonosítására. Egyedül a biometrikus azonosítás az a technológia, amely az emberek egyedi, lehetőség szerint megmásíthatatlan és hamisíthatatlan tulajdonságait vizsgálja. A jelenlegi rendszerek sem sebezhetetlenek, azonban a folyamatos fejlesztéseknek köszönhetően egyre magasabb biztonsági és kényelmi követelményeknek felelnek meg.[3]

Az említett biometrikus azonosítási lehetőségekből több is nagyon pontos és egyedi eredményt kínál, ezekkel a módszerekkel azonban az a fő gond, hogy kényelmetlenséget okoznak. Ujjnyomat-ellenőrzéskor az ujjat szenzorra kell helyezni, és ott tartani bizonyos ideig. Íriszvizsgálat esetén az érintettek aggódnak a látásuk épségéért. Az ujjnyomat-ellenőrzés bizonyos körülmények esetén nem okoz problémát, például pénzügyi tranzakció hitelesítésekor, de beléptetőpontok esetében, ahol nem tartják elegendőnek egy elektronikus kártya birtoklását és biometriai azonosítást is igénybe vennének, már fennakadásokat okozhat az elhúzódó beléptetési folyamat. A cél, hogy az ellenőrzés majdnem érzékelhetetlen legyen, vagyis érintésmentes biometrikus azonosítást alkalmazzanak.[4] Ezekben az esetekben az arcfelismerés megfelelő megoldást adhat.

Az arcfelismerés fontosságát az azonosításban viszonylag korán felismerték és már a hetvenes évektől elkezdték a fejlesztést. Jelentős fejlődés azonban csak a kilencvenes évektől figyelhető meg, ekkorra jelentek meg megbízhatóbb módszerek és a nagy számításigény ellátására alkalmas hardverek.

2 Földesi Krisztina: A biometrikus azonosítási eljárások alkalmazhatósága a rendőri munkában. PhD-értekezés. Óbudai Egyetem, 2017, 70. o.

3 Otti Csaba: Belépési pontok meghatározása markovi modellel, nagy létszámú üzemek biometrikus beléptetésénél. Hadmérnök, 2017/2.

4 Baráth Artur: Biometrikus azonosítási eljárások bemutatás, elemzése és az RFID-rendszer vizsgálata I. rész. Dunakavics, 2016/II., 5–20. o.

A kezdetekben az arcfelismerés a mesterséges intelligencia egyik legnehezebb részterületének tűnt. Az utóbbi évtizedben azonban folyamatosan születnek kutatási eredmények, ez lehetővé tette a gyakorlati alkalmazások elterjedését.

Az arcfelismerésben alapvetően a következő két módszer terjedt el:

1. Mintaalapú (vagy fotometrikus): lényege, hogy az arc vagy az arc részleteinek (szem, ajkak, orr) globális tulajdonságait vetik össze a tárolt mintával, mintákkal.
2. Geometriai: az arc különböző részleteinek – szem, ajkak, orr, áll stb. – egymáshoz viszonyított elhelyezkedését és méretét elemzik.

Az arc detektálása

Elsődleges feladat a beérkező kép-/videoadatokon felismerni az arcokat (ha vannak), ez lesz a vizsgálati terület. Csak itt található az algoritmus számára hasznos információ, ezért a későbbi eredmények az arc detektálására épülnek, így ezt nagy pontossággal kell végezni. Azonban valós környezetben nehéz a felismerés. A fej pozíciója, arcvonások, arckifejezések különbözhetnek a mintáktól. Az arcot részben takarhatja valami, a személy arcszőrzete, haja vagy akár egy szemüveg viselése is gondot okozhat. Több módszer létezik az arc érzékelésére:

1. Komponensalapú módszer: megkeresi az arc egyes részeit (szem, orr, száj), majd megvizsgálja, hogy megfelelnek-e az arc geometriájának.
2. Ellipszisillesztés: élkiemelés után egy ellipszist illeszt a képre. A pontos arcérzékelés érdekében az arc felépítése, arányai alapján feltételek szabhatók meg az ellipszis tulajdonságaira.
3. Bőrszínalapú szegmentálás: színes képeknél a bőrszínt kihasználva kiemelhető az arc. Előnye, hogy független a fej pozíciójától, és igen gyors módszer.

Az arcfelismerő rendszerek elterjedtsége

Az Egyesült Államok fizikai, kísérleti laboratóriuma *(National Institute of Standards and Technology; NIST)* rendszeresen végez bármely arcfelismerő alkalmazásokat gyártó számára elérhető független teszteket. Ezeken mindenki számára azonos feltételeket teremtenek. Az utolsó kiértékelt vizsgálat pub-

likálására 2017 márciusában került sor[5]: tizenhat gyártó több mint harminc algoritmusa versenyzett egymással. Ezek olyan gyártók, amelyek aktívan jelen vannak az amerikai piacon is, és a termékeik elismerése presztízst jelent. Arról nincs információ, hogy a világ más részein mekkora a piaci szereplők aránya, de a tizenhat piaci szereplő jelentősnek nevezhető. A tesztelés során életszerű helyzeteket teremtettek[6], ilyen volt például a repülőgép fedélzetére vezető folyosón, vagy a beszállókártya automata kapujában, a repülőtér várótermében vagy a vasútállomás kapuiban elhelyezett kamera. A teszteken azonos körülményeket teremtve lehet a képességet összehasonlítani.

A fizetési szolgáltatásokról szóló európai irányelv *(European Payment Service Directive; PSD2)*[7] előírja, hogy a pénzintézeteknél vezetett számlákhoz tartozó bankkártyás fizetésekhez két független autentikáció szükséges. Az egyik lehet biometrikus azonosítás, amely esetében az írisz- és ujjnyomat-azonosítás mellett már elkészült az arcfelismerésre képes azonosítási mód is.[8]

Az arcfelismerő rendszerek pontossága

Az arcfelismerő rendszerek két fő csoportra oszthatók. Az egyik a képalapú arcfelismerés, a másik pedig a videóból való arcfelismerés. Mindkét típus alapja egy már előre rögzített és a rendszerbe feltöltött képeket tartalmazó adatbázis. A két metódus közötti különbség, hogy a képalapú arcfelismeréskor a rendszer egy számunkra ismeretlen időpontban elkészített fényképet vet össze az adatbázissal, míg a videóból való arcfelismerésnél akár élő videófolyam is vizsgálható, így például zártláncú kamerarendszerben is üzemeltethető.

A rendszer lehető legjobb pontosságú működéséhez meg kell teremteni az ideális környezetet és a megfelelő technikai hátteret. Az emberi szem számára a tévéképernyőn vagy monitoron megjelenített arc akkor ismerhető fel, ha a pupillák közötti távolság[9] minimum tizenkét pixel. Ha ez a feltétel nem teljesül, még mi, emberek sem látjuk emberi arcnak a kép tartalmát. Hasonlóan működnek az arcfelismerő rendszerek különböző algoritmusai is. Más-más számú pixelnek kell lennie a szemek közötti távolságnak ahhoz, hogy észlel-

5 https://doi.org/10.6028/NIST.IR.8197
6 https://doi.org/10.6028/NIST.IR.8173
7 2015/2366 EU Directive
8 https://www.morpho.com/en/strong-costomer/autentication-psd2
9 Dmitry O. Gorodnichy: Video-Based Framework for Face Recognition in Video. In: The Second Workshop on Farc Processing in Video. May 8–11, 2005, Victoria, British Columbia, Canada

ni tudja az arcot a videófolyamon vagy egy képen. Az állóképes arcfelismerésnél hatvan pixelben határozható meg az a érték, amely a fényképen szereplő arc két szemének pupillái közötti minimális távolság. A videófolyamon megjelenő arcok esetében ez a szám körülbelül ötven pixel.

Kamera

A jó minőségű nagy felbontású kamerák használata elengedhetetlen. Ezekkel lehet használható képeket vagy videót küldeni az arcfelismerő szoftvernek. Ez nem azt jelenti, hogy egy kisebb felbontású kamerával a rendszer nem használható vagy nem üzemképes, de a minél nagyobb fokú pontosság érdekében jobb, ha a kamerák kiváló minőségűek. A készülékek kiválasztásakor figyelembe kell venni, hogy milyen módon szeretnénk alkalmazni az arcfelismerő szoftvert. Egy beléptetőpontnál, ahol körülbelül hetven-nyolcvan centiméter szélességű az emberek által használható „folyosó", nem kell egy 4K felbontású berendezést alkalmazni, hiszen erre a célra megfelelő egy két megapixeles Full HD kamera. A manapság kapható legjobb termékek az IP-alapú kamerák, amelyek képesek jó minőségű képek rögzítésére és továbbításra az arcfelismerő szoftvernek. Márkanévtől, típustól függetlenül a paramétereiket elsősorban a felbontási képességükben mérjük, amelyet kétféleképpen határozhatunk meg:

– hány képpont alkotja a képet vízszintesen és függőlegesen (például 1280 x 720);
– hány millió képpont alkotja a képet (például három megapixel = hárommillió képpont)[10].

Ebből adódóan minél több pixelt tartalmaz egy kép, annál jobb és részletgazdagabb képet kapunk, ami segíti az arcfelismerést.

A másik fő paraméter a fényérzékenység, amely megadja, hogy mi az a legkisebb fényerősség, amely a képek elkészítéséhez szükséges. A színes kamerák nagyobb megvilágítást igényelnek, mint fekete-fehér társaik, de egyegy professzionális darab esetében még így is lehet a fényérzékenység 0,1 lux alatti.[11]

10 http://cameradepo.hu/termektamogatas/a-biztonsagi-kamerak-felbontasarol
11 http://oktel.hu/szolgaltatas/kamerarendszer/kamerak/kamera-parameterek/

Objektívek

A kamera megválasztásán túl a hozzá tartozó objektívre is figyelni kell. Egy bizonyos felbontású kamerához csak hasonló vagy nagyobb felbontású objektívet szabad választani. Az objektív egyik fő paramétere a fókusztávolság (f), amely a nagyítás mértékét határozza meg. A gyártók mm-ben adják meg ezt az értékét. Fontos, hogy ha közelíteni szeretnénk a kamerával egy pontra, vagyis nagyítunk, akkor csak az optikát használjuk, és mellőzük a digitális nagyítást.[12]

Ha az arcfelismerő rendszerből a lehető legtöbbet akarjuk kihozni, a pontosság növelése érdekében néhány külső tényezőt is optimalizálni kell. Először is figyelembe kell venni, hol akarjuk üzemeltetni a rendszert; a felszerelt kamerák előtt milyen sűrűségű és sebességű lesz az emberek áthaladása (van beléptetés, vagy csak irányított áthaladás). Célszerű olyan helyre felszerelni a kamerákat, ahol az áthaladás korlátozott vagy lassabb. A jobb arcfelismerő szoftverek képesek egy időben több arcot is lefuttatni. Ha azonban nagyobb pontosságot szeretnénk elérni, illetve a felismert arc „tulajdonosával" szemben bármilyen intézkedést szeretnénk foganatosítani, akkor a beléptető az egyik legjobb megoldás.

Pozíció

Arcfelismerés szempontjából egy kamera akkor van ideális helyen, ha horizontálisan és vertikálisan is szemben helyezkedik el a vizsgálandó emberekkel. Ez csak akkor kivitelezhető, ha az arcfelismerést beléptetőpontokon használjuk. Ilyenkor az alany együttműködő a rendszerrel, hiszen az arcának a felismerése kell a bejutáshoz. Abban az esetben, ha csak területet figyelünk, és ott nincs irányított mozgás (rendezvények területén vagy közterületen), akkor az alanyok nem lesznek együttműködők a rendszerrel, így ez nehezíti a feladatot, csökkentheti a hatékonyságot. Pontosan emiatt ez a rendszer térfigyelő kamerák bevonásával nem üzemeltethető, mert azok pozíciója általában nagyon magasan van, tehát az elhelyezésből adódó nagy beesési szög, vagy a nagy távolság miatt nem kapunk megfelelő méretű képet. Ha mindenképpen közterületen szeretnénk arcfelismerő rendszert üzemeltetni, akkor célszerű a térfigyelő és az arcfelismerő kamerákat párhuzamosan alkalmazni.

12 http://www.fenykepes.hu/html/z2_optikaI.html

Fény

Fontos külső környezeti tényező az arcfelismerő rendszer kamerái körüli megfelelő megvilágítás. Ennek hiányában a működés, illetve a találatok tévesek lehetnek, illetve el is maradhatnak. Ez a beltéri üzemeltetésnél könnyen megoldható, mert a helyiségben található fényforrások általában elegendők az arcok kellő megvilágításához. Ha mégsem, akkor kiegészítő lámpatestekkel könnyen elérhető a kívánt fényerő. Ugyanez egy kültéri helyszín esetében nehezebben kivitelezhető, főleg ha a rendszert sötétedés után, esti/éjszakai időszakban is használni szeretnénk. Ebben az esetben is gondoskodnunk kell a megfelelő megvilágításról. Ilyen kültéri helyszínek esetében az időjárás egyéb tényezőit is figyelembe véve (eső) mindenképp védett, fedett helyen célszerű működtetni a rendszert. Az ideiglenes fedett építmény tartószerkezeteire olyan fényforrások felszerelése javasolt, amelyek szórt fényt adnak, és fényerejük eléri a négyezer lument.

Referenciaképek

A találati pontosságot az adatbázisba feltöltött referenciaképek minősége is nagyban befolyásolja. Azok minősége is olyan kell hogy legyen, hogy azt a rendszer elfogadja, és feltölthető legyen. Az 530 x 420-as felbontású, vagy más szóval 0,2 megapixel méretű klasszikus igazolványképek a leginkább megfelelők. Az igazolványképeken túl egy egyszerű, személyről készült fénykép is felhasználható, ha megfelel a következő feltételeknek:

– a fotó szemből készül;
– fülek, szemek, homlok tisztán látható;
– fej nem biccentett.

Az arcfelismerő rendszerek felhasználásának jogosultsága

Arcfelismerés céljából kamerákat sok helyen el lehet helyezni, például bankokban, reptereken, boltokban, áruházakban, stadionokban, sportrendezvényeken, államigazgatási épületekben, kaszinókban. Napjainkban számos arcfelismerő rendszert használnak különféle célokra.

A rendvédelmi szervek bűnüldözési célra hasznosíthatják, így kiszűrhetik a tömegből azokat, akik körözés alatt állnak, vagy akiket valamilyen okból keresnek, legyen szó bűnözőkről vagy terroristákról. Természetesen mindezt csak akkor, ha van róluk egy-egy használható (a leírt paramétereknek megfelelő) kép, amely feltölthető a rendszerbe.

A hipermarketek statisztikákat készítenek az arcfelismerő rendszerek adataiból. Ezek egyik eleme például, hogy hány ember tartózkodik a boltokban. Külön kimutatható, hogy mennyi férfi és nő fordul meg az üzletekben, így az érdeklődési körükről is információ gyűjthető.

Ezen felül a kamerarendszereket nemcsak szűrésre vagy elemzésre használhatjuk, hanem belépési jogosultságok is ellenőrizhetők. Például egy vállalat épületébe történő beléptetésnél alkalmazható úgy, hogy a jogosultnak érintkeznie sem kell semmivel az azonosítása során.

Az arcfelismerő rendszerek azonban még nem túl elterjedtek (kivéve Kínában)[13], és az emberi szabadságjogok megsértése miatt rengeteg szervezet erősen bírálja őket, ugyanis az arcfelismerő szoftverrel támogatott kamerák sokaságának üzemeltetésével lehetőség nyílik a polgárok folyamatos megfigyelésére akár közterületen is, így a totális megfigyelésre.[14]

Az arcfelismerő rendszerek tömegtartózkodási helyeken

Tömegtartózkodási helyen az egyidejűleg háromszáz embernél több személy befogadására alkalmas helyiségeket értjük.[15] Jelen pontban egy fiktív rendezvényen mutatjuk be egy beléptetés támogatására használt arcfelismerő rendszer felépítését. A tömegtartózkodási helyeken általában olyan személyek kapcsán alkalmazzuk a rendszert, akik „nem együttműködők", vagyis annyira nem szeretnék, ha esetükben sikeres lenne az arcfelismerés. Egy rendezvényen elengedhetetlen a beléptetés, ezáltal az áteresztő kapuk létesítése, ami hozzájárul ahhoz, hogy az emberek egyesével lépjenek be az ellenőrzött te-

13 Molnár Csaba: 176 millió kamera kereszttüzében: a kínai Nagy Testvér mindenkire odafigyel. Magyar Nemzet, 2018. április 7. https://mno.hu/tudomany/176millio-kamera-kereszttuzeben-a-kinai-nagy-testver-mindenkire-odafigyel-2458366

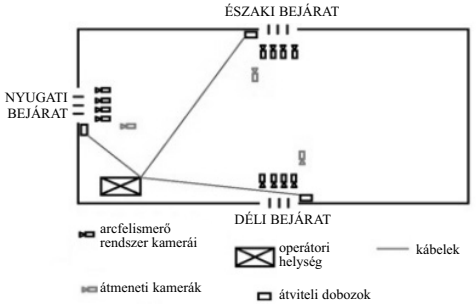
14 https://steve4security12.blog.hu/2013/12/20/arcfelismero_kamerarendszerek

15 Az országos településrendezési és építési követelményekről szóló 253/1997. (XII. 20.) kormányrendelet 1. számú melléklete.

rületre, ezzel lassítva az áthaladást és elősegítve, hogy a kamerák lássák az emberek arcát.[16]

Fontos, hogy a rendezvényre történő beléptetéskor használt arcfelismerő rendszer esetében minden áteresztő csatornához kell a szükséges darabszámú kamera. A gyakorlatban ez azt jelenti, hogy ha például három beléptetési pontunk van egy rendezvényre és mind a három helyen négy kapu van, akkor kapunként egy kamerát ajánlott felszerelni, azaz jelen esetben tizenkettőt, amely hozzá van rendelve az arcfelismerő rendszerhez, így lefedi a beléptetés egészét. Természetesen érdemes felszerelni minden beléptetési ponthoz legalább egy átnézeti kamerát, amellyel belátni az áteresztő részeket, ez legyen forgatható, ha esetleg követni szeretnénk valakit *(ábra)*.

Rendezvénybeléptetés arcfelismerő kamerákkal



Forrás: http://www.oselions.hu

A kamerákat közvetlenül az arcokkal szemben nem lehetséges felszerelni, ezért úgy kell őket elhelyezni, hogy ne zavarják az áthaladó embereket, ne lehessen könnyen elérni, és olyan távolságban legyenek, hogy a rálátási szög ne legyen túl nagy, az emberek pedig ne legyenek túl messze ahhoz, hogy a rendszer ne ismerje fel őket. Ha a kamerát két és fél méter magasan helyezzük el, akkor egy átlagos magasságú ember könnyen áthaladhat alatta, és a berendezést is nehéz elérni. Az optika és az ember feje által bezárt szög tíz méteren is 4,57° lesz, ami elhanyagolható az arcfelismerés szempontjából.

16 http://www.oselions.hu

A kamerák tápjai az átviteli dobozokban helyezkednek el több más berendezéssel együtt, Az adatfolyam továbbítását egy router vagy switch végzi, így az operátori helyiségben láthatóvá válnak a képek. Az átvitel mehet optikai vagy rézkábelen, de akár vezeték nélküli megoldás is lehetséges.

Az operátori helyiség melletti szerverszobában a beérkezett felvételek alapján történik az elemzőmunka, amelyet az arcfelismerő rendszer szerverei végeznek el. Az eredményeket továbbítják a felhasználói végpontokra, amelyek lehetnek az operátori helyiségben telepített PC-k, de akár mobiltelefonra vagy tabletre is érkeztethetők a találatok.

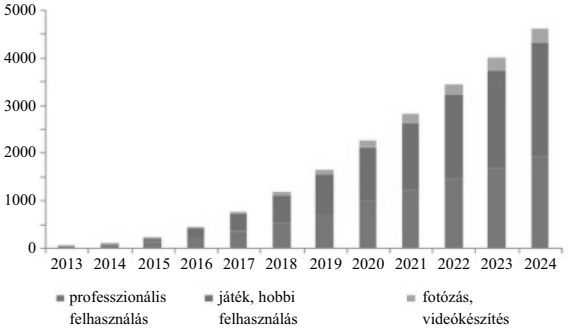
DOI: 10.38146/BSZ.2019.1.11

JAROLIN JÓZSEF

Eljárások drónok felderítésére

Az utóbbi években ugrásszerűen elterjedtek a pilóta nélküli repülő eszközök[1], és ez a tendencia vélhetően továbbra sem változik, tulajdoníthatóan az egyre inkább megfizethető árnak, amely egyre bővebb funkcionalitással párosul. Az eszközöket nagyrészt magáncélra, hobbiszinten használják, de mind nagyobb mértékben alkalmaznak speciális, feladatorientált eszközöket *(ábra)*.

Az észak-amerikai drónpiac forgalmának várható alakulása (2013–2024; millió amerikai dollár)



Forrás: http://www.grandviewresearch.com/industry-analysis/consumer-drone-market

Gyakorlati példák is alátámasztják, hogy a drónok jó, illetve rossz ügyek szolgálatába is állíthatók, és a leghasznosabb képességeket a legártalmasabb célokra is lehet használni. Természetesen a drónok használhatóságának sokrétűsége alapjaiban is veszélyeket rejt magában, a nem megfelelően képzett

1 A továbbiakban: „drón", egyaránt alkalmazva az *UAV (Unmanned Aerial Vehicle,* pilóta nélküli légi jármű): olyan légi jármű, amely repülését, a légtérben való közlekedését a fedélzeten lévő személyzet nélkül végzi és *UAS (Unmanned Aerial System,* pilóta nélküli légijármű-rendszer): a pilóta nélküli légi járművet, annak földi vezérlő/irányító állomását, a járművön elhelyezett hasznos terhet és a két pont közötti adatkapcsolatot, irányítást, telemetriát magában foglaló rendszer fogalmak helyett.

pilóták, illetve esetleges minőségi problémákból eredő meghibásodások okán. Belátható azonban, hogy ezek az eszközök könnyen alkalmazhatók kifejezetten ártó szándékkal is. Az elterjedtségből eredő tömegtermelés miatt az áruk kifejezetten megfizethető, így a velük elkövetett káros cselekmények (illegális migráció támogatása, csempészet, terrorcselekmény robbanóanyaggal, tömegpánik-okozás, személyisérülés-okozás) meglehetősen gazdaságosan kivitelezhetők, a bőséges funkcionalitás pedig könnyebben végrehajthatóvá teszi az elkövetést.

Károkozási lehetőségek

A következőkben felsorolt esetekben közös pont, hogy a drónok képességeinek kihasználását állítják az elkövetendő cselekmények szolgálatába. Ezek közül a legfontosabbak a

– kis, feltűnésmentes méret;
– repülési, így nagy mobilitási képesség;
– megbízhatóság;
– hasznos teher cipelésének képessége;
– képalkotási lehetőségek.

Egyértelmű, hogy ezek a képességek külön-külön is, kombinálva még inkább egyszerűvé, hatékonyabban kivitelezhetővé teszik a károkozást. Külön kiemelendő, hogy a távolról vezérlés (az eszköz és az irányító személyének elválása) sok esetben a drón, és így az elkövetendő cselekmény személyhez kötését is megnehezíti. A károkozás típusai a következők:

Gondatlan veszélyeztetés: alapvetően a többitől eltérő cselekvési forma, ebben az esetben nem feltétlenül domináns tényező az ártó szándék. Kevés tudással, nem megfelelő tapasztalattal, esetleg hanyagul történő reptetés következtében előállhat gazdasági kárral, esetlegesen személyi sérüléssel járó baleset.

Kiemelt létesítmény elleni támadás, anyagi vagy erkölcsikár-okozás: az adott létesítmény (repülőtér, kritikus infrastruktúra, katonai létesítmények stb.) megfigyelése, működésének megzavarása ugyanúgy lehet cél, mint a létesítménnyel szembeni károkozás. Könnyen megérthető, hogy a tilos vagy korlátozott helyeken történő reptetés által okozott veszélyhelyzet illetve baleset katasztrófához is vezethet.

Rendezvény megzavarása, pánikkeltés: történhet tudatosan, pánikkeltési, illetve médiabeli reakciót kiváltó okból, figyelmetlenségből, hanyagságból

egyaránt, hasonló következményekkel. Bármelyik valósul is meg, nem nehéz elképzelni, hogy egy tömegrendezvény esetén egy kisebb károkozás is kelthet pánikot, amelynek hatását a tömeg jelentősen felerősíti. Ehhez elegendő, ha egy tömegbe zuhanó drón személyi sérülést okoz, ami a tömegből kontrollálhatatlan menekülést válthat ki.

Csempészet (drog-, fegyver-, cigaretta-, kommunikációseszköz-, lőfegyver-): a repülési hatótávolság és teherhordási képesség növekedésével a drónok ideális eszközévé váltak ennek a tevékenységnek. Kisebb súlyú (néhány kilogramm), nem engedélyezett, vagy kifejezetten tiltott eszközök/áruk szállítása könnyen megvalósítható ily módon. Ez főként határon való átjuttatást vagy őrzött intézménybe történő bejuttatást jelent.

Felderítés és képrögzítés: ebbe a kategóriába értendő a néha a személyiségi jogok megsértésével is együtt járó képek és videók készítése, egyúttal események, objektumok megfigyelése is. Veszélyességi szempontból ehhez kapcsolódhat, a cselekmény esetleges lelepleződésekor a megfigyelt személy vagy csoport drónnal szembeni agresszív fellépése (tüzelés éles lőfegyverrel, így a drónban vagy annak környezetében okozott kár). Mindamellett szintén óhatatlan a károkozás, ha „katasztrófaturista típusú" felhasználás esetén az elkövető a védelmi egységek (tűzoltó-, mentőhelikopter) repülő eszközeit akadályozza.

Rádiófrekvenciás, illetve egyéb technikai zavarás: a károkozás legszofisztikáltabb, nem is sűrűn alkalmazott módja. Olyan kis méretű eszköz szállítása, majd terítése, amely képes valamilyen szolgáltatás megzavarására. Ezek lehetnek

– rádiófrekvenciás zavaró, amely akár teljesen ellehetetleníti a rádióforgalmazást, így egyebek között akár a telefonforgalmat (hosszú ideig nem fenntartható az energiaszükséglet miatt, ami a drón fedélzetén véges);
– technikai zavaró vagy szennyező anyagok célba juttatása – például széntartalmú anyagok szórása, amely a radarok elvakítására szolgál, egy következő dróntámadás előkészítése céljából;
– szén- vagy más vezetőszálakkal zárlatokozás, az elektromos hálózat működésének szabotálása érdekében.

Lőfegyverek alkalmazása: nehezen kivitelezhető eljárás, mivel meg kell oldani a visszarúgás, hátrasiklás kérdését, ráadásul a lőfegyver és a fedélzeten tárolt lőszer súlya és mérete is korlátozó tényező.

Precíziós rögtönzött robbanóeszköz célba juttatása hasznos teherként: a lőfegyverhez képest alkalmazásának sokkal nagyobb az esélye, a következők miatt:

a) a robbanóeszköz megépítése sokkal kevesebb szaktudást igényel;
b) a drón precíz vezérlése, így az eszköz célba juttatása nagyobb esélyt ad a sikeres végrehajtásra és a menekülésre is;
c) nem kell kifürkészni a cél útvonalát, nem kell semmit telepíteni vagy álcázni.

Vegyi, biológiai, radioaktív hasznos teher célba juttatása: ezek már kis mennyiségben is veszélyes anyagok, így a súly és a méret nem jelent korlátozó tényezőt. Szinte észrevétlenül, nagy távolságról célba juttatható, és a légtérben való eloszlás miatt nagy területen képes kárt okozni. A kár mértékét a terített anyag határozza meg, akár jelentős élőerő-veszteséget vagy pszichológiai hatást okozva.

Drónfelderítés, -elhárítás

A drónok jelentette új veszélyforrás természetes módon magával vonja az ellene való védekezés kialakulásának módozatait. A veszély mértékét egyre több érintett szerv, valamint gyártó cég is felismerte, kezdetben ez utóbbiak a szakterületüknek megfelelő eszközök kifejlesztését hajtották végre (radart gyártó cég drónokra specializált radart, rádióvevő készüléket gyártó cég rádiós megoldást készített). A cégek később rájöttek, hogy egyenként, a veszély összetettségéből adódóan csak – nem elégséges – részvédelem kialakítására képesek, ezért erre szakosodott rendszerintegrátor cégek bevonásával, több cég termékéből alkottak komplex védelmi rendszereket.

Felderítési metódusok

Az eljárások célja a drónok közelben történő működésének felismerése, lehetőség szerint lokalizálása, valamint a veszélyesség fokának esetleges meghatározása. A következőkben összefoglalom, milyen eljárások alkalmazhatók a feladat-végrehajtásban, amelyek egyrészt kiegészítik egymást, másrészt megerősítik egymás adatait.

Akusztikus felderítés – a metódus alapelve, hogy mikrofonokkal (mikrofonokból álló hálózattal/ráccsal/mezővel) ellenőrzik a környezetben észlelhető hangteret, és a drónokra (rotorokra) jellemző hangkép észlelésekor kelet-

kezik riasztás. A felderítési metódus esetén a drónok meghajtása a fő szempont, hiszen belátható, hogy egy kereskedelmi forgalomban kapható, kis méretű multirotoros gép kisebb hangintenzitás keltésére alkalmas, mint egy gázturbinás hajtású, így az észlelési távolság kisebb. Az akusztikus szenzorok néhány száz méteres hatótávolsága mindenképpen korlátozó tényező. Fontos továbbá, hogy lakott területen történő alkalmazásukkor a környezeti zajok mennyire befolyásolják a működés hatékonyságát.

Radarfelderítés – az eljárás alapelve, hogy a radar által kibocsátott magas frekvenciás sugárzás esetén a szilárd tárgyak visszaverő közegként viselkednek, a visszavert jel irányából és az eltelt időből meghatározható az adott visszaverő közeg, esetünkben a drón elhelyezkedése, mozgási iránya és sebessége. Ennél a felderítési metódusnál fő tényező a drón mérete és anyaga. A nagyobb méret alapesetben nagyobb visszaverő felületet eredményez (speciális esetben a felületet sok éllel és csúccsal tagolják, így visszaverési paramétereit szándékosan rontják a radarral történő nehezebb észlelés érdekében), amely megkönnyíti az észlelést. Érthető módon radarral könnyebb egy nagy, merev szárnyú légi eszköz detektálása, mint egy kis méretű, multirotoros gépé. Az esély utóbbiaknál is fennáll, mivel a rotorok környezetében kialakuló elektromágneses tér is visszaverő közeg. Anyagfelhasználást tekintve a speciális rádiófrekvenciás elnyelő anyagokból felépített vagy ilyen jellegű festékkel kezelt drón észlelése nehezebb radarral, mivel ezek akadályozzák, illetve részben elnyelik a rádióhullámok visszaverődését.

Rádiós felderítés – a módszer alapelve a távvezérlő és a drón közötti rádióforgalmazás detektálása (vezérlőjel és/vagy videojel), ennek alapján az eszközök esetleges lokalizálása. Hátránya, hogy ha a drón nem manuálisan távvezérelt (autonóm navigációjú, GPS-koordináták alapján repülő eszköz), rádiósan inaktív, így nincs kisugárzott, detektálható jele, ezért rádiós úton nem lehet felderíteni. Ebből látható, hogy ennél a felderítési metódusnál elsődleges a drón vezérlésének típusa (bár kevésbé elképzelhető, de nem kizárt, hogy egy autonóm módon repülő drón videojelet sugározzon vissza). Az eljárás előnye, hogy a rádióhullámok minden irányú terjedése magával vonja azt is, hogy bármely irányból fel is deríthető, ehhez „csak" a rádiós rálátásnak kell megvalósulnia, ami egy levegőben lévő tárgy esetén kilométeres távolságból is működik.

Optikai felderítés – az eljárás alapelve a légtér kamerákkal történő megfigyelése, az abban történő változások, mozgások észlelése esetén a térrész pontosabb (nagyított, képfeldolgozó algoritmusokkal megtámogatott) ellenőrzése a mozgás okának beazonosítása céljából. Természetesen rossz látási

viszonyok (éjszaka, köd, szürkület) esetében történő feladat-végrehajtásnál előtérbe kerülhet az infrakamerák alkalmazása. A módszer fő kritériuma a drón mérete, valamint sebessége. Fontos megjegyezni, hogy erre az eljárásra negatív befolyással lehetnek az időjárási viszonyok, mindamellett a repülő objektumról, az esetleges hasznos teherről ez szolgálhat a legrészletesebb információval.

A felderítési metódusok különbségei

Az ismertetett eljárások közötti fő különbség a hatótávolság. Míg fizikai rálátás esetén a radarjelek és a rádióhullámok kilométerekről is hatékonyan detektálhatók, addig például az akusztikus vagy optikai szenzorok csupán pár száz méterről hatékonyak. Az erősebb védelmi rendszereknek éppen ezért van komplex felderítőképességük. Távolból történő észlelésre leginkább radart és/vagy rádiós eszközöket, míg közelebbi beazonosításra optikai berendezéseket vetnek be, így többszintű felderítést valósítanak meg (az első szinten – radar, rádió – nem állapítható meg, hogy a drón milyen, mekkora, hordoz-e hasznos terhet).

Fontos kiemelni továbbá, hogy amíg a radar és a rádiós szenzor reális időn belül 360 fokos lefedettséget képes nyújtani, a távollátó kamerák esetén a belátható szög ennél jóval kevesebb. Egy radar vagy rádiószenzor által észlelt jel esetén azonban az optika irányba fordítása pontosabb beazonosítást, precízebb sebességmeghatározást tesz lehetővé.

Az egyes eljárások alkalmazási feltételeinek különbsége teszi szükségessé komplex rendszer alkalmazását, és ezáltal a hatékonyabb védelem megteremtését. Egy rádiósan nem kommunikáló, autonóm módon repülő jármű esetén a rádiós szenzor önmagában semmit sem ér, ugyanakkor a vele párban alkalmazott radar felderítheti a légtérben megjelenő eszközt. Egy speciálisan kialakított vagy nagyon kis méretű drón radarral történő felderítése nehézkes, azonban ha rádiós vezérlésű, akkor a rádiószenzor detektálja. Az optikai érzékelők alkalmazása minden esetben pontosabbá teszi a konkrétabb eszköz, illetve elhelyezkedés beazonosítását, esetlegesen információt szolgáltathat annak ártó szándékú voltáról (hordott teher).

A komplex rendszer másik fő erőssége, hogy az egymást támogató alkotóelemek egységet alkotnak. A radarral történő észlelés vagy rádiós detektálás hatására az optikai szenzor emberi beavatkozás nélkül irányba fordul és a célkövetés is megvalósul, így nagyságrendekkel megnöveli az azonosítás hatékonyságát. Komplex rendszer nélkül, a detektálás után az optikával történő

célkeresést manuálisan kell végrehajtani, megtalálni a repülő eszközt. Ugyanez igaz az eszköz elhárítására is, a detektálás után nemcsak az optika, hanem a zavaróegység is irányba fordul, így teremthető meg a célzott, csak a drónra irányzott zavarás, amely komplex rendszer nélkül szintén manuális beavatkozást igényel. Napjainkban a drónok óránkénti ötven-száz kilométer sebességre képesek, ami azt jelenti, hogy a gép másodpercenként tizenöt–huszonöt métert tesz meg, ebből következően a beavatkozás esetében kritikus tény az idő, amely nem engedi meg az emberi beavatkozásból és döntésből származó késlekedést. Szintén fontos tényező, hogy a felderítő rendszer komplexitása tovább növelhető kockázatelemző modul alkalmazásával. Ennek funkciója, hogy az egyes szenzorokról érkező adathalmaz összefüggéseiből következtetéseket von le, ezzel segítve és felgyorsítva a döntés meghozatalát. Például egy nagy sebességgel közelítő (radar- és rádiószenzorok alapján), terhet cipelő (optika), nagyobb méretű drónt a rendszer veszélyesebbnek ítél, mint egy mikroméretű, lassú eszközt.

Elhárítási metódusok

Egy drón feladat-végrehajtásának megakadályozására sokféle megoldás létezik, kockázatmentes megakadályozására azonban jóval kevesebb. Ennek a kettősségnek az oka, hogy az elhárítási megoldások a drón cselekedetének befolyásolására szolgálnak, miközben a környezetet nem veszik figyelembe. Nem foglalkoznak – mert tökéletes megoldást nem tudnak nyújtani – azzal, hogy a drón esetleges lezuhanása milyen következményekkel jár, milyen fizikai károkat, esetleg személyi sérüléseket okoz. Egy kritikus infrastruktúra védelménél nem feltétlenül szükséges számolni ezekkel a tényezőkkel, mivel a védendő érdek túlmutat ezen, illetve az objektumok környezete is legtöbbször lehetővé teszi az ettől való eltekintést. Belvárosi környezetben egy tömegrendezvény esetén azonban ezektől a járulékos következményektől nem lehet eltekinteni.

Rádiós zavarás: az eljárás alapelve, hogy a nemkívánatos jel frekvenciáján egy nagyobb jelet sugározunk. A nemkívánatos jel drónok esetében a vezérlőjel, vagy a navigációs műholdról a drónhoz érkező jel (GNSS[2]) lehet. Egyszerűbb a szóba jöhető frekvenciasávok teljes zavarása (nem konkrét frekvenciák, hanem nagyobb frekvenciaterek), ami viszont a közelben talál-

2 Globális navigációs műholdrendszer *(Global Navigation Satellite Systems),* az egész Földre kiterjedő, műholdakon alapuló navigációs rendszer általános meghatározása.

ható WLAN-hálózatok működését is zavarhatja. Célirányosabb megoldás a drón vezérlőjeléből vett minta irányított visszasugárzásával történő zavarás. Zavarás esetén a drón viselkedése kiszámíthatatlan, beépített védelmi funkcióitól függően „hazatér", lezuhan, vagy lebeg.

Drónelfogó háló: az alapelv, hogy a drón belegabalyodik a rá kilőtt hálóba, a rotorok így fizikailag nem képesek mozgásban tartani. Ezzel kapcsolatosan jókora nehezítő tényező, hogy a célzás egy nagy sebességgel és valójában az irányítás miatt kiszámíthatatlanul mozgó céltárgy esetén nem egyszerű. Az eszköz maximum néhány száz méter távolságból hatásos, mindamellett siker esetén a drón lezuhanása, esetleg ernyővel történő leereszkedése továbbra is okozhat károkat.

HPEM (High Power Electro Magnetics): az eszköz nagy teljesítményű elektromágneses impulzuslökettel a drón vezérlőelektronikáját, ezáltal magát a drónt teszi működésképtelenné maximum háromszáz méter távolságból. Ennél az eljárásnál egyértelműen kijelenthető, hogy siker esetén a drón lezuhan.

GNSS Spoofing: az eljárás alapján megfelelő teljesítményszinttel hamis GNSS-jeleket sugároznak, ezáltal a drón hamis pozíciókat érzékel. Ha a kisugárzott pozíciók folyamatosan kis eltéréssel követik egymást, akkor az autonóm módon repülő drón elméletileg megfelelő földrajzi pontra irányítható, gyakorlatilag lassan eltávolítható a védett térrésztől. Az eljárás hátránya, hogy csak autonóm módon repülő drónok esetében hatékony, előnye, hogy ezeknél a drón a célterülettől eltávolítható a lezuhanás kockázata nélkül.

Távvezérlés átvétele: a metódus alapelve a drón hamis vezérlési utasításokkal való ellátása rádiós úton, így befolyásolva az útvonalát, repülését, működését. A megfelelő hamis vezérlési utasítások előállításához az eszköz teljes mértékű beazonosítása szükséges, ez teszi ugyanis lehetővé a vezérlési algoritmus azonosítását, ennek megfelelően a helyes utasítások alkalmazását. Mivel a vezérlési algoritmusoknak több fajtája létezik, egy hatékonyan működő rendszernek az összeset ismernie kell (adatbázis folyamatos frissítése) a drón pontos típusának meghatározásán felül. Ez az eljárás összetettségét, bonyolultságát tekintve nem lesz meghatározó a közeljövőben.

Megsemmisítés: bár a Nemzetbiztonsági Szakszolgálat feladataival nem összeegyeztethető, de a teljesség igénye miatt célszerű szerepeltetni a repülő eszközök lőszerrel, rakétával, lézerrel, egyéb módokon történő fizikai megsemmisítését, amely inkább katonai felhasználásban, illetve kritikusinfrastruktúra-védelem esetében elfogadható eljárás.

Előzetes tervezés: drónfelderítés, -elhárítás esetén kiemelten fontos az előzetes tervezés. Ennek a fázisnak ki kell terjednie a szenzorok megfelelő el-

helyezésére, egyúttal a célterület környezetében szükséges meghatározni azokat a zónákat is, amelyeken az elhárítás végrehajtható, azaz ahol a drón által elkövetett cselekményből kialakuló, vagy az esetleges lezuhanásából eredő károk minimalizálhatók. Nem nehéz belátni, hogy például egy kiemelt objektum védelmére fixen telepített rendszer esetében ez egyszeri feladat, míg tömegrendezvények biztosítására alkalmazott eszközöknél mindig az alkalomhoz, helyszínhez mérten kialakítandó. Utóbbi esetben fontos kiemelni, hogy az elhárító eljárások nagy része a drón kiszámíthatatlan viselkedését vagy lezuhanását okozza, így az ezzel járó kockázatok felmérése kötelező és szükségszerű, a rezsimszabályok megalkotásával együtt. A tervezés folyamán kell meghatározni a végrehajtáshoz szükséges szenzorok, valamint az elhárításhoz szükséges berendezések számát. A nehezen védhető helyszínek, ahol a biztonsági zónák a védett területtől messze vannak, nagyban befolyásolhatják ezeket a darabszámokat.

Nemzetközi kitekintés

A nagyvilágban nagyon sok gyártó készít szenzorokat, hatalmas minőségbeli különbségekkel. A gyártók felismerték az üzleti lehetőséget, amelyet a drónok nagymértékű elterjedése, illetve az általuk keltett veszély mértéke jelent, így kifejezetten ellenük készített eszközök gyártásába fogtak. Ha a komplexitást is a fő kritériumok közé soroljuk, azaz a szenzorok együttes működését, valamint a döntés-elősegítő algoritmusokat is az alapkövetelmények közé helyezzük, akkor már kevesebb potenciális rendszert találunk. Természetesen ott készítenek drónfelderítő/-elhárító rendszereket, ahol a gyártókapacitás, a gazdasági körülmények és az elméleti lehetőségek is rendelkezésre állnak.

A teljesség igénye nélkül, inkább csak kitekintésként, három komplex rendszert említenék meg.

Az egyik az angol AUDS[3] *(Anti-UAV Defence System)* rendszer, amely radart, optikát, valamint rádiós zavarót alkalmaz. A radarrendszer a felderítésért felel, és észlelés esetén a közös platformra épített optikát és zavarót irányba forgatja. A környezeti tényezők alapján a nappali vagy az infrakamera végzi az azonosítást, szükség esetén pedig végrehajtható a vezérlés és/vagy a GNSS zavarása.

3 http://www.auds.com

A német Guardion[4] rendszert jellemzi jelenleg az egyik legbőségesebb alkotóelem-kínálat. A rádiófrekvenciás iránymérőre, radarra, optikai és akusztikus szenzorokra épülő felderítést rádiós zavarással, nagy teljesítményű elektromágneses impulzuson alapuló működésképtelenné tétellel, valamint kézi és gépjárműre szerelhető hálóvetővel megvalósított elhárítással kombinálták.

A Hologarde[5] rendszer felderítési szempontból szintén a radar, rádiófrekvenciás, valamint optikai szenzorok egységét alkalmazza.

Összegzés

A drónok rendeltetésszerű és megfelelő használata előremutató és modern alkalmazási lehetőségeket teremt, mindamellett a védelmi szektornak nem szabad megfeledkeznie a rosszindulatú alkalmazás lehetőségéről sem. Már léteznek a drónok felderítésére alkalmas, hatékony eszközrendszerek – meglehetősen borsos beszerzési áron –, de az alkalmazásuk a feladathoz illesztett kiemelt tervező-, előkészítő munkát igényel. Mivel a drónok nagy sebessége miatt az adott beavatkozás időkritikus tevékenység, valamint az esetlegesen okozott károk felismerése és meghatározása okán felelősségteljes feladat, így az előkészítés, a szükséges erőforrások felmérése és a felkészülés úgyszintén idő- és anyagiforrás-igényes folyamat.

Az Nemzetbiztonsági Szakszolgálatot korlátozott mértékű rádiós drónfelderítő és -elhárító képesség jellemzi. Az észlelőképesség az úszó-világbajnokságon már bizonyított: a rendezvények helyszínein tizenhét nap alatt kilencvenkét drón működését észleltük.

4 http://drohnenabwehr.de/en/home/
5 http://hologarde.com

DOI: 10.38146/BSZ.2019.1.12

BALLA ZOLTÁN

Útlevélfejlesztés a rendszerváltástól napjainkig

A polgári demokratikus átalakulás következtében 1989–1990-től elérhetővé vált sok olyan technológia, amely korábban COCOM-[1] listán szerepelt. Ezek a technológiák, szabványrendszerek alapvetően megváltoztatták az okmányfejlesztés technikai környezetét is.

A Nemzetközi Polgári Repülési Szervezet *(International Civil Aviation Organization; ICAO)* normáinak[2] megfelelő, gépi adatolvasásra való áttérés műszaki megoldásaiban korszerűbb, védelmi módszereit tekintve sokkal magasabb szintű útlevélcsalád kibocsátását tette szükségessé. Az *1992. január 1-jétől* végrehajtott okmánycsere a magán-, a szolgálati és a diplomata-útlevelet is érintette. A szemléletbeli (okmánycsaládban való gondolkodás) és technológiai váltás következtében valamennyi említett okmány azonos alapanyagok felhasználásával, azonos műszaki háttérrel és gondosan kidolgozott, egységes védelmi rendszer alkalmazásával készült, amely a határrendészeti ellenőrzést is megkönnyítette. A változás leginkább az okmány kitöltésében mutatkozott meg. A korábbi kézi kitöltést mátrixrendszerű okmánynyomtatóval történő kitöltés váltotta fel, amely meggyorsította az útlevelek megszemélyesítését, amire a határnyitás miatt jelentős mértékben megnövekedett útlevéligény miatt szükség is volt.

1996–2004

A technikai és gazdasági liberalizáció a nyomdatechnikai vállalkozások számának ugrásszerű növekedésével járt. A vállalkozásokhoz érkező megrendelések mennyisége azonban nem követte ezt a növekedést, így többen az okmányhamisításban látták meg a lehetőséget. Ennek következtében az 1992-ben kiadott, első köztársasági címeres útlevél támadhatósága már néhány év után felszínre került. Az útlevélfüzet hátsó borítójának belső oldalára helyezett adatoldal kényelmes megoldás volt ugyan a határőrizeti szervek szempontjából, hiszen azonnal ott tudták az okmányt kinyitni, ahol az adatok voltak, de a fényképcse-

1 Coordinating Committee for Multilateral Export Controls.
2 ICAO Doc. 9303

re elleni védelem nem volt megoldott. A fényképcserét az adatbiztosító fólia melegítésével és felemelésével hajtották végre. A határőrizeti szervek sok esetben ki tudták szűrni a hamisított okmányokat annak alapján, hogy a melegítés hatására a fólia kis mértékben megnyúlt, hullámosodott. A szakértői bizonyítás azonban sokszor nehézségekbe ütközött.

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény felhatalmazása alapján megszületett a 86/1996. (VI. 14.) kormányrendelet, amely a biztonsági okmányok védelmével kapcsolatos feladatokat szabályozta és az okmányvédelem, -kibocsátás és -felügyelet vonatkozásában hatósági jogkört adott a Nemzetbiztonsági Szakszolgálat Szakértői Intézetének. A kormányrendelet lehetővé tette (teszi), hogy indokolt esetben a hatóság saját hatáskörbe vonja a biztonsági okmányok okmányvédelmének teljes körű kidolgozását. Ennek alapján – belügyminiszteri engedéllyel – kezdődött meg már 1996-ban az *1998. szeptember 1-jétől* kibocsátott újabb útlevélcsalád okmányvédelmi fejlesztése is a szakértői intézetben. Az új útlevél kidolgozásáig is szükség volt azonban arra, hogy megerősítsék a fényképcsere elleni védelmet. Erre a célra az 1997-ben bevezetett érvényesítő címke szolgált, amely az útlevélbe beragasztva, de már integráltan, lézergravírozással megszemélyesítve tartalmazta az arcképet, az útlevél számát és az érvényességi időt.

A technológia fejlődésével lépést tartva a Nemzetközi Polgári Repülési Szervezet az általa újrafogalmazott, az útlevelekre vonatkozó ajánlásában a beragasztott fénykép helyett az alapanyagba integrált arckép-megjelenítést preferálta, ezért szükség volt egy olyan modern technika meghonosítására, amely az arcképet közvetlenül az adatoldalban hozta létre.

Különböző megszemélyesítési módszerek (ink-jet printelés, lézernyomtatás, termotranszfer-nyomtatás) hosszas tesztelése után a választás a lézergravírozásra esett. A technika a kilencvenes évek közepén jelent meg, elsősorban kártyaigazolványok megszemélyesítésére. (A lézergravírozásos okmánymegszemélyesítés első hazai alkalmazása 1995 szeptemberében, a BM-kártyaokmány-családdal [rendőrség, határőrség, tűzoltóság, polgári védelem stb.] kezdődött.) A transzparens fedőrétegekkel borított fehér nyomathordozó műanyag rétegeken, a fedőréteg alatt lézersugárral égetett képpontokat lehet létrehozni anélkül, hogy a felületen sérülés keletkezne. Az égetés energiájától függően a keletkező pontok a szürke különböző árnyalatait hozzák létre, így alakítva ki az árnyalatos arcképet. A fedőréteg alatt keletkező képet csak a fedő műanyag fólia sérülésével lehet eltávolítani.

A technikai megoldás útlevélfüzetre történő átültetése több országban is megtörtént, de mindegyik esetben egy vastag műanyag lap (füzet méretű mű-

anyag kártya) alkotta az adatoldalt. A szakértői intézet által kidolgozott megoldás újdonsága az volt, hogy a vastag (0,76 mm) műanyag lap helyett vékony (0,2 mm), lézergravírozható műanyag rétegekkel borított biztonsági papírból állt az adatoldal. Ez *a világon elsőként* alkalmazott módszer kombinálta a vízjeles biztonsági papírok védelmi értékét a lézergravírozás biztosította arckép- és adatintegrációs lehetőséggel, így jelentősen megnehezítette a fényképcserés hamisítást. Első hazai okmányként ez az útlevél tartalmazott egyedi grafikai kialakítású Kinegram®-ot, azaz mozgó effektusokat és egyéb védelmi megoldásokat tartalmazó, optikailag változó diffraktív biztonsági elemet. Az így kidolgozott, új grafikai és védelmi megoldásokat felvonultató adatoldal sikerét bizonyítja, hogy 2001-ig egyetlen hamisítási kísérletet sem tártunk fel.

A szakértői intézet a 2001-ben feltárt új hamisítási módszer vizsgálata alapján módosította az arcképvédelmet. Az adatoldal UV-grafikáját megváltoztatva a vizsgált hamisítási módszer kiszűrése a határforgalom-ellenőrzéskor ismét egyszerűvé, gyorssá és biztonságossá vált.

Az útlevél-füzetlapok (belívek) grafikailag, nyomdatechnikailag és okmányvédelmi szempontból csak kis eltérést mutattak az 1992-ben bevezetett okmányhoz képest, mert az útlevél e részein nem volt statisztikailag kimutatható, minőségileg releváns hamisítási kísérlet.

2006–2017

A 2004. május 1-jei uniós csatlakozás után a Nemzetbiztonsági Szakszolgálat Szakértői Intézete megkezdte az Európai Unió Tanácsának rendelete[3] által előírt biztonsági, valamint a formai követelmények[4] alapján az e-útlevél fejlesztését. A biometrikus azonosításra alkalmas okmányok kibocsátása a 2001. szeptember 11-i események következtében az Egyesült Államok által elindított Visa Waiver program miatt vált szükségessé. A program ugyanis kimondta, hogy 2006-tól a korábban vízummentességet élvező országok azon állampolgárai léphetnek csak be Amerikába, akiknek biometrikus azonosításra alkalmas útlevelük van.

Az elektronikus adatstruktúra és az elektronikus adatok meghamisítása elleni védelem szempontjából egységes, interoperábilis útlevélchip fejlesztése

3 2252/2004/EK rendelet
4 Council Resolution of 23 June 1981

a 6. cikk bizottság[5] BIG[6] albizottságában folyt. A 6. cikk bizottságban Magyarországot a szakértői intézet szakértői képviselik.

Az elektronikus adathordozó és a biometria alkalmazásának alapvető célja a személy és az útlevél adatainak egyértelmű összerendelhetősége volt. Az új technológia alkalmazása az útlevél hamisítás elleni védelmét is jelentősen megerősítette, új védelmi megoldással egészítette ki.

A hazai fejlesztés a teljes útlevélcsalád okmányvédelmét, grafikai tervezését, valamint az okmány biztonsági alkatrészeinek kidolgozását foglalta magában. Az útlevélcsalád bevezetésének időpontja *2006. augusztus 29.* volt. Ekkortól az útlevelek az Európai Unió Bizottsága határozatának[7] megfelelő, biometrikus azonosító (arckép) tárolására alkalmas rádiófrekvenciás[8] chipet tartalmaztak, amit a borítón elhelyezett ICAO-chiplogó és a „Tudnivalók" rovatban olvasható kezelési felhívás jelzett. A chipben tárolt adatokhoz való jogosult hozzáférést, az okmányolvasó és a chip közötti rádiófrekvenciás kommunikáció illetéktelen lehallgatás elleni védelmét az úgynevezett alap hozzáférés-ellenőrzési eljárás *(Basic Access Control; BAC)* protokoll tette lehetővé. A chipben tárolt adatok hitelességét a kibocsátó ország elektronikus aláíró tanúsítványa igazolja. A tanúsítványok kibocsátását, nyilvántartását és visszavonását a Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság szervezeti rendszerében működő Országaláíró tanúsítvány hatóság *(Country Signing Certificate Authority; CSCA)* hatóság végzi. Az országok közötti tanúsítványcsere eleinte diplomáciai úton, később a Nemzetközi Polgári Repülési Szervezet Nyilvánoskulcs-könyvtár *(Public Key Directory; PKD)* rendszerén keresztül valósult meg.

Az adatoldal teljes látványát, összeállítását, védelmi rendszerét, papírját, a lamináló fólia domborgrafikáját, valamint a belívoldalak és a füzetborító grafikáját és okmányvédelmét a Nemzetbiztonsági Szakszolgálat Szakértői Intézete tervezte. Az útlevélfüzetet előállító Pénzjegynyomda Zrt. az előzékek metszetnyomtatott grafikájával és az okmány teljes körű nyomdai kivitelezésével járult hozzá a sikeres kibocsátáshoz.

A személyes és érvényességi adatok, az arckép és a gépi olvasásra alkalmas sáv *(Machine Readable Zone),* az unió és a repülési szervezet előírásainak megfelelően helyezkedik el. Az adatoldalt borító fólia felülete egyedi présszerszámmal domborított, amely a bal szélen a köztársasági címert, kö-

5 A tanács 1683/95/EK rendelete 6. cikke alapján felállított szakértői bizottság.
6 Brussels Interoperability Group.
7 B(2006)2909 végleges Brüsszel, 2006/VI/28 bizottsági határozat.
8 ISO 14443

zépen a Himnusz első versszakának eredeti, kézzel írott szövegét is tartalmazza. A személyes adatok okmányba integrálása a korábbi útlevél esetében már bevált lézergravírozással történt, de modernebb, nagyobb felbontású lézergravírozó alkalmazásával.

Az e-útlevél chipje *2009. június 28.* óta a tulajdonos két mutatóujjának lenyomatát is tartalmazza. Az Európai Unió Bizottságának említett határozata írja elő annak sorrendjét is, hogy mely ujjak lenyomatát kell felvételezni abban az esetben, ha a mutatóujj(ak) nem alkalmasak ujjlenyomatminta-adásra. Ez az érzékeny személyes adat azonban csak az erre felhatalmazott hatóság számára olvasható ki az adattároló chipből, ugyanis a chip addig nem adja ki az ujjlenyomat-információt, amíg meg nem győződött arról, hogy az olvasónak megvan a szükséges ellenőrző tanúsítványa. Az ellenőrző tanúsítványok kibocsátását, nyilvántartását és visszavonását a BM Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság szervezeti rendszerében működő Országellenőrző tanúsítvány *(Country Verifying Certificate Authority; CVCA)* hatóság végzi.

Az ujjlenyomat-információhoz hozzáférést biztosító protokoll, a kiterjesztett hozzáférés-ellenőrzési eljárás *(Extended Access Control; EAC)* futtatása a külföldi és a magyar hatóságok napi rendszerességű ellenőrzőtanúsítvány-cseréjéhez kötött, így biztosítva az ujjlenyomat-információhoz való hozzáférés-jogosultság ellenőrzésének folytonosságát és védve a rádiófrekvenciás kommunikációs csatornát az illetéktelen lehallgatástól, az adathalászattól. A napi szintű tanúsítványcsere érdekében a bizottság[9] határozatban állapította meg a szükséges technikai feltételeket, az úgynevezett SPOC *(Single Point of Contact)* létrehozására. A CSCA, CVCA és SPOC (együtt-)működése nélkül az ujjlenyomat biometrikusadat-kiolvasása nem lehetséges a határátkelőhelyeken. A magyar és külföldi tanúsítványkibocsátó hatóságok harmonikus együttműködése, az érvényes tanúsítványok és naprakész tanúsítványvisszavonási listák elérhetősége nélkülözhetetlen.

Az alaptörvényben meghatározott országnévváltozás miatt 2012. március 1-jétől az útleveleket a korábbi Magyar Köztársaság felirat helyett Magyarország felirattal állítják ki. Az elsőre egyszerűnek tűnő változás a gyártás során sok módosítást igényelt, hiszen az országnév nemcsak az útlevél borítóján, hanem számos nyomatban és biztonsági elemben is megjelent, ezek cseréje hosszabb előkészítést igényelt.

9 C(2009) 7476 végleges Brüsszel, 2009. 10. 5.

Az informatika hardver- és szoftvereszközeinek rohamos fejlődése következtében, a korábban biztonságosnak ítélt BAC hozzáférési protokoll feltörhetővé vált, ezért az unió előírásának[10] megfelelően *2015. január 1-jétől* az elsődleges biometrikus adat (az arckép) és a személyes adatok elektronikus védelme megújult. Az e-útlevelek rádiófrekvenciás chipjében tárolt adatok védelmére már a jóval hatékonyabb védelmet nyújtó kiegészítő hozzáférés-ellenőrzési eljárás *(Supplemental Access Control; SAC)* alkalmazására kerül sor. A SAC protokoll lehetővé teszi a korábbi BAC hozzáférés-védelemmel ellátott okmányok kiolvasását is, de a 2015. január 1-je után kiadott e-útlevelek esetében már elsődlegesen a jelszóval hitelesített kapcsolat-létesítési eljárást *(Password Authenticated Connection Establishment; PACE)* alkalmazza. A Nemzetközi Polgári Repülési Szervezet ajánlása szerint 2018-tól már nem szükséges a SAC protokoll használata, elegendő tisztán a PACE alkalmazása.

Napjainkban

A belügyminiszter feladatszabásának megfelelően megkezdődtek a jelenlegi e-útlevelet leváltó okmány fejlesztési munkái. Kivételes helyzet, hogy a kibocsátás megkezdése óta eltelt tizenkét év alatt a szakértői intézetben vizsgálatra megfordult magyar e-útlevél-hamisítványok száma még a százas nagyságrendet sem érte el. A fejlesztések megkezdését – a korábbiaktól eltérően – nem a hamisítások nagy száma indokolta. Felvetődik a kérdés: ha ilyen jó az útlevelünk okmányvédelme, mi értelme továbbfejleszteni?

Először is le kell szögeznünk, hogy nincs hamisíthatatlan okmány. Amit ember megalkotott, azt másik (megfelelően felkészült) ember le tudja másolni, meg tudja hamisítani különösen akkor, ha arra megfelelő (fizetőképes) kereslet mutatkozik. A magyar e-útlevél több mint száz országba nyújtja az előzetes vízumkényszer nélküli beutazás lehetőségét, a schengeni övezetben szabad mozgást tesz lehetővé, így kellően értékes célpontja lehet a hamisítóknak. Az okmányfejlesztés és okmányhamisítás vonatkozásában is értelmezhető a darwinizmus dinamizmusa. A leggyengébb válik áldozatul, jelen esetben a hamisítás célpontjává, ezért ha nem akarsz áldozattá válni, akkor fejlődj. A környező országokban már elkezdődött fejlesztési folyamatokkal lépést kell tartanunk, különben mi magunk válunk célponttá. Ne felejtsük el azt sem, hogy a ma tíz év érvényességgel kiadott útlevél 2028-ban jár le.

10 C(2013) 6181 végleges Brüsszel, 2013. 9. 30.

(Más kérdés, hogy az információtechnológia, a digitális képalkotási technikák, a reprodukciós technológiák gyors fejlődésének korában van-e létjogosultságuk a tíz év érvényességgel kiadott okmányoknak, figyelembe véve azt is, hogy az arcazonosításon alapuló ABC-kapuk [*Automated Border Control*; automatikus határátlépés-ellenőrző rendszer] kezelni tudnak-e egy tízéves öregedési folyamatot.)

A fejlesztés másik mozgatója a biometrikus információt tartalmazó chipek tárolókapacitásának és olvasási sebességének növekedése. Az 1992. évi LXVI. tv 29. § (12) bekezdése szerint *„A polgár személyazonosságát a személyazonosító igazolványon túl az érvényes útlevéllel vagy kártyaformátumú vezetői engedéllyel igazolhatja”.* Az e-útlevél-chip és az e-személyazonosító igazolvány chipjének „tudása” a fejlesztéssel azonos szintre hozható. (A vezetői engedélybe is beépíthető chip, de határátlépésre még EU-n belül sem jogosíthat.) Az új e-útlevél így lehetővé teheti az elektronikus személyazonosító igazolvánnyal azonos szolgáltatások biztosítását, az elektronikus kormányzati szolgáltatások (e-gov) elérését és jogügyletek online ügyintézését az eID elektronikus hitelesítés és eSIGN elektronikus aláírás funkción keresztül, továbbá eIDAS-[11] kompatibilis biztonságos azonosító eszközként is működhet. Az állampolgárnak nem kellene mindkét okmányt kiváltania (egyiket az unión kívüli utazásokhoz, másikat az e-gov-ügyintézésekhez), hanem dönthetne arról, melyik szükséges számára az adott élethelyzetben. Az útlevél érvényességi idejét ennek megfelelően célszerű lenne az e-személyazonosító igazolvánnyal azonosan, hat évben meghatározni.

A fejlesztés természetesen az új e-útlevél jövőbeni kibocsátásával sem fog megállni. Példaként említhető az ICAO munkacsoportjában *(New Technologies Working Group; NTWG)* folyó e-vízum- és e-határátléptetőbélyegző-fejlesztés. Új technológiák, új igények jelennek meg, amelyek együtt járnak a hamisítási típusok megújulásával is. A szakértői munka során tapasztaltak nélkülözhetetlenek a fejlesztői feladatok teljesítéséhez, mert ezek szolgáltatják a leghasznosabb információkat az adott okmány támadhatóságáról.

11 910/2014/EU rendelet a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK rendelet hatályon kívül helyezéséről.

DOI: 10.38146/BSZ.2019.1.13

SOLTI ISTVÁN

Fából vaskarika?

A Szabó–Vissy-ügy hatása a nemzetbiztonsági célú titkos információgyűjtésre

2014. május 13-án az Eötvös Károly Közpolitikai Intézet két munkatársa *(Szabó Máté* és *Vissy Beatrix)* az Emberi jogok európai egyezményének (egyezmény) 34. cikke alapján keresetet nyújtott be az Emberi Jogok Európai Bíróságához (EJEB) az egyezmény 8. cikkének sérelmére hivatkozva. Az előterjesztők arra hivatkoztak, hogy a Terrorelhárítási Központ (TEK) a rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.) 7/E § (3) bekezdése szerinti megfigyelésének akár indokolatlanul és a magánélet aránytalan sérelmével is alanyai lehetnek, különösen bírói kontroll hiányában.[1]

A sérelmezett jogszabályi hely értelmében a TEK az igazságügyért felelős miniszter engedélyével az Nbtv. rendelkezései szerint titkos információgyűjtést végezhet

– Magyarország nemzetbiztonsági érdekei érvényesítésének elősegítéshez, aminek keretében megelőzi, felderíti és elhárítja azokat a törekvéseket, amelyek Magyarország területén terrorcselekmény elkövetésére irányulnak; illetve
– a külföldön bajba jutott magyar állampolgárok mentéséhez, hazatérésének elősegítéséhez, aminek keretében megszerzi, elemzi, értékeli és továbbítja a szükséges külföldre vonatkozó és külföldi eredetű információkat.

Az idézett jogszabályhelyre hivatkozással a kérelmezők formailag a TEK-re vonatkozó igazságügy-miniszteri engedélyezési eljárás ellen nyújtottak be panaszt. Azonban az ügyben született ítélet és az EJEB korábbi döntéseinek ismeretében fontos hangsúlyozni, hogy a bíróság által górcső alá vettek központi kérdése nem szigorúan a TEK eljárására vonatkozó rendelkezések voltak. Az EJEB ugyanis közvetlenül a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) rendelkezéseit vizsgálta, vagyis a teljes

1 Szabó és Vissy kontra Magyarország-ügy (37138/14. sz. kérelem). 2016. január 12-i ítélet, 3. pont.

nemzetbiztonsági célú titkos információgyűjtés eszközeinek alkalmazási eljárásairól és azok miniszteri engedélyhez kötöttségéről hozott határozatot.[2]

Szintén fontos megjegyezni, hogy a hatályos hazai rendszer vizsgálatával az EJEB nem csupán arra – a magyar sajtó által felkapott – kérdésre keresett választ, hogy a nemzetbiztonsági célú titkos információgyűjtés igazságügyért felelős miniszter általi engedélyezése megfelel-e az egyezményben foglalt és az EJEB korábbi ítéleteiben kibontott követelményeknek. Vizsgálatának tárgya a nemzetbiztonsági célú titkos információgyűjtés magyar rendszerének jóval több elemére terjed ki. Az eljárása befejezésekor jogerős ítéletben arra a következtetésre jutott, hogy: *„Mivel az intézkedések köre gyakorlatilag bárkire kiterjedhet, mivel az intézkedések elrendelése teljes egészében a végrehajtó hatalom hatáskörében történik, mégpedig a szigorú szükségesség elvének mérlegelése nélkül, mivel a legújabb technológiák révén a Kormány akár az intézkedés eredeti hatályán kívül eső személyekről is könnyedén és tömegesen szerezhet adatokat, és mivel nemhogy bírósági, de semmilyen egyéb hatékony jogorvoslati lehetőség nem biztosított, a Bíróság arra a következtetésre jutott, hogy megsértették az Egyezmény 8. cikkét."*[3]

Az idézett szöveg a hazai nemzetbiztonsági célú titkos információgyűjtés több komponensét elhibázottnak tartja. E szerint a rendszerszintű szabályozás egyes jogintézményeinél a törvényesség (azon belül is az előreláthatóság), a szükségesség és az ellenőrizhetőség alapelveknek való megfelelés lehet problémás. Természetesen a megállapítások megalapozottságát lehet vitatni, viszont megváltoztatni nem. Az ítélet jogerős és így végrehajtandó.[4] Tekintettel arra, hogy Magyarország egyelőre nem módosította a kifogásolt rendelkezéseket, a tanulmányban megvizsgálom először azokat a rendszertani komponenseket, amelyeket az EJEB hibásnak mondott ki, majd sorra veszem azokat a rendelkezéseket, amelyek átalakításával az egyezménysértés orvosolható lehetne. A legvégén pedig azt is megvizsgálom, hogy a 2018. július 1-jén hatályba lépő, jelenleg elfogadott rendszertani átalakítások menynyiben érintik az inkriminált részeket.

2 Az Rtv.-ben felsorolt esetekben a TEK az Nbtv. szabályai szerint végzi a titkos információgyűjtést, ami valamennyi nemzetbiztonsági ügyben releváns.

3 Szabó és Vissy kontra Magyarország-ügy… i. m. 89. pont

4 Az EJEB az ügyben 2016. január 12-én hozta meg az ítéletet, amelynek Nagykamara elé vitelét kérte a magyar állam. A Nagykamara a magyar állam kérelmét 2016. június 7-én elutasította, az ítélet végleges.

Az előreláthatóság problematikája[5]

A kérelmezők beadványukban vitatták, hogy a bepanaszolt magyar jogszabályok kellően pontosak és részletesek lennének ahhoz, hogy megfeleljenek az előreláthatóság kívánalmainak. E kérdésben az EJEB részben fogadta el a kérelmezők véleményét. Egyrészről ugyanis úgy vélte, hogy a terrorcselekmények veszélye és a mentési műveletek szükségessége világos fogalmak. Hangsúlyozta, hogy az előreláthatóság okán az államok nem kötelesek a titkos megfigyelés megindításához szükséges döntést kiváltó valamennyi helyzetet jogszabályban részletesen felsorolni.

Másrészről viszont azt is hangsúlyozta, hogy a nemzetbiztonság területén, az önkényes beavatkozás kizárásához a törvényeknek világosan rögzíteniük kell a hatóságok mérlegelési jogköreinek hatályát és gyakorlásának módjait. Megítélése szerint az Rtv. 7/E § (3) bekezdés alapján Magyarországon bárki megfigyelhető, mert az alkalmazásra hívott Nbtv. nem írja le a megfigyelhető személyek körét, átfedés van a személyi kör meghatározása és a jogalapot adó helyzetekre vonatkozó feltételek között.

Abban igazat adhatunk az ítéletben foglaltaknak, hogy a magyar rendszer a nemzetbiztonsági célú titkos információgyűjtésbe vonható személyek körét jogszabályi szinten nem részletezi. Megelégszik azzal, hogy a nemzetbiztonsági célú titkos felderítésben érintett személyekkel szemben, pusztán az érintettség okán, az egyedi ügyben, a titkos információgyűjtő eszköz alkalmazása iránti engedélykérelemben kell név szerint megadni, vagy felismerhetően körülírni. Az ítélet szerint viszont problémás az *„érintett”* kifejezés. Az EJEB szerint e kifejezésbe *„bárki beletartozhat, így az állampolgárok tömeges és korlátlan megfigyeléséhez vezető út kikövezéseként is értelmezhető”*[6]. Érvelésében abból indult ki, hogy *„a hatóságokat semmi sem kötelezi arra, hogy bizonyítsák az »érintett« személy vagy személyek közötti tényleges vagy feltételezett kapcsolatot és a terrorcselekmény megelőzését – különösen nem úgy, hogy az lehetővé tenné az engedélyező számára szigorú szükségesség elvének elemzését a célok és az eszközök vonatkozásában”*[7]. Nem fogadta el a magyar kormány érvelését,

5 Az előreláthatóság az EJEB gyakorlatában azt jelenti, hogy nemzeti jognak kellően világosnak kell lennie ahhoz, hogy az állampolgárok részére megfelelően jelezze, hogy milyen körülmények között és feltételek mellett jogosultak az állami hatóságok velük szemben titkos információgyűjtést folytatni. Viszont nem jelenti azt, hogy az egyén előre értesül a hatóságok megfigyeléséről, hogy így ehhez igazíthassa a viselkedését. Lásd Case of Roman Zakharov v. Russia (Application no. 47143/06) Judgment of 4 december 2015, 229. pont.

6 Szabó és Vissy kontra Magyarország-ügy… i. m. 67. pont

7 Uo.

miszerint az Nbtv. megfelelően leszűkíti az ellenőrzés alá vonhatók körét, az érintetteket az azonosításukhoz szükséges adatok megjelölésével kell feltüntetni az engedélykérelemben. Így kontrolláltan, előre behatárolt személlyel vagy személyi körrel szemben lehet titkos információgyűjtést folytatni, tehát az ellenőrzés az eljárás során jól körülhatárolt személyekre korlátozódik.

Az is kijelenthető, hogy az EJEB megállapítása nem meglepő. E kérdésre valamennyi korábbi releváns ítéletében azonos választ adott.[8] A téma hazai kutatói[9] és az Alkotmánybíróság (Ab) több határozatában[10] is utalt a hazai szabályozás ilyen jellegű hiányosságára. Ennek ismeretében a jogalkotó valamiért mind ez idáig nem követte az elvi útmutatásokat és nem tartotta szükségesnek új rendelkezések megalkotását. Pedig, mint ahogy a kormány maga is hivatkozott rá az EJEB előtti eljárásban, az engedélyezési szakasz gyakorlatában a jogszabályban meghatározottaknál szigorúbb követelmények érvényesülnek, amely gyakorlatot akár az általános részben is ki lehetne emelni. Éppen ezért megítélésem szerint a jogszabályok megfelelő módosítása semmilyen presztízsveszteséggel, vagy káros szakmai következménnyel nem járna. Már csak azért sem, mert a kialakult gyakorlat átültetéséről lenne szó. Ennek következtében mind a szabályozás, mind az egyedi eljárások szintjén viszonylag egyszerűen orvosolható álproblémáról beszélhetünk. Egy lehetséges megoldásként célszerűnek tartom az Nbtv. 53. § szakaszának kiegészítését azzal, hogy: a nemzetbiztonsági szolgálatok feladataik teljesítése érdekében a titkos információgyűjtés erőit, eszközeit és módszereit csak azokkal szemben alkalmazhatják, akiknek az adott nemzetbiztonsági ügy kapcsán információik lehetnek, vagy akik nemzetbiztonsági ügyben közvetlenül érintettek. Hasonlóan azoknak az információgyűjtéseknek a jogalapja is megteremthető, ahol nincs az üggyel kapcsolatba hozott, beazonosítható személy. Ekkor információgyűjtés azokkal szemben lenne alkalmazható, akik a nemzetbiztonsági ügyben indokoltan felmerülő helyiséggel kapcsolatba hozhatók, az elektronikus hírközlési szolgáltatást igénybe veszik, illetve számítástechnikai eszközt használják. Továbbá, ha az engedély kötelező tartalmi elemei közé bekerül, hogy az érintettséget igazoló dokumentumokat és adatokat az engedélykérelemnek tartalmaznia kell, akkor a magyar rendszertan az előreláthatóság valamennyi követelményének eleget tehetne.

8 Néhány kiragadott jelentősebb példa: az 1978-as Klass-ügy, az 1984-es Malone-ügy és a 2000-ben véget érő Rotaru-ügy.

9 Bejczi Alexa: Titkos információgyűjtés vs. jogállam. PhD-értekezés. ELTE Állam- és Jogtudományi Kar, Budapest, 2011; Gyurcsó Judit: A titkos információgyűjtés és titkos adatszerzés (újra)szabályozásához. Belügyi Szemle, 2011/7–8., 126–151. o.; Dezső Lajos – Hajas Gábor: A nemzetbiztonsági tevékenységre vonatkozó jogszabályok: kommentár a gyakorlat számára. HVG-ORAC, Budapest, 2000

10 31/2001. (VII. 11.) AB határozat; 2/2007. (I. 24.) AB határozat

A szigorú szükségesség problematikája

Az EJEB a hatályos magyar szabályozásnak a szükségesség alapelvére vonatkozó rendelkezéseit sem tartotta megfelelőnek. Az Nbtv. 57. § (2) bekezdés b) pontja kimondja ugyan, hogy az előterjesztésnek tartalmaznia kell a titkos információgyűjtés szükségességének indoklását, de az EJEB arra az álláspontra helyezkedett, miszerint: *„A vonatkozó rendelkezéseket együtt olvasva azonban a Bíróság nincs meggyőzve arról, hogy a nemzetbiztonsági feladatok megvalósítása során elérni kívánt célok és felhasznált eszközök megfelelő elemzése lehetséges vagy garantált. Ami azt illeti, pusztán az a kötelezettség, hogy a hatóságoknak meg kell indokolniuk a kérelmükben a titkos megfigyelés szükségességét, nem minősül a szigorú értelemben vett szükségesség elemzésének. Nincs olyan jogi garancia, amely arra kötelezné a TEK-et, hogy szolgáltasson alátámasztó anyagokat vagy még inkább kielégítő tényszerű alapot a titkos információgyűjtés engedélyezésére irányuló kérelméhez, amelyek alapján már meg lehetne vizsgálni a javasolt intézkedés szükségességét, ráadásul a célszemélyre vonatkozó egyéni gyanú alapján.”*[11] Az EJEB szerint tehát a magyar szabályozás nem biztosítja a beavatkozás szigorú szükségességnek megfelelő mérlegelését. Vagyis a jelenlegi megoldás, a kérelem indokolási kötelezettségének előírása ehhez nem elegendő. Megfelelő az lenne, ha jogszabályba foglaltan történik meg annak megfogalmazása, hogy a kérelmező köteles tényekkel és dokumentumokkal alátámasztani az érintettel szembeni gyanút.

Az EJEB következetesen képviseli, hogy a titkos információgyűjtés sajátos jellege és az állampolgárok magánszférájának megsértésére alkalmas modern megfigyelési technológiák miatt, a szükségesség követelményét két szempontból is szigorúan szükségesként kell értelmezni. Mindezt a Szabó–Vissy-ítéletben is megfogalmazta: *„Csak akkor lehet összhangban az Egyezménnyel, ha az – általános megfontolásként – szigorúan szükséges a demokratikus intézmények védelméhez, valamint – konkrét megfontolásként – szigorúan szükséges kulcsfontosságú információk megszerzéséhez egy adott műveletben.”*[12] Konzekvens álláspontja szerint ugyanis a követelményeknek nem megfelelő szabályozás lehetőséget teremt a hatóságok visszaélésére.

A kormány védekezése szerint annak ellenére, hogy a jogszabály csak indoklási kötelezettséget ír elő, a kialakított joggyakorlat rendezte a kérdést. A gyakorlatban ugyanis az indoklásnak része az igényt alátámasztó dokumentumok és adatok csatolása. A miniszternek lehetősége van a releváns iratanyagba betekin-

11 Szabó és Vissy kontra Magyarország-ügy… i. m. 71. pont
12 Uo. 73. pont

teni. Viszont az EJEB e kérdésben sem tartotta elegendőnek a magyar kormány érvelését. Az ítélet szerint ragaszkodik ahhoz, hogy a kérdés rendezése ne csupán a joggyakorlat, hanem a jogszabályok szintjén történjen meg.

E tényező vonatkozásában az a tanulság vonható le, hogy nem elegendő rendszertani szinten a szükségesség követelményének megfelelő eljárásokat folytatni, az egyes eljárási szabályokat jogszabályba szükségeltetik foglalni. Ehhez mindössze annyi kell, hogy a jogalkotó az Nbtv. 57. § (2) bekezdésében az engedélykérelem kötelező elemeit kiegészíti az igényt alátámasztó dokumentumokkal, valamint az 53. § módosításával az engedélyező számára előírja a szigorú szükségesség két tényezőjének vizsgálatát. Mindez a kormány érvelésének tekintetében sem jelenthetne különösebb eljárási problémát, mindössze a kialakult joggyakorlat jogszabályba foglalását.

Ezzel kapcsolatban hangsúlyozni kívánom, hogy feltétlenül fontos lenne általánosan és nem kizárólag a külső engedélyhez kötött eszközök alkalmazásakor érvényesíteni a szigorú szükségesség követelményeit. Ugyanis az EJEB által vizsgált polémia nem csupán a miniszteri, hanem a nem engedélyköteles eszközök – különösen az adatkérés, a konspirált környezettanulmány, a konspirált figyelés, a nyilvános helyen, vagy kültéren folytatott beszélgetések lehallgatása – esetében is felvethető. Jelen esetben ez a terület nem volt tárgya a bírósági eljárásnak. Azonban ha csak a külső engedélyezés szabályainak módosítása történik meg, akkor a belső engedélyezési rendben alkalmazott eszközök esetében az EJEB által kifogásolt polémia továbbra is fennmarad. Mindez pedig szükségtelen támadási felületet teremt a nemzetbiztonsági célú titkos információgyűjtés kapcsán.

A külső engedélyhez kötött titkos információgyűjtés engedélyezésének problematikája

Az EJEB ítélete a rendszertan legsúlyosabb hibáját az ellenőrzési mechanizmusok hiányában látja.[13] Mindez abból következik, hogy gyakorlatában a titkos eszközök alkalmazhatóságánál különös hangsúlyt helyez a jogalapot szavatoló normák minőségére és az önkényesség megakadályozását szolgáló eljárási garanciákra. Lényeges szempont az is, hogy a titkos eljárások mind-

13 Esetjogában az EJEB egyértelművé teszi, hogy a titkos információgyűjtéssel szemben támasztott követelmények érvényesülését mind az engedélyezés időszakában, mind a végrehajtás alatt, mind a végrehajtás után egyaránt szavatolni kell. E tekintetben nem tesz különbséget a nemzetbiztonsági, a rendészeti és a bűnüldözési célból végzett titkos információgyűjtések között.

három szakaszát (az engedélyezést, a műveletek végrehajtását, a végrehajtást követő utólagos kontrollt) önállóan vizsgálja. További alaptétele, hogy a garanciális követelményeket illetően nem tesz különbséget a bűnüldözési és a nemzetbiztonsági célból alkalmazott titkos megfigyelések között.

Az engedélyezés típusai közül a bírósági engedélyezést preferálja. Véleménye szerint azonban egy kiterjedt utólagos bírói ellenőrzés ellensúlyozhatja a nem bírói előzetes engedélyezés hiányosságait. Azonban a médiára irányuló titkos megfigyelés esetén csak az előzetes bírói engedélyezést tartja elfogadhatónak. Nem bírói engedélyezést kizárólag három esetben ismer el:

1. Ha az engedélyező kellően független a végrehajtó hatalomtól.
2. Ha bíróság az engedélyező tevékenységét utólag ellenőrzi.
3. Ha független szerv az engedélyező tevékenységét utólag ellenőrzi.

Az engedélyezés kérdésében a magyar rendszer és az EJEB véleménye között lényegi különbség van, de – megítélésem szerint – nincs kibékíthetetlen ellentét. A magyar rendszer abból indul ki, hogy a nemzetbiztonsági célú titkos információgyűjtés kizárólag az Nbtv. 74. § a) pontjában meghatározott nemzetbiztonsági érdek védelmében folytatható. Ez alapján a bűnüldözési célú titkos információgyűjtéstől élesen elhatárolható, hiszen a bűncselekmény, mint viszonyítási alap, hiányzik.

Ahogy az Ab a 2/2007. számú határozatában rámutatott, a bűnüldözési célú titkos információgyűjtés esetén az érintettek alapjogainak sérelme és a bűnüldözési érdek között, a nemzetbiztonsági célú titkos információgyűjtéskor a büntetőeljárási következményekkel nem feltétlenül együtt járó nemzetbiztonsági érdek és az alapjogi sérelem között kell mérlegelni. Ezt megelőzően a 31/2001. számú határozatában azt is megállapította, hogy a nemzetbiztonsági érdek védelme alkotmányos cél és állami kötelezettség. Az ország szuverenitása és alkotmányos rendje a demokratikus jogállam működéséhez nélkülözhetetlen alapérték. A szuverenitás érvényre juttatása, politikai, gazdasági és honvédelmi érdekeinek megóvása a szuverenitást, illetve az alkotmányos rendet sértő vagy veszélyeztető tevékenységek felderítése és elhárítása az államnak az alkotmányból fakadó kötelezettsége. A magyar álláspont szerint a nemzetbiztonsági érdek értékelésének kötelessége indokolja, hogy a nemzetbiztonsági célú titkos információgyűjtéskor bíró helyett a végrehajtó hatalom politikai felelősséget viselő képviselője, esetünkben az igazságügyért felelős miniszter járjon el engedélyezőként.

Az igazságügyért felelős miniszteri engedélyezésre összefoglalóan a következő indok hozhatók fel:

– nemzetbiztonsági érdek mérlegelése esetében az igazságszolgáltatás szempontjai másodlagosak;
– a döntésben politikai szempontok is szerepet játszanak;
– politikai felelősség keletkezik;
– a bírók politikai felelőssége fogalmilag kizárt, az alaptörvény 26. § (1) bekezdése értelmében a bírók politikai tevékenységet nem folytathatnak;
– a nemzetbiztonsági szolgálatok működéséért egy interpellálható miniszternek, ezen keresztül a kormánynak kell politikai felelősséget viselnie;
– az igazságügyért felelős miniszter a nemzetbiztonsági szolgálatoktól független;
– döntéskor mérlegeli a nemzetbiztonsági érdek és az alapjogi sérelem viszonyát;
– képes elvégezni a beavatkozás szigorú szükségességi tesztjét;
– az Nbtv. rendelkezésein túl a jogállamiság alaptörvényben lefektetett alapelveinek a figyelembevételével köteles a döntését meghozni.

Ezzel szemben, az EJEB érvelése szerint, a titkos eszközök alkalmazásának engedélyezését a nemzeti bírósági szervezet rendszeréhez kapcsolódóan lehet az egyezmény sérelme nélkül megtenni. A végrehajtó hatalmon belül kialakított engedélyezési mechanizmus nem felel meg az ellenőrzöttség alapelvének. Az imént sorolt érvekkel szemben úgy ítéli meg, hogy *„ez a felügyelet – amely kimagaslóan politikai jellegű, bár a TEK-től és a Belügyminisztériumtól formálisan független igazságügyi miniszter látja el – lényegénél fogva nem képes biztosítani, hogy a visszaélésnek kitett célok és eszközök szempontjából értékeljék a szigorú szükségesség követelményét. Különösen figyelemre méltó e tekintetben, hogy bár a biztonsági szolgálatok a miniszternek küldött előterjesztésben kötelesek ismertetni a titkos információgyűjtés szükségességét, ez az eljárás nem biztosítja a szigorú szükségesség követelményének vizsgálatát, különösen nem az érintett személyek és helyszínek körét illetően.”*[14]

A magyar álláspont reális értékeléséhez azt is hozzá lehet tenni, hogy a nemzetbiztonsági szolgálatok a nemzetbiztonsági célú titkos információgyűjtés keretében – egyes esetekben – kvázi bűnüldözési célú titkos információgyűjtést folytatnak. Hiszen, ahogy *Finszter Géza* is bemutatja, a terrorcselekményekkel kapcsolatos titkos felderítések jellegüket tekintve közelebb állnak a bűnüldözési célú titkos felderítéshez, mint a nemzetbiztonságihoz.[15] A bűn-

14 Szabó és Vissy kontra Magyarország-ügy… i. m. 75. pont
15 Finszter Géza: Bűnüldözés és jogállam. Ügyészségi Szemle, 2016/1.

üldözési célú titkos információgyűjtés esetében pedig nem állnak fenn olyan élesen a politikai felelősségre vonatkozó hivatkozások.

Véleményem szerint a hazai rendszertan igényelt orvoslása két módon történhet meg. Az első megoldás egy önálló, a TEK-re vonatkozó új engedélyezési rendszer kialakítása, hiszen az ítélet tárgya a TEK terrorcselekményekkel kapcsolatos titkos eljárása volt. A megoldás hátránya, hogy az ítélet valójában az Nbtv. engedélyezési rendszerét minősítette, ezért nemzetközi fórumok előtt továbbra is támadható maradna. A másik út az Nbtv. engedélyezési rendszerének felülvizsgálata. Eredményeként akár meg is maradhat az igazságügyért felelős miniszter engedélyezési joga, ha ennek ellenőrzésére a végrehajtó hatalomtól független ellenőrzési mechanizmus felállítására kerül sor.

A javaslatom az, hogy állítsanak fel egy háromfős, a parlament által választott ellenőrző testületet, amelynek egy-egy tagjára az Országos Bírósági Hivatal, a legfőbb ügyész és a kormány tegyen javaslatot, és legyen a parlament nyilvános ülése előtti éves beszámolási kötelezettségük. Tagjai kizárólag a bírói kinevezés feltételeinek megfelelő személyek lehetnének, akiknek megbízatása legalább hét évre szólna.

Fontosnak tartok az engedélyezés problematikájába – hasonlóan a szükségességnél felvetettekhez – még egy szempontot beemelni, mégpedig a nem külső/bírói engedélyköteles eszközök esetét. Ezek között az eszközök között ugyanis szintén találhatók olyanok, amelyek az alapjogokat jelentős mértékben sértik, de még az előzőkben tárgyaltakhoz képest sincs semmilyen garanciális elem az elrendelési eljárásba építve.[16] Megítélésem szerint ezek esetében is alkotmányos aggályok vethetők fel.

A végrehajtás ellenőrizhetősége és az utólagos kontroll problematikája

Az EJEB hasonlóan szigorú követelményeket fogalmaz meg a titkos információgyűjtés második szakaszának, a végrehajtásnak az ellenőrzésére. A végrehajtó hatalomtól és az engedélyező szervtől független felügyeleti mechanizmus kialakítását követeli meg. A felügyeleti szerv tevékenységének nyilvánosan ellenőrizhetőnek kell lennie, ennek hiányában alkalmatlannak véli az önkényes intézkedések elleni hatékony fellépésre.

16 Adatkérés, konspirált környezettanulmány, konspirált figyelés, beszélgetéslehallgatás.

Ha megnézzük a magyar nemzetbiztonsági célú titkos információgyűjtés rendszerét, azt látjuk, hogy többszintű végrehajtást ellenőrző mechanizmust is tartalmaz:

1. A nemzetbiztonsági szolgálatok tevékenységével kapcsolatban bárki panaszt nyújthat be a felügyelő miniszterhez, aki köteles a panaszt kivizsgálni.[17] Az eredményről és a megtett intézkedésekről harminc napon belül tájékoztatja a panaszost.
2. Az Országgyűlés a nemzetbiztonsági szolgálatok parlamenti ellenőrzését a nemzetbiztonsági bizottság közreműködésével látja el.[18] A bizottság
   a) tájékoztatást kérhet az igazságügyi minisztertől és a nemzetbiztonsági szolgálatokat irányító miniszterektől, valamint a szolgálatok főigazgatóitól a külső engedélyhez kötött titkos információgyűjtésről és a kivételes engedélyezési eljárásokról;
   b) kivizsgálhatja a nemzetbiztonsági szolgálatok jogellenes tevékenységére utaló panaszokat, a megállapításairól tájékoztatja az érintettet;
   c) ha valamely nemzetbiztonsági szolgálat jogszabályellenes vagy nem rendeltetésszerű tevékenységét feltételezi, vizsgálat lefolytatására felkérheti a minisztert, aki a vizsgálat eredményéről tájékoztatja a bizottságot;
   d) ténymegállapító vizsgálatot folytathat le, amelynek során betekinthet a nemzetbiztonsági szolgálatok nyilvántartásában lévő, az adott ügyre vonatkozó iratokba, meghallgathatja a nemzetbiztonsági szolgálatok munkatársait;
   e) ha bármely módon valamely nemzetbiztonsági szolgálat jogszabályellenes vagy nem rendeltetésszerű működését észleli, felhívhatja a minisztert a szükséges intézkedés megtételére, és kezdeményezheti a felelősség megvizsgálását, a miniszter a vizsgálat eredményéről tájékoztatja a bizottságot.[19]
3. Bárki adatkéréssel fordulhat a nemzetbiztonsági szolgálatokhoz, hogy a személyes adatai kezeléséről tájékoztatást kérjen.[20] A szolgálat a tájékoztatást nemzetbiztonsági érdekekre hivatkozva megtagadhatja.[21] Erre az esetre a bírói gyakorlat kimondta, hogy az adatot igénylő elutasított igényét bíróság előtt érvényesítheti.[22]

17 Nbtv. 11. § (5) bek.
18 Nbtv. 14. § (1) bek.
19 Nbtv. 14. § (4) bek.
20 Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 14. §.
21 Nbtv. 48. § (1) bek.
22 EBH 2008.1872 számú elvi döntés, Legfelsőbb Bíróság Pfv. IV. 20.871/2008.

4. Az alapvető jogok biztosa bárki bejelentésére vizsgálhatja a rendvédelmi szervek tevékenységét. Évente jelentést készít az Országgyűlésnek a kivizsgált esetekről, és felkérheti az Országgyűlést adott ügy kivizsgálására.[23]

Kijelenthető, hogy a hazai közbenső ellenőrzési mechanizmus több lehetőséget is kínál. Ennek ellenére az EJEB szerint a magyar ellenőrzési és jogorvoslati rendszer nem megfelelő. Értékelése szerint az ellenőrzési mechanizmus a jogorvoslat lehetőségét nem adja meg azon érintettek számára, akik a titkos megfigyelésről nem értesültek. Megítélése szerint a problémát a miniszterek kötelező éves jelentési kötelezettsége sem szünteti meg, mert ezek a jelentések a nyilvánosság számára hozzáférhetetlenek. Hasonlóan vélekedik a nemzetbiztonsági bizottság jogosultságairól, ugyanis *„kétségei maradtak afelől, hogy ez a vizsgálat jogorvoslatot szolgáltatna a titkos megfigyelés által okozott esetleges egyéni sérelmekre, illetve hatékonyan – tehát a működésre is kiterjedően – ellenőrizné a megfigyelést végző szervek napi működését, különösen, hogy a bizottság láthatóan nem fér hozzá a vonatkozó dokumentumok részleteihez. E testület felügyeleti köre tehát korlátozott."*[24]

Az Nbtv. 11. § (5) bekezdésében rögzített panasztételi eljárás gyengeségét az EJEB két tényezőben látja. Az első kifogás, hogy az érintett állampolgárok nem értesülnek a velük szemben alkalmazott titkos megfigyelésekről, így módjuk sincs panasszal élni. A második kifogás, hogy a panaszt a belügyminiszter vizsgálja ki, aki nem mondható kellően függetlennek.

Az utolsó érvet, az alapvető jogok biztosa által alkalmazható ellenőrzési jogosultságot az EJEB azzal semlegesítette, hogy a kormány nem tudta cáfolni a kérelmezők állítását[25], miszerint az alapvető jogok biztosa működése alatt egyszer sem vizsgált titkos megfigyeléssel kapcsolatos ügyet.

Mindezek eredményeképpen az utólagos kontrollt illetően az EJEB követelményként állapította meg, hogy az érintetteket utólag tájékoztatni szükséges a titkos információgyűjtés végrehajtásáról, ha a tájékoztatás a művelet célját már nem veszélyezteti. De a tájékoztatási kötelezettségre alternatív megoldást is kínál. Megfelelőnek látja a nemzeti rendszert, ha minden olyan személy, aki alappal feltételezheti, hogy titkos információgyűjtés alanya lehet, egy erre a célra felállított független testülethez fordulhat az aggályai kivizsgálása érdekében. Feltétel, hogy a független testület joghatósága nem

23 A alapvető jogok biztosáról szóló 2011. évi CXI. törvény 18. § f) pont.

24 Szabó és Vissy kontra Magyarország-ügy… i. m. 82. pont

25 A kérelmezők benyújtották az Alapvető Jogok Biztosának Hivatala által 2014. július 9-én adott nyilatkozatot, amely szerint soha nem indított vizsgálatot titkos megfigyeléssel kapcsolatban.

függhet az érintett személy értesítésétől (bárki panaszt tehet, aki közvetett érintettségét igazolni tudja) és az érintettnek nem kell bizonyítania valamely megfigyelésben való közvetlen érintettségét. Vagyis bárki, aki attól tarthat, hogy titkos eszközöket alkalmaznak vele szemben, egy speciális, a kormánytól független testülethez fordulhat az aggályai kivizsgálása érdekében.[26]

A magyar rendszer ezzel teljesen ellentétes álláspontot képvisel. A szolgálatok szinte elképzelhetetlennek tartanak olyan helyzetet, amikor az értesítési követelménynek eleget lehetne tenni.[27] De egyelőre a független ellenőrző szerv felállítása is elmaradt, holott véleményem szerint a magyar rendszer esetében a végrehajtás ellenőrizhetőségére ez lehetne megfelelő megoldás. Az EJEB által kifogásolt ellenőrzési mechanizmusok megfelelő átalakítása a magyar rendszert nem borítaná fel. Valamelyest megemelné a szolgálatok adminisztrációs feladatait, de megfelelő eljárási rend kidolgozása esetén nem jár a szolgálatok tevékenységének ellehetetlenítésével. Konkrét megoldásként akár az angol (külön specializált bírói testület), akár a holland példát követve (az adatvédelmi ombudsman ellenőrzési jogainak kiszélesítésével) kialakítható olyan hatékony és az egyezményt nem sértő eljárási rend, amely a nemzetbiztonsági és rendvédelmi szolgálatok számára is elfogadható. Mindezt pedig az érintettek közvetlen tájékoztatása nélkül.

Összegzés

Összegzésként megállapítható, hogy az EJEB az évtizedek alatt kialakított gyakorlatának megfelelően vizsgálta az elé kerülő magyar jogszabályokat és ítélete nem tartalmazott meglepetéseket. Viszont az is igazolható, hogy az igényelt változtatások nem jelentenek megoldhatatlan feladatot a magyar nemzetbiztonsági szféra számára, hiszen a joggyakorlat szinte valamennyi területen kialakította már a szükséges mechanizmusokat. Ahol pedig még a gyakorlat sem alakult ki, ott politikai konszenzussal és megfelelő jogalkotással a jogintézmények zökkenőmentesen felállíthatók lennének.

26 Case of Kennedy v. the United Kingdom (Application no. 26839/05), Judgment of 18 May 2010.

27 A tájékoztatási kötelezettség folyamatos ütközési pont a jogvédő és a szakmai szervezetek között. Az is kijelenthető, hogy a két szemlélet között az ellentét kibékíthetetlennek tűnik. Az EJEB ítéleteiben mondja ki a kötelező értesítés bevezetését, amit a szakmai képviseletek folyamatosan vitatnak. Megítélésem szerint az alapvető probléma az, hogy az EJEB nem veszi figyelembe, hogy a szolgálatok titkos eljárásai egy-egy konkrét ügy befejezésével nem érnek véget, hanem csupán nyugvó állapotba kerülnek, és a későbbiekben bármikor újraindulhatnak. A felderítő szervek nem látják előre és nem is tudhatják előre, hogy az adott eljárásuk negatív eredménye mennyire ad útmutatást a jövőre.

FELHASZNÁLT IRODALOM

Bárándy Gergely – Enyedi Krisztián: Leplezett eszközök és titkos információgyűjtés, avagy az új büntetőeljárási törvény margójára. http://ujbtk.hu/dr-barandy-gergely-dr-enyedi-krisztian-leplezett-eszkozok-es-titkos-informaciogyujtes-avagy-az-uj-buntetoeljarasi-torveny-margojara/#_ftn45

Bejczi Alexa: Titkos információgyűjtés vs. jogállam. PhD-értekezés. ELTE Állam- és Jogtudományi Kar, Budapest, 2011.
https://doktori.hu/index.php?menuid=193&lang=HU&vid=8987

Dezső Lajos – Hajas Gábor: A nemzetbiztonsági tevékenységre vonatkozó jogszabályok: kommentár a gyakorlat számára. HVG-ORAC, Budapest, 2000

Finszter Géza: Bűnüldözés és jogállam. *Ügyészségi Szemle,* 2016/1.

Gyurcsó Judit: A titkos információgyűjtés és titkos adatszerzés (újra)szabályozásához. *Belügyi Szemle,* 2011/7–8.

JOGSZABÁLYOK

1994. évi XXXIV. törvény a rendőrségről

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

31/2001. (VII. 11.) AB határozat

2/2007. (I. 24.) AB határozat

EBH 2008.1872 számú elvi döntés, Legfelsőbb Bíróság Pfv. IV. 20.871/2008.

2011. évi CXI. törvény az alapvető jogok biztosáról

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

JOGESETEK

Case of Klass and Others v. Germany (Application no. 5029/71) Judgment of 6 September 1978. http://hudoc.echr.coe.int/eng?i=001-57510

Case of Malonne v. the United Kingdom (Application no. 8691/79) Judgment of 2 August 1984. http://hudoc.echr.coe.int/eng?i=001-57533

Case of Rotaru v. Romania (Application no. 28341/95), Judgment of 4 May 2000. http://hudoc.echr.coe.int/eng?i=001-58586

Case of Kennedy v. the United Kingdom (Application no. 26839/05), Judgment of 18 May 2010. http://hudoc.echr.coe.int/eng?i=001-98473

Case of Roman Zakharov v. Russia (Application no. 47143/06) Judgment of 4 december 2015. http://hudoc.echr.coe.int/eng?i=001-159324

Szabó és Vissy kontra Magyarország-ügy (37138/14. sz. kérelem) 2016. január 12-i ítélet. http://ekint.org/lib/documents/1480415991-Szabo_es_Vissy_itelet.pdf