NEMZETBIZTONSÁGI SZEMLE

A NEMZETI KÖZSZOLGÁLATI EGYETEM NEMZETBIZTONSÁGI INTÉZETÉNEK ELEKTRONIKUS (ONLINE) MEGJELENÉSŰ TUDOMÁNYOS FOLYÓIRATA

7. évfolyam 2. szám • 2019

Impresszum

Nemzetbiztonsági Szemle
A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének
elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756

Kiadó
Nordex Nonprofit Kft. – Dialóg Campus Kiadó
www.dialogcampus.hu • www.uni-nke.hu
1083 Budapest, Ludovika tér 2.
kiado@uni-nke.hu • +36 1 432 9000
A kiadásért felel: Petró Ildikó ügyvezető
Olvasószerkesztők: Balla Nóra, Pokorádi Zsófia, Resofszki Ágnes, Gergely Zsuzsánna
Tördelő: Kőrösi László

Tartalom

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 3–18. • DOI: 10.32561/nsz.2019.2.1

Solti István[1]

Az OSINT információgyűjtő eszközeiről

About the Information Gathering of OSINT

Az OSINT,[2] függetlenül attól, hogy katonai, polgári vagy üzleti hírszerzésről beszélünk, a mindennapi élet elismert és önálló része, amit valamennyi terület saját igényei szerint használ és alakít. Ebben a tanulmányban a szerző az OSINT hírszerzési ciklusának egyik szakaszát, az adatok és információk begyűjtési fázisát vizsgálja meg, mégpedig a nyílt információforrás és a nyílt információ dinamikáját veszi górcső alá. Ennek eredményeként kimutatja egyes információgyűjtő eszközökről, hogy az OSINT keretében felhasználhatók-e vagy sem, illetve meghatároz olyan magatartási formákat, amelyek az OSINT során nem alkalmazhatók.

Kulcsszavak: OSINT, nyílt információforrás, nemzetbiztonság, adatszerzés, információgyűjtés

The OSINT per se – regardless of whether it is military, civil or business intelligence – is authenticated as the part of life, which is used and formed by all the users according to their needs. In this essay the author scrutinises one part of the OSINT, namely the phase of collecting data and information, or in other words examines the dynamics of open information sources and open information. And as a result, the author presents whether certain information gathering means and methods are allowed or not to be used under OSINT and identifies such course of conducts which cannot be used thereunder.

Keywords: OSINT, open source information, national security, data acquisition, information gathering

[1] Dr. Solti István PhD, jogász. ORCID-azonosító: 0000-0003-4140-7782.

[2] A nyílt forrású információszerzés (Open Source Intelligence) hazai szakirodalom által is használt angol nyelvű rövidítése.

Bevezető

A nemzetbiztonsági és rendvédelmi célú információgyűjtéssel foglalkozó tudományos tevékenységet művelők közösségében általánosan elfogadott, hogy az OSINT az utóbbi évtizedekben a nemzetbiztonsági és a rendvédelmi szolgálatok egyre inkább nélkülözhetetlen információs eszközévé vált.[3] Elismert információgyűjtő eszköz, de túlmutat a hírszerzési, elhárítási, felderítési tevékenységeken, és a civil élet egyes területein is teret követelt magának.[4] Ezen véleményekkel e tanulmány szerzőjeként teljes egészében egyetértek. Tényként kezelem az OSINT kiemelt szerepét és szektorokon átívelő mivoltát. Viszont ehhez azt is szükséges hozzá tenni, hogy már koránt sincs ekkora egyetértés az OSINT lényegét érintő néhány alapvető kérdésben. Érzékelhetően nincs konszenzus például abban, hogy melyek azok az információgyűjtő eszközök, amelyek az OSINT keretein belül felhasználhatók, és melyek azok, amelyek ezeken a kereteken kívül vannak és más típusú információszerzés felségterületére tartoznak. Vagy ahogy Vida Csaba fogalmazott: „Megemlítendő, hogy az OSINT-tevékenység során is felmerülhetnek illegális vagy nem etikus, jogi következményekkel járó mozzanatok. Ilyen lehet például személyek profiljának az engedélyük nélküli feltörése, hozzáférési adataik megszerzése és felhasználása. Az OSINT-területen is figyelembe kell venni a szerzői jogi kérdéseket a megszerzett dokumentumok, fotók stb. felhasználása során."[5] Hogy e kérdésben mennyire eltérő, sőt esetleg egymásnak ellentmondó kutatói vélekedések vannak, elég megnézni a közelmúltban a témában megjelent hazai tanulmányokat, ahol találunk Vida véleményével ellentétes és ezzel egyetértő véleményeket is.[6]

Éppen ezért e tanulmányban arra teszek kísérletet, hogy bemutassam azokat a szempontokat és sarokpontokat, amelyek döntő jelentőséggel vannak az OSINT keretében végrehajtható információgyűjtés határainak meghatározásakor. Jelen keretek között azonban nem vállalkozom arra, hogy az OSINT-tevékenységet végző valamennyi terület (katonai hírszerzés és felderítés, polgári hírszerzés és elhárítás, rendészeti felderítés és bűnüldözési célú felderítés, civil és üzleti hírszerzés stb.)

---

3 Burke 2007

4 Az OSINT a 21. század első évtizedére túlmutat a hírszerzés keretein, és gyakorlatilag valamennyi ágazat (hírszerzés, elhárítás, bűnügyi felderítés, bűnmegelőzés) alkalmazott eszköze lett. Izsa Jenő az OSINT-tal kapcsolatban azt tartotta fontosnak kiemelni, hogy a nyílt forrású információszerzés mindenki számára szabadon elérhető forrásokat használ fel, ezért ez nem klasszikus hírszerzési tevékenység, az itt megjelenő információk szándékosan felkutatott, megkülönböztetett, azonosító adatokkal ellátott, megszűrt információk, amelyek további felhasználásra kerülnek. Izsa 2009, 49.

5 Vida 2013, 104.

6 Jellemző példaként két véleményt ismertetek. A *Hadmérnök* című folyóiratban jelent meg Deák Veronika tanulmánya 2018 szeptemberében, amelyben az OSINT-eszközök között sorolta fel a konspiratív környezettanulmányhoz, a konspiratív figyeléshez hasonló információgyűjtő eszközöket, legenda felhasználását, valamint többek között bemutatta a Shodan nevű kereső alkalmazást, amely „lehetővé teszi a felhasználók számára, hogy különböző szűrőket alkalmazva feltárják az Internethez csatlakozó eszközöket (pl. számítógépeket, okostelefonokat, tableteket, szervereket, webkamerákat és azok videóit stb.), illetve még akár azok tartalmát, részletes adatait, sebezhetőségeit is". Deák 2018, 399. Vida Csabával azonos nézetet képvisel Bányász Péter: „A felhasználók többsége kevésbé érzékeny az adat-és információbiztonságára, így a növekvő internethasználat következtében rengeteg információt gyűjthetünk össze a személyekről […] Fontos azonban hangsúlyozni a tanulmány elején említett kitételt: ez az eljárás nem képezi részét a nyílt forrású hírszerzésnek, hiszen a nyilvánosság elől védett információkhoz is hozzáfér." Bányász 2015, 30.

szempontjait megvizsgáljam, hanem csak két jellemző területre, a magánvállalatok által folytatott, valamint a nemzetbiztonsági és rendészeti szervek által folytatott tevékenységekre koncentrálok.

A vizsgálat elvégzéséhez a fentieken túl további két alapvető szempontot tartok fontosnak kiemelni:

- Az OSINT mindig rendelkezni fog nemzeti jegyekkel, aminek következtében nemzeti szinten önállóan vizsgálható és vizsgálandó.
- Az OSINT önálló és kifejezett szabályozása[7] jellemzően nem történt meg sem demokratikus, sem egyéb berendezkedésű országok esetében. Ezzel párhuzamosan a demokratikus államok jogszabályi szinten kifejezetten szabályozzák az információgyűjtés titkos formáit, valamint a személyes adatok kezelésének lényeges területeit.

Az első szempontot azért fontos kiemelni, mert ennek következtében a témában Magyarországon kívül alkalmazott információszerzési eljárások automatikusan nem ültethetők át, minden esetben helye van a hazai alkalmazási környezethez való illesztésnek. A második említett szempont jelentősége pedig abban áll, hogy a titkos információgyűjtés (a továbbiakban: TIGY) és az információs önrendelkezéshez való jog magyar jogi szabályozása bizony az OSINT eszközrendszerének korlátait jelenthetik.

A rövid bevezető gondolatokat követően a keretek vizsgálatához az OSINT egyes fogalmi elemeit hívom segítségül. Ez esetben azonban nehézséget jelent, hogy egyelőre nem született meg a teljes nemzetbiztonsági és rendvédelmi szféra által elfogadott egységes meghatározás. Tekintettel viszont arra, hogy jelen tanulmánynak nem tárgya az OSINT jelentését önmagában vizsgálni, ezért több, köztük a magyar tudományos diskurzusban elfogadott jelentős nemzetközi szervezet által alkalmazott meghatározásokat és a hazai kutatók fogalmi meghatározásait veszem alapul.

Az OSINT információgyűjtő szakaszáról általában

A NATO OSINT Handbook[8] meghatározása szerint „az OSINT olyan információ, amelyet tudatosan megszereztek, kiválasztottak, kivonatoltak és felterjesztettek egy kiválasztott felhasználó körnek, általában a parancsnok és közvetlen beosztottja számára speciális kérdések megvizsgálása szempontjából. Az OSINT más szóval a hírszerzés bevált eljárási módszereit alkalmazza a sokféle nyílt forrású információ gyűjtése során, amely értesülések megszerzéséhez vezet”.[9]

---

7 Az önálló és kifejezett szabályozás hiányát azért tartom fontosnak hangsúlyozni, hiszen a jogállamok az információs önrendelkezéshez való jog alapjogként való elismerésével és szabályozásával közvetetten az OSINT-tevékenységre is hatással vannak.

8 A NATO OSINT-kézikönyv a nyilvánosság számára szabadon elérhető, 2001-ben publikált kiadvány, amelynek célja, hogy a nyílt forrású hírszerzés tárgyában alapvető oktatási segédlet legyen az egyesített és a szövetséges képzések alkalmával.

9 „OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence.” NATO 2001, 2.

Az USA-ban a 2006. évi költségvetési évre kiadott Nemzeti Biztonsági Felhatalmazási Törvény szintén tartalmazott egy OSINT-meghatározást,[10] amelyet azt követően több dokumentum is irányadónak fogadott el. Irányadónak fogadta el a Nemzeti Hírszerző Igazgató által a nyílt forrású információszerzésről megjelentetett 301. számú direktíva,[11] vagy a *Második Generációs Nyílt Forrású Hírszerzés (OSINT) meghatározása a Védelmi Vállalkozások számára* című kiadvány.[12] E dokumentumok szerint az OSINT keretében kizárólag nyilvánosan elérhető információk gyűjthetők és hasznosíthatók, ahol a nyilvánosan elérhető információk alatt azok az információk értendők: „amihez bárki jogszerűen hozzáférhet akár kérés, vásárlás vagy egyszerű észlelés útján".[13]

A NATO-definíciótól eltérő terminológia található a témával foglalkozó Lévay Gábor és Vida Csaba magyar kutatók tanulmányaiban. A nyílt forrású információszerzés Lévay Gábor szerint: „A katonai felderítés és hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti."[14] Tartalmi elemeit tekintve az OSINT hasonló meghatározását adja Vida Csaba is, aki szerint „az OSINT-tevékenység: az önálló nyílt adatszerző tevékenység valamely személy vagy szervezet által közzétett, nyilvánosan, legális eszközökkel megszerezhető vagy korlátozott körben terjesztett, de nem minősített adatoknak a hírszerzési igények kielégítésére, speciális módszertan alapján történő felkutatását, gyűjtését, szelektálását, értékelését és felhasználását jelenti".[15]

Ha a fent hivatkozott megfogalmazásokat egymással összevetjük, akkor az eltérő fogalmazásbeli különbségek mellett egy lényeges tartalmi különbséget fedezhetünk fel. Az USA-dokumentumok a hírszerző eljárások tárgyaként hangsúlyosan a *nyílt forrású információt* nevezik meg, függetlenül attól, hogy egyébként az információ maga képez-e bármilyen titkot, míg a nyílt információforrás Lévay és Vida szavai szerint: a közzétett, vagyis a publikum számára nyilvánosan, legális eszközökkel megszerezhető, vagy ugyan korlátozott körben terjesztett, de nem minősített információforrásokat jelenti. Az említett magyar elemzők ezzel az angolszász irodalomban alkalmazott kereteket valamelyest korlátozzák, hiszen nem elégednek meg a forrás nyilvános minőségével, hanem az információ nyílt jellegét is hangsúlyozzák. Vagyis az információ nem lehet *minősített.* De, hogy mégis mit tekinthetünk nyílt információforrásnak,

10 „Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." National Defense Authorization Act for Fiscal Year 2006, 3411.

11 ODNI 2006, 8.

12 Williams–Blum 2018, 8.

13 „Open Source Information: Publicly available information that anyone can lawfully obtain by request, purchase, or observation." ODNI 2006, 8.

14 Lévay 2006, 6.

15 Vida 2013, 101.

arról a hivatkozott dokumentumokban csak általános felsorolásokat és szélesen értelmezhető megfogalmazásokat találhatunk.[16]

A nyílt információs források mint az OSINT forrásai

Az alábbiakban megvizsgálom azokat az információforrásokat, amelyek az OSINT esetében megjelennek, ehhez pedig a NATO kézikönyv felsorolását veszem alapul. A NATO kézikönyv nyílt információforrásként a következőket sorolja fel:[17]

- *Hagyományos média:* A sajtótermékeket, sugárzott televízió- és rádióadókat jelenti, függetlenül attól, hogy a média hozzáférése vezetékes vagy sem, fizetős vagy ingyenes, online elérhető vagy kizárólag hagyományos elérési módjai vannak. Ide sorolja a kézikönyv azon médiumok szolgáltatásait is, amelyek nemcsak saját készítésű híranyagokat szolgáltatnak, hanem más médiumok anyagaiból úgynevezett sajtószemléket készítenek. Mára a NATO-kézikönyv kiadásakor ismert hagyományos média jelentősen átalakult, lényegesen nagyobb súllyal vannak jelen az online térben elérhető médiatartalmak. Újabb platformok jöttek létre, mint például a blog, a vblog, a kép- és videómegosztók, illetve a közösségi média egyéb területei, amik az információforrás szintjén elmossák a határokat a média és az internet között. Viszont – bármelyik platformon is történik a médiamegjelenés – közös jellemzőjük, hogy akik közzéteszik, azok újságként, folyóiratként, televízióként, rádióként, illetve újságíróként, médiamunkásként határozzák meg magukat. Úgy vélem, hogy a hagyományos média termékeinek a felhasználása mélyebb értelmezésbeli kérdéseket nem vet fel. Ezen sajtótermékek egyértelműen a nyilvánosságnak szólnak még azokban az esetekben is, amikor a felhasználói kör valamilyen módon (például előfizetéshez kötött, szakmai szervezet tagjai számára elérhető stb.) korlátozott. Problémaként talán a ritka, néhány példányban létező sajtótermék legális módon történő megszerzése, valamint a zárt közösség számára biztosított tartalmak megszerzése jöhet elő, de ezeket a kérdéseket a következő forrásoknál részletesen tárgyalom.
- *Internet:* A kézikönyv keresőfelületként és elérési lehetőségként határozza meg. Az online közösségi média térhódításával napjainkra az OSINT számában és minőségében is jelentős információforrásokhoz jutott, elegendő, ha csak végigböngésszük az eszközök és erőforrások felsorolását tartalmazó kézikönyvet.[18]

---

16 „Open Source Data (OSD). Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual." ODNI 2006, 2. „Open Source Information (OSIF). OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world." NATO 2001, 2.

17 NATO 2001, 5–11.

18 Open Source Tools and Resources Handbook, 2018.

Az internet esetében fontos hangsúlyozni, hogy a nyilvános adatokon és tartalmakon túl számos olyan tartalom, adat és adatbázis érhető el, amelyeknél alapesetben nem, vagy csak pontosan meghatározott jogosulti kör számára biztosított a hozzáférés, illetve vannak olyan adatok, amelyek az online térben különböző technikák alkalmazásával elérhetők, de az adatok gazdái azokat nem a nyilvánosságnak szánják. Éppen ezért az internetnek mint OSINT-információforrásnak a használata már jóval több értelmezési kérdést vet fel. Például a) meg lehet-e támadni egy online adatbázist olyan adatokért, amelyek az általános felhasználók számára nem állnak rendelkezésre; b) már megszerzett hozzáférési jogosultsággal be lehet-e lépni valakinek a profiljába; vagy c) felhasználható-e egy álprofil adatok megszerzésére?

Ha ezeket a példákat mélyebben megvizsgáljuk, akkor az OSINT lehetséges információgyűjtő eszközeinek több korlátjára, így a médiánál felvetett problémára is magyarázatot kaphatunk.

a) A mindennapokban használt számítógépes alkalmazásoknak több-kevesebb biztonsági hibáik vannak. A biztonsági hibák egy részét már feltárták, egy másik részét majd csak később teszik meg, és minden bizonnyal lesznek olyan biztonsági hibák, amelyeket soha nem tárnak fel. A biztonsági hibák azt jelentik, hogy az alkalmazások, valamint az informatikai rendszerek által kezelt adatok a biztonsági hibát ismerők által elérhetők és megszerezhetők. A feltárt biztonsági hibák egy része nyilvánosan megismerhető, leírásuk elolvasható, hozzáértő által fel-, illetve kihasználható. Ezenkívül vannak olyan feltárt biztonsági hibák, amelyek nem kerülnek nyilvánosságra, csupán egy szűk kör ismeri és használja őket. A biztonsági hibák kihasználásával a hacker a megtámadott alkalmazás vagy számítógépes rendszer nem nyilvános területeihez fér hozzá, amelyekből akár személyes, akár szervezeti, akár az informatikai rendszerre vonatkozó belső adatokat szerezhet meg. Mindezt pedig egyébként *nyilvános* ismeretek birtokában teszi. Mindent összevetve azt mondhatjuk, hogy a hackingmódszerek[19] felhasználásával történő adatszerzés egy olyan célzott, előre eltervezett aktív és jogosulatlan tevékenység, ahol a hacker szándékoltan olyan adatokat szerez meg, amelyeket az adatgazda nem tárt a nyilvánosság elé. Hogy az ezúton történő adatszerzést besoroljuk, a vonatkozó EU-s és hazai jogszabályokat veszem alapul.

Az Európai Parlament és a Tanács által *Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról* címmel kiadott 2013 / 40 / EU irányelv határozottan kijelenti, hogy az egyes információs rendszerekhez való jogosulatlan hozzáférés az EU területén bűncselekménynek minősül, és a tagállamok ennek megfelelően kötelesek jogrendszerüket kialakítani.[20] E szemléletet követi a magyar Büntető Törvénykönyv is, amely szerint bűncselekményt követ el az, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával belép.[21] Amellett, hogy a magyar jog a jogosulatlan belépést általánosságban tiltja, vannak olyan pontosan meghatározott állami szervezetek, amelyek számára törvényi felhatalmazással, TIGY keretében lehetővé

[19] Hackingmódszereknek azokat az alkalmazott támadási technikákat nevezhetjük, amelyek segítségével a hacker megtalálja és kihasználja az informatikai ezközök és rendszerek sebezhetőségét.

[20] 2013/40/EU irányelv (8) pont.

[21] Btk. 422. §.

is teszi azt.[22] Tekintettel az OSINT és a TIGY viszonyára, fogalmilag kizárt, hogy mind a két információszerző mód alkalmazza ugyanazt az információszerző eszközt, amiből pedig az következik, hogy az OSINT során nem használható hackingmódszereket alkalmazó eszköz.

A jogi környezet alapján tehát azt láthatjuk, hogy az EU-ban – és így Magyarországon is – az információs rendszerekbe történő jogosulatlan behatolás az állam által üldözendő magatartásnak minősül. Legálisan ilyen tevékenységet kizárólag az erre direkt felhatalmazott szervezetek, külön felhatalmazás alapján, TIGY keretében folytathatnak.

b) Ismeretlenek online elérhetővé tettek egy adatbázist, amely sok millió felhasználó e-mail-hozzáférési adatait tartalmazza. A listában lévő belépési adatokkal az érintett tudta és beleegyezése nélkül bárkinek a személyes postafiókjába be lehet lépni és a levelezését meg lehet szerezni. Sőt, vannak olyan szolgáltatók (mint például a Google), akiknél a levelezésen túlmenően sokkal többféle információ (saját készítésű képek és videók, hónapokra visszamenőleg tartózkodási adatok, véletlenszerűen rögzített hanganyagok, levelezési és címlisták, egyéb, a felhőszolgáltatásba feltöltött dokumentumok, naptárbejegyzések stb.) található egyetlen fiókba történő belépésnél. A felhozott példa esetében nem is csak egy, hanem két adatszerzéssel kapcsolatos kérdés is felmerül:

1. Vajon harmadik személy által nyilvánosságra hozott személyes adat (hiszen a hozzáférési adat személyes adatnak minősül) bárki által jogszerűen megszerezhető és kezelhető?
2. Vajon a megszerzett hozzáférési adat felhasználható információszerzésre az OSINT keretében?

Az első kérdésre adandó válasznál jelen tanulmány keretei között nem kívánom valamennyi lehetséges esetet önállóan megvizsgálni, csupán két alapesetet – magántársaságot, illetve állami hírszerző, elhárító és felderítő szervet – vizsgálom meg.

Az Alaptörvény II. cikke szerint az emberi méltóság sérthetetlen, ezért alkotmányos szinten védelem illeti meg az egyén magán- és családi életét, a személyes kapcsolatrendszerét, az otthonát és jó hírnevét.

A védelmi rendszer legfelső szintjén nemzetközi egyezmények (például Európai Unió Alapjogi Kartája) állnak, nemzeti szinten az Alaptörvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint egyes ágazati törvények adatkezelési rendelkezései találhatók. A személyes adatok védelmét biztosító többszintű rendszer megfelel a törvényesség és a hátrányos megkülönböztetés kívánalmainak, szem előtt tartja a szükségesség és az arányosság követelményeit, illetve biztosítja a bírósághoz és más független szervhez történő fordulás lehetőségét.

A legmagasabb szinten az Alaptörvény kimondja a személy beazonosítására alkalmas és személyiségéhez tapadó adatok nyilvánosságának általános tilalmát. Eszerint személyes adataival mindenki maga rendelkezik, és alapvetően maga dönt

[22] Nbtv., Rtv., Be., NAV tv. Ütv.

azok megismerhetőségéről, vagy jogszabály rendelkezhet egyes személyes adatok mások által történő kezeléséről. Az Alaptörvény rendelkezéseit részletezve az Infotv. megadja a különböző típusú személyes adatok meghatározását, definiálja és részletezi az adatkezelés szabályait és deklarálja az alapelveit. Ezenkívül meghatározza, hogy milyen felhatalmazással kezelhető személyes adat: személyes adatot kezelni kizárólag az érintett hozzájárulása, törvény vagy helyi önkormányzati rendelet felhatalmazása, az érintett hozzájárulását átmenetileg pótló törvényi felhatalmazás vagy az érintett vélelmezett hozzájárulása alapján lehet.

Tekintettel arra, hogy magántársaságok esetében a személyes adatok kezelésének egyik jogalapja sem áll rendelkezésre az OSINT égisze alatt, ezért már a személyes adatok kezelésének eddig bemutatott legalapvetőbb ismérvei alapján is megállapítható, hogy egy hozzáférési jogosultságot megszerző magánszemély jogszerűen nem kezelheti, vagyis még csak nem is rögzítheti és semmilyen formában nem használhatja fel azt, így be sem léphet vele más személyes fiókjába.

Második alapesetben az OSINT-tevékenységet végző állami hírszerző, elhárító és felderítő szerveket vizsgálom, amihez a tevékenységüket szabályozó törvényeket kell alapul venni. Hiszen, ha a rájuk vonatkozó ágazati törvény tevékenységük végzéséhez felhatalmazza a hatóságokat harmadik személy személyes adatainak kezelésére, akkor a hozzáférési adatokat megszerezhetik és kezelhetik. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) az adatkezelés szabályai között felhatalmazza a magyar szolgálatokat a személyes adatok kezelésére, és meghatározza az adatok beszerzésének módjait is.[23] Eszerint a szolgálatok adatokat szerezhetnek be nyílt forrásból történő adatgyűjtéssel. Ebből pedig az következik, hogy a szolgálatok az interneten talált hozzáférési jogosultságokat rögzíthetik és kezelhetik. Viszont az nem következik, hogy OSINT keretében további információgyűjtésre használhatnák fel, éppen ellenkezőleg. Az Nbtv. későbbi rendelkezéseiből ugyanis az olvasható ki, hogy kizárólag TIGY során léphetnek be vele felhasználói fiókba és használhatják információszerzésre, mivel az Nbtv. külső engedélyhez kötött TIGY keretében jogosítja fel a szolgálatokat arra, hogy információs rendszerben kezelt adatokat titokban megismerjenek és az ott észlelteket technikai eszközzel rögzítsék.[24]

Mindezek szellemében az állapítható meg, hogy Magyarországon alapesetben felhasználói adatok nem használhatók fel további információszerzésre OSINT keretében, hiszen a példánkban az e-mail-fiókba történő belépéskor és a levelezési adatok megismerésekor már hiányzik a nyílt forrású információgyűjtés alapvető feltétele: a nyílt információforrás. Azzal, hogy a szolgálat nyílt forrásból szerezte meg a hozzáférési jogosultságot, csupán az információhoz való hozzáférés egyik lehetséges módja nyílt meg előtte, a forrás minősítése nem változott, az továbbra is zárt maradt. Ennek következtében azok a szervek, amelyek TIGY végrehajtására törvényi felhatalmazás hiányában nem jogosultak, vagy ugyan jogosultak, de az adott ügyben nem folytatnak jogszerűen TIGY-t, nem léphetnek be az e-mail-fiókba és nem ismerhetik meg annak tartalmát. Viszont azok a TIGY végrehajtására felhatalmazott szervek, amelyek adott

[23] Nbtv. 38. §.
[24] Nbtv. 56. § e) pont.

esetben jogosultak az információs rendszerben kezelt adatokat titkosan megismerni, TIGY keretében elvégezhetik az adatgyűjtést.

c) A harmadik példánkban az információgyűjtéssel érintett személy Facebookon folytatott tevékenységét szeretné valamely szerv figyelemmel kísérni. Az érintett a Facebookon a mindenki számára nyilvános felület mellett általa létrehozott privát helyszíneket is használ. Kérdés, vajon meddig terjednek az OSINT lehetőségei: csak a nyilvános felületeken megadott információk begyűjtésére, vagy valamennyi felület információinak megszerzésére. Ennek érdekében vajon létrehozható egy álprofil és hozzá kapcsolódó legenda, akinek jelentkezését az érintett elfogadja a privát helyszínekre is?

Megítélésem szerint a b) pontnál bemutatott jogi környezet ebben az esetben is meglehetősen pontos utasítást ad arra, hogy közösségi felületeken meddig folytatható a nyílt forrású információgyűjtés, és mi az, ami már a TIGY területére tartozik. Az előző példában bemutatott okfejtéshez képest ez esetben az a lényeges különbség, hogy az Nbtv. egy másik jogszabályi rendelkezése alapján lehet álprofil és legenda alkalmazásával információhoz jutni. Míg az előzőnél egy külsőengedély-köteles titkos információszerző eszköz alkalmazása történik, addig a mostani példa esetében egy külső engedélyhez nem kötött titkos információgyűjtő eszköz felhasználására kerül sor.[25]

Mindezek következtében egyetértek Vida Csaba azon megállapításával, miszerint: „A közösségi oldalak a nyílt információszerzés új, de a kiberadatszerzéssel határos területe, mert abban az esetben, ha a hírszerzés már megtévesztő, esetenként legendával alátámasztó megtévesztő információkkal folytat keresést, akkor az már nem nyílt, hanem műveleti adatszerzés."[26]

A fent bemutatott három eset alapján összefoglaltan az állapítható meg, hogy az internet alapvető OSINT-forrásként való megjelölése nem vitatható, azonban az online térben automatikusan nem alkalmazható minden információgyűjtő eszköz az OSINT során. Nem tartoznak az OSINT területére azok az információgyűjtő tevékenységek, amelyeknél

- hackingeszközök felhasználásával,
- megszerzett jogosultságok felhasználásával vagy
- szándékolt, az érintett megtévesztését célzó magatartás tanúsításával történik információszerzés.

- *Az online kereskedelmi szolgáltatók:* Kereskedelmi alapon nyújtanak online válogatott és rendszerezett tartalmakat az előfizetőik számára. Az online kereskedelmi szolgáltatóknak számos formája létezik, a NATO-kézikönyv több fontos szolgáltató felhasználási lehetőségeit is leírja.[27] Lényeges ismertetőjük, hogy az általuk létrehozott tartalmakat és adatbázisokat ellenszolgáltatás fejében biztosítják

[25] Nbtv. 54. § (1) A titkos információgyűjtés keretében a nemzetbiztonsági szolgálatok
a) […]
b) a nemzetbiztonsági jelleg leplezésével információt gyűjthetnek.

[26] Vida 2013, 107.

[27] Vida 2013, 6–9.

partnereik számára. A szolgáltatás nem feltétlenül működik online, előfordulhat, hogy digitális adathordozón vagy egyéb elektronikus módon és úton juttatják el az információkat az ügyfeleik részére.

Ahogy Lévay Gábor bemutatja, ebbe a körbe olyan szolgáltatók tartoznak, amelyek jellemzően egy-egy szakterületre szakosodtak. A szakterületek rendkívül széles skálán mozoghatnak, kezdve a biztonságpolitikától a gazdasági és pénzügyi elemzéseken át egészen az energiabiztonságig. Termékeik mögött az adott témában komoly szakmai ismeret és tevékenység húzódik. Példaként a Stratfor[28] és a Jane's[29] cégeket említi, amelyek szolgáltatásai között szerepel komplett értékelések-elemzések és prognózisok készítése, jól strukturált kereshető adatbázisok biztosítása.[30]

Önmagában az online kereskedelmi szolgáltatók OSINT-információs forrásként történő felhasználása alapvető információszerző módszertani kérdést nem vet fel, csupán egyetlen esetben merülhet fel a hovatartozás kérdése. Akkor, ha egy szolgálat HUMINT keretében álcázott személy útján, az online kereskedelmi szolgáltatót a partner személyében megtévesztve szerzi meg a terméket. Ezt az esetet azonban később, az interjúztatás témakörében részletezem.

- *A szürke irodalom:* Olyan nyílt információkat tartalmazó dokumentumokat takar, amelyek egy jól meghatározott szűk kör számára készülnek, a széles nyilvánosság felé nem feltétlenül publikálják őket. Ide sorolhatók az akadémiai értekezések, disszertációk, bizottsági beszámolók, konferenciaanyagok, technikai jelentések és technikai szabványok, vitairatok, előnyomatok, kormányzati beszámolók, hírlevelek, üzleti vagy piaci előrejelzések, kutatási beszámolók, fordítások, úti beszámolók, munkaanyagok stb. A legtöbb szürke irodalom kategóriájába tartozó információgyártó szervezet a nemzeti kormányok és kormányzati szervek, a politikai pártok, a kutatóintézetek, egyetemek, akadémiák, valamint a kereskedelmi társaságok.[31]

  Az előző ponthoz képest a szürke irodalom esetében azt lehet mondani, hogy az információ előállításának és publikálásának módja okán már több módszertani kérdés vethető fel. Elsősorban az, hogy van-e a publikált terméknek nyilvános elérési módja, vagy csupán jól körülhatárolt felhasználói kör számára publikált. Utóbbi esetben ugyanis a kereskedelmi szolgáltatóknál is megemlített probléma merül fel, amelyet a későbbiekben fogok tárgyalni. Másodsorban a dokumentum minőségi problematikáját is meg kell vizsgálni, hiszen az így készült tartalmak egy jelentős része valamilyen – még akkor is, ha ez egyébként nincs a tartalmon egyértelműen feltüntetve – titkot képezhet vagy védendő személyes adatot tartalmazhat. A titok kérdéskörét szintén e tanulmány későbbi részében vizsgálom meg.

---

28 A Stratfor egy amerikai geopolitikai magán hírszerző platform és kiadó, amelyet 1996-ban alapítottak meg Austinban. Elérhető: www.stratfor.com/ (A letöltés dátuma: 2019. 04. 02.)

29 A Jane's Information Group egy katonai, repülési és közlekedési témákra szakosodott brit kiadó. Elérhető: www.janes.com/ (A letöltés dátuma: 2019. 04. 02.)

30 Lévay 2004, 54.

31 Lévay 2004, 55.

- *A szakértők és megfigyelők:* A szakértők és megfigyelők esetében az OSINT-irodalom több forrást is megjelöl, úgymint a szakértők és megfigyelők személyes tapasztalatai alapján készített leírásokat, beszámolókat és a tapasztalásaikról szóló személyes interjúkat. Mindezek a források addig nem is vetnek fel problémát, amíg nyilvános forrásból elérhetők, viszont amint már valamilyen, az előzőkénél is említett korlátozás áll fenn, akkor az ott felvetett módszertani probléma itt is jelentkezik. Sőt, külön szükséges kiemelni az interjúztatás kérdését, hiszen egészen más megvilágításban jön elő a nemzetbiztonsági hírszerző, elhárító és felderítő szolgálat, és egészen másként a gazdasági társaságok esetében.

  Az utóbbi megteheti, hogy nyíltan, magát megnevezve, akár a célját is felfedve megkeresi a szakértőt és átveszi vagy megveszi a tapasztalatait. A nemzetbiztonsági szolgálatok esetében azonban a szakértő interjúztatása valamilyen szervezeti kapcsolat nélkül meglehetősen valószínűtlen, ezért az információgyűjtés könnyedén átcsúszhat a leplezett vagy titkos oldalra. Mindez abból következik, hogy egy nemzetbiztonsági szolgálat többféleképpen építhet ki kapcsolatot olyan személlyel, aki nem érintettje a vizsgált eseménynek, hanem csak szakismerete okán bír értékes tudással. Megtörténhet, hogy a kapcsolatfelvételnél a szolgálat:
  - titkolja kilétét és titkolja célját,
  - titkolja kilétét, de nem titkolja célját,
  - nem titkolja kilétét, de titkolja célját,
  - nem titkolja kilétét és nem titkolja célját.

  Megítélésem szerint az első két esetben bármilyen kapcsolaton keresztül is történik az interjú elkészítése, nem beszélhetünk OSINT-ról. A szolgálat ugyanis leplezi nemzetbiztonsági jellegét, ami az Nbtv. 54. § (1) bekezdés b) pontja értelmében külső engedélyhez nem kötött titkos információgyűjtő eszköz. A harmadik esetben az ügynökség szintén alkalmaz valamilyen legendát, amivel megtéveszti és tévedésben tartja az interjúalanyt, ráadásul a szolgálat felvilágosítást kér, ami pedig az a) bekezdés értelmében minősül külső engedélyhez nem kötött titkos információgyűjtésnek. Valószínűleg ebben az esetben jogosan felvethető, hogy a hatályos törvényi rendelkezések helyesen sorolják-e ezen tevékenységet a TIGY keretében alkalmazható információgyűjtő eszközök közé, hiszen a mindennapi élethez szorosan kapcsolódó, számtalanszor előforduló természetes viselkedési formáról van szó. A negyedik esetben sem egyértelmű, hogy nyílt forrású információszerzésről beszélhetünk-e. Ebben a szituációban fontos szempont az interjúalany és az ügynökség viszonya. Amennyiben kettőjük között bármilyen szervezetszerű kapcsolat áll fenn, vagyis az interjúalany az ügynökség valamilyen rendű kapcsolata, akkor az egyértelműen a TIGY körébe tartozik.[32] Ha viszont az alannyal semmilyen szervezetszerű kapcsolat nem áll fenn, az interjúztató személyével és céljával sincs tévedésben, akkor is ott van a felvilágosításkérést TIGY-nek minősítő törvényi szakasz. Ebben az esetben az információgyűjtés minősítését már az döntheti el, hogy az interjúztatás tényéről harmadik személy tudomást szerezhet-e, vagy az interjúalany köteles azt titokban tartani.

[32] Nbtv. 54. § (1) bekezdés c) pont.

Az interjúztatás apropóján leírtak alapján a magyar nemzetbiztonsági szolgálatok és a források kapcsolatainál eddig felvetett problémákra együttesen vonható le következtetés. Mégpedig az, hogy az információforrással legenda felhasználásával való személyes kapcsolat kialakítása és valakinek az interjúztatása az Nbtv. hatálya alá tartozó szervek esetében egy-két egyedi kivételtől eltekintve TIGY keretében alkalmazható információgyűjtő eszköz.

- *A kereskedelmi műholdak felvételei:* Mára a katonai műholdak mellett egyre több kereskedelmi műhold is működik, amelyek felvételei bárki számára elérhetőek, aki megfizeti. E tekintetben a nemzetbiztonsági szolgálatok esetében ismét a hogyanra adott válasz lehet a vízválasztó.

A NATO-kézikönyvben felsorolt OSINT-forrásokat a tudomány magyar művelői továbbiakkal egészítik ki. Forrásnak minősítik a nyomtatott kiadványokat, az oktatási intézményeket, az újságírókat, a nyelviskolákat, az üzleti életet, a nemzetközi szervezeteket, a nem kormányzati szervezeteket és a már említett közösségi oldalakat,[33] valamint ezeken is túlmenően a helyszíni előadásokat, konferenciákat, a tudományos kutatószervezeteket, a könyvtárakat és az információbrókereket.[34] Ezek számbavétele során azt láthatjuk, hogy az alkalmazható információszerző eszközök meghatározása a fenti forrásoknál bemutatott elhatárolásokkal analóg módon tehető meg. Valamennyiüknél megtalálhatók azok a produktumok és termékek, amelyek – legyen az akár valamelyest korlátozott is – a nyilvánosságra hozás szándékával, vagy a nyilvánosság számára készülnek. Azonban szinte mindegyik esetében lehet olyan produktumokat említeni, amikor az információhoz való hozzájutás módja miatt nem lehet egyértelműen kijelenteni, hogy ezektől a forrásoktól minden megszerezhető OSINT során. Például ezen területek online elérhető adatait csak addig a pontig tekinthetjük az OSINT számára felhasználhatónak, ameddig az valóban legális eszközökkel történik. Vagyis – ahogy azt az internetnél bemutattam – az online térben ez azt jelenti, hogy a világhálóra a nyilvánosságra hozás szándékával feltett információk begyűjtése érdekében bármilyen eszköz, szolgáltatás, keresőmotor stb. felhasználható. Mindaddig, amíg a szolgálatok nem alkalmaznak megtévesztést, kerülik a hackingeszközöket és – új szempontként említem – tiszteletben tartják a szerzői jogokat. Ezen forrásoknál is érvényes, hogy egy megtévesztéssel megszerzett hozzáférési jogosultsággal folytatott információgyűjtés már a titkos kategóriába tartozik, hasonlóan a malware-rel történő adatlopáshoz.

A nyílt információ mint az OSINT-tevékenység kizárólagos tárgya

Az OSINT fogalmának második lényeges ismérve a forrás mellett a hazai tudományos diskurzusban a nyílt információ. Azért tartom lényegesnek ennek hangsúlyozását, mert az angolszász irodalom ezzel szemben megelégszik azzal, hogy az információ nyílt forrásból származzon. Ahogy viszont az OSINT jellemzőinek bemutatásakor is

[33] Vida 2013, 105.
[34] Lévay 2004.

kiemeltem, a hazai meghatározás azt is kiköti, hogy az információ nem lehet minősített adat. Ebben a fejezetben azt fogom megvizsgálni, hogy ennek a fogalmi elemnek a hazai OSINT esetében valóban van-e relevanciája, vagy esetleg elhagyható lenne.

A minősített adat fogalmát jelenleg a minősített adat védelméről szóló 2009. évi CLV. törvény határozza meg. A törvény a minősített adat két formáját ismeri. Nemzeti minősített adatnak tekintendő a minősítői joggal rendelkező személy által beminősített adat. A minősítés szükséges feltétele, hogy a minősítő a minősített adat adathordozóját a törvényben előírt alaki kellékekkel lássa el. Ezenkívül a törvény ismeri a külföldi minősített adatot, amely alatt az EU valamennyi intézménye és szerve, továbbá az EU képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adatot értünk, amelyhez történő hozzáférést az EU intézményei és szervei, az EU képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.

Mint látható, a minősített adat alatt viszonylag jól körülhatárolt adathalmazt értünk, amelyet vagy erre feljogosított magyar szervek, vagy külföldi államok – jellemzően, de nem kizárólag EU- és NATO-tagállamok – szervei láttak el minősítéssel. A minősített adatot csak az szerezheti és ismerheti meg, akinek erre a minősítő vagy törvény felhatalmazást ad. A hazai jog a minősített adat jogosulatlan kezelését és megszerzését szankcionálja, jogosulatlan kezelését szabálysértésnek,[35] míg jogosulatlan megszerzését és felhasználását bűncselekménynek minősíti.[36]

Tekintettel arra, hogy a minősítő nagy eséllyel nem biztosít megismerési jogosultságot az OSINT-tevékenységet végző magántársaságoknak, illetve törvényi szinten sem lehető fel erre vonatkozó felhatalmazás, továbbá még az Nbtv. sem tartalmaz a nemzetbiztonsági szolgálatoknak szóló, erre vonatkozó általános felhatalmazó rendelkezéseket, ezért minősített adat bárki által történő megszerzése, még ha az nyílt forrásból is történik meg, jogszerűtlen magatartásnak minősül. Ehhez azonban azt is fontos hozzátenni, hogy az állítás csak abban az esetben igaz, ha az adat adathordozóján egyértelműen megtalálhatók a minősítés alaki kellékei. Ezek hiányában, ami azért például egy digitális adathordozón fellelhető adat esetében korántsem elképzelhetetlen, nem derülhet ki egy adatról, hogy az minősített-e vagy sem.

De vajon mi a helyzet azokkal a *minősített adatokkal,* amelyeket a magyar jog nem ismer el minősített adatnak, és így megszerzését, felhasználását és kezelését nem szabályozza és nem is szankcionálja? A kérdésben a válasz is megtalálható. Mivel a magyar jog nem ismeri el minősített adatnak, ezért a hatálya alá tartozó személyek és szervezetek tekintetében sem minősül minősített adatnak. Ennek következtében jogi védelemben nem részesül, vagyis bárki által szabadon gyűjthető. Viszont, ha ez kiderül, akkor azért az adatforrás országát a későbbiekben érdemes elkerülni, hiszen nagy valószínűséggel az adat a hazaihoz hasonló szintű védettséget élvezett az adott államban.

A minősített adatokon kívül vannak olyan adatok, amelyek valamilyen széles körben elfogadott társadalmi norma alapján bizalmasnak vagy titkosnak számítanak.

35 Szabstv. 206. §.
36 Btk. 265. §.

„[Minden] olyan ismeret, ami csak egy adott személyi kör számára áll rendelkezésre, és amit azok, akik a birtokában vannak, igyekeznek kisajátítani, mások számára hozzáférhetetlenné tenni (különböző titokvédelmi rendszabályok alkalmazásával). Az információt birtokló, azt a saját érdekében felhasználni kívánó csoport szempontjából a »kívülállók« illetéktelennek számítanak, nem jogosultak az adott információ megismerésére és felhasználására."[37] Ide tartozónak tekinthetjük például a foglalkozásokból eredő titkokat (ügyvédi, üzleti, orvosi és gyónási titok stb.), valamint az egyes emberi viszonyokból eredő titkokat (hitéletbeli, biztosítási, szerződési, üzleti titok stb.). Titkosnak tekinthetők továbbá a személyes adat és a különleges adat, amelyek közvetlen jogi védelem alatt állnak. A titok alapból feltételezi, hogy nyílt forráson nem található meg, vagyis csak illegális eszközökkel beszerezhető. A titok viszont csak addig lesz titok, amíg azt birtokosa direkt akarattal vagy egyszerűen csak hanyagságból nem teszi illetéktelenek számára elérhetővé. Ha valaki például a betegségével kapcsolatos adatokat kiteszi egy közösségi oldal mindenki által elérhető felületére, vagy nyilvános blogon tesz fel egy bizalmas szerződésével kapcsolatos konkrét kérdést, vagy gazdasági társaság bizalmas üzleti szerződést tesz elérhetővé honlapján, akkor az így megadott információk az OSINT szempontjából nyílttá válnak és az OSINT tárgyai lehetnek.

Összefoglaló gondolatok

Az OSINT információszerző szakaszával kapcsolatban az eddig kifejtettek alapján összegzésképpen azt mondhatjuk, hogy önmagában nem elegendő az OSINT alá sorolni az információforrást, mert a forrás általános megnevezése alapján nem feltétlenül dönthető el, hogy az adott adat az alkalmazni kívánt információszerző eszközzel valóban megszerezhető-e OSINT-tevékenység keretében, vagy sem, az eldöntéséhez az alkalmazni kívánt információgyűjtő eszköz besorolására is szükség van. Ráadásul mindez az OSINT-tevékenységet végzők szintjén is eltérő lehet, más szempontokat kell figyelembe venni egy magántársaság esetében és megint más szempontokat egy rendvédelmi szerv esetében.

További lényeges megállapítás, hogy az OSINT információszerző eljárásoknak nem kizárólagos feltétele a megszerezni kívánt információ nyílt minősége, jogos a Vida Csabánál és Lévay Gábornál tett szigorítás, mert a nemzeti és bizonyos külföldi minősített adatok nem képezik OSINT-információszerzés tárgyát. Ezzel párhuzamosan fogalmi szinten további korlátozást is indokoltnak tartok, hiszen személyes adatoknál az OSINT-tevékenységet végzőkre vonatkozó jogi szabályozás egyértelműen szűkíti a gyűjtési lehetőségeket, míg a titkok és a hazai jog által nem védett minősített adatok esetében a forrás határozza meg ezt.

[37] Rácz 2010, 6.

Felhasznált irodalom

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. évf. 2. sz. 21–36. Elérhető: https://folyoiratok.uni-nke.hu/online-egyetemi-folyoiratok/nemzetbiztonsagi-szemle/korabbi-szamaink/20152-szam (A letöltés dátuma: 2019. 04. 25.)

Burke, Cody (2007): *Freeing knowledge, telling secrets: Open source intelligence and development.* CEWCES Research Papers. No. 13. Bond University. Elérhető: https://pure.bond.edu.au/ws/portalfiles/portal/28737919/Freeing_knowledge_telling_secrets.pdf (A letöltés dátuma: 2019. 02. 20.)

Deák Veronika (2018): A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során. *Hadmérnök,* 13. évf. 3. sz. 391–402. Elérhető: www.hadmernok.hu/183_29_deak.pdf (A letöltés dátuma: 2019. 04. 25.)

Izsa Jenő (2009): *Nemzetbiztonsági Alapismeretek (A Titkosszolgálatok Működése).* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

Lévay Gábor (2004): A nyílt források felhasználásának lehetőségei a hírszerző munkában. *Felderítő Szemle,* 3. évf. 3. sz. 48–65.

Lévay Gábor (2006): *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

NATO Open Source Intelligence Handbook (2001). Elérhető: www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20-Handbook%20v1.2%20-%20Jan%202002.pdf (A letöltés dátuma: 2018. 09. 07.)

ODNI (2006): *Intelligence Community Directive Number 301.* Washington, D. C., Office of Director of National Inteligence. Elérhető: www.hsdl.org/?abstract&did=469452 (A letöltés dátuma: 2019. 04. 10.)

Open Source Tools and Resources Handbook 2018 (2018). Elérhető: www.i-intelligence.eu/osint-tools-and-resources-handbook-2018/ (A letöltés dátuma: 2019. 04. 23.)

Rácz Lajos (2010): A titkos információszerzés néhány elméleti kérdése. *Szakmai Szemle,* 3. sz. 5–32.

Vida Csaba (2013): Nyílt forrású adatszerzés (OSINT). In Kobolka István szerk.: *Nemzetbiztonsági Alapismeretek.* Budapest, Nemzeti Közszolgálati Egyetem. 101–109.

Williams, Heather J. – Blum, Ilana (2018): *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* Santa Monica, Rand Corporation. DOI: https://doi.org/10.7249/RR1964

Jogforrások

1995. évi CXXV. törvény a nemzetbiztonságról

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2012. évi C. törvény a Büntető Törvénykönyvről

2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről

Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=EN (A letöltés dátuma: 2019. 04. 02.)

National Defense Authorization Act for Fiscal Year 2006, Public Law 109–163, Department of Defense Strategy for Open-Source Intelligence, January 6, 2006.

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 19–31. • DOI: 10.32561/nsz.2019.2.2

Csizner Zoltán[1]

Az OSINT határai

The Limits of OSINT

A nyílt forrású információgyűjtés korábban is hasznos segítséget jelentett, de ezt az informatikai forradalom, a világháló és a közösségi média térnyerése tovább fokozta. Ugyanakkor a lehetőség sok veszélyt és korlátot is hordoz magában, ami az alkalmazókban talán nem mindig tudatosul. Az alábbi pár gondolat figyelemfelhívás ezekre a veszélyekre és korlátokra, amelyek szem előtt tartása talán biztonságosabbá teheti a hírszerzés ezen szegmensét.

Kulcsszavak: OSINT, veszélyek és korlátok, felejtés joga, digitális lábnyom, jogszerűség

The open source intelligence gathering has been a useful tool earlier, but the information revolution, the world wide web and the social media made it more essential. Meanwhile this opportunity includes many dangers and limits which the users may not be aware of. These few thoughts below could contribute to the raising of the awareness of those dangers and limits; keeping them in mind should make this segment of the intelligence safer.

Keywords: OSINT, dangers and limits, the right to forget, digital footprint, legality

A nyílt forrású hírszerzés

Történelmi példák mutatják, hogy a köznapi ember számára is észlelhető, megismerhető adatok tudatos értelmezése és elemzése a politikai döntésekben – a múltban jellemzően a háborúkban – is hasznosíthatóvá válhatnak. A második világháborúban például német tudósok a londoni Big Ben harangjátékának élő közvetítéséből vontak le következtéseket az aktuális időjárási viszonyokról, amelyeket a Luftwaffe parancsnokai az angol főváros bombázásának tervezéséhez használtak fel.[2] Az persze már

[1] Csizner Zoltán r. ezredes, doktorandusz, a Terrorelhárítási Információs és Bűnügyi Elemző Központ főosztályvezetője. ORCID-azonosító: 0000-0002-1867-8560.

[2] Harari 2015, 354.

a módszer egyes korlátait (például megbízhatóság, ellenőrzésre szorultság) igazolja, hogy miután a brit hírszerzés erre rájött, felvételről kezdték sugározni a harangszót, és ezzel már dezinformálni tudták az ellenséget.

A nyílt forrású hírszerzés, az OSINT[3] fogalmi értelmezése szerint felölel minden elérhető nyílt forrást, így a médiaforrásokat (például újságok, magazinok, rádió- és televízióadások, számítástechnikai eszközökön megszerezhető adatok), közadatokat (például kormányzati jelentések, politikai nyilatkozatok, meghallgatások, törvénykezési viták), szakértői és kutatási adatokat (konferenciák, szakértői társaságok, tudományos folyóiratok).[4] Azonban a mai világban mégis az internet, pontosabban az azon futó világháló (www: World Wide Web) jelenti a legnagyobb forrást, és egyre ritkább a *Keselyű három napjá*ban[5] látott elemzési munkamódszer.

Ugyan pontos és mindenki által elfogadott meghatározása nincs az OSINT-nak, de az alábbi két idézet talán rávilágít a lényegre.

Az első Lévay Gábortól származik:[6] „Az OSINT a katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti…"

A másodikat az NSA[7] és a CIA[8] egykori igazgatójának, Michael Hayden nyugalmazott tábornoknak tulajdonítják: „A források nyilvánosak. Az érdeklődési körünk nem az. A szakmánkban nem mindig a titkos információk a legértékesebbek. Valójában, sokkal élvezetesebb megoldani egy problémát vagy megválaszolni egy nehéz kérdést olyan információk alapján, amit valaki meggondolatlanul nyilvánosan is hozzáférhetővé tett."

Az már csak a hírszerző társadalom leleményessége, hogy a nyílt forrású hírszerzést is tovább bontotta, és a hétköznapi tapasztalatok alapján megalkottak új – igaz, kevésbé tudományos – területeket is.

Így alakult ki többek között a PIZZINT, a pizzahírszerzés, amelynek alapját az USA-ban tevékenykedő szovjet hírszerzők megfigyelési eredményei jelentették. Ezek szerint ha a megszokottnál több pizzaszállító jelent meg a Fehér Ház, a Külügyminisztérium, a Védelmi Minisztérium vagy a CIA épületénél, akkor az valamilyen válsághelyzetet jelentett, ami miatt többen maradtak bent.

A legendák szerint hasonló ismeretek alapján jött létre a LAVINT (a mosdóhírszerzés), a RUMINT (a folyosói hírszerzés), valamint a DIVINT (az isteni hírszerzés).[9]

A 21. század technikai robbanása magában hordozta a keletkezett információ mennyiségének ugrásszerű fejlődését is. Soha nem látott mértékű személyes adat, ismeret, titok érhető el a hozzáértő számára a világhálón pár kattintással, rövid idő alatt. Egy amerikai tanulmány[10] szerint már 2012-ben is naponta 2,5 milliárd gigabyte (GB)

---

3 Open Sourche Intelligance – nyílt forrású hírszerzés.
4 Lowenthal 2017, 178.
5 James Grady (1949–) regényéből készült amerikai film, amelynek főhőse a CIA alkalmazásában naphosszat regényeket, cikkeket olvas és dolgoz fel az azokban található ötletek, információk felhasználhatósága érdekében.
6 Lévay 2006, 6.
7 National Security Agency – Nemzetbiztonsági Ügynökség (USA).
8 Central Intelligence Agency – Központi Hírszerzési Ügynökség (USA).
9 Lowenthal 2017, 179.
10 Monnappa 2019.

adat keletkezett. Az információ keletkezése soha nem látott módon gyorsul; 2020-ra az előrejelzések szerint minden másodpercben, személyenként 1,7 megabyte adatmennyiséget állítunk majd elő a Földön.

Ezzel párhuzamosan a tárolókapacitások növekedése, egyre olcsóbb elérhetőségük, az elemzési rendszerek és módszerek fejlődése megteremtette az igényt is az úgynevezett készletező adatgyűjtésre, azaz hogy konkrét cél nélkül, egy esetleges későbbi felhasználásra szerezzék be és tárolják az információkat. Ezt a fajta hírszerzési módszert tárta a világ elé 2013-ban Edward Snowden.[11] Ennek következtében a jelentősebb tartalomszolgáltatók az ügyfelek bizalmának visszanyeréséhez igyekeztek elzárkózni a hatóságokkal való együttműködéstől és minél több adatvédelmi garanciát beépíteni a működési rendjükbe.

A neten folyamatosan gyarapodó információhalmaz azonban továbbra is létezik, ami ezáltal felértékelődött, és nagy része könnyedén elérhető maradt. Mint minden területen, a keresés és kutatás emberi képességeinek korlátait itt is kitágítják speciális programok, applikációk és keresőmotorok, amelyek képesek könyvtárnyi dokumentumot a megadott keresési szempontok szerint a másodperc törtrésze alatt szelektálni, átvizsgálni.

Régi dilemma, hogy vajon az internethasználók tisztában vannak-e azzal, mennyire válnak sebezhetővé egy-egy bejegyzéssel, posztolással, vagy hogy mennyi információ válik ezáltal mások számára is hozzáférhetővé. A biztonságos-tudatos internetezésre szerencsére már fiatalkorban megkezdődik az oktatás, és egyre inkább válnak közismertté ezek a kockázatok. Azonban vajon az interneten kutakodók – akár laikusokról, akár hivatásszerű alkalmazókról beszélünk – ismerik-e a korlátokat és veszélyeket, tisztában vannak-e a jogi keretekkel? Hol a határ az interneten szabadon fellelhető adatok összegyűjtése és a hírszerzés vagy a jogi terminológia szerinti titkos információgyűjtés között? Milyen digitális lábnyomok árulkodnak az érdeklődésünk középpontjáról, vagy akár a magáról a kutakodást végző személyről? Valóban annyira mély a *deep web,* és annyira sötét a *darknet?* Az alábbiakban ezeket a kérdéseket próbálom megvilágítani.

A jogi korlát

A nyílt forrású információgyűjtés, hírszerzés fogalma mellett a jogi szabályozása sem egyértelmű és nem egységes. Az egyik elfogadott nézet szerint, ami az interneten fellelhető, annak a felhasználása nem ütközik semmilyen korlátba. Ez valószínűleg igaz, ha az információ megszerzéséhez nincs szükség valamilyen rendszerbe történő, engedélyhez kötött belépésre vagy esetleg jelszó alkalmazására, azaz az internet felszínen látható részéről, a *surface webről* beszélünk. De mi a helyzet, amikor valamely információ, adat megismerése feltételekhez kötött?

Az OSINT-tevékenységgel összefüggésben meg kell különböztetni a minden feltétel nélkül, bárki által megismerhető adatok megszerzését – ezt szokás passzív eljárásnak nevezni –, míg a csoportosítás másik fele az úgynevezett aktív információgyűjtés

[11] Edward Snowden (1983–) az NSA és a CIA volt alkalmazottja, a tömeges megfigyeléseket 2013-ban leleplező cikkek forrása; utóbbi időben az informatikai biztonság kérdéskörében nyilatkozik meg.

és hírszerzés, amely már valamilyen kiegészítő mozzanatot, tevékenységet igényel. Ez utóbbi esetben már nemcsak szemlélője, megfigyelője a hírszerző az eseményeknek, hanem valamilyen szinten beavatkozik a folyamatokba, ráhatással bír azokra. Ez a beavatkozás sok esetben külön engedélyhez vagy jogosultsághoz kötött, amelynek hiányában általában jogellenes az adat megszerzése. Az engedély és jogosultság származhat az adat birtokosától vagy az adatot kezelő szervezettől, informatikai rendszer üzemeltetőjétől, de szigorú feltételek mellett felhatalmazást adhat rá törvény is, mint például a titkos információgyűjtés vagy a leplezett eszközök alkalmazásának esetében.

A hazai büntető törvénykönyv[12] (Btk.) a XLIII. fejezetében külön tárgyalja az informatikai rendszerek védelmét, illetve szankcionálja ezek megsértését. A 423. § szerint két évig terjedő szabadságvesztéssel büntetendő az, aki információs rendszerbe az annak védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad. Ugyancsak szabadságvesztéssel büntetendő többek között az is, aki ehhez jelszót, programot készít, forgalmaz, hozzáférhetővé tesz.

A 422. §-ban a személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerésének egyes elkövetési magatartásait szintén szabadságvesztéssel rendeli büntetni a Btk., így például az elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatok kifürkészését, és az észleltek technikai eszközzel történő rögzítését is.

A Btk. értelmezi is az információs rendszer fogalmát: a 459. § (1) bekezdésének 15. pontja szerint az az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

Azonban a jogi korlátok a passzív kutatás esetében is fennállhatnak, ha az elérhető tartalom megtekintése, megszerzése (letöltése) vagy birtoklása már önmagában is bűncselekmény. Ilyen például a Btk. 204. §-ban nevesített gyermekpornográfia körébe tartozó adat (például fénykép, videó), de egyes államokban a terrorizmushoz köthető információk, tartalmak is ebbe a kategóriába tartoznak. Legutóbb az Egyesült Királyság döntött úgy, hogy a 2019. évi Terrorizmus Elleni és Határvédelmi Törvény[13] szerint a terrorista propagandatartalmak megtekintése akár 15 évig terjedő szabadságvesztéssel lesz büntethető.

Amennyiben ezen tartalmak megtekintésére, indokolt letöltésére a nyomozó hatóság részéről az eljárási szabályok betartása mellett büntetőeljárásban kerül sor, nem merülhet fel a felelősségre vonás kérdése. De ha ezt konspiráltan, leplezetten kell végrehajtani, már nem ennyire egyértelmű a helyzet. Ekkor már felmerülhet fedett nyomozó igénybevételének és előzetes ügyészi engedély szükségességének a kérdése.

További érdekes kérdést feszegetett Gál István László egyetemi docens 2014-ben *Az OSINT (Open Source Intelligence), mint a kémkedés lehetséges elkövetési magatartása*[14] című szakmai cikkében. A levezetett gondolatmenete szerint a kémkedés elméleti

12 2012. évi C. törvény.

13 Counter-Terrorism and Border Security Act 2019. Elérhető: www.independent.co.uk/news/uk/home-news/terrorist-propaganda-law-thought-crime-click-link-online-prison-a8866061.html (A letöltés dátuma: 2019. 04. 29.)

14 Gál 2014.

lehetősége ugyan felmerülhet a nyílt forrásból megszerezhető adatok összegyűjtése és elemzése során, de annak társadalomra veszélyessége, illetve a bizonyíthatósága eléggé kérdéses marad. Gyakorlatban is reálisnak tűnő büntetőjogi felelősségre vonást a szerző csak olyan lebukott és tényleges kémtevékenységet folytató hírszerző esetén lát, akinél a minősített adatok átadása helyett csak azt lehetne bizonyítani, hogy rendszeres kapcsolattartás mellett egy idegen szervezet részére folyamatosan adott át nyílt forrásból származó, de általa megszűrt, elemzett információkat.

A megismert adatok további felhasználása is felvethet jogi kérdéseket. A közösségi médiából kinyert fényképekkel, adatokkal érintett egyén személyiségi jogai vagy a szerzői jogok védelme sem hagyható figyelmen kívül. Ez még akkor is igaz, ha a közösségi oldalon posztoló saját döntése alapján osztja meg adatait, képeit.

Akár aktív, akár passzív információszerzés végrehajtására kerül sor, a számítógépet használónak pontosan kell ismernie azokat a határokat, amelyek átlépése büntetőjogi felelősségre vonást eredményezhet. És ezeket a határokat meg kell tartani még akkor is, ha informatikai ismereteiben bízva biztos abban, hogy őt lehetetlen azonosítani.

A megbízhatósági korlát, az ellenőrzés igénye

A nyílt forrású információgyűjtés egyik legnagyobb hátránya, hogy nem tekinthető megbízható, ellenőrzött forrásnak. Ennek okai többrétűek. Egyrészt az adatokat elhelyezőket nem kötelezi semmiféle szabály a hitelességre. Elég csak arra gondolni, hogy a közösségi oldalak profiljain mennyi negatív tulajdonság található. Valóban ennyire makulátlanok a felhasználók, vagy – finoman fogalmazva – csak szűrten tájékoztatják egyéniségükről a többieket? A fiktív identitások, a valótlan életutak és állítások nem meglepők a világhálón. Ugyancsak nem biztos, hogy egy-egy fénykép tényleg ott készült, ahol állítják, és még hosszan folytatható a bizonytalanságok sora. A digitális és a virtuális identitások gyorsan cserélhetők és szinte ellenőrizhetetlenek.

A digitális személyazonosság – amit egy-egy közösségi oldalon vagy más fórumoknál alkalmazunk – egy tudatosan felépített információhalmaz (adatok, fényképek, vélemények), amely alapján az online világban egy képet tudnak rólunk alkotni. A valóságos, fizikai profilunkkal szemben azonban ennek megváltoztatása vagy törlése csak pillanatok műve. Igaz, a profillal végzett tevékenységek nagy része a törléstől függetlenül hagy maga után nyomokat, amelyek a hozzáértők számára észlelhetők lesznek később is.

A virtuális identitás, az *avatár* már egy játékfelületre célzatosan létrehozott személyiség, amelyben már a valóság látszatát sem kell kelteni.

Mindkét esetben megnyílik annak a lehetősége, hogy egy képzelt, fiktív személyiség mögé rejtőzve tegyünk meg olyan dolgokat, amiket a valóságos világban nem tudunk vagy nem merünk.

A bizonytalanság másik fő tényezője az időbeliség. A fellelhető adatok valóságtartalma mellett fontos bizonytalansági tényező a valós információk aktualitása is. Sokan kevésbé rossznak gondolják, ha valami olyat állítanak, ami valamikor igaz volt, függetlenül attól, hogy már nem az. Ilyen például a jól fizető munkahelyek megjelölése, a divatos hobbik (például golfozás, repülés, vadászat, vitorlázás) vagy akár a drága környéken bérelt korábbi lakás megjelölése.

Ezek mellett – mivel az internet nem selejtez – nagyon fontos az információ értékelése során a letöltés, hozzáférés dátumát, illetve a keletkezés és feltöltés időpontját is figyelni, ellenőrizni, ami sok téves megállapítástól és felesleges munkától óvhat meg.

A tudatos félrevezetés mellett a felületes vagy el nem végzett ellenőrzés is eredményezhet súlyos hibákat. Erre volt jellemző példa a 2015-ös bostoni terrorcselekménnyel kapcsolatos sajtóhiba. 2015. április 15-én a Bostonban megrendezett maratoni futás befutójánál két, szemeteskukákba rejtett pokolgéppel megöltek 3 embert, és közel 150 személyt megsebesítettek a később azonosított, csecsen származású Carnajev testvérek. Az egyik legnagyobb tévétársaság, a CNN már nem sokkal a merényletet követően a Twitterből kinyert adatok felületes feldolgozása után hírül adta, hogy az elkövető színes bőrű, és a letartóztatásáról is beszámolt. Később ez valótlannak bizonyult, és a csatorna magyarázkodásra kényszerült.[15] Ez a baklövés mind a tévétársaság elismertségét és hitelességét, mind pedig a nyílt forrású hírszerzés megbecsülését visszavetette.

A fenti bizonytalanságok ellenére a megszerezhető információk nagyban tudnak segíteni; lehetőséget adnak az ellenőrzésre, azok megerősítésére vagy cáfolatára, irányt mutatva ezzel az elemzőnek és hírszerzőnek. Az egyik legnagyobb hiba, ha a nyílt forrású kutatás során beszerzett adatokat mindenféle értékelés, ellenőrzés nélkül tényként fogadjuk el.

Az időbeli korlát, a felejtés jogának kérdése

Az informatikai fejlődés egyik melléktermékeként az az adathalmaz, amely évről évre gyűlik a szerverek memóriájában. Egy kitöltött adatlap, egy munkahelyi önéletrajz, egy kiposztolt esemény évek után is elérhető. Már a volt barátnővel készült és a közösségi oldalra kiposztolt nyaralási fotó is kellemetlen perceket okozhat egy új kapcsolatban, nem beszélve a korábbi munkahelynek megadott bizalmas adatokról. Az aktuális hírekben szereplő személyek és események az idő múlásával már érdektelenné válhatnak, a róluk szóló híradások azonban továbbra is elérhetők maradnak. Az évekkel ezelőtti állapotok elérhetősége sokak szerint alapvető jogokat sért, de az információs rendszerek halmazában szinte lehetetlen selejtezni.

Az áttörést az Európai Unióban Mario Costeja González spanyol állampolgár 2010-ben benyújtott panasza jelentette. Ebben azt sérelmezte, hogy a Google keresőmotorja a nevére indított lekérdezés eredményeként a *La Vanguardia* nevű, nagy példányszámú spanyol újság többéves közleményét is feladta találatként, amelyben az akkori társadalombiztosítási tartozás miatt elárverezett házával kapcsolatban nevesítették őt. A több fórumot megjárt bírósági perben végül az Európai Bíróság kimondta,[16] hogy a magánszemélyek jogosultak név alapján a Google-hoz hasonló keresőmotoroktól a lekérdezésekre kapott találatok eltávolítását kérni.

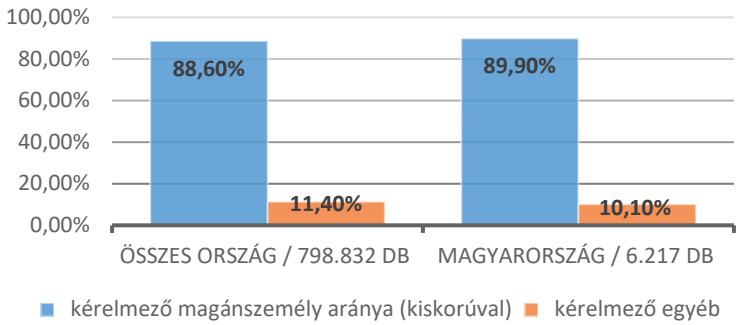
[15] Brogen 2015.

[16] Európai Bíróság C-131/12. számú ítélete. Elérhető: http://curia.europa.eu/juris/liste.jsf?num=C-131/12&language=HU (A letöltés dátuma: 2019. 04. 29.)

A keresőmotornak eleget kell tennie ennek akkor, ha a kérdéses linkek „nem megfelelők, nem vagy már nem relevánsak, illetve túlzók". Az eltávolításhoz a keresőmotor üzemeltetője jogosult figyelembe venni a kérelmező személy esetleges közéleti szerepét is.

A Google már az ítélet hatálybalépése előtt megkezdte a kérelmek befogadását, amelyek teljesítését és elutasítását folyamatosan közzéteszi.[17] Ezekből megállapíthatók a beérkezett kérelmek statisztikai adatai (összesítve, illetve országokra bontva), így többek között az összes kérelem száma, a kérelmezők jellege (magánszemély, egyéb személy), az eltávolításra kérelmezett URL-ek[18] száma, illetve a kérelmek elintézési módja (teljesítve vagy elutasítva).

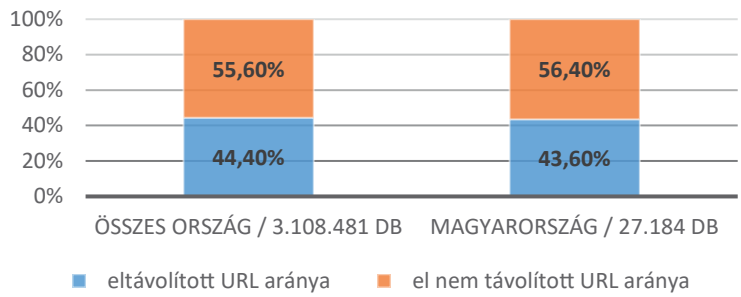
A 2014. május 28. és 2019. április 29. közötti időszak adatait az alábbi diagramok ábrázolják:



1. ábra

A beérkezett kérelmek eloszlása

Forrás: transparencyreport.google.com



2. ábra

Az eltávolításra kérelmezett URL-ek elintézési módja

Forrás: transparencyreport.google.com

[17] Elérhető: https://transparencyreport.google.com/eu-privacy/overview 2014. 05. 28. – 2019. 04. 29. közötti adatok. (A letöltés dátuma: 2019. 04. 29.)

[18] Uniform Resource Locator – Egységes Erőforráshely.

A statisztikai adatok szerint Magyarországon a kérelmeket benyújtók megoszlási aránya, illetve a kérelmezett intézkedések teljesítésének aránya megegyezik az összesített adatokkal.

A fentiekben említett ítélet, illetve az időközben hatályba lépett GDPR[19] hatására várhatóan az interneten egyre szűkül majd a korlátlan ideig fellelhető adatok, információk köre. Ez a tény szűkíti majd a nyílt forrású hírszerzés, kutatás forrásbázisát, de nem feltétlenül jelenti a hatékonyság csökkenését.

Biztonsági korlátok, a digitális lábnyomok veszélyei

Az általánosan elfogadott meghatározás szerint a digitális lábnyom fogalma azokra a jelekre, nyomokra vonatkozik, amelyek a felhasználó online jelenléte után maradnak, és amelyekből következtetni lehet a tevékenységére. Minden aktivitásunk, és sokszor a passzív jelenlétünk és megfigyelésünk is kitörölhetetlen nyomot hagy az informatikai rendszerekben.

Ebből adódóan a nyílt forrású kutatás kétélű fegyver is lehet. Hiszen ha a kutatás célszemélye kellő szakértelemmel és megfelelő technikai eszközökkel rendelkezik, úgy könnyen azonosíthatja az utána érdeklődőket. A kereséshez, kutatáshoz használt keresőszavak vagy az alkalmazott informatikai eszköz és hálózat azonosítói (mint például az IP-cím vagy -tartomány, a DNS,[20] a domain vagy nickname, mobileszközök IMEI-száma) könnyen elárulhatják az érdeklődőt. Sok esetben ez természetesen nem jelent konkrét dekonspirációs veszélyt, de adott körülmények között már maga az érdeklődés tényének felismerése, az érdeklődő szervezet azonosítása, esetleg a nagyobb számú vagy huzamosabb időn át tartó lekérdezések elemzése értékes információkkal szolgálhat a célszemélyi kör számára.

Ezt minden körülmények között mérlegelni kell, és szükség esetén meg kell teremteni a fedésnek, a lekérdezések leplezésének technikai feltételeit a biztonságos kutatáshoz.

A szakértelem hiányának korlátai, a végrehajtás központosításának kérdése

Szintén régi dilemma, hogy vajon a nyílt forrású információszerzést központosítva, egy erre kijelölt olyan speciális szervezetnek kell-e végrehajtani, ahol mind a technikai feltétel és a humán szakértelem jelen van, avagy minden ilyen irányú igényt ki lehet elégíteni a tényleges felhasználás szintjén. Mivel mindkét álláspont mellett és ellen is lehet érveket felsorakoztatni, az igazság szerintem valahol a két szélsőséges vélemény között van.

[19] General Data Protection Rules – Általános Adatvédelmi Szabályzat; az Európai Parlament és a Tanács (EU) 2016/679 számú, 2018. május 25-én hatályba lépett adatvédelmi rendelete.

[20] Domain Name System – az internetes tartománynevek rendszere.

Nem lehet azt elvárni, hogy egy egyszerű háttérelemzéshez minden olyan adatot, amely az interneten vagy más nyílt forrásból fellelhető, egy másik szervezettől kelljen megkérni. Sok kérdés egy egyszerű Google kereséssel megválaszolható, de az összetettebb kérdésekre is könnyen gyűjthet le adatokat egy rövid képzésen átesett felhasználó.

Ugyanakkor az a mélységű keresés, kutatás és információgyűjtés, amely már speciális programokat és kellő rutint igényel, nem várható el olyan felhasználótól, aki csak ritkán és korlátozott technikai feltételekkel felvértezve kényszerül erre. Különösen igaz ez akkor, ha már az információszerzés tényét is leplezni szeretnénk. Sem a szervezett kiberbűnözésben érintett célszemély, sem egy kiképzett hírszerző ellenőrzése, kapcsolatrendszerének felkutatása nem végezhető el biztonságosan megfelelő fedés, speciális képzettség, hardverek és szoftverek nélkül.

Ez a kérdés az USA hírszerző közösségében is hangsúlyos. Az OSINT-ot egy kicsit szakmán kívülinek érzik. Ezen elterjedt – álláspontom szerint tévedésen alapuló – előítélet egyik magyarázata, hogy a titkosszolgálatok fő feladata a titkok felkutatása, amihez kevésbé illenek a mindenki által hozzáférhető, nyílt adatok. Míg a többi *-INT* (például HUMINT,[21] SIGINT,[22] GEOINT[23]) identitását és szakmaiságát a rendelkezésükre álló specialisták jelentik, addig az OSINT-hoz mindenki ért egy kicsit.

Az USA 2004. hírszerzési törvénye[24] már választás elé állította a DNI-t[25] abban a kérdésben, hogy szükségesnek tartja-e egy központosított speciális egység felállítását. A WMD Bizottság[26] a CIA-n belül javasolta egy Open Source Center[27] (OSC) létrehozását, amely javaslat végrehajtását az USA elnöke szintén a DNI-ra delegálta. Végül a DNI egy CIA-irodát, a Foreign Broadcast Information Service-t[28] (FBIS) nevezett ki OSC-nek, míg irányító végrehajtója a CIA lett.

2015-ben az OSC-ből Open Sourche Enterprise[29] (OSE) lett, és a részleges függetlenségét elveszítve a CIA újonnan létrehozott *Directorate of Digital Innovation*[30] (DDI) alá integrálták be. Az elképzelések szerint az OSE lehetőséget biztosítana a szakértők képzésére, fejlesztésekre, amelyek nélkül az OSINT nem tudna lépést tartani a kihívásokkal. A szakemberek véleménye szerint az OSINT önálló hírszerzési elismertsége most a DDI kezében van, és kérdés, hogy a korábbi előítéleteket mennyire lesz képes kioltani.[31]

Hazánkban is 2015-ben merült fel először a nyílt forrású kutatással, hírszerzéssel foglalkozó speciális egység felállításának igénye. A terrorizmus jelentette fenyegetés hatására először a Szervezett Bűnözés Elleni Központ (SZBKK) keretében osztály

21 Human intelligence – humán (élőerős) hírszerzés.
22 Signals intelligence – jelhírszerzés.
23 Geospatial intelligence – térinformatikai hírszerzés.
24 IRTPA of 2004: Intelligence Reform and Terrorism Prevention Act of 2004 – Hírszerzési reform és a terrorizmusmegelőzési törvény.
25 Director of National Intelligence – nemzeti hírszerzési igazgató.
26 Weapons of Mass Destruction; 2005-ben felállított bizottság az USA tömegpusztító fegyvereket érintő hírszerzési lehetőségeiről.
27 Nyílt Forrású Központ.
28 Külföldi Hírközlési Információs Szolgálat.
29 Nyílt Forrású Vállalkozás.
30 Digitális Innovációs Igazgatóság.
31 Lowenthal 2017, 181.

jogállással kezdett működni, majd a jogutódként 2016 júliusában életre hívott Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK) szervezetéhez került, ahol később főosztállyá bővült. Az Nbtv. alapján a TIBEK „nyílt információgyűjtést és feldolgozást végző szolgáltató és támogató szervet működtet".[32] Ugyan az Nbtv. szerint az egység feladata szolgáltatás nyújtása, de az jól érzékelhető Magyarországon is, hogy az összes igényt nem képes egy szakegység kielégíteni, nélkülözhetetlen a közvetlen végrehajtók általi nyílt forrású kutatás és hírszerzés.

A kutatható terület korlátai, a darknet kérdése

Az Europol évente elkészülő, a szervezett bűnözés aktuális helyzetét értékelő jelentésében[33] kiemelt hangsúlyt fektet a kiberbűnözés veszélyeire és kihívásaira. Ezek között is elsődleges helyen szerepel a darkneten elérhető illegális áruk és szolgáltatások kereskedelme (lőfegyver, kábítószer, új típusú pszichoaktív anyagok), de emellett az illegális fizetési műveletek (kriptovaluták használata, terrorizmus finanszírozása, pénzmosás) is előkelő helyet foglalnak el a veszélyeztetettségi skálán.

Először is kicsit pontosítani kell magát deep web és a darknet fogalmát. Abban megyezenek, hogy egyik területét sem képesek a hagyományos keresőmotorok (például Google, Bing, Yahoo!) keresni. A deep web legális és jellemzően legális tevékenységre használatos, míg a darknet megalkotásának a célja is az illegális kereskedelem, tevékenység leplezése volt.

Egyes becslések szerint a deep web terjedelme mintegy ötszázszorosa a felszíni (nyílt, mindenki által látható) felületnek, azaz a surface webnek. Ebbe beletartoznak többek között a regisztrációhoz kötött fiókok, levelezőrendszerek, netbankos oldalak, szakmai vagy tudományos portálok, de akár a személyes adatokat is tartalmazó felületek is.

A darknet – amelynek terjedelmére becslések sem születtek – használatához már speciális böngészők szükségesek, és az ott található oldalak sem a hagyományos elnevezésekkel, azaz URL-ekkel rendelkeznek. A legismertebb böngészők a TOR,[34] az I2P és a Freenet, amelyek alkalmazása gyakorlatilag ellehetetleníti mind a felhasználó, mind a felkeresett oldal azonosítását.[35]

A darknet egyik legismertebb kereskedőfelülete a 2011-ben létrejött Silk Road (Selyemút) volt a 2013-ban történt felszámolásáig. Egy 2013-ban készült tanulmány[36] szerint a Silk Roadon keresztül értékesített kábítószer értéke az USA-ban megközelítőleg 23 millió dollár volt évente, míg az egész éves kábítószer-forgalom becsült éves mértéke 300 milliárd dollár. Ez ugyan nem tűnt nagymértékű részesedésnek, de a bitcoin és az illegális piactér kombinálása dinamikus fejlődést prognosztizált.

32 Nbtv. 8/A. § (3) bekezdés d) pont.
33 SOCTA: Serious and Organised Crime Threat Assessment – súlyos és szervezett bűnözés fenyegetettségi értékelés.
34 The Onion Router – Hagyma Elosztó.
35 Ciancaglini et al. 2013.
36 Martin 2014, 351–367.

A felfelé ívelő karriernek az FBI[37] 2013. októberi akciója vetett véget. Eljárás alá vonták az üzemeltetéssel vádolt *Dread Pirate Roberts* néven ismert Ross Ulbrichtot, akit 2015-ben többek között pénzmosásért, szervezett bűnözésben való részvételért és kábítószer-kereskedelemért első fokon kétszeres életfogytig tartó szabadságvesztésre ítéltek. 2017 júniusában az ítélet elleni fellebbezését elutasította San Franciscóban a Másodfokú Fellebbviteli Bíróság, így reálisan élete végéig börtönben marad a most 35 éves férfi.

Hasonló forgalmú, közismert darknetes kereskedőfelület volt a 2017 júliusában szinte egyidőben felszámolt *Hansa* és az *AlphaBay*, míg 2019. május elején Németországban szüntették be a *Wall Street Market* nevű, hasonlóan aktív portált az azt üzemeltető három személy elfogásával együtt.

Hiú ábránd lenne azt gondolni, hogy ezekkel az intézkedésekkel megszűnt a darknet illegális kereskedelme. Az illegális árukra – különösen a kábítószerre – az igények nem csökkenek, így a folyamatos megújulás sem maradhatott el. 2013. novemberétől 2014. márciusáig a Silk Road 2.0-n lehetett kábítószert vásárolni,[38] majd 2017 májusában már a Silk Road 3.0 elindulásáról adtak hírt,[39] de aktuálisan a Silk Road 3.1 érhető el. Az egyszerű kereséssel könnyen megtalálhatók az internet nyílt felületén üzemelő azon honlapok, ahol az aktuális kereskedőfelületek hirdetik. Ilyen például a *darkwebnews.com/dark-web-market-list* is, amelyen a piactér aktuális állapota (online/offline), illetve az egyes marketek eléréséhez szükséges információk is megtalálhatók.

Az extraprofit, az illegális áruk és szolgáltatások iránti kereslet és a kriptovaluták elterjedése biztosítja a folytonosságot, amellyel szemben az egyik fellépési lehetőség lehet a nyílt forrású hírszerzés.

Összegzés

Ugyan megbecsülhetetlen mennyiségű értékes információ található olyan tárgyiasult adathordozókon, mint a könyvek vagy újságok, azonban a mai világban a nyílt forrású hírszerzés legnagyobb forrása a digitális alapú világháló. Ennek alkalmazása azonban sok esetben olyan korlátot állít a felhasználók elé, amelyek ismeretének vagy betartásának hiánya téves vagy jogszerűen fel nem használható adatokat eredményez.

Ennek elkerülése, megelőzése érdekében szükséges lenne a nyílt forrású információgyűjtést végrehajtók számára szervezett oktatást – a módszertan, a gyakorlati fogások, illetve az informatikai rendszerek és eszközök alkalmazási ismeretei mellett – a kockázati tényezőkre és korlátokra is kiterjeszteni.

[37] Federal Bureau of Investigation – Szövetségi Nyomozó Iroda (USA).
[38] Osborne 2019.
[39] Richard 2017.

Alkalmazott rövidítések

- Btk.: a Büntető Törvénykönyvről szóló 2012. évi C. törvény
- CIA: Central Intelligence Agency – Központi Hírszerző Ügynökség (USA)
- DDI: Directorate of Digital Innovation – Digitális Innovációs Igazgatóság (CIA)
- DNI: Director of National Intelligence – nemzeti hírszerzési igazgató (USA)
- FBI: Federal Bureau of Investigation – Szövetségi Nyomozó Iroda (USA)
- GDPR: General Data Protection Rules – Általános Adatvédelmi Szabályzat; az Európai Parlament és a Tanács (EU) 2016/679 számú, 2018. május 25-én hatályba lépett adatvédelmi rendelete
- GEOINT: Geospatial intelligence – térinformatikai hírszerzés
- HUMINT: Human intelligence – humán (élőerős) hírszerzés
- IRTPA: Intelligence Reform and Terrorism Prevention Act of 2004 – Hírszerzési reform és terrorizmusmegelőzési törvény (USA)
- Nbtv.: a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
- NSA: National Security Agency – Nemzetbiztonsági Ügynökség (USA)
- OSC: Open Source Center – Nyílt Forrású Központ (USA)
- OSE: Open Source Enterprise – Nyílt Forrású Vállalkozás (USA)
- OSINT: Open Intelligence – nyílt forrású hírszerzés
- SIGINT: Signals Intelligence – jelhírszerzés
- SOCTA: Serious and Organised Crime Threat Assessment – súlyos és szervezett bűnözés fenyegetettségi értékelés
- SZBKK: Szervezett Bűnözés Elleni Koordinációs Központ
- TIBEK: Terrorelhárítási Információs és Bűnügyi Elemző Központ
- WMD: Weapons of Mass Destruction – tömegpusztító fegyverek

Felhasznált irodalom

Brogen, Mary Kate (2015): How Twitter is Changing Narrative Storytelling: A Case Study of the Boston Marathon Bombings. *Elon Journal of Undergraduate Research in Communications,* Vol. 6, No. 1. Elérhető: www.inquiriesjournal.com/articles/1135/how-twitter-is-changing-narrative-storytelling-a-case-study-of-the-boston-marathon-bombings (A letöltés dátuma: 2019. 05. 04.)

Gál István László (2014): Az OSINT (Open Source Intelligence) mint a kémkedés lehetséges elkövetési magatartása. *JURA,* 20. évf. 1. sz. 51–55. Elérhető: https://jura.ajk.pte.hu/JURA_2014_1.pdf (A letöltés dátuma: 2019. 04. 29.)

Harari, Yuval Noah (2015): *Sapiens: A Brief History of Humankind.* New York, Harper.

Lévay Gábor (2006): *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Egyetemi jegyzet. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

Lowenthal, Mark L. (2017): *Hírszerzés. A titoktól a politikai döntésig.* Budapest, Antal József Tudásközpont.

Martin, James (2014): Lost on the Silk Road: online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice,* Vol. 14, No. 3. 351–367. DOI: https://doi.org/10.1177/1748895813505234

Jogforrások

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
2012. évi C. törvény a Büntető Törvénykönyvről
Counter-Terrorism and Border Security Act 2019. Elérhető: www.independent.co.uk/news/uk/home-news/terrorist-propaganda-law-thought-crime-click-link-online-prison-a8866061.html (A letöltés dátuma: 2019. 04. 29.)
Európai Bíróság C-131/12. számú ítélete. Elérhető: http://curia.europa.eu/juris/liste.jsf?num=C-131/12&language=HU (A letöltés dátuma: 2019. 04. 29.)
IRTPA of 2004: Intelligence Reform and Terrorism Prevention Act of 2004

Internetes források

Ciancaglini, Vincenzo – Balduzzi, Marco – Goncharov, Max – McArdle, Robert (2013): *Deepweb and Cybercrime. It's Not All About TOR.* Elérhető: www.trendmicro.ie/media/wp/deepweb-and-cybercrime-whitepaper-en.pdf (A letöltés dátuma: 2019. 05. 05.)
Osborne, Charlie (2019): *Failed student jailed for Silk Road, dark web drug profiteering.* Elérhető: www.zdnet.com/article/failed-student-jailed-for-silk-road-dark-web-drug-profiteering/ (A letöltés dátuma: 2019. 05. 05.)
Richard (2017): *Silk Road 3.0 Back From The Dead.* Elérhető: https://darkwebnews.com/darknet-markets/silkroad-3-back/ (A letöltés dátuma: 2019. 05. 05.)
Monnappa, Avantika (2019): *Data Science vs. Big Data vs. Data Analytics.* Elérhető: www.simplilearn.com/data-science-vs-big-data-vs-data-analytics-article (A letöltés dátuma: 2019. 01. 19.)
https://transparencyreport.google.com/eu-privacy/overview (A letöltés dátuma: 2019. 04. 29.)

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 32–37. • DOI: 10.32561/nsz.2019.2.3

Regényi Kund Miklós[1]

OSINT a második generációs internetet megelőző korokban

OSINT Prior to the Second Generation WorldWideWeb

A cikk az OSINT kezdeteit és fejlődését mutatja be. A modern titkosszolgálatok megjelenésekor az OSINT, ha még nem is így nevezték, egyenrangú volt a többi felderítési móddal, és döntően az értékelő-elemző munkában használták. Már korán az OSINT-munka részévé vált a térképek figyelemmel kísérése, és a különböző névjegyzékek révén lehetőség nyílott a személyre vonatkozó OSINT alkalmazására. Már ekkor fontos volt az OSINT-termékek és -források tárolása és visszakeresése. A titkos felderítés differenciálódásával önálló OSINT-termékek is megjelentek. Az OSINT fontos műfajának volt tekinthető a sajtótükör, amely aránylag könnyen továbbfejleszthető volt IT-alapú médiatükörré.

Kulcsszavak: OSINT, jelentésmódosulás, 19. és 20. század, értékelő-elemző munka, összforrású elemzés, titkos felderítési módok, hibrid, nyílt forrású jelentések, személyekre vonatkozó OSINT kezdetei, sajtószemle, médiaszemle

The study presents the beginning and the development of open source intelligence. When modern intelligence services were born, the OSINT – although without a specific name – was second to none of other intelligence gathering methods and was primarly used in the analysis and reporting work. Focusing on maps was an early phenomenon, too. Different personal registers soon enabled the person-focused OSINT. OSINT sources and products were archivated and searched regularly. With the differentiation of secret intelligence, only alonestanding OSINT products appeared. Press mirrors can be considered an important OSINT genre, which could be easily developed to IT based media mirror.

Keywords: modifications of the OSINT notion, OSINT during the 19th and 20th centuries, OSINT as a part of analysis and reporting, all-source analysis, hybrids of OSINT and other secret intelligence gathering methods, open source analysis, the beginning of the person-focused OSINT, press mirror, media mirror

[1] Dr. Regényi Kund Miklós egyetemi adjunktus, Nemzeti Közszolgálati Egyetem. ORCID-azonosító: 0000-0003-1833-9523.

Napjainkban, a 21. század második-harmadik évtizedének fordulóján a nyílt forrású információgyűjtés, azaz az OSINT (Open Source INTelligence) egyfajta jelentésmódosuláson, jelentésszűkülésen megy keresztül, hiszen a kinyerhető információk mennyiségével és minőségével összhangban az internetes, ezen belül is a szociális média kerül előtérbe fogalmi szempontból éppúgy, mint az információszerzés súlypontját tekintve. (Ezt a jelentésmódosulást, jelentésszűkülést tükrözik a WEBINT – WEB INTelligence, illetve SOCINT – SOCial INTelligence szakkifejezések is.)

A mai értelemben vett állambiztonsági szervezetek megjelenésének idején, a 19. század közepe táján a nyílt forrású információgyűjtés másfajta többletjelentéssel ruházható fel. Akkor a mai értelemben vett OSINT terepe a bárki számára korlátozások nélkül hozzáférhető, általában nyomdai, ritkábban kéziratos kiadványok voltak, ideértve a könyveket, periodikákat, folyóiratokat, de az atlaszokat és térképeket is. A kinyerhető információk szövegekből származtak, maguk is zömükben szövegszerűek voltak, jelentősen megkönnyítve a felhasználó dolgát.

A médiumok, a korban elsősorban a nyomtatott sajtótermékek információszerzés terén betöltött kiemelkedő jelentőségével a kortársak is tisztában voltak. Jól tükrözi ezt a helyzetet az a Lord Palmerston brit miniszterelnöknek tulajdonított mondás, miszerint: „Nincs szükségünk kémekre. Olvassuk a Timest."

A korabeli osztrák–magyar szabályzat[2] tanulmányozásával az OSINT további sajátosságai is azonosíthatók. A kor szakemberei tisztában voltak a források kiválasztásának fontosságával: a szervezet céljait elősegítő, magas színvonalú szakmai folyóiratok, napi- és hetilapok, könyvek, de térképek, név- és címtárak azonosítása és beszerzése is mind a központ, mind a célországokban működő katonai attasék feladata volt. Az ellenérdekelt országokból a sajtótermékek beszerzése semleges országokba bejegyzett fedőcímekre történt. Ebbe a folyamatba nemcsak a szervezet vagy az ország hivatásos állományú munkatársai, de egyes kémügynökök is bekapcsolódtak.

A névtárak, az úgynevezett sematizmusok már lehetővé tették a nyílt forrású információk személyre vonatkozó, tehát az úgynevezett műveleti munkához kapcsolódó felhasználását, hiszen például egy csendőrségi évkönyv[3] részletesen tartalmazta egy adott csendőrtiszt szolgálatát érintő részleteket, így egy esetleges leplezett megközelítéshez éppúgy támaszt adhatott, mint egy titkosszolgálati fedés megerősítéséhez vagy cáfolatához.

A nyílt forrású információk felhasználása terén az a gyakorlat azonosítható, miszerint az információ minősége, nem pedig forrása volt a meghatározó. Ennek megfelelően a nyílt forrású ismeretek és a mai terminológia szerinti műveleti ismeretek a jelentő munkában, a hírigények kielégítése érdekében együtt, egymást kiegészítve szerepeltek. (Ezt a gyakorlatot nevezzük korszerű kifejezéssel all-source analysisnek.) A nyílt forrású ismereteket természetesen a felderítő utazásokra való felkészülés során is hasznosították. A nyílt forrású ismereteket felhasználták a sajátos szempontú adattárakba való bedolgozás során is. Ez a tudáskincs a kémügynököktől származó

[2] Boda–Parádi–Regényi 2014, 113., 115.; Regényi 2014, 51–68., 55.
[3] *A magyar csendőrség zsebkönyve* (1905).

ismeretek minőségének, ezzel ellenértékének meghatározásakor, a kémügynökök részére kiszabásra kerülő feladatok megfogalmazásakor is jelentős szerepet játszott.[4]

Ezzel megadtuk azt a szervezeti elemet is, amely az OSINT-információkat felhasználta: ez a mai terminológiával értékelő-elemző-nyilvántartó részleg volt, amely a nyugat-európai modellben egyben az állambiztonsági szervezet időben legelső elemét, azaz gyökerét és eredetét is képezte.

Az OSINT-információk tárolását vizsgálva az irattárat és a könyvtárat említhetjük. A máig megtalálható gyakorlat ismeretében kijelenthető, hogy a tematikus keresés elősegítésére – a kor nyilvános könyvtáraihoz hasonlóan – cédulakatalógus állt rendelkezésre.

Az OSINT információs munkától eltérő hasznosulására is találunk korai példákat: az első világháborúban az ellenségnek okozott veszteséget tudták meghatározni a sajtóban megjelent veszteséglisták összesítésével – még úgy is, hogy központi veszteséglista közzétételére, épp információvédelmi okokból, nem került sor.

A második világháború alatt az OSINT-ot érintő egyik legszembetűnőbb mozzanat, hogy a vezetői tájékoztatásban felhasználták az ellenérdekelt vagy a szövetséges féltől származó filmhíradókat, illetve – akkor még csak kevesek kiváltságaként – friss játékfilmeket is. A visszaemlékezések tanúsága szerint gyakorlatilag valamennyi hadviselő fél legfelső vezetése élt az előbbiekben vázolt lehetőséggel.[5]

A hadműveletek pedig felértékelték a csapatok mozgásának nélkülözhetetlen segédeszközét, a térképet. Ezen a téren elsősorban a francia Michelin cég[6] autóstérképei érdemelnek említést, amelyek nélkülözhetetlen segítséget nyújtottak a brit és amerikai gépesített csapatok észak-afrikai, itáliai és franciaországi előrenyomulása során. Az ismeretlen, távoli országokba átcsoportosított katonák (diplomaták, titkosügynökök) számára pedig a beilleszkedést és a mindennapokat könnyítették meg a célországról szóló útikönyvek, illetve az ezek alapján készült tájékoztatók.

A sajtóval és a rádióval kapcsolatos, de álláspontom szerint nem tartozik az OSINT kérdésköréhez azok felhasználása személytelen kapcsolattartásra. Erre az esetre legismertebb példa, amikor a francia ellenállást a BBC-ben sugárzott kódmondatokkal tájékoztatták a normandiai partraszállásról, illetve adtak utasítást az ezzel összefüggő, előre egyeztetett szabotázsakciók végrehajtására. Hasonló, de személyhez, azaz akár titkos kapcsolathoz is szóló közlésre adtak lehetőséget a nagy napilapok apróhirdetései is.

Az állambiztonsági szervezetrendszer a második világháború alatt, illetve után jelentős mennyiségi fejlődésen ment keresztül, és az általános technikai fejlődés következtében bővült a rendelkezésre álló információszerző eszközök köre is. Ez a fejlődés az OSINT súlyát, jelentőségét nem vonta kétségbe, erre legismertebb példa az egyik OSS-, illetve CIA-vezetőnek, Alan Dullesnek tulajdonított és gyakran parafrazált állítás, miszerint a hírszerző információk meghatározó része, 80-90%-a nyílt forrásokból származik.

---

4 Lásd például: Haraszti–Kovács–Szita 2007.

5 A visszaemlékezések közül ehelyütt kettőt emelünk ki: Meacham 2018; Radzinszkij 2015–2016.

6 Ma lásd: www.viamichelin.com (A letöltés dátuma: 2019. 04. 01.)

A szervezeti differenciálódás, illetve a technikai fejlődés hatása az OSINT terén abban ragadható meg, hogy a nyílt forrású információkat már nemcsak a minősített forrásból származókkal mintegy összekeverve használták fel, hanem mind az állambiztonság, mind a magánbiztonság keretei között megjelennek a kizárólag nyílt forrásból származó válogatások, amelyek általában rendszeres időközönként jelentek meg. Előbbire a legismertebb példa a CIA úgynevezett *Factbookjai,* illetve országjelentései. Utóbbira pedig példaként az eredetileg hadihajók azonosítására szóló gyűjtemény kiadója, a fogalommá váló brit Jane's különböző, egyre differenciáltabb tematikus kiadványait említhetjük. Mindkettő[7] napjainkban is létezik – az interneten is, sőt, egyre inkább csak ott.

A következő elterjedt OSINT-műfaj a sajtóválogatás volt. Ez szintén a vezetői tájékoztatás egy formája, abból az érthető törekvésből származik, hogy a vezető, akinek ideje drága, képben legyen a szervezettel vagy egy témával kapcsolatos aktuális hírekkel, de ne kelljen valamennyi, ezzel kapcsolatos releváns kiadványt személyesen végigolvasnia.

A sajtóválogatás műfaja természetesen feltételezi a szemlézett sajtótermékek körének gondos kiválasztását, illetve a kiválasztás folyamatosan, de legalább meghatározott időközönként történő felülvizsgálatát, korszerűsítését is. A sajtóválogatás elkészítése maga pedig egy jól strukturálható, bizonyos időközönként, általában naponként ismétlődő folyamat, amely kiterjed a sajtótermékek beszerzésére, az egyes cikkek és tanulmányok, gyakran hírügynökségi hírek kiválasztására, a válogatás összeállítására, sokszorosítására és a felhasználókhoz való eljuttatására. A naponként végrehajtott munkafolyamatot előkészíti a kiválasztás szempontrendszerének kidolgozása és a végrehajtók erre vonatkozó felkészítése. A folyamat végén indokolt a sajtóválogatás kutatható formában, irattári vagy könyvtári rendben való archiválása is.

A sajtóválogatás nagyon jól használható egy nemzetbiztonsági szolgálat pozitív imázsának kialakítására és erősítésére. Tekintettel arra, hogy nyílt forrású anyagokból építkezik, a sajtóválogatás nem árulkodik titkosszolgálati eszközök és módszerek alkalmazásáról. Magát a készterméket sem kell minősíteni, sem pedig a titkos ügyiratkezelés szabályai szerint továbbítani, tárolni és kezelni. A felhasználók körét ennek megfelelően a megszokottnál lényegesen szélesebbre – akár az egyes ország határait meghaladó méretekre is – lehet szabni, azaz ebben a szélesebb körben lehet demonstrálni a szolgálat képességeit, erősségeit.

A sajtóválogatás műfaja természetesen nem korlátozódik a saját nyelven megjelent kiadványokra, ellenkezőleg, a korábbi, már említett hagyományok mentén szorosan idetartozik a külföldi sajtótermék feldolgozása is. A válogatás elkészítésének fentebb bemutatott folyamata gyakran kiegészül a fordítás fázisával, amelynek különösen az egyedi nyelvet használó és idegen nyelvet nem vagy csak szűk körben beszélő országok esetében van megkerülhetetlen szerepe. A fordítás időigénye miatt a külföldi sajtótermékek esetében az egyes válogatások általában nem naponta, hanem hetente vagy havonta készülnek el.

[7] www.janes.com (A letöltés dátuma: 2019. 04. 01.); www.cia.gov/library/publications/the-world-factbook (A letöltés dátuma: 2019. 04. 01.)

A technika egyre fokozódó ütemű fejlődésével újabb lehetőségek keletkeztek a felderítés műfajainak keveredésére: míg a külföldi sajtótermékek humán kapcsolat révén, külföldről való beszerzése a HUMINT és a OSINT műfajának keveredéseként is felfogható, úgy polgári célú, térképezésre használt műholdak által készített termékek kereskedelmi forgalomban való beszerzése és szakmai célú felhasználása nem más, mint az IMINT és az OSINT sajátos hibridje.

Az információtechnológia robbanásszerű fejlődése, az internet terjedése jól adaptálhatónak bizonyult az OSINT hagyományos munkafolyamataihoz. A sajtófigyelést ki lehetett és kellett terjeszteni a rádió- és tévéadásokra (ideértve a frekvenciákon és interneten továbbítottakat egyaránt), az internetes sajtótermékekre. A válogatást immár nem papíralapon, hanem elektronikus formában (azaz például elektronikus levélben) lehetett készíteni és továbbítani. Archiválásra, illetve az archívumban való utólagos kutatásra pedig szintén remek lehetőséget adtak a különböző adatbáziskezelő szoftverek, illetve azok testreszabásával készített egyedi programok. Az akkori jövőbe, azaz a mába mutató jelenségként értékelhető, hogy a szöveg mellett a kép (kisebb mértékben pedig a hang is) egyre nagyobb és növekvő szerepet kapott a gyűjtött és tárolt információk között.[8]

Jelen rövid fejtegetés is mutatja, hogy a második generációs internet nem megteremtette, „csupán" megdöbbentő módon kiterjesztette az OSINT műfaját. A fejlődés elsősorban az adatok mennyiségében (robbanásszerű növekedés); jellegében (személyre vonatkozó, személyektől származó); költségigényében (csökkenő); az adatok megszerzésének és feldolgozásának időigényében (erőteljesen csökkenő); földrajzi kötöttségeinek változásában (azaz eltűnésében) ragadható meg. Az információhordozók között a szöveg helyét egyre inkább átveszi az álló- és a mozgókép, illetve a térkép, amely jelenség az információk kitermelésének és felhasználásának, archiválásának során egyaránt szembeötlő. Az archiválás és keresés terén pedig várhatóan egyre nagyobb szerepet játszik majd a mesterséges intelligencia.

Felhasznált irodalom

A magyar csendőrség zsebkönyve (1905). Budapest. Elérhető: http://epa.niif.hu/02900/02994/00019/pdf/EPA02994_mkir_csendroseg_zsebkonyve_1905.pdf (A letöltés dátuma: 2019. 04. 01.)

Boda József – Parádi József – Regényi Kund Miklós szerk. (2014): *Felderítő-szolgálati utasítás.* Budapest, NBSZ-SZBMRTT.

Haraszti György – Kovács Zoltán András – Szita Szabolcs szerk. (2007): *Vallomások a holtak házából.* Budapest, ABTL–Corvina.

Meacham, Jon (2018): *Franklin és Winston. Egy nagyívű barátság bensőséges története.* (Sóskuthy György – Soproni András ford.) Budapest, Park.

Radzinszkij, Edvard (2015–2016): *Koba. Sztálin apokalipszise I-II.* (Soproni András ford.) Budapest, Európa.

[8] Lásd Regényi 2013, 202.

Regényi Kund Miklós (2013): Az Alkotmányvédelmi Hivatal Integrált ügyeleti főosztályának kialakítása és tapasztalatai. In Gaál Gyula – Hautzinger Zoltán szerk.: *Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények,* XIV. Pécs, Magyar Hadtudományi Társaság. 199–204.

Regényi Kund Miklós (2014): A „Felderítő-szolgálati utasítás" szakmai szemmel. In Boda József – Parádi József – Regényi Kund Miklós szerk.: *Felderítő-szolgálati utasítás.* Budapest, NBSZ-SZBMRTT. 51–68.

Internetes források

www.cia.gov/library/publications/the-world-factbook (A letöltés dátuma: 2019. 04. 01.)
www.viamichelin.com (A letöltés dátuma: 2019. 04. 01.)
www.janes.com (A letöltés dátuma: 2019. 04. 01.)

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 38–49. • DOI: 10.32561/nsz.2019.2.4

Gál István László[1]

A kémkedés a magyar büntetőjogban

Spying in the Hungarian Criminal Law

Napjainkban számolnunk kell olyan nemzetbiztonsági kockázatokkal, amelyek abból erednek, hogy a nyílt forrásokból (internet, országos és helyi média stb.) származó, összegyűjtött, elemzett és értékelt információk hozzáférhetők idegen hatalmak vagy szervezetek (ellenérdekelt titkosszolgálatok) számára is. A büntetőeljárásokban felmerülhet tehát, hogy ezek a cselekmények kémkedésnek minősíthetők-e, közelebbről: lehet-e ez bűncselekmény a magyar büntetőjog szerint? A jelen rövid tanulmány erre a kérdésre keresi a választ.

Kulcsszavak: kémkedés, OSINT, büntetőjog, hírszerző tevékenység

Nowadays we have to take into consideration national security risks arising from forwarding collected, classified, analysed and concluded information through opened sources (such as the Internet, national and local mediums) that can be available for foreign powers or organisations (counter-interested secret services). The question arose during a criminal procedure whether such action can be classified as a criminal act of espionage according to the Criminal Code, or going further: can it be a crime according to the Hungarian criminal law? This short study aims to answer this question.

Keywords: espionage, OSINT, criminal law, intelligence

Az állam elleni bűncselekmények általános jellemzői

Az állam elleni bűncselekmények minden korban a fennálló politikai rendszer büntetőjogi védelmét szolgálták. Ezért szokták politikai bűncselekményeknek is nevezni őket, szemben a büntetőjog különös részében található összes másik fejezetben található, úgynevezett köztörvényes bűncselekményekkel. A politikai bűncselekmény

[1] Prof. Dr. Gál István László ügyvéd, tanszékvezető egyetemi tanár, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Büntetőjogi Tanszék; egyetemi tanár, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, Katonai Nemzetbiztonsági Tanszék. ORCID-azonosító: 0000-0002-0258-8587.

elkövetője nem minden esetben bűnöző a szó hétköznapi értelmében: ami az egyik ország vonatkozásában bűn, annak az elkövetője egy másik ország szempontjából lehet akár hős is. Erre tipikus példa a kémkedés elkövetője.

A magyar jogtörténetben az állam elleni bűncselekmények gyökerei írott formában Werbőczy *Hármaskönyv*ében, az I. rész XIV. címében szabályozott hűtlenség 18 esetében már fellelhetők. A *Csemegi-kódex* Különös részének I. fejezete, „Az állam léte és alapintézményei elleni bűncselekmények" körében határozta meg a felségsértés és a hűtlenség tényállását, a II. fejezetben „Az államhatalom békés működését fenyegető büntetendő cselekmények" pedig a lázadás és az alkotmány, a törvény, a hatóságok vagy a hatósági közegek elleni izgatás tényállása nyert szabályozást. A kódex felségsértésnek tekintette az állam, illetve annak leglényegesebb intézményei megsértésére irányuló (tehát a belső intézményeket belülről bomlasztó) erőszakos tetteket, hűtlenségnek az állam külbiztonságát az állampolgári hűség megszegésével fenyegető magatartásokat (amelyek az államot külső veszélynek, háborúnak teszik ki), és ugyancsak külön fejezetben írt elő büntetéseket a király és a királyi ház tagjainak bántalmazása és megsértése miatt.

A Csemegi-kódex első 40 évében állam elleni bűncselekmények nem fordultak elő nagy számban a bírói gyakorlatban. Az első világháború után azonban zavaros idők jöttek. Ahogy Angyal Pál megfogalmazta az egyik monográfiájában: „Az 1918. és 1919. évek értékromboló eseményei kiáltó bizonyságot tettek arról, hogy ha egy nemzetben a fegyelmezettség s az áldozatos hazaszeretet meggyengül, ha az összetartás kapcsai meglazulnak, s ha ennek folytán széthúzó és többnyire pusztító erők kerekednek felül: megbomlik az erkölcsi és gazdasági élet rendje, fennakad a kulturális fejlődés menete s napokon belül tönkremegy mindaz, amit századok építettek."[2] 1921-ben vált tehát a magyar büntetőjog részévé a hírhedt 1921. évi III. törvény, az úgynevezett rendtörvény, amely a korábbi forradalmi mozgalmak csírájában történő elfojtását volt hivatott szolgálni. A második világháború azonban elsöpörte ezt a jogszabályt az őt megalkotó rendszerrel együtt, de hamarosan újra zavaros idők jöttek. Volt ugyan egy rövidebb ideig tartó, reménykedésre okot adó történelmi időszak is, amely alatt új büntetőjogi szabályok születtek az állam elleni bűncselekmények témakörében. Az Ideiglenes Nemzeti Kormány kiadta a népbíráskodásról szóló 81/1945. (II. 5.) ME számú rendeletet. Az 1440/1945. (V. 1.) ME rendelettel módosított 81/1945. (II. 5.) ME számú rendeletet az 1945. évi VII. törvény emelte törvényerőre. Ez a törvény még a demokratikus államrend és a köztársaság védelméről szólt.

A hatályos anyagi büntetőjogi szabályok hivatalos összeállítása (BHÖ) 1952-ben a Népköztársaság elleni bűncselekmények cím alatt az állam belső biztonsága elleni (I. fejezet), az állam külső biztonsága elleni (II. fejezet), a honvédelem érdekeit sértő (III. fejezet) és a béke elleni, háborús és nép elleni (IV. fejezet) bűncselekményeket határozta meg. „A restaurációs kísérletek elleni harc egyik leghatékonyabb eszköze a büntetőjog. A büntetőjogi harc azoknak a jogszabályoknak az alkalmazásával történik, amelyeket a szocialista állam törvényhozó szervei éppen az ellenforradalmi cselekményekkel szembeni védekezés céljára alkottak" – olvashatjuk egy korabeli

[2] Angyal 1928, 1.

tankönyvben.[3] Az 1956-os forradalom és szabadságharc leverésekor ezeket a büntető jogszabályokat alkalmazták a magyar bíróságok. Az eljárások ugyan lehettek formálisan jogszerűek, tartalmilag ugyanolyan igazságtalannak érezzük őket, mint az 1921. évi III. törvénycikk alapján lefolytatott büntetőeljárásokat.

Az 1961-es Btk., az 1961. évi V. törvény Különös Része az első (IX.) fejezetében szabályozta az állam elleni bűncselekményeket. A fejezet a következő bűncselekményeket tartalmazta: összeesküvés, lázadás, kártevés, rombolás, merénylet, izgatás, hazaárulás, ellenség támogatása és a kémkedés. Ezekhez járult még a feljelentési kötelezettség elmulasztása, és büntetendő volt, ha bármely bűncselekményt más szocialista állam ellen követik el.

Az 1978. évi IV. törvény, vagyis a korábbi Btk. eredetileg teljesen hasonlóan szabályozta az állam elleni bűncselekményeket, mint az 1961-es Btk.

1989. október 15-én újrakodifikáltuk az állami elleni bűncselekményekre vonatkozó büntetőjogi szabályokat. Megszűnt a halálbüntetés kiszabásának a lehetősége – még a halálbüntetés Alkotmánybíróság általi eltörlését megelőzően. Jogi tárgya az alkotmányos rend lett, amely gyakorlatilag megegyezik az új Alaptörvény szerinti állami rend kategóriájával. Jellemző ezen bűncselekményekre a jogi tárgy ellen irányuló célzat, és összesen tíz bűncselekmény maradt a fejezetben.

A 2012. évi C. törvény, a jelenleg hatályos Btk. az állam elleni bűncselekmények szabályozásán nem változtatott, a XXIV. fejezet gyakorlatilag megegyezik az 1978. évi IV. törvény X. fejezetében található szabályozással.

Az állam elleni bűncselekmények szabályozása mindig, minden korban szoros összefüggésben állt és áll az adott állam alkotmányával. A magyar állam politikai berendezkedését meghatározó, 2012. január 1-től hatályos alkotmány, Magyarország Alaptörvénye lefektette azokat a szabályokat, amelyek a politikai intézményrendszer alapjait jelentő állami rendet definiálják (azt az állami rendet, amelyet a Btk. a társadalomra veszélyesség fogalmát meghatározó 4. § (2) bekezdésében expressis verbis megnevez mint a bűncselekmény egyik különös jogi tárgyát, vagyis azt a törvényhozó által védeni kívánt társadalmi viszonyt, amelyet minden állam elleni bűncselekmény elkövetője sért vagy veszélyeztet). Magyarország Alaptörvénye már rögtön az Alapvetés B) cikkében kimondja, hogy:

„(1) Magyarország független, demokratikus jogállam.

(2) Magyarország államformája köztársaság.

(3) A közhatalom forrása a nép.

(4) A nép a hatalmát választott képviselői útján, kivételesen közvetlenül gyakorolja."

Az alapvetés C) cikk (2) bekezdése pedig kimondja, hogy:

„Senkinek a tevékenysége nem irányulhat a hatalom erőszakos megszerzésére vagy gyakorlására, illetve kizárólagos birtoklására. Az ilyen törekvésekkel szemben törvényes úton mindenki jogosult és köteles fellépni."

Ezeket az Alaptörvényben lefektetett szabályokat védi a maga sajátos eszközeivel a magyar büntetőjog a Btk. XXIV. fejezetében található állam elleni bűncselekmények kriminalizálása által.

[3] *Büntetőjogi tankönyv II.* 1959, 19.

Az állam elleni bűncselekményeket hagyományosan két kategóriába sorolhatjuk: az állam belső biztonsága elleni bűncselekmények (a régi magyar büntetőjogban ezek a felségsértés esetei voltak) és az állam külső biztonsága elleni bűncselekmények (ezeket régen a hűtlenség esetei közé sorolták). Általában elmondható ezekről a bűncselekményekről, hogy:

- az egyik társadalomra legveszélyesebb bűncselekménycsoportot képezik;
- politikai bűncselekményeknek tekintjük őket, szemben a Btk. összes többi fejezetében található köztörvényes bűncselekménnyel;
- valamennyi bűntettet képez (kivéve a járulékos feljelentés elmulasztását);
- általában büntetendő az előkészületük;
- a szabadságvesztés végrehajtási fokozata tipikusan fegyház (ha a kiszabott büntetés három év vagy ennél hosszabb);
- szigorúak a szankciók;
- valamennyi bűncselekményhez feljelentési kötelezettség társul;
- üldözésük körében az állami önvédelmi elv (reálprincípium) érvényesül;
- mellékbüntetésként kitiltásnak is helye van;
- a nyomozás elrendeléséig az Alkotmányvédelmi Hivatal végzi ezen bűncselekmények felderítését (1995. évi CXXV. törvény 5. § h) pont).

A kémkedés három változata a hatályos magyar büntetőjogban

A kémkedés a hatályos magyar büntetőjogban három tényállásban szabályozott jogellenes magatartás 2014 óta. A kémkedés mind az Európai Unió intézményei ellen, mind a szövetséges fegyveres erő ellen a hagyományos büntetőjogi dogmatika szerint az állam külső biztonságát sértő bűncselekmény, bár rögtön hozzá kell tennünk, hogy nemzetbiztonság-tudományi tekintetben valamennyit ezzel egyidejűleg az állam belső biztonságát veszélyeztető cselekményeknek is tekinthetjük.

Kémkedés

261. § (1) Aki idegen hatalom vagy idegen szervezet részére Magyarország ellen hírszerző tevékenységet folytat, bűntett miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

(2) Aki az (1) bekezdésben meghatározott kémkedést szigorúan titkos minősítésű adat kiszolgáltatásával követi el, öt évtől tizenöt évig terjedő szabadságvesztéssel büntetendő.

(3) Aki kémkedésre irányuló előkészületet követ el, egy évtől öt évig terjedő szabadságvesztéssel büntetendő.

(4) Nem büntethető a hírszerző tevékenységre ajánlkozás vagy vállalkozás miatt, aki – mielőtt egyéb hírszerző tevékenységet fejtett volna ki – az ajánlkozását vagy

vállalkozását a hatóságnak vagy az állam illetékes szervének bejelenti, és a külföldi kapcsolatát teljesen feltárja.

A kémkedés alaptípusa a Btk. 261. §-ában szabályozott bűncselekmény. *Jogi tárgya Magyarország Alaptörvény szerinti állami (alkotmányos) rendje*, közelebbről az állam biztonsága, valamint hazánk minden fontos politikai, katonai, társadalmi vagy gazdasági érdeke.

A kémkedés alanya állampolgárságra tekintet nélkül bárki lehet. A külföldi állampolgárok tipikusan a nagykövetségeken belül végzik a kémtevékenységet, diplomáciai fedésben. A nagykövetségek az esetek többségében az úgynevezett rezidentúrák központjai is egyben. A külföldi diplomatákat viszont megvédi a diplomáciai mentesség, büntetőjogi felelősségre vonással Magyarországon csak a magyar állampolgároknak és a nem diplomatafedésben dolgozó külföldi ügynököknek kell számolniuk. A kémkedést csak szándékosan lehet elkövetni, egyenes és eshetőleges szándékkal egyaránt.

Az elkövetési tárgy bármely adat lehet, amely alkalmas a Magyarország érdekeivel ellentétes felhasználásra. A tényállás minősített esete speciális elkövetési tárgyat tartalmaz, ez a szigorúan titkos minősítésű adat.

A bűncselekményt megvalósító elkövetési magatartás: hírszerző tevékenység, amelynek fogalma a következő területeket öleli fel a hagyományos[4] titkosszolgálati osztályozás[5] szerint:

a) *HUMINT (Human Intelligence[6]):* A titkos és bizalmas információk megszerzése érdekében minden állami és magán titkosszolgálat humán forrásokat létesít külföldön, illetve külföldi irányultsággal belföldön is. A humán források köre az alkalmi adatszolgáltatóktól a szervezetszerű (külföldi ügynöki) együttműködésig terjed. A titkos kapcsolati kör olyan személyekből áll, akik a külföldi titkok megszerzéséhez már meglévő vagy kialakítható lehetőségekkel rendelkeznek.

b) *TECHINT (Technical Intelligence[7]):* A technikai hírszerzés egy átfogó megnevezés, amely a hagyományos titkosszolgálati eszközök (például lehallgatás) alkalmazásától az elektronikus eszközökkel folytatott felderítésig és tudományos módszerekkel kidolgozott eljárásokig terjed. A technikai információszerzés fogalma a távközlési csatornákból és adatátviteli hálózatokból történő, továbbá a rejtjelző és irodatechnikai berendezések műszaki eszközökkel és módszerekkel való támadásával megvalósuló információszerzést foglalja magában.

A távközlési csatornákból történő információszerzés a nemzetközi – elsősorban egyes külföldi kormányzati – távközlési csatornák támadásával valósul meg. A műszaki támadás a rejtjelző és irodatechnikai eszközök működése közben keletkező, illetve azok valamely beavatkozással gerjesztett kísérőjelenségeinek vételére, feldolgozására és a támadott berendezéseken írt nyílt információk visszaállítására irányuló, tudományos módszerek és technikai eszközök kombinált alkalmazásával folytatott tevékenység.

---

4 Természetesen léteznek ennél szélesebb spektrumot felölelő csoportosítások és definíciók is.

5 www.mkih.hu/hivatal_hirszerzes.shtml (A letöltés dátuma: 2011. 10. 02.)

6 Jelentése: humán hírszerzés, emberi erőforrások felhasználásával végzett adatgyűjtés és információszerzés.

7 Technikai hírszerzés.

c) *OSINT (Open Source Intelligence*[8]*):* a titkosszolgálatok figyelemmel kísérik a nyílt információs forrásokat is. Ezek a sajtókiadványok, a tömegkommunikáció műsorai, nyílt adatbázisok és információs rendszerek és az internet lehetnek. Az így elérhető nagytömegű adathalmazból kell kiszűrni a szükséges információkat.
d) *Nemzetközi együttműködés:* az egyes nemzeti titkosszolgálatok általában részt vesznek több multilaterális titkosszolgálati együttműködésben. Partneri kapcsolataink valamennyi relációban a kölcsönösségen, a közös érdekeken és az egyenjogúságon alapulnak.

A hírszerző tevékenység fogalmát az ezredforduló után megjelent hazai büntetőjogi tankönyvek már a korábbiaktól eltérően, sokkal tágabban értelmezik: „Napjainkban a kémkedés rendszerint már nem korlátozódik a titkos adatszerző, adatszolgáltató tevékenységre, hanem annál lényegesen tágabb körű tevékenység. Magában foglal olyan cselekményeket is, mint például a hírszerző szervezet részére megfelelő személy felkutatása, a célszemélyek kompromittálása, hírszerző rezidentúrák működtetése stb. A modern hírszerzés felhagyott a kémkedés hagyományos formáival (beszervezés, beszervezési nyilatkozat felvétele) is, és inkább a kapcsolattartás lazább formáit választják. A tényállás tartalmilag a hírszerző szervezetek részére történő titkos, konspirált információszerző és azt elősegítő tevékenységet nyilvánítja büntetendővé."[9]

A hírszerző tevékenység végzése a hatályos tényállás szerint két irányban történhet:
a) idegen hatalom vagy
b) idegen szervezet részére.

Az idegen hatalom tipikusan egy állam, az idegen szervezet pedig általában egy külföldi titkosszolgálat. Bármilyen szervezet szóba jöhet, amelyik rendeltetésszerű tevékenységét nem Magyarországon fejti ki. Ha egy idegen titkosszolgálat által működtetett fedőcég az idegen szervezet, akkor a tulajdonosi szerkezetében akár magyar állampolgárok is lehetnek, ettől függetlenül a cselekmény tényállásszerű. (Az viszont már más kérdés, hogy felmerül az ilyen cégtulajdonos magyar állampolgárok büntetőjogi felelőssége is.)

A bűncselekmény tényállása eredményt nem tartalmaz, vagyis a kémkedés befejezetté válik a tényállásszerű magatartás tanúsításával. A törvényhozó célzatot nem kíván meg a cselekmény tényállásszerűségéhez, a motívum is közömbös. Az elkövetés akkor is megállapítható, ha az elkövetőt nem politikai, hanem anyagi érdek motiválja.

A hírszerző tevékenység folytatásával a kémkedés befejezetté válik. Tevékenységet folytatni a következetes bírói gyakorlat szerint egyetlen magatartással nem lehet, ahhoz időben és térben elkülönülő magatartások szükségesek. Maga a hírszerző tevékenység is egy folyamatos cselekménysorozatot jelent a titkosszolgálati szakzsargon szerint, a bűncselekmény tehát egyetlen tevékenységi aktussal nem követhető el. Ha az elkövető csak egyetlen magatartást tanúsított, akkor vagy a kémkedés kísérlete, vagy más bűncselekmény (például valamilyen titoksértő bűncselekmény, esetleg

[8] Nyílt forrású hírszerzés.
[9] Belovics–Molnár–Sinku 2005, 35–36.

más állam elleni bűncselekmény) állapítható meg, vagy ha sem a kísérlet, sem más bűncselekmény nem állapítható meg az elkövető terhére, akkor bűncselekmény hiányában fel kell menteni. (Tehát például egyetlen alkalommal futártevékenység ellátása egy külföldi titkosszolgálat javára vagy érdekében, vagy minősített adatokat nem tartalmazó információk átadása, azokból egyetlen alkalommal elemző-értékelő jelentés készítése idegen hatalom vagy idegen szervezet részére még nem minősül bűncselekménynek az új Btk. alapján.) Kísérlet csak akkor állapítható meg, ha az elkövető az adat megszerzésére irányuló magatartását megkezdi, de ahhoz nem jut hozzá, illetve ha egyetlen adatot vagy akár több adatot tartalmazó egyetlen jelentést továbbít, továbbá bizonyítható, hogy a kapcsolat huzamosabb időre jött létre a hírszerző és az idegen hatalom vagy idegen szervezet között. A gyakorlat szempontjából ez azzal a következménnyel jár, hogy különös alapossággal kell dokumentálni és bizonyítani egy hírszerző tevékenységgel gyanúsított személy tevékenységét ahhoz, hogy a kémkedés elkövetése megállapítható (és a bíróság előtt bizonyítható) legyen. A törvény az előkészületet is büntetni rendeli, kifejezve ezzel a kémkedés fokozott társadalomra veszélyességét.

A tényállás eredményt nem értékel, az elkövetési magatartás tanúsításával, vagyis a hírszerző tevékenység végzésével a bűncselekmény befejezetté válik.

A bűncselekmény minősített esete, ha a kémkedést szigorúan titkos minősítésű adat kiszolgáltatásával követik el.

A kémkedés tevékenység folytatásával valósul meg, vagyis folyamatos, tartós bűncselekmény. Emiatt ha valaki azonos szervezet vagy idegen hatalom részére rendszeresen vagy folyamatosan végez hírszerző tevékenységet, a kémkedés természetes egység. Ha több szervezet vagy több idegen hatalom részére történik a kémkedés, akkor a sértett, vagyis a magyar állam azonosságára tekintettel álláspontunk szerint folytatólagos egység állapítható meg. Halmazat megállapítására csak abban a ritka és a gyakorlatban valószínűtlen szituáció esetében állapítható meg, ha több szervezet vagy hatalom részére végez hírszerző tevékenységet az elkövető, és a folytatólagosság a részcselekmények között eltelt hosszabb idő miatt nem állapítható meg.

A tényállás büntetlenséget biztosít annak az elkövetőnek, aki mielőtt egyéb hírszerző tevékenységet fejtett volna ki, az ajánlkozását vagy vállalkozását a hatóságnak bejelenti és a külföldi kapcsolatát teljesen feltárja. Ez a törvényi rendelkezés egy hatékony eszköz lehet a magyar elhárítás számára a külföldi ügynökök azonosítása után a „visszafordításukra", vagyis arra, hogy kettős ügynökként alkalmazva a lebukott kémet, játszmába kezdjenek a külföldi hírszerző szervezettel, hamis adatokkal félrevezetve azt. Fontos kérdésként merülhet fel a gyakorlatban, hogy a kettős ügynök információkkal való ellátása során néha szükségképpen valós adatokat is adni kell neki, mert a kizárólag hamis információk szállítása révén hamar dekonspirálódhatna, lelepleződhetne. Ebben az esetben formálisan megvalósul ugyan a kémkedés tényállása, ha azonban a szakma szabályait betartva adják ki a hamis mellett a valódi információkat is a külföldi hírszerző szervezetnek a magyar elhárítás munkatársai a kettős ügynökön keresztül, álláspontom szerint bűncselekmény nem valósul meg a társadalomra való veszélyesség hiánya miatt. Ebben az esetben azonban különösen körültekintően, a szakma szabályai szerint kell eljárni, és csak a lehető legszűkebb körben lehet valós információkat kiadni idegen hatalom vagy idegen szervezet részére.

A titoksértő bűncselekményekkel a kémkedés a következő viszonyban áll: mind a specialitás, mind a konszumpció elve alapján (tehát a súlyosabb büntetési tétel miatt is) a kémkedést állapítjuk meg látszólagos alaki halmazat esetén.

A kémkedést a gazdasági titok megsértésétől álláspontunk szerint a következő szempontok alapján lehet elhatárolni: ha a hírszerző tevékenység mint elkövetési magatartás bizonyítható (az újabb jogirodalmi álláspontok alapján, tekintettel a hírszerző tevékenység fogalmának meglehetősen kiterjesztett értelmezésére, ez nem nehéz), és gazdasági titoknak minősülő adatot továbbít valaki idegen hatalom vagy idegen szervezet részére, kémkedést követ el (gazdasági kémkedést). Ha a gazdasági titkot valaki önmagának szerzi meg, vagy olyan belföldi szervezet részére továbbítja, amely esetében nem bizonyítható a külföldi (idegen) titkosszolgálatokkal való kapcsolat, csak gazdasági titok megsértése valósul meg (ez a szakirodalomban ipari kémkedésnek nevezett eset). A legfontosabb elhatároló elem egyébként az, hogy képes-e az adat illetéktelen kezelésével a terhelt sérteni Magyarország fent felsorolt gazdasági, pénzügyi stb. érdekeit. Ha igen, akkor kémkedést kell megállapítani, ha nem, akkor bármekkora is a kár, csak gazdasági titkot sértettek. Ennek a büntetési tétele jelentősen enyhébb a kémkedésénél.

A hivatalos statisztika szerint alig válik ismertté kémkedés Magyarországon. Nem véletlenül. A lebukott kémeket a legritkább esetben célszerű büntetőjogi úton felelősségre vonni. Egy ország nemzetbiztonsági érdekeit sokkal hatékonyabban szolgálhatja az elfogott kém „visszafordítása", vagyis kettős ügynökként történő foglalkoztatása, ami által az ellenérdekű titkosszolgálat hamis információkkal félrevezethető. Emellett a külföldön dekonspirálódott ügynökök magyar ügynökökkel történő kicserélése miatt is szükség lehet arra egyes esetekben, hogy a büntetőeljárás lefolytatására ne kerüljön sor. Néha azonban lefolytatják a büntetőeljárást a kémek ellen hazánkban is. (A büntetőeljárással nemzetközi hírverés is generálható, és így az ország alkupozíciója javulhat, ha a magyar érdekeket szolgáló kémek kicserélése felmerül.) Előfordul azonban, hogy a büntetőeljárás szigorú szabályainak megfelelően, perrendszerűen nem lehet bizonyítani a „majdnem biztosan" tudott tényeket és körülményeket, ilyenkor a bíróság felmentő ítéletet hoz bűncselekmény vagy bizonyítottság hiányában.

Kémkedés az Európai Unió intézményei ellen

261/A. § A 261. § szerint büntetendő, aki az Európai Unión kívüli harmadik állam részére az Európai Parlament, az Európai Bizottság vagy az Európai Unió Tanácsa ellen hírszerző tevékenységet folytat.

A bűncselekmény a kémkedés egyik speciális alakzatát szabályozza, 2014. január 1-jétől hatályos. Ezzel a tényállással egy fontos büntetőjogi joghézagot szüntetett meg a jogalkotó, aminek fontosságát az is jelzi, hogy szinte rögtön a hatálybalépése után indult is egy büntetőügy ilyen bűncselekmény gyanújával, amely ügy még jelenleg is folyamatban van.

A bűncselekmény tényállása úgynevezett utaló diszpozíciót tartalmaz, vagyis visszautal a 261. §-ra, így vonatkozik rá az ott szabályozott minősített eset és büntethetőséget megszüntető ok, és ennek is büntetendő az előkészülete.

A bűncselekmény jogi tárgya speciális: az Európai Parlament, az Európai Bizottság és az Európai Unió Tanácsa érdekeit védi.

Az Európai Parlament az Európai Unió parlamentáris szerve, amelyet az EU állampolgárai közvetlenül választanak, ötéves időtartamra. A Miniszterek Tanácsával együtt alkotja az EU törvényhozói hatalmi ágát. Hivatalosan a székhelye Strasbourg (emellett Brüsszelben is ülésezik).

Az Európai Bizottság az Európai Unió egyik legfontosabb intézménye, az EU egészének érdekeit képviseli és támogatja. Új európai jogszabályokra vonatkozó javaslatokat szövegez, emellett az uniós politikák végrehajtásával és az uniós források elköltésével kapcsolatos mindennapi feladatokat irányítja.

Az Európai Unió Tanácsa az Európai Parlamenttel közösen alkotja az Európai Unió (EU) törvényhozó szervét. Minden tagállam kormányának a miniszterét tartalmazza. Az Európai Unió Tanácsát a hivatalos uniós dokumentumok helyenként Tanácsként említik és gyakran hivatkoznak rá Miniszterek Tanácsa néven. Székhelye Brüsszel (azonban meghatározott időközönként Luxembourgban ül össze).

Speciális tényállási elem a passzív alany: az Európai Parlament, az Európai Bizottság és az Európai Unió Tanácsa. Emellett a tényállásszerűséghez az is kell, hogy a hírszerző tevékenységet EU-n kívüli harmadik állam részére folytassák.

A bűncselekmény álláspontunk szerint nem áll látszólagos alaki halmazatban a kémkedéssel az eltérő jogi tárgy miatt.

A szövetséges fegyveres erő ellen elkövetett kémkedés

262. § A 261. § szerint büntetendő, aki a kémkedést Magyarország vagy a kölcsönös katonai segítségnyújtás kötelezettségét tartalmazó hatályos nemzetközi szerződés szerint Magyarországgal szövetséges állam területén, szövetséges fegyveres erő ellen követi el.

A bűncselekmény a kémkedés egyik speciális alakzatát szabályozza, tényállásának elemzése kapcsán mindenben a 261. §-ra támaszkodhatunk, hasonlóan az Európai Unió intézményei elleni kémkedés bűncselekményének elemzéséhez.

A bűncselekmény tényállása itt is utaló diszpozíciót tartalmaz, vagyis visszautal a 261. §-ra, így vonatkozik rá az ott szabályozott minősített eset és büntethetőséget megszüntető ok, és ennek is büntetendő az előkészülete. (Talán célszerű lett volna a 261/A. §-ban szabályozott bűncselekménnyel összevonnia a jogalkotónak.)

A bűncselekmény jogi tárgya speciális: Magyarország és a vele szövetséges (NATO-tag) állam katonai érdeke. Magyarország az 1999. évi I. törvénnyel kihirdetett nemzetközi szerződéssel csatlakozott a NATO-hoz. Ezen csatlakozási szerződés talán legfontosabb pontja az 5. cikk, amely kimondja:

„A Felek megegyeznek abban, hogy az egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. Cikke által elismert egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Felekkel egyetértésben,

azonnal megteszi azokat az intézkedéseket, ideértve a fegyveres erő alkalmazását is, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart."

Speciális tényállási elem az elkövetés helye, illetve a passzív alany. Az elkövetés helye Magyarország vagy a kölcsönös katonai segítségnyújtás kötelezettségét tartalmazó hatályos nemzetközi szerződés szerint Magyarországgal szövetséges állam területe. A passzív alany is speciális: a szövetséges fegyveres erő. Ennek a fogalmával kapcsolatban a Btk. 459. § (3) bekezdése ad eligazítást:

„Ahol e törvény szövetséges fegyveres erőt, külföldi hadműveleti területen végzett humanitárius tevékenységet, békefenntartást vagy humanitárius műveletet említ, azon a honvédelemről és a Magyar Honvédségről szóló törvényben meghatározott fogalmakat kell érteni."

A Btk. területi és személyi hatályáról szóló 3. § (2) bekezdés a) pont ab) alpontja alapján ez a bűncselekmény nem magyar területen történő elkövetés esetén csak akkor büntethető, ha magyar állampolgár követi el, vagy amennyiben nem magyar állampolgár az elkövető, de az elkövetés helyének törvénye szerint is büntetendő ez a cselekmény.

A bűncselekmény látszólagos alaki halmazatban állhat a kémkedéssel, ilyenkor a specialitás elve alapján csak a szövetséges fegyveres erő ellen elkövetett kémkedést lehet megállapítani.

Elkövethető-e a kémkedés kizárólag nyílt adatok gyűjtésével és elemzésével?

Az előzőekben láthattuk, hogy nem könnyű feladat a büntetőjog eszköztára segítségével minden kétséget kizáróan bizonyítani a kémkedést. Az eddigi magyar gyakorlatban kizárólag olyan ügyek fordultak elő, amikor az elkövető minősített információkat (is) kiadott idegen szervezetek részére. Enélkül nagyon nehéz feladat a kémkedés bizonyítása a büntetőbíróság előtt. Talán a legérdekesebb hazai ügyünk a 2009-ben elhunyt Belovai István[10] büntetőügye volt, aki önéletrajzában, a *Fedőneve: Scorpion* című könyvben (1998) leírja, hogy hosszas vívódás után döntött úgy, kapcsolatba lép a CIA[11]-val, hiszen ezzel egy újabb világháborút előz meg – állítja. Gyakorlatilag az ő tevékenysége folytán bukott le később a Conrad-összeesküvés, ami később a világsajtót is bejárta. Clyde Lee Conrad (1948–1998) Németországban állomásozó amerikai katonatiszt rendszeresen szigorúan titkos katonai információkat adott át a Magyar Népköztársaságnak 1974–1988 között. Ezek közül a stratégiai szempontból

[10] Egy érdekes adalék a közelmúltból: A bolíviai ügyészség szerint Belovai István révén állt kapcsolatban az amerikai CIA-val Eduardo Rózsa Flores, aki a bolíviai ügyészség szerint terrorista csoportot szervezett bolíviai szeparatista erők szolgálatában. Rózsa Flores és a CIA számára dolgozó Belovai valószínűleg a Balkánon lépett kapcsolatba egymással, és utóbbi később technikai és pénzügyi segítséget nyújtott Rózsa Flores bolíviai tevékenységéhez – jelentette a bolíviai sajtó. Lásd: www.mixonline.hu/Cikk.aspx?id=37012 (A letöltés dátuma: 2011. 10. 23.)

[11] Central Intelligence Agency (Központi Hírszerző Ügynökség) az USA egyik szövetségi hírszerző szervezete a Hírszerző Közösség tagjaként. 1947-ben alapították.

legfontosabb a Kelet- és Nyugat-Európát elválasztó atomaknazár tervrajza volt, amelynek segítségével a szovjet páncélosok akadálytalanul juthattak volna ki a La Manche-ig. 1990-ben Conradot egy német bíróság kémkedés miatt életfogytiglani szabadságvesztésre ítélte. Belovai azonban korábban, még a '80-as évek közepén bukott le, amikor éppen átvett egy dokumentumot egy rejtekhelyen. Az ehhez használt preparált kő, mint tárgyi „postaláda", kiállított múzeumi tárgyként ma is megtalálható Budapesten, az Alkotmányvédelmi Hivatal központi épületében. Az ügyész a tárgyaláson egyébként az akkor hatályos Btk. alapján halálbüntetést kért Belovaira, de végül életfogytiglani börtönre és teljes vagyonelkobzásra ítélték, majd 1990-ben Göncz Árpád köztársasági elnök kegyelemben részesítette, a büntetése hátralévő részét nem kellett letöltenie (az életfogytig tartó szabadságvesztésből hátralévő mintegy 20 évet a köztársasági elnök 5 év próbaidőre felfüggesztette, ez a döntés példa nélküli a magyar büntetőjogban).

„Az OSINT az amerikai titkosszolgálatok által kifejlesztett módszer, amely az internet terjedésével általánossá vált nemcsak a titkosszolgálatoknál, hanem az üzleti élettől a kormányzati tevékenységig széles spektrumon. Az interneten keresztül az elmúlt évtizedekben olyan mennyiségű adat halmozódott fel, hogy követése, kutatása már csak célirányos eszközökkel és módszerekkel lehetséges. Míg korábban a nyilvános információk gyűjtése a titkosszolgálatok másodlagos feladatai közé tartozott, az információs forradalom terjedésével a tv-műsorok, webújságok, rádiók, blogok és közösségiportál-bejegyzések mind olyan hírforrássá alakultak, amelyeket megfelelő és módszeres szűrés segítségével hasznos adattá lehet formálni."[12] Mivel az OSINT nyilvánosan hozzáférhető információk elemzése útján nyer a kiinduló adatokhoz képest minőségileg újabb információkat, fel kell tennünk a kérdést, hogy a kizárólag nyílt forrásból származó adatok gyűjtése és továbbítása

1. lehet-e tényállásszerű a kémkedés vonatkozásában, valamint
2. minősülhet-e bűncselekményként kémkedésnek.

1. Az első kérdéssel kapcsolatban szét kell választanunk az adatgyűjtési és -elemzési fázist az adatok továbbításától. Pusztán nyilvánosan hozzáférhető adatbázisok elemzése, azokból adatok gyűjtése álláspontunk szerint büntetőjogilag teljesen semleges cselekmény még akkor is, ha például ennek révén minőségileg új információkhoz jut hozzá az adatbányászatot folytató személy. (Az internetre felkerült információk akkor is nyilvánosan hozzáférhető információknak minősülnek, ha egyébként minősített adatok is keveredhetnek vagy keverednek közéjük, gondoljunk itt csak a Wikileaks-kiszivárogtatással kapcsolatos botrányra.) Amennyiben a nyilvánosan hozzáférhető adatokból nyert információkat továbbítják idegen hatalom vagy idegen szervezet részére, akkor viszont már a tényállásszerűség megvalósulhat. Nem mindegy azonban, hogy milyen információkat és milyen idegen szervezet vagy hatalom részére továbbít az elkövető. Például nyilvánosan hozzáférhető orvosi, műszaki vagy tudományos adatok gyűjtése és továbbítása egy idegen kutatóintézetben dolgozó személy részére nem tényállásszerű. Tényállásszerű lehet viszont egy ellenérdekelt

[12] Resperger 2018, 138.

titkosszolgálat részére kormányzati, politikai vagy gazdasági információk gyűjtése, elemzése, feldolgozása és továbbítása.

2. A tényállásszerűség vizsgálata után a társadalomra veszélyesség és a bűnösség vizsgálata következik. A társadalomra veszélyesség meglétének bizonyítása ebben az esetben nem könnyű feladat. A cselekménynek sértenie vagy veszélyeztetnie kell Magyarország érdekeit. Ráadásul az elkövető sok esetben sikeresen hivatkozhat társadalomra veszélyességben való tévedésre is. A bűnösség körében a szándékosság bizonyítása szintén nehézséget jelenthet az eljáró hatóság számára: azt kell ugyanis bizonyítani, hogy az elkövető tisztában volt vele, hogy az általa gyűjtött információk magyar érdekeket sérthetnek, tudatában volt továbbá annak is, hogy idegen hatalom vagy idegen szervezet részére továbbítja azokat, és tudatában volt annak is, hogy ezzel a magatartásával potenciálisan kárt okoz vagy okozhat Magyarországnak.

A kémkedés tehát csak sokszorosan szűkítő feltételek alkalmazása mellet állapítható meg azon elkövetők terhére, akik kizárólag nyílt forrásból szerzik az információikat.[13] Nyílt forrású hírszerzés (OSINT) büntetőjogi üldözésére, és az elkövető megbüntetésére legfeljebb akkor látok gyakorlati lehetőséget a jövőben, amikor egy már lebukott kém esetében a minősített adatok átadását nem lehet ugyan bizonyítani, de azt igen, hogy az elkövető rendszeres kapcsolatban állt egy idegen szervezettel, és folyamatosan küldött a részére nyílt forrásból származó, de ugyanakkor általa megszűrt, elemzett információkat.

Felhasznált irodalom

Angyal Pál (1928): *Az állami és társadalmi rend hatályosabb védelméről szóló 1921: III. t.-c.* Budapest, Athenaeum.

Belovai István (1998): *Fedőneve: Scorpion.* Budapest, Szerzői kiadás.

Belovics Ervin – Molnár Gábor – Sinku Pál (2005): *Magyar büntetőjog. Különös rész*. Budapest, HVG-ORAC.

Büntetőjogi tankönyv II. Különös rész (1959). Budapest, BM Tanulmányi és Módszertani Osztály.

Kish, John (1995): *International Law and Espionage.* The Hague – Boston – London, Springer.

Resperger István szerk. (2018): *Nemzetbiztonsági alapismeretek.* Budapest–Pécs, Dialóg Campus.

Internetes forrás

www.mkih.hu/hivatal_hirszerzes.shtml (A letöltés dátuma: 2011. 10. 02.)

[13] A nyílt forrású hírszerzés büntetőjogi üldözése – ha ez nem csak egy limitált, szűk körre korlátozódik – felvetheti a különböző emberi jogok és a nemzetbiztonsági érdekek konfliktusát is. E témakörben kiváló elemzést tartalmaz a magyar származású szerző, Kiss János Ferenc monográfiája: Kish 1995.

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 50–67. • DOI: 10.32561/nsz.2019.2.5

Nyeste Péter[1] – Szendrei Ferenc[2]

Nyílt forrású információszerzés a bűnüldözésben

OSINT in Law Enforcement

A nyílt forrású információszerzés napjainkban nagyon fontos szerepet játszik a bűnüldöző hatóságok bűnmegelőzési és bűnüldözési tevékenységében. Ennek segítségével könnyebben feltérképezhetők a szervezett bűnözői tevékenységek, a bűnszervezetek felépítése, tagjai. Ugyanakkor a nyílt forrású információszerzés komoly segítséget tud nyújtani a már elkövetett bűncselekmények felderítésében és bizonyításában is. Írásunkban megvizsgáljuk a bűnüldözési célú nyílt forrású információszerzés jogi hátterét, módszertanának egyes kérdéseit és gyakorlati alkalmazását.

Kulcsszavak: bűnüldözési célú nyílt forrású információszerzés, szervezett bűnözés, bűnmegelőzés, OSINT-módszertan

Open Source Intelligence plays a very important role today in crime prevention and law enforcement. It helps to detect an organised criminal activity, the structure of criminal organisations and members. On the other hand, open source intelligence can hold a strong help for detecting and prove the crimes. In our paper, we will examine the legal background, practise and some methodology questions of the Criminal OSINT.

Keywords: criminal open source intelligence, organised crime, crime prevention, OSINT methodology

[1] Dr. Nyeste Péter egyetemi adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési és Gazdaságvédelmi Tanszék. ORCID-azonosító: 0000-0002-2440-6414.
[2] Dr. Szendrei Ferenc tanszékvezető egyetemi docens, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési és Gazdaságvédelmi Tanszék. ORCID-azonosító: 0000-0002-7890-913x.

Bűnüldözési stratégiák és az információszerzés és -értékelés

A bűnüldöző hatóságok bűnüldözési feladatai hagyományosan hármas felosztásúak lehetnek. Ezek a *megelőzés, a bűncselekmények megakadályozása és az elkövetett bűncselekmények felderítése, bizonyítása*.

A bűncselekmények, illetve az életvitelszerűen folytatott bűnözői tevékenységek megelőzésének a *közösségi rendészet* szerint fontos eleme a közterületi rendészeti erők látható jelenléte, de „önmagában azonban a megnövelt rendőri jelenlét bűncselekmény-csökkentő hatása nem igazolható meggyőzően".[3] Egyes tanulmányok szerint „10%-os rendőrijelenlét-fokozásnak 3%-os bűncselekmény-csökkentő hatása lehet a kisebb értékű vagyon elleni és azokhoz kapcsolódó bűncselekményekre",[4] de az erőszakos bűncselekményekre gyakorolt hatása már nem egyértelműen kimutatható. Az eseményorientált, reaktív rendészet kritikájaként és alternatívájaként dolgozták ki az 1970-es években a problémaorientált rendészet modelljét, amelyet gyakran SARA-modellnek[5] is neveznek, amely a bűnüldözési probléma megvizsgálását, elemzését, az azokra való célzott reagálást, illetve az eredmény értékelését jelenti. Ez a rendészeti modell azonban olyan komoly elemzőkapacitást igényel, amely nem feltétlenül áll arányban az elvárt eredménnyel. A *hírszerzésalapú rendészet* közelebbről fókuszál a bűnüldözésre, valamint a büntető igazságszolgáltatás eszközeire és céljaira. A definíció szerint a hírszerzésalapú rendészet a bűnügyi hírszerző elemzés szigorú döntéshozatali eszközként való alkalmazása azzal a céllal, hogy hatékony rendészeti stratégiákon keresztül előmozdítsa a bűncselekmények számának csökkenését és a bűnmegelőzést.[6] *A hírszerzésalapú rendészetet* sikeresen alkalmazzák az előforduló főbb bűnügyi problémák ellen, de önmagában nem elég hatékony az új bűnelkövetési minták, folyamatok feltárásában és a válaszlépések megfogalmazásában.[7] A bűncselekmények egyre kifinomultabb, konspiráltabb, szervezettebb elkövetése, a határokon átnyúló szervezett bűnözés terjedése miatt már több nagy rendőrség döntött úgy, hogy a hírszerzésalapú megközelítést rendészeti stratégiájának meghatározó részévé teszi. Erre az egyik legjobb európai példa az angol National Intelligence Model (Nemzeti Hírszerzési Modell).[8] A NIM strukturális kialakításának célja, hogy a megfelelő, aktuális információkat megosszák a teljes rendszer különböző szintjein (helyi, teljes szervezeti, nemzetközi). A gyakorlatban azonban problémákat jelent, hogy mely információkat osszák meg a felsőbb szintek irányába; a releváns információkat inkább a felsőbb szintekről az alsóbb szervek irányába terjesztik, és kevés információt kapnak a helyi szintektől.[9]

Mindegyik stratégiai rendészeti modellről elmondható, hogy kiemelkedő szerepet tulajdonít a beszerzett információk értékelésének és elemzésének, függetlenül attól, hogy élőerősen vagy technikai úton szerezték meg a releváns információt.

---

3 Bradford 2011.
4 Levitt 1997.
5 SARA: Scanning – vizsgálódás, Analysing – elemzés, Responding – reagálás, Assessment – értékelés.
6 Ratcliffe 2008.
7 Maguire 2008.
8 Szendrei 2018.
9 Maguire–John 2003.

Az OSINT (Open Source Intelligence – nyilvános forrású információszerzés) eredetileg az amerikai titkosszolgálatok által kifejlesztett módszer, amely az internet terjedésével általánossá vált nemcsak a titkosszolgálatoknál, hanem az üzleti élettől a kormányzati tevékenységig széles spektrumon.[10] A nyílt hozzáférésű információk a minősített forrásokat nem tudják kiváltani, de kiegészíthetik, ellenőrzöttebbé tehetik a minősített és egyéb forrásokból szerzett információkat, illetve azok megfelelő értékelést és elemzést követően önmagukban is felhasználhatók.

Az OSINT az alább felsorolt modern információszerzési módszerek közé tartozik, amelyek többsége jellemzően a katonai, nemzetbiztonsági területen használatos, néhányat azonban már a bűnüldözés is átvett és eredményesen használ.

- *HUMINT (Human Intelligence)* – emberi erőforrással folytatott hírszerzés;
- *SIGINT (Signal Intelligence)* – rádióelektronikai felderítés;
- *COMINT* (*Communication Intelligence*) – rádiókommunikációs felderítés;
- *ELINT (Electronic Intelligence)* – rádiótechnikai felderítés;
- *TELINT (Telemetry Intelligence)* – a telemetriai felderítés;
- *RADINT (Radar-transmitted Intelligence)* – a radarkisugárzás-felderítés;
- *CYINT (Cyber Intelligence)* – a kiberhírszerzés;
- *IMINT (Imagery Intelligence)* – képi felderítés;
- *MASINT (Measurement and Signitures Intelligence)* – a mérési és jelmeghatározó hírszerzés;
- *GEOINT (Geospatial Intelligence)* – a geoinformációs felderítés;
- *TECHINT (Technical Intelligence)* – technikai adatszerzés;
- *OSINT (Open-Source Intelligence)* – nyílt forrású információszerzés;
- *SOCMINT (Social Media Intelligence)* – közösségi hálózatokból folytatott információszerzés.

Az OSINT-információk forrásai a NATO[11] OSINT-kézikönyv[12] szerint:

- nyomtatott és elektronikus média;
- internet, deep web;[13]
- kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
- „szürke irodalom", a szűk körben hozzáférhető, nyomtatott és digitális dokumentumok, tanulmányok;
- tudományos előadások, konferenciák;
- személyes tapasztalatok;
- kereskedelmi műholdak felvételei;
- tudományos szervezetek, egyetemek.

Robert D. Steele, az Open Source Solutions[14] (OSS.Net) vezérigazgatója szerint „minősített forrásokból a felhasználható információ 20%-a szerezhető meg, amire a költségek

[10] Bálint 2018, 139.
[11] NATO: North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete.
[12] *NATO OSINT Handbook* (2001).
[13] Deep Web: „a láthatatlan web" az internet keresőmotorok részére nem indexelt adatai, szolgáltatása.
[14] Open Source Solutions: nyílt forású megoldások.

95%-át kell áldozni […] nyílt forrásokból a felhasználható információ 80%-a származik, amihez a költségek 5%-át kell felhasználni".[15]

Ezek az adatok jól jelzik, hogy milyen fontos szerepet játszhatnak mind a megelőzés, mind a bűncselekmények utólagos felderítése és bizonyítása során a nyílt forrásokból elérhető információk beszerzése és azok szakszerű értékelése-elemzése.

A társadalomban robbanásszerűen lezajló információs forradalom és az Y, Z generációk szokásainak változása gyökeresen megváltoztatta az információkhoz való hozzájutás és az információk, adatok feldolgozásának módját. Manapság már csak felületesen olvasunk át nagy terjedelmű anyagokat, illetve sokkal gyakoribb a téma szerinti rövid tartalmak gyors áttekintése, váltogatása. Becslések szerint a világ rohamosan növekvő lakossága 28%-ának (több mint 2 milliárd embernek) közvetlen hozzáférése van a *World Wide Webhez,* és közel 5 milliárd ember mobiltelefonnal rendelkezik. Minden nap átlagosan 247 milliárd e-mailt küldenek el. Ez a százalékarány minden évben 24%-kal növekszik.[16]

A bűnügyi célú OSINT alkalmazása hatékonyan, célirányosan segítheti a bűnügyi hírszerzést és a bűnügyi nyomozást folytató felderítők, nyomozók, vezetők döntéseit a rendvédelmi szerveknél.

Jogi háttér

Az Európai Unió 2010-ben elfogadott *belső biztonsági stratégiája*[17] kihívásokat, alapelveket és iránymutatásokat fogalmazott meg. A stratégia alapján az elkövetkező években a következő legsürgetőbb kihívások megválaszolása áll az EU biztonsága, a hírszerző, elhárító, bűnüldöző szervezetek előtt: *embercsempészet, kábítószer- és lőfegyvercsempészet, pénzmosás, valamint illegális hulladékszállítás és -lerakás Európán belül és kívül, hamisított vagy veszélyes áruk értékesítése, terrorizmus, számítástechnikai bűnözés, határbiztonság.*

Ezek a cselekmények szervezett bűnözői csoportok működését feltételezik, amelyek elleni hatékony fellépésnek összehangoltnak, európai szintűnek kell lennie.

Az Európai Unió Belső Biztonsági Stratégiája által megfogalmazott főbb célkitűzések:

- nemzetközi bűnözői hálózatok felgöngyölítése;
- a terrorizmus, radikalizálódás és toborzás megelőzése;
- a virtuális tér biztonságának növelése a polgárok és vállalkozások számára;
- a biztonság megerősítése a határigazgatás útján;
- Európa válságokkal és katasztrófákkal szembeni ellenálló képességének javítása.

A stratégia szerint a *megelőzés és előrejelzés proaktív, hírszerzésen alapuló felderítést, megközelítést feltételez.*

A rendőrségi törvény 2018-ban hatályba lépett módosítása az úgynevezett *rendészeti célú titkos információgyűjtést* a büntetőeljárási törvény leplezett eszközeinek

[15] Kenedli 2013, 183–193.
[16] Rolington 2015.
[17] 5842/2/2010 tanácsi dokumentum: Az Európai Unió belső biztonsági stratégiája: Az európai biztonsági modell felé.

fogalmához igazítva határozta meg, és ez alapján olyan, a magánlakás sérthetetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő alapvető jogok korlátozásával járó, a rendőrség által végzett különleges tevékenységként jellemzi, amelyet a rendőrség erre feljogosított szervei az érintett tudta nélkül végeznek. Amennyiben konkrét bűncselekményre vonatkozó információk merülnek fel, illetve a titkos információgyűjtés során végzett értékelő-elemző munka végtermékeként ilyen értékelt információ kerül előállításra, akkor azok további ellenőrzése már csak büntetőeljárási törvény által szabályozott keretek között kerülhet sor hagyományos vagy *leplezett eszközök*, nyomozási tevékenységek végrehajtásával.

A rendőrségi törvény a *bűnmegelőzési tevékenységet olyan bűnügyi hírszerző tevékenységként határozza meg*, amelynek tárgya nem egy adott bűncselekmény, hanem a Magyarország társadalmi rendjét veszélyeztető *bűnözés*. Az indokolás szerint a rendőrség információszerző, -értékelő, kockázatelemző tevékenységének eredményéhez tartozik a rendőrség intézkedési kötelezettsége is, amelynek része lehet egy adott bűncselekmény elkövetésének megakadályozása is. Definiálták a bűncselekmények megelőzését mint a titkos információgyűjtés egyik lehetséges célját, és az annak eléréséhez alkalmazható intézkedések meghatározására *lépcsőzetesen került sor.*

A törvényben elsőként egy általános bűnmegelőzési fogalom- és feladatrendszert határoztak meg, amely az úgynevezett értékelt-elemzett bűnüldözési információkon alapuló rendészet *(intelligence-led policing)* modelljének megfelelő működést feltételez.

A törvény szerint a rendőrség az alaptörvényben, az ágazati törvényben és törvény felhatalmazása alapján más jogszabályban meghatározott bűnmegelőzési, bűnüldözési, államigazgatási és rendészeti feladatkörében végzi a bűncselekmények megelőzését, amelynek során *figyelemmel kíséri Magyarország bűnügyi helyzetét, feltárja a bűncselekmények elkövetésének kockázatait, a bűncselekmények elkövetésére irányuló törekvéseket, továbbá megszerzi, elemzi, értékeli, ellenőrzi és továbbítja a bűnözéshez kapcsolódó, a bűncselekmények megelőzése, illetve megakadályozása céljából szükséges információkat.*

Ez az általános célú, ágazati bűnmegelőzési feladatrendszer jelenti a rendőrség stratégiai és taktikai[18] hírszerzésének alapját, amely nem kifejezetten csak bűnügyi irányultságú, hanem más szolgálati ágak információit is becsatornázza és egyben a hírigényeiket is kielégíti.

Az általános bűnmegelőzés célrendszerében alkalmazható intézkedéseken túl szűkített feltételek fennállása esetén vehetők igénybe a titkos információgyűjtés ágazati törvényben szabályozott, bírói engedélyhez nem kötött lehetőségei.

A törvény 65. § (1) bekezdésében szereplő normatív szempontrendszer rögzíti, hogy bűncselekmény elkövetésének megelőzése céljából csak akkor folytatható titkos információgyűjtés, ha *megalapozottan feltehető,* hogy attól a bűnözésre vonatkozó olyan információk megszerzése várható, amelyek elemzése és értékelése révén feltárhatók a bűncselekmények elkövetésére irányuló törekvések, és lehetővé válik a bűncselekmények megelőzése, illetve megakadályozása.

[18] Nyeste 2013.

Ezzel a titkos információgyűjtés egyszerűbb, a jogkorlátozásra kevésbé alkalmas eszközei is csak indokolás alapján működtethetők.

A legsúlyosabb jogkorlátozó, bírói engedélyhez kötött titkos információgyűjtési lehetőségeket csak a szervezett bűnözéssel szembeni fellépés során engedi meg a törvény bűnmegelőzési céllal.

A jogalkotó elképzelései alapján a jogalkalmazó szervek pontosan definiált bűnmegelőzési célokból folytathatnak titkos információgyűjtő tevékenységet. A bűnmegelőzési tevékenység mint a rendészet egyik jövőbeli stratégiai célja, detektálja a bűncselekményeket kiváltó okokat, deviáns magatartásokat, a bűnözés állapotát monitorozza, amelynek során egy fontossági sorrend alapján feladatrendszert állítanak fel, tevékenységük célpontjait, irányait meghatározzák. Ebben komoly szerepet játszhat a rendőrség nyílt forrású információszerzési tevékenysége. A rendőrségi törvény alapján folytatott nyílt forrású információszerzés céljai lehetnek többek között a szervezett bűnözői csoportok, terrorista csoportok feltérképezése, a csoport tevékenységében fontosabb szerepet játszó személyek beazonosítása, kapcsolatrendszerük feltárása, tartózkodási helyük megállapítása, elérhetőségeik, kommunikációs eszközeik, csatornáik feltárása. A rendvédelmi szervek (és a titkosszolgálatok) által folytatott bűnöző szervezetek felépítésének megismerésére és azok bomlasztására irányuló titkos információgyűjtő tevékenység az Európai Unióban már régóta elfogadott és alkalmazott tevékenység.[19]

Svédországban 2009 óta egy integrált megközelítést[20] alkalmaznak a szervezett bűnözés megelőzése és az ellene való fellépés érdekében, amelynek módszertana az úgynevezett bűnügyi arborisztikus módszer,[21] amely a kertészetben alkalmazott metszési módszerek ellentéteként fogható fel, mivel a bűnügyi fakertészeti módszer lényege nem a gyenge részek eltávolítása, hanem éppen ellenkezőleg, a bűnözői szervezet kulcsfontosságú személyei ellen irányul. A módszertan lényege szerint a bűnözői csoportok felépítését, kapcsolatrendszerét kell tanulmányozni elsősorban, a belső magot alkotó stratégiai fontosságú személyeket kell beazonosítani (képességeik és fontosságuk alapján) és „kimetszeni" a bűnözői hálózatból, ezzel elérhető a bűnözői csoportok meggyengítése és végső soron felszámolása. A módszer alkalmas stratégiai és taktikai célok segítésére egyaránt. A módszer alkalmazásának elsődleges céljai:

- a „rejtőzködő" stratégiai fontosságú személyek beazonosítása, az információgyűjtés és -elemzés számára egy közös struktúra megalkotása, a belső magot alkotó stratégiai személyek képességeinek a feltérképezése, az eddig ismeretlen bűnöző személyek gyorsabb beazonosítása telefonlehallgatás, helyiséglehallgatás, megfigyelés segítségével;
- az együttműködő személyek kiválasztásánál stratégiai információk nyújtása az információk forrásainak az értékeléséhez, továbbá segítséget jelent az együttműködők információkhoz való hozzáférési lehetőségeinek értékelésénél;
- objektív alapokat teremt a döntések és a fontossági sorrendek felállításakor, összekapcsolja a stratégiai elképzeléseket a műveleti munkával, a kiválasztott

[19] Nyeste 2012, 28.
[20] Balláné Füszter – Szendrei szerk. 2011, 133.
[21] Nilval–Mattson 2016, 83.

személyek ellen irányuló intézkedések hatásának előrejelzését segíti, valamint a visszacsatolást segíti a strukturált felépítésű jelentések és a beavatkozással kapcsolatos hatások értékelése.

A rendőrségi törvény a bűnmegelőzési célból végezhető bírói engedélyhez nem kötött titkos információgyűjtés eszközeinek sorában nevesíti az elektronikus hírközlési eszközön vagy információs rendszeren folytatott kommunikáció tényének a megállapításához, az elektronikus hírközlési eszköz vagy információs rendszer azonosításához, illetve hollétének megállapításához szükséges adatok megszerezését, amelyek alkalmazására sor kerülhet a nyílt forrású információszerzés adatainak értékelése alapján is. Az ilyen információszerzés végrehajtása a rendőrségi törvényben meghatározott bármelyik bűnüldözési feladatot elősegítheti, az információk ellenőrzöttebbé tételével, megalapozásával, kiegészítő információk beszerzésével. Ez a tevékenység végezhető akár az általános bűnüldözési feladatok ellátása során, vagy a törvényben nevesített titkos információgyűjtési célokból, mint személybiztosítás, létesítményvédelem, fedett nyomozó védelmét szolgáló, tanúvédelmi tevékenység, vagy akár a körözési munka elősegítése is.

A konkrét bűncselekmények felderítését és bizonyítását is nagymértékben elősegítheti a nyílt forrású információszerzés, támogatja az elkövetett cselekmény elkövetési helyének, módjának megállapítását, a cselekménnyel összefüggésbe hozható helyek felkutatását, az elkövetéshez használt eszközök felderítését, a lehetséges motivációk, az elkövetést lehetővé tevő körülmények megállapítását, bizonyítékok beszerezhetőségét.

A nyílt forrású információszerzés mellett számos egyéb felderítési lehetőség áll a bűnüldöző hatóságok rendelkezésére, amellyel a beszerzett információkat ellenőrizhetik, kiegészíthetik azokat. A bűnüldöző hatóságok adatszerző tevékenységet folytathatnak a büntetőeljárás szabályai szerint, de konspirált módon titkos megfigyelést vagy a büntetőeljárásban rejtett figyelést folytathatnak, konspirált módon koncentrált adatgyűjtést végezhetnek környezettanulmány formájában, vagy együttműködő személyeket, fedett nyomozót alkalmazhatnak, vagy amennyiben feltételei adottak, lehallgatást végezhetnek a célszeméllyel, büntetőeljárásban gyanúsítottal szemben.

Az alkalmazható *OSINT-eszközök:*

- innovatív adatbányászati és adatelemzési módszerek,
- intelligens nyelvészeti alapokra épülő keresési módszer,
- intelligens keresőmotorok,
- tematikus leválogató rendszer (például RSS-csatornák figyelésének automatizálása),
- közösségi oldalak figyelése (például flashmobok azonnali kockázati értékelése),
- honlapok forráskódjának értékelése, rejtett tartalmak megjelenítése,
- domain search, whois tools (a honlap domain-előfizetőjéhez kapcsolható adatok kinyerése),
- magyar és nemzetközi sajtófigyelés.

Fontosabb OSINT-területek:

- internetes hírek,
- szürke irodalom,
- közösségi háló,

- hagyományos média,
- nyílt adattárak,
- nyilvántartások (például Céginfo, Takarnet).[22]

Becslések alapján a világhálón 15 milliárd és 1 trillió közötti oldal található. A legtöbb népszerű és leggyakrabban alkalmazott keresőprogram – mint a Google – a teljes webadatok tartalmának csak a 3–4%-át fésüli át, mivel azok csak a megszerkesztett weboldalakat figyelik. A fennmaradó tartalom (96–97%) a világháló mélyebb részéhez, a deep webhez tartozik, ahol a webtartalom csak adatokat és nem szerkesztett oldalakat tartalmaz. Utóbbiak csak meta-keresőprogramokkal, kulcsszavakra történő kereséssel érhetőek el (például Chunkit, Kayak, DeeperWeb, Dogpile, MetaLib).

Több tagállam, ország felismerve a nemzetbiztonsági szolgálatok és a rendvédelmi szervek információi megosztásának egyre égetőbb szükségességét, valamint a koncentrált információszerzés előnyeit, úgynevezett fúziós központokat hozott létre az információk összegyűjtése, elemzése, értékelése érdekében. A Nemzeti Biztonsági Stratégia[23] megfogalmazza, hogy minden kormányzati intézmény feladata, hogy saját szakterületén folyamatosan értékelje a nemzeti és nemzetközi biztonság és fenyegetettség elemeit, és megtegye a szükséges lépéseket azok kezelésére és elhárítására. A stratégia külön kiemeli a nemzetbiztonsági szolgálatok és a bűnügyi hírszerzés biztonságpolitikai stratégiai feladatait.

A stratégiai hírszerzési és elhárítási célok eléréséhez szükséges, hogy rendelkezésre álljanak a terrorizmusra, a szervezett bűnözésre, az egyéb illegális tevékenységek jelentette aszimmetrikus fenyegetésekre, más globális, regionális és belső kihívásokra vonatkozó információk. A Nemzeti Biztonsági Stratégia meghatározza, hogy a Magyarországot érintő biztonsági kihívásoknak megfelelően – a hazai szervek koordinált tevékenysége mellett – szorosabb együttműködést kell kialakítani és fenntartani a szövetséges államok hírszerző és elhárító szervezeteivel, valamint az egyes kérdésekben hasonló biztonságpolitikai célokat követő más államok szolgálataival. A stratégia meghatározza, hogy a nemzetközi kapcsolatokat is fel kell használni *az új bűnügyi trendek feltérképezésére, az új bűnözési jelenségek megismerésére, a legjobb gyakorlatok átvételére.*

A fenti alapdokumentumok egy folyamatos, átfogó, koordinált stratégiai tervezést és annak részeként megjelenő hírszerzési képességet fogalmaznak meg a nemzetbiztonság és a bűnüldözés területén is.

A nemzetbiztonsági és bűnüldözési felderítési információk megosztási csatornájaként 2001. január 1-jei hatállyal létrejött a Szervezett Bűnözés Elleni Koordinációs Központot (SZBKK). A központ alapfeladata volt a szervezett bűnözés megelőzésének, megszakításának, felderítésének elősegítése a *nemzetbiztonságok és a rendvédelmi* szervek által szolgáltatott adatok gyűjtése, feldolgozása, elemzése és a szolgáltató szervezetek részére történő visszacsatolás által, valamint a szervezett bűnözés elleni fellépéshez szükséges kormányzati döntések információs igényének a kielégítése. Majd 2011-ben a Nemzeti Információs és Bűnügyi Elemző Központról szóló

[22] Bálint 2018, 139.
[23] A kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról.

törvénytervezet[24] sikertelen benyújtását követően 2016. július 15-i hatállyal létrejött egy új polgári nemzetbiztonsági szolgálat, a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK) a SZBKK jogutódjaként.

A központ új feladatává vált a légitársaságok által továbbított utasnyilvántartási adatok kezelése, valamint elemzése és értékelése, összhangban az uniós adatvédelmi előírásokkal. Továbbá a TIBEK feladata a nemzetbiztonságot, bűnüldözést, közbiztonságot vagy más alapvető biztonsági érdeket sértő adatok feldolgozásának, elemzésének eredményeként a lehető legátfogóbb kép összeállítása az ország terror-, illetve esetleges más fenyegetettségéről, a belső biztonsági helyzetről, a közbiztonság állapotáról. Minderről tájékoztató rendszert működtet, értékelő jelentéseket készít, és azokat a miniszter útján eljuttatja a kormánynak.

A TIBEK az együttműködő szervek nyomozási és felderítő tevékenységét a *titkos információgyűjtések és a büntetőeljárások kezdeti stádiumától taktikai szinten támogatni tudja, valamint eljárást kezdeményező indító jelzéseket, elemzéseket adhat, készíthet*.

A TIBEK információfúziós és elemző-értékelő tevékenységével a bűnüldözési hírszerzési és speciális, leplezett nyomozási feladatokat is egyaránt segíteni tudja. Továbbá a kiemelt bűncselekményi körbe tartozókon túl feldolgoz olyan bűncselekményeket is, ahol az elkövető személye vagy a bűncselekmény társadalomra veszélyessége, illetve a cselekmény gyakori ismétlődése miatt az azokkal összefüggő adatok elemzése, értékelése indokolttá válik. Ezzel a tevékenységgel nemcsak a speciális, leplezett nyomozási tevékenységeket igénylő bűncselekményeket, hanem az egyszerűbben felderíthető, de komolyabb elemzést igénylő ügyek felderítését is segíteni tudja.

A *Terrorelhárítási Információs és Bűnügyi Elemző Központ* folyamatosan vizsgálja Magyarország *biztonsági és bűnügyi helyzetét*, elemzi Magyarország nemzetbiztonsági, bűnügyi és terrorfenyegetettségi helyzetét.

A Terrorelhárítási Információs és Bűnügyi Elemző Központ támogató, koordinációs elemző-értékelő tevékenysége során elemző, tájékoztató és koordinációs tevékenysége kiterjed az együttműködő szervek hatáskörébe és illetékességébe utalt valamennyi információra. *Nyílt információgyűjtést és -feldolgozást végző szolgáltató és támogató szervet működtet (OSINT-központ).*

Ezzel a feladattal létrejött a központi bűnügyi OSINT szervezeti eleme, jelenleg főosztályi szervezeti formával végzi feladatait, nyújtja szolgáltatásait.

„A hazai és külföldi blogok, hírforrások figyelése, értékelése és elemzése révén a központi OSINT képes kiszűrni például:

– A legújabb dizájnerdrogok fejlesztésének várható irányait (kockázatos vegyületek), a terjesztői online hálózatokat, a célközeget, a terjesztés lehetséges online vagy valós helyszíneit (chat, blog).

– A radikalizálódás folyamatában a kockázati szintekben történő változásokat, csoportképződési kezdeményezéseket.

– Vagyonvisszaszerző tevékenysége során olyan, már látókörbe került szervezett bűnözői csoportok vagyoni helyzetének változását, amelyek kivonni igyekeznek a bűnös profitot a hatóságok látóköréből.

[24] T/5004. törvényjavaslat egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról.

– A hazai és külföldi bűnszervezetek közötti kapcsolatokat, a bűnelkövetésből származó pénzek mozgását.

– A központi OSINT egyik feladata a külföldi törvényhozás azon szegmensét érintő változások figyelése, amely hatással van a magyar társadalmat veszélyeztető bűncselekmények megjelenésére."[25]

Magyarország nemzetbiztonsági, *terrorfenyegetettségi és bűnügyi helyzetével*, ezek meghatározott elemeivel, konkrét kockázatokkal vagy bűncselekményekkel kapcsolatos *tájékoztató jelentéseket, háttér- és kockázatelemzéseket készít az együttműködő szervek* részére a hatáskörükbe tartozó feladatok törvényes, szakszerű és eredményes ellátásának elősegítése céljából.

Feltárja az együttműködő szervek által folytatott *párhuzamos adatkezeléseket,* különösen a több együttműködő szerv által ugyanazon bűncselekmény, személy vagy egyéb tárgykör vonatkozásában párhuzamosan folytatott titkos információgyűjtéseket, illetve az ugyanazon bűncselekmény miatt párhuzamosan folytatott nyomozásokat, és ezekről tájékoztatja az érintett együttműködő szerveket.

- *Figyelemmel kíséri a bűnszervezetek és terrorszervezetek*, valamint *a szervezett bűnözői és terrorista csoportok tevékenységét,* az ilyen szervezetek és csoportok egymáshoz való viszonyát, kapcsolatait; jogsértő módon szerzett vagyonuk, illetve az ilyen vagyon jogsértő eredetének leplezésére irányuló törekvéseik és az ilyen célt *szolgáló vállalkozásaik elemzésével segítséget nyújt az ellenük való fellépéshez*.
- A Terrorelhárítási Információs és Bűnügyi Elemző Központ ellátja az *utasadat-információs egység feladatait.*

Az OSINT módszertana[26]

Az OSINT hírszerzési ciklus módszertana a szakirodalom alapján négy elemre osztható: az információk begyűjtése, feldolgozása, szövegösszefüggésbe helyezése, osztályozása és megosztása.

Az első szakaszban történik *a potenciálisan hasznos, releváns információtartalmak beazonosítása és azok begyűjtése.* Ez a szakasz erőteljes számítástechnikai támogatást igényel. A hírszerzési igényeknek megfelelő információk prioritási sorrendjének megfelelő információk kinyerése, leválogatása történik. A modern demokratikus társadalmakban a szolgáltatók által tárolt személyes adatokhoz való hozzáférés számos jogi akadályba ütközik, ezért azok összegyűjtése még bűnügyi célú felhasználás esetén is időigényes vagy nem lehetséges.

A hírszerzési ciklus második fázisa az összegyűjtött adatok *feldolgozása*, azok értékelése, az elemzés számára hasznosíthatóvá tétele. Ennek két eleme van: az információk, adatok *lefordítása és azok összesítése*. Ezek nem feltétlenül kell, hogy kövessék egymást, de segítséget nyújthatnak ebben a fázisban. Az *összesítés* kritikus pontja

[25] Bálint 2018, 253.
[26] Williams–Blum 2018.

a ciklusnak, mivel itt csökkentik az adattartalom méretét, és a fordított tartalmakat egybeillesztik.

A számítógépes szakembereknek nehézséget okozhat annak pontos megállapítása, hogy melyik adatbázisokból gyűjtötték össze a kinyert, összesített adatokat, hogy azok tartalmát hitelesíteni tudják, és megfelelő szövegösszefüggésbe helyezik. Az elemzés a következő fázis, amely során meg kell állapítani a kinyert információ helyességét, valós értékét. Az elemzésnek három szakasza van: hitelesítés, hitelesség értékelése, szövegösszefüggésbe helyezés.

Az *OSINT-termék megosztása* a végző fázisa a ciklusnak. Itt már gyakran a beszerzett és elemzett információk a többlettartalom miatt belső felhasználású vagy minősített információknak minősülnek és az arra jogosult személyek részére továbbíthatóak.

Az OSINT-metodika eszközei: *a lexikális elemzés, hálózatelemzés, térinformatikai elemzés,* illetve ezek kombinációi.[27]

A lexikális elemzés a nyílt forrású elemzés legerőteljesebb eszköze, amely során a különböző forrású és nagy mennyiségű szöveges tartalmak egyidejű elemzése történhet. Az alapszintű lexikális elemzés megmutatja a keresőmotorokon leggyakrabban használt kifejezéseket, legtöbbet keresett tartalmakat.

A közösségihálózat-elemzés segítségével felderíthetjük a személyek kapcsolatrendszerét, a hálózatelemzés a csomópontokra összpontosít, a külső és belső körök, kapcsolatrendszerek feltárására. A csomópontok közötti kapcsolatok száma, az interakciók sűrűsége a személyek fontosságát, információszerzési lehetőségeit határozhatja meg. Ennek segítségével megállapíthatók a kulcsfontosságú személyek és a lehetséges támadási pontok.

Térinformatikai elemzés az új közösségimédia-platformokra alapozott, a használók eszközeinek, terminéladatoknak felhasználásával kinyert térinformatikai elemzés – kombinálva az előbbi lehetőségekkel – gazdagabb képet tud nyújtani a célszemélyről, az elkövetőről, és bizonyítékként is felhasználhatók a kinyert adatok.

Bűnügyi OSINT a gyakorlatban

Az OSINT alkalmazási lehetőségei gyakorlatilag bármilyen bűnügyi rendőri tevékenységben tetten érhetők. Segítheti, illetve eredményei felhasználhatók lehetnek bármelyik büntetőeljárásban, illetve titkos információgyűjtésben, ugyanakkor speciális elemző-értékelő feladatként is megjelenhet, ahol a már összegyűjtött információk további feldolgozása is megtörténik.

A rendőrség keretein belül az alábbi szervezeti egységeknél találhatunk feladatszerűen OSINT-tal foglalkozó munkatársakat:

- ORFK Bűnügyi Főigazgatóság Bűnügyi Elemző-értékelő Főosztály
- ORFK Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály
- ORFK Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyonvisszaszerzési Hivatal

[27] Nyeste 2019.

A Bűnügyi Elemző-értékelő Főosztály esetében a vezetői döntéseket előkészítő elemzésekhez, a bűnügyi-közbiztonsági helyzet felméréséről szóló jelentésekhez, a bűnügyi munkához, kiemelten a büntetőeljárásokhoz kapcsolódó elemző-értékelő tevékenységhez használhatják fel a nyílt forrásból származó információkat.

A másik két egység ennél speciálisabb feladatként végez OSINT-ot:

- A Kiberbűnözés Elleni Főosztály a hatáskörébe tartozó bűncselekmények felderítése és nyomozása során szükségszerűen használja az internet adta lehetőségeket, így a nyílt forrású információszerzést is. Ugyanakkor a szakterületen meglévő speciális ismereteiknek köszönhetően sok esetben más szervek felkérése, megkeresése alapján szolgáltatnak OSINT-tal beszerzett információkat.
- A Vagyonvisszaszerzési Hivatal saját eljárásaiban, illetve más szervek felkérésére is végez nyílt forrású információszerzést a bűncselekményekből származó vagy igazolatlan eredetű vagyon feltárása és végső soron elvonása érdekében.

Természetesen a fentiek nem jelentik azt, hogy ezeken kívül, más egységeknél vagy gyakorlatilag akár a teljes bűnügyi rendőrségnél ne beszélhetnénk nyílt forrású információszerző tevékenységről. Saját ügyeiben, saját keretei között, saját ismereteinek megfelelően minden nyomozó és vizsgáló, tudatosan vagy kevésbé tudatosan, de használja az OSINT lehetőségeit.

Ugyanakkor azzal is tisztában kell lennünk, hogy bár legtöbben és leggyakrabban az internettel és a közösségi oldalakon történő kutatással azonosítják az OSINT-ot, valójában számos más, korábban kifejtett OSINT-megoldás, -módszer és lehetőség is létezik.

Másrészről azt is látni kell, hogy önmagában az OSINT sem old meg minden problémát, nem helyettesíthet más felderítési módszereket, információgyűjtő tevékenységeket, annak ellenére, hogy információs társadalmunkban szinte alapelvárás, hogy valaki a virtuális térben is létezzen, folyamatosan jelen legyen ezeken az oldalakon, posztoljon, blogoljon, fényképeket töltsön fel.

Látnunk kell azt is, hogy ezek a közösségi hálók sem változatlanok, sőt az is folyamatosan változik, hogy éppen mi számít trendinek, mit használ a többség. Természetesen nyelvi és földrajzi jellemzők alapján is lehet sorrendeket és kedvenceket találni, ami nálunk a Facebook, az Oroszországban a VK, Kínában a RenRen, a Sina Weibo, QZone, és ezek csak a legnagyobbak, ezeken kívül több mint 250 olyan közösségi (szociális) oldal működik, amelynek több százezer tagja, követője van, amelyek között vannak egészen speciálisak is, gondoljunk csak például arra, hogy az FBI most kezdte el használni azokat a DNS-adatbázisokat a nyomozásaihoz, amelyeket családkutató és egyéb célokból hoztak létre, és gyakorlatilag bárki által hozzáférhetők.

Milyen felderítési célok elérésére, milyen információs igény kielégítésére lehet alkalmas az OSINT?

A célszemély beazonosítása: az eljárások kezdeti szakaszában viszonylag kevés információ áll a nyomozó hatóság rendelkezésére, általában nem rendelkeznek a célszemély pontos személyi adataival. Ami rendelkezésre áll, azok jellemzően nevek, lakcímek, IP-címek, domainnevek, telefonszámok, felhasználónevek és e-mail-címek ömlesztve. Ebben az esetben segítséget jelenthetnek azok a netes oldalak vagy szoftverek, amelyek ilyen töredékadatokból is képesek teljes személyiséget összeállítani azáltal, hogy végigböngészik az internetet és összekapcsolják az ott feltalálható töredékinformációkat. Eljuthatunk a célszemély valamely közösségi oldalához, ahol nagy valószínűséggel találunk róla fényképet, illetve további adatokra is szert tehetünk.

Ilyen oldalak például:

- numberingplans.com – telefonszám alapján,
- imei.info – IMEIszám alapján,
- sync.me – telefonszám alapján,
- sudo app – valódi személy keresése,
- pointofmail.com – e-mail-alapú keresés,
- pipl.com – név-, e-mail-, felhasználónév-, telefonszám-alapú keresés.

A célszemély életvitelszerű tartózkodási helyének megállapítása: amennyiben a célszemély, elkövető lakóhelye, tartózkodási helye ismeretlen, közösségi oldalakon találhatunk olyan fényképeket, bejegyzéseket, amelyekből következtethetünk valamilyen földrajzi helyre, címre. Egy lakás teraszán pózoló és a kilátásban gyönyörködő célszemélyről készült fénykép segíthet a cím meghatározásában. Egy eseményről szóló bejegyzés, például egy vendéglátóhelyről szóló értékelés szintén segíthet valamely cím beazonosításában, és más, akár leplezett eszközök alkalmazásával a célszemély tartózkodási helyének megállapításában. Ugyanakkor egy célszemély által használt IP-cím azonosítása is közelebb vihet minket a kívánt lakóhely azonosításához (például iplogger.com – IP-cím keresése).

A célszemély családi körülményeinek, kapcsolatrendszerének feltérképezése: a célszemély életkörülményeinek teljes körű feltérképezéséhez elengedhetetlen, hogy családi körülményeit és egyéb kapcsolatait is megismerjük. Ez később akár tettestársak, orgazdák és egyéb, a bűncselekmény elkövetésében közreműködő személyek azonosításához is vezethet. A közösségi hálókon megjelenő képek, a különböző családi eseményeket megörökítő fényképek, a haveri bulikon, kocsmázáson, fesztiválokon készített fényképek, a sporteseményeken, koncerteken, nyaraláson, vagy akár horgászat közben készített képek valóságos aranybányát jelentenek egy jószemű OSINT-elemzőnek. Természetesen a fényképeken lévők beazonosítása rengeteg időt és energiát igényel, vagy további OSINT-lehetőségek felhasználásával, vagy egyéb rendelkezésre álló nyilvántartások igénybevételével, illetve más eszközök segítségével beszerzett információk is szükségesek a kérdéses személyek azonosításához.

A célszemély munkahelyének, munkakörének megállapítása: feltéve, hogy célszemélyünk dolgozik valahol, és más rendelkezésünkre álló adatbázisok (például

a NAV nyilvántartásai) nem hoztak eredményt, ismét fordulhatunk a nyílt források segítségével összegyűjthető információkhoz. A fentiekben említett kapcsolatrendszer feltérképezése is hozhat valamiféle munkahelyi, munkatársi információkat, a közös munkahelyi összetartásokon, továbbképzéseken készült képek, a munkahelyen pózolós fényképek közelebb vihetnek a szükséges információk megszerzéséhez. Ugyanakkor a különböző internetes oldalakon tett bejegyzések, like-ok szintén utalhatnak valamiféle foglalkozásra, munkahelyre.

A célszemély vagyoni helyzetének feltérképezése: a büntetőeljárás egyik legfontosabb feladata, hogy megállapítsa a bűnös tevékenységből származó vagyon nagyságát, meghatározza annak pontos helyét, és ezáltal elősegítse annak későbbi elvonását, a vagyoni reparációt. Az elkövetők oldaláról ezzel szemben természetes törekvésként jelentkezik, hogy a bűncselekményből származó vagyonukat, pénzüket elrejtsék, azokat más forrásból származónak vagy más személyhez tartozónak tüntessék fel, ugyanakkor él bennük az az igény is, hogy vagyoni helyzetüket másoknak is megmutassák, ezáltal is hangsúlyozva társadalmi pozíciójukat, összeköttetéseiket, magas életszínvonalukat. A célszemély közösségi oldalain megjelenő ingatlanokról, gépjárművekről, hajókról, magánrepülős utakról, nyaralásokról, költséges hobbikról szóló, azokat bemutató fényképek nyújthatnak segítséget egy vagyoni háttérnyomozáshoz. Ennek legjellemzőbb példája talán a dél-amerikai drogkereskedőkről készült, az interneten fellelhető fényképek, ahol rengeteg ékszerrel, (arany)fegyverekkel, egzotikus állatokkal, nagy teljesítményű autókkal, hajókkal, repülőkkel szerepelnek a különböző bandák tagjai. A napjainkban divatos kriptovaluták, illetve bizonyos pénzügyi aktivitás is nyomon követhető az OSINT lehetőségeivel.

A célszemély szabadidős tevékenységének, nézeteinek felderítése: a kapcsolatrendszer feltérképezésének részeként juthatunk ilyen információk birtokába is. A hobbija, szabadidős tevékenysége utalhat vagyoni helyzetére, adhat egyfajta kapcsolati hálót. A célszemély nézeteinek, esetlegesen szélsőséges vallási vagy politikai hitvallásának megismerése is fontos feladat lehet, különösen bizonyos speciális felderítési területeken (lásd: terrorelhárítás). Ezekre utalhatnak a célszemély által kedvelt oldalak, ezeken az oldalakon vagy egyéb blogokon tett bejegyzések, amelyeket leginkább a különböző speciális keresőmotorok használatával, illetve a lexikális elemzés módszerével ismerhetők meg. Adott esetben bizonyos zárt csoportokba bejutás, az ott zajló kommunikáció megismerése vagy speciális leplezett eszközök, fedett nyomozó felhasználását, vagy valamiféle pszeudoszemélyiség létrehozását és felhasználását igényelheti a felderítő szervektől.

A *célszemély speciális ismereteinek, az általa használt eszközök körének megállapítása:* bizonyos speciális ismereteket feltételező és speciális eszközigényű bűncselekmények nyomozása során fontos lehet annak bizonyítása, hogy az elkövető (gyanúsított) rendelkezik a szükséges ismeretekkel, és rendelkezésére álltak a megfelelő eszközök is az elkövetéshez. Ez eredhet egyrészt a már feltárt munkaköréből, foglalkozásából, de más webes információkból, adatokból is, például a célszemély a műhelyében készült fényképen látható, és a háttérben az adott eszköz is a képre került.

Az érintett helyiség felderítése, alkalmazható technológiák meghatározása: egy házkutatás vagy valamely más nyomozási cselekmény előkészítése során, vagy

a titkos kutatást, illetve a hely titkos megfigyelését megelőzően fontos lehet, hogy előzetesen információkkal rendelkezzünk az adott helyről. Ebben segítségünkre lehetnek az adott helyiségről készült és a közösségi oldalakra feltöltött fényképek, lakáshirdetések, az ezekben megjelenő alaprajzok, a kivitelező által közzétett alaprajzok, látványtervek, fényképek.

Az elkövetett cselekmény elkövetési módjának megállapítása: Magyarországon talán még nem jellemző, hogy az elkövetők az elkövetésről töltsenek fel képeket, videókat a közösségi hálóra, de egyes (mexikói) kábítószerkartelleknél már láthattunk ilyet, amikor elsősorban megfélemlítési célból tettek fel fényképeket az általuk elkövetett emberölésekről (kivégzésekről), vagy akár a terrorszervezetek kivégzéseiről a videómegosztó oldalakra felkerült videók esetében.

A cselekménnyel összefüggésbe hozható helyek felkutatása, az elkövetéshez használt eszközök felderítése: elsősorban ismeretlen bűncselekmény-helyszínek és elkövetési eszközök beazonosításához nyújthat segítséget az OSINT. Például van egy minden jel szerint emberölésbe torkolló eltűnési ügy, ahol már a gyanúsított is a hatóságok látókörébe került, azonban nincs meg a holttest. Az OSINT segíthet a gyanúsítotthoz kötődő helyek beazonosításában, azoknak a helyeknek a megállapításban, ahol a kérdéses időszakban megfordult, ahol fényképet készített, ahonnan bejelentkezett valamilyen internetes fórumra vagy csoportba, ahol bármilyen helymeghatározáshoz kapcsolódó tevékenységet végzett.

A lehetséges motivációk megállapítása, az elkövetést lehetővé tevő körülmények megállapítása: amennyiben az OSINT nyújtotta információhalmaz alapján képesek vagyunk egy viszonylag pontos képet és jellemrajzot felállítani a célszemélyünkről, akkor a nézetei, megnyilvánulásai mellett motivációira, szándékaira is tehetünk megállapításokat, vonhatunk le következtetéseket. Az elkövetést lehetővé tévő körülmények feltérképezésében sokat segíthetnek azok a közösségi oldalak, amelyek egy adott lakókörnyezet információival, visszásságaival foglalkoznak, a tagok folyamatos bejegyzésekben jelzik a rendellenességeket, hiányosságokat, amelyeket bűnügyi szempontból elemezve feltárhatjuk a bűncselekmények elkövetéséhez vezető lehetőségeket.

Az online térben végzett OSINT információforrásait tekintve általában mindenkinek a *közösségi oldalak* ugranak be, azonban ennél sokkal szélesebb a paletta, sokkal több lehetőséggel tud dolgozni, aki nyílt forrású információkat keres.

Keresőmotorok (Google, Google+, Google képkeresés, Google Reverse Image Search, Graph Search, Creepy stb.), amelyek címszavakra egyszerű és összetett keresésekre képesek, illetve képesek adatok alapján képet, vagy fordítva, kép alapján adatokat keresni. Ugyanakkor ezek csak a legismertebb, a többség által használt keresőmotorok, egy komoly titkosszolgálati vagy bűnügyi elemző ezeknél sokkal hatékonyabb lehetőségekkel is rendelkezik.

Közösségi média (Facebook, Instagram, Twitter, LinkedIn, üzenetküldő szolgáltatások): az internethasználók közel fele rendelkezik Facebook-profillal, amelyek a fentebb tárgyaltak szerint rengeteg lehetőséget adnak az OSINT-tevékenységre.

E-mail- és/vagy telefonszám-adatbázisok (Numberingplans.com, Imei.info, Sync.me, mobilszolgáltatók weboldalai): a nevéből adódóan e-mail-címek használóit

tudja beazonosítani vagy éppen telefonszámok előfizetőjét vagy használóját lehet megállapítani.

IP vagy domain keresése (WHOIS-adatbázisok, Centralops.net): a célszemélyünk által használt IP-címet és az alapján valamilyen tartózkodási helyet tud produkálni, illetve az általa használt domainnév alapján a domainszolgáltatótól a regisztráció során közölt adatok kinyerhetők. Az IP-cím megállapítása során problémás lehet, hogy a célszemély interakciójára van szükség, vagy le kell töltenie, vagy meg kell nyitnia valamit, ezáltal esetleg az OSINT-ot végző lelepleződhet.

Adatbázisok (Haveibeenpwned.com, Pastebin.com, Shodan.io): ezekből rengeteggel találkozhatunk és rengeteget használhatunk az interneten, van, amelyik bankszámla-információk után keres, van, amelyik nagyobb mennyiségű szöveget képes bizonyos szempontok szerint elemezni, van, amelyik több ezer webkamera képét tudja a gépünkre hozni.

Tartalomszolgáltatók (Wayback-archívumok, weboldalak archív oldalai, Google Cache): archivált oldalakon, archivált tartalmakban történik a keresés valamely kulcsszóra.

Az online térben végzett OSINT-adatgyűjtés megvalósulhat aktív vagy passzív formában is.

- Passzív adatgyűjtés: semmilyen kontakt nincs a célszemély profiljával.
- Aktív adatgyűjtés: bármilyen kapcsolati pont kihasználása (amelyről a célszemély is értesül).

Az online térben végzett OSINT-tevékenységünk során tekinttel kell lennünk arra, hogy minden online keresés, illetve egyéb tevékenység nyomot hagy maga után, tehát nemcsak az a feladatunk, hogy rábukkanjunk a célszemélyünk nyomaira, hanem az is, hogy saját nyomainkat minél jobban igyekezzünk eltüntetni.

Néhány taktikai jó tanács:

- Olyan eszközöket, illetve kapcsolatot használjunk, ami nem köthető a nyomozó hatósághoz, illetve a személyünkhöz!
- Mindig figyeljünk a dekonspiráció veszélyére!
- Amelyik interakció eredményében nem vagyunk biztosak, azt ne hajtsuk végre (például bejelölés, meghívás, „elfelejtett jelszó")!
- Maradjunk rejtve!
- Alakítsunk ki külön felhasználói környezetet, használjunk másik számítógépet, akár virtuális gépet (VMWare, VirtualBox), válasszuk külön a munkameneteket, használjunk más böngészőt, mint általában, kapcsoljuk be az inkognitómódot, vagy válasszunk privát böngészést!
- Igyekezzünk a kapcsolataink elfedésére, használjunk fedett fiókokat, azonosítókat, e-mail-címeket, telefonszámokat!
- VPN-kliens alkalmazása (Opera-VPN).

A cél a lehető legtöbb információ beszerzése a lehető legkevesebb nyom hátrahagyása mellett. Ennek érdekében gyakran kell a számítógépen kívül további feltételeket is biztosítani (VPN-kapcsolat, e-mail-címek, telefonszámok, felhasználói fiókok, feltöltőkártyás internet).

Külön problémát jelenthet a darkneten való információgyűjtés. Darknetnek vagy deep webnek nevezzük azokat a rejtett hálózatokat, amelyek csak speciális célszoftverekkel érhetők el és a normál keresőmotorok számára láthatatlanok.

Arányaiban az internet körülbelül 80%-a ebbe a kategóriába tartozik, ami miatt mégis megkerülhetetlen az internet ezen része, hogy a bűnözők felismerték ennek előnyeit, és kommunikációs csatornának használják, gyakorlatilag bármilyen illegális dolog adásvételének (fegyver, kábítószer) platformot biztosít, a pedofil hálózatok gyűjtőhelye, illetve a kriptovaluták forgalmazásának a terepe.

Természetesen azért itt is megvannak azok a speciális keresőmotorok és egyéb lehetőségek, amelyek által bizonyos információk kinyerhetők (célszoftverek: például Tor, I2P, Freenet, Deepdotweb.com, Reddit, GRAMS).

Összegezve, az OSINT lehetőséget ad a bűnös tevékenységek feltérképezésére, szervezett bűnözői csoportok beazonosítására, bomlasztására, bűncselekmények megelőzésére, korábban elkövetett cselekménnyel kapcsolatos információk beszerzésére, bővítésére, a célszemély kilétének megállapítására, a célszeméllyel kapcsolatos adatok bővítésére, a bűncselekmény elkövetési módjának megállapítására, tanulmányozására.

Felhasznált irodalom

Balláné Füszter Erzsébet – Szendrei Ferenc szerk. (2011): *A szervezett bűnözés kézikönyve: Kiegészítő megközelítések és intézkedések a szervezett bűnözés megelőzése és az ellene való küzdelem érdekében – Összeállítás az EU tagállamainak jó gyakorlataiból.* Budapest, Rendőrtiszti Főiskola.

Bálint László (2018): Terrorelhárítási Információs és Bűnügyi Elemző Központ. In Resperger István szerk.: *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus.

Bradford, Ben (2011): *Police numbers and crime rates – a rapid evidence review.* London, HMIC.

Williams, Heather J. – Blum, Ilana (2018): *Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise.* Santa Monica, California, Rand Corporation. DOI: https://doi.org/10.7249/RR1964

Kenedli Tamás (2013): *A nemzetbiztonság általános elmélete*. Egyetemi jegyzet. 183–193.

Levitt, S. (1997): Using Electoral Cycles in Police Hiring to Estimate the Effect of Police on Crime. *The American Economic Review,* Vol. 87, No. 3. 270–290.

Maguire, Mike (2008): Criminal investigation and crime control. In Newburn, T. ed.: *Handbook of Policing.* Cullompton, Willan.

Maguire, Mike – John, Tim (2003): Rolling out The National Intelligence Model: Key Challenges. In Bullock, Karen – Tilley, Nick eds.: *Crime reduction and problem-oriented policing.* Cullompton, Willan.

NATO OSINT Handbook (2001). Saclant, Norfolk.

Nilval, Kim – Mattson, Fredrik (2016): The Criminal Arboristic Perspective – A method to combat Organised Crime. In Töttel, Ursula – Bulanova-Hristova, Gergana – Flach, Gerhard eds.: *Research Conferences on Organised Crime at the Bundeskriminalamt in Germany Vol. III.* Bumdeskriminalamt, Wiesbaden. 83.

Nyeste Péter (2013): A Nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú startégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén. *Felderítő Szemle,* 12. évf. 1. sz. 100–119.

Nyeste Péter (2012): A bűnügyi hírszerzés. *Magyar Rendészet,* 12. évf. 4. sz. 28.

Nyeste Péter (2019): A bűnügyi OSINT. In Szendrei Ferenc szerk.: *A bűnügyi hírszerzés kézikönyve.* Budapest–Pécs, Dialóg Campus.

Ratcliffe, Jerry H. (2008): *Intelligence-led Policing.* Cullompton, Willan Publishing.

Rolington, Alfred (2015): *Hírszerzés a 21. században – A mozaikmódszer.* Budapest, Antall József Tudásközpont.

Szendrei, Ferenc (2018): Az európai bűnügyi hírszerzési modell előzményei Angliában. In Dobák Imre – Hautzinger Zoltán szerk.: *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére.* Budapest–Pécs, Dialóg Campus. 613–627.

Jogforrások

5842/2/2010 tanácsi dokumentum: Az Európai Unió belső biztonsági stratégiája: Az európai biztonsági modell felé.

A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról.

T/5004. törvényjavaslat egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról.

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 68–82. • DOI: 10.32561/nsz.2019.2.6

Szabó Károly[1]

Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről

OSINT – Thoughts about the Activity and the Medium of Application

A világunkat elárasztó adat- és információmennyiség célirányos monitorozására és kutatására aligha lenne lehetőség a nyílt forrásból származó információgyűjtés nélkül. A nemzetbiztonsági szolgálatok eszköztárában az OSINT[2] egyre inkább meghatározó szerepet tölt be. A tanulmány az OSINT felhasználásának és a módszer alkalmazásának néhány jellemzőjét kívánja bemutatni, elsősorban a hazai nemzetbiztonsági sajátosságok szemszögéből. A szerző meggyőződése szerint a módszerrel kapcsolatos elméleti és gyakorlati vizsgálódás egyre időszerűbb, különös tekintettel a magyar nemzetbiztonsági rendszer eszköztárába történő beillesztése, harmonizálása kapcsán. Az írás ennek kérdéskörét vizsgálja.

Kulcsszavak: OSINT, nemzetbiztonsági tevékenység, a titkos információgyűjtés eszközei és módszerei

Targeted monitoring and research of the amount of data and information that flood our world would hardly be possible without gathering information from open source. OSINT plays an increasingly important role in the toolbox of national security services. This study aims to present some of the features of OSINT and the application of its method, primarily from the point of view of the domestic national security aspects. The author is convinced that the theoretical and practical examination of the method is more and more relevant, especially in connection with its integration and harmonisation into the Hungarian national security system. This paper examines the above mentioned issue.

Keywords: OSINT, national security activities, tools and methods for gathering secret information

[1] Szabó Károly ezredes, tanársegéd, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet; doktorandusz, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. ORCID-azonosító: 0000-0002-9177-6351.

[2] Open Source Intelligence – szűkebb értelemben nyílt forrású hírszerzés; a hazai, nem a forrásalapú megközelítés alapján szerveződő struktúrában nyílt forrású információgyűjtés, információszerzés, illetve adatszerzés; összességében olyan információ megszerzésére irányul, amely legálisan – bárki által – hozzáférhető.

Bevezetés

A 21. század második évtizedének végén a biztonság garantálásáért és megőrzéséért folytatott küzdelemben már nem egyszerűen csak az adatok, az információk és az ismeretek rendelkezésre állása a meghatározó, hanem leginkább az abból kinyerhető tudás áll a középpontban. A tudás megszerzésében az emberi gondolkodás mellett meghatározó szerepet játszanak az innovatív technológiák is. A nyílt forrásokból hozzáférhető ismerethalmaz dinamikusan változik, tartalmi sokszínűségét és mennyiségi bővülését egy egyre gyorsuló és exponenciálisan növekvő folyamat jellemzi.

A számottevő mértékben növekvő információmennyiség és a hozzá kapcsolódó források kezelése elsősorban technikai oldalon jelent komoly kihívást az információk feldolgozásában. Az ilyen forrásból megszerezhető ismeretek kezelése egyre nagyobb kapacitásokat igényel a célzott feldolgozást végző szereplőknél, így a nemzetbiztonsági szolgálatoknál is.[3] Az információs robbanás, valamint a vele párhuzamosan bekövetkezett informatikai forradalom, az internet működése és gyors elterjedése szükségessé tette az OSINT (Open Source Intelligence – nyílt forrásból származó információszerzés) eljárásainak és rendszerének kidolgozását, folyamatos fejlesztését.[4] Ahhoz, hogy ezzel a fejlődési ütemmel lépést lehessen tartani, a nemzetbiztonsági elmélet gondozásában közreműködőknek a szakmai tudásbázis megőrzése mellett gondot kell fordítania annak bővítésére is.

A nemzetbiztonsági rendszer sikeres működéséhez a rendelkezésre álló eszközök és módszerek alkalmazási sokoldalúsága járul hozzá leginkább. Ez a nyílt forrásból származó információk felhasználására is igaz. Az OSINT megismerésére, így a módszerhez kapcsolódó ismeretek rendszerezésére, elsősorban az alkalmazás gyakorlata, a tapasztalatszerzés ad lehetőséget, hiszen ezen a területen az elmélet gyakorta „lépéshátrányban" van a praxissal szemben. Szinte közhely, hogy az OSINT gyakorlati alkalmazása általában megelőzi az elméletet. Az OSINT-tal kapcsolatos szakmaelméleti kérdésekben történő eligazodásban ezenkívül a nemzetközi kitekintések nyújthatnak segítséget. Itt sem egyértelmű azonban a helyzet.

Annak ellenére, hogy az OSINT rendkívül kurrens tudományos kutatási területté vált, mind a mai napig nem alakult ki a nemzetközileg elismert és elfogadott, sztenderd fogalomrendszere. Ebben a tekintetben a hazai, a témával foglalkozó irodalom is számos fogalmi változattal dolgozik.[5] Ezek feldolgozása is alapját képezhetné egy külön tanulmánynak. Ami a nemzetközi szinten is mutatja a téma egységes keretekben történő feldolgozásának nehézségeit, hogy a szabályozók és útmutatások terén meghatározó befolyással rendelkező NATO[6] a mai napig adós az évek óta kidolgozás alatt álló OSINT-doktrínával. Azt ugyanakkor senki nem vitatja, hogy az OSINT ma már szinte minden vezetési szinten a napi eljárások szerves része, a döntéshozatal nélkülözhetetlen forrása.[7]

---

3 Dobák 2017.
4 Vida 2013a.
5 Vida 2013a.
6 Az Észak-atlanti Szerződés Szervezete (angolul North Atlantic Treaty Organisation – NATO, franciául Organisation du Traité de l'Atlantique Nord – OTAN).
7 Vida 2013b.

Az OSINT normarendszerének problémái

A negyedszázaddal ezelőtt megalkotott jogszabályi környezet több módosuláson esett át az idők során.[8] A nemzetbiztonsági struktúrát, és ezzel együtt annak tartalmát érintően is több lényeges változás következett be: új szervezetek jöttek létre,[9] több helyütt bővült, illetve kiegészült a nemzetbiztonsági feladatrendszer,[10] a titkos információgyűjtés eszközeivel és módszereivel kapcsolatos tartalom árnyaltabbá vált,[11] és nem utolsósorban a nemzetbiztonsági szolgálatokat irányító minisztériumok tekintetében is tanúi lehettünk változásoknak.[12] A felsoroltak mind tudatos politikai / szakmai döntés eredményei voltak, olyan rendszerszintű alkalmazkodásról tanúskodnak, amelyek a normaszövegben formálisan is megjelentek.

Nem csak általánosságban mondható el tehát, hogy a nemzetbiztonsági tevékenység jelen korunkban a kihívásokhoz történő alkalmazkodásról szól. Az alkalmazkodás vetületei között találunk azonban olyan részleteket is, amelyek egyértelműen a nemzetbiztonsági tevékenység szakszerű ellátását szolgálják, ám azok egyáltalán nem vagy csak részben kerültek be „hivatalosan" az ágazat komplex struktúrájába. Így van ez a témánkat adó OSINT esetében is. A nyílt forrásokon alapuló információszerzés alkalmazása nélkül ma már nem képzelhető el érdemi szakmai tevékenység, annak intézményesült formája mégsem kapott helyet az ágazatot érintő sarkalatos törvényben. A témával kapcsolatos szakmai párbeszéd azért is szükségszerű, mert vitathatatlan, hogy az OSINT az utóbbi időszakban a nemzetbiztonsági és a rendvédelmi szervezetek egyre kevésbé nélkülözhető eszközévé vált.[13]

Az OSINT ugyanazon a közegen keresztül vált generális részévé a hazai nemzetbiztonsági rendszernek, mint a többi forrásalapú megközelítésen nyugvó információszerzési lehetőség. A tevékenységet tradicionálisan a hírszerzés egyik önálló ágaként tudjuk azonosítani, és mint ilyet, az összadatforrású hírszerzés organikus részeként tartjuk számon, amelynek éppúgy eleme például a rádióelektronikai, a humán, a képi és a technikai felderítés is. Az OSINT tehát az angolszász fogalmi rendszerben használt hírszerzés „exportcikke". A tevékenység centrumában lévő hírszerzési ciklus[14] tradicionális felépítését figyelembe véve az OSINT az adatszerzés szakaszában a legmeghatározóbb. Ma már azonban szinte elképzelhetetlen, hogy egy döntéshozónak

8 Dobák–Kovács 2017.

9 Szentgáli 2015, 84.

10 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 6. §-a a Katonai Nemzetbiztonsági Szolgálat számára állapított meg új feladatokat: feladatkörét érintően információkat gyűjt a válságkörzetekről, illetve a Magyar Honvédség műveleti területen lévő alakulatait és azok állományát veszélyeztető törekvésekről és tevékenységekről, valamint részt vesz a Magyar Honvédség műveleti területen alkalmazott erőinek nemzetbiztonsági védelmében, felkészítésében és támogatásában; biztosítja a Honvéd Vezérkar hadászati-hadműveleti tervező munkájához szükséges információkat, működteti Magyarország katonai felderítő rendszerét. [Módosította: 2014. évi CIX. törvény 30. § (1) b) pont.]

11 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 61. §-a a titkos információgyűjtésre és a leplezett eszközök alkalmazására vonatkozó egyéb szabályok tekintetében. [Módosította: 2017. évi XCIII. törvény 24. § (2) bek.]

12 Szentgáli 2015, 80.; Dobák–Kovács 2017, 190.

13 Burke 2007.

14 A ciklus öt szakaszra osztható: az információigények fogadása, az adatszerzés, a feldolgozás és rendszerezés, az elemzés-értékelés és tájékoztatók készítése, valamint a felhasználók tájékoztatása. Lásd Vida 2013b; Robertson 2007.

szóló tájékoztató a nyílt forrású információszerzés lehetőségeinek felhasználását mellőzve készüljön.

A nyíltan hozzáférhető információk exponenciálisan növekvő mennyisége miatt az OSINT egyre nagyobb hangsúlyt kap a felhasználók információigényeinek kielégítésében, így a döntéshozók számára összeállított jelentések elkészítése során is. Döntéshozói tájékoztató tevékenységet pedig minden szolgálat végez. Noha a nyílt forrásokból származó információk nem helyettesíthetik a minősített információkat, de számos téren képesek kiegészíteni azokat. Az OSINT kiválóan alkalmas többek között arra is, hogy igénybevételével meghatározzák a költségesebb információszerzési eljárások[15] erőkifejtésének fő irányait, ezzel együtt arra is képes, hogy aktuális információkkal lássa el a felhasználókat. E kettősség kiaknázása ugyancsak minden szolgálat elemi érdeke.

Az OSINT-képességek kialakítása és fejlesztése a hazai nemzetbiztonsági rendszerben, főszabály nem lévén, szervezeti elkülönülésben következett be. A kialakításnál a nemzetbiztonsági tevékenység specifikumai, funkciói játszottak döntő szerepet. Ezt a folyamatot a hazai nemzetbiztonsági struktúrában a szolgálatok belső ügyként kezelték és kezelik, a feltételrendszer megteremtése is eszerint, tehát a saját belső szakmai igényeik mentén alakították ki. Ennek megfelelően a nemzetbiztonsági és rendvédelmi szervezetek többségében az OSINT önálló tevékenységgé vált, amely sok esetben strukturálisan is megjelent az egyes szervezeteken belül. Az eltérések és a hangsúlyeltolódások abból adódhatnak, hogy az OSINT képességcsomagját az alkalmazók számára meghatározott feladatok, valamint a rendelkezésükre álló humán és pénzügyi források figyelembevételével alakították ki. A nyílt forrásból származó és felhasznált információk a nemzetbiztonsági tevékenység mérhető tartományába illeszkednek. Valószínűleg minden nemzetbiztonsági szolgálat vezet statisztikát arra vonatkozóan, hogy az általa beszerzett adatok mekkora hányada származik nyílt forrásból. Lényegesebb kérdés persze ennél az, hogy az ilyen úton megszerzett adatok közül milyen arányban történik valódi hasznosulás. Nem vitatható tehát, hogy az OSINT a hazai nemzetbiztonsági tevékenység komplex rendszerének szerves részévé vált.

Jogos tehát a felvetés; ha a korábban említett esetekben sor került a nemzetbiztonsági rendszer lényegi elemeinek megváltoztatására, illetve módosítására, akkor ugyanilyen megközelítésben miért nem sikerült „konszolidálni" az OSINT alkalmazásával és felhasználásával kapcsolatos problémakört, és miért nem történtek kísérletek a hazai nemzetbiztonsági eszköztárba történő beillesztésre, egy egységes álláspont kialakítására. Ezt a problémát az információgyűjtéssel kapcsolatban érdemes áttekinteni.

A hazai nemzetbiztonsági rendszerben az információgyűjtés eszközeinek és módszereinek jól körülhatárolható katalógusa van. Ha tüzetesen megvizsgáljuk e regiszter tartalmát, arra a megállapításra kell jutnunk, hogy abban az OSINT mint önálló módszer nem szerepel.[16] Ennek ellenére nehezen vitatható, hogy a nyílt forrásokon alapuló információszerzés létezik, és alkalmazása már szerves részét képezi a hazai nemzetbiztonsági eszköztárnak. Arról van szó csupán, hogy a magyar nemzetbiztonsági

[15] Az OSINT-tevékenységet alapvetően nem sorolják a költséges információszerzési eljárások közé, azonban alkalmazásának hatékonysága a rendelkezésre álló anyagi lehetőségek függvényében jelentősen növelhető.

[16] A titkos információgyűjtés eszközeit és módszereit tárgyaló, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 54. §-a és 56. §-a alapján.

rendszerben az információgyűjtés nem az információforrások mentén építi fel struktúráját, hanem abban kizárólag az eszköz- és módszeralapú felosztás dominál. Ezért okoz problémát az OSINT besorolása.

Az akadálymentes illeszkedés másik oka az információgyűjtés nyílt és titkos jellegének szükségszerű megkülönböztetéséből ered. A lehatárolást azért kell végrehajtani, mert az OSINT alkalmazásának számos lehetőségétől függetlenül, alapvetően nem módszerspecifikus tevékenység, hanem abban kizárólag a forrás a meghatározó.

E tanulmány keretei nem adnak lehetőséget a terminológiát érintő kérdések teljes körű és részletes áttekintésére, azonban annyit mindenképpen érdemes megjegyezni, hogy a nyílt forrású információszerzés határvonalait a tárgy tekintetében a nyilvános adatok gyűjtésében, az eszközök oldaláról vizsgálva pedig azok legális alkalmazásnál lehet meghúzni. A legalitást a nyílt forrású információszerzés esetében a legáltalánosabb kontextus szerint kell érteni. Az e kereteket meghaladó információgyűjtést a nemzetbiztonsági szolgálatok által végzett titkos információgyűjtésbe kell sorolni. Természetesen a titkos és a nyílt információszerzés optimális esetben egyszerre van jelen a nemzetbiztonsági szolgálatok eszköztárában. Ennek megfelelően a nyílt információs térből történő adatfelvétel módszerének alkalmazása nem zárja ki azt, hogy az ilyen úton megszerzett információk a feldolgozás során a minősítéssel védendő közérdek kategóriájába sorolódjanak.

A nemzetbiztonsági feladatok ellátása, a nemzetbiztonsági cél elérése rendszerint a nyílt és a titkos eszközök és módszerek kombinált alkalmazását feltételezi és teszi szükségessé. Ez jó esetben egy mellérendelő viszony biztosítása mellett valósul meg. A titkos információgyűjtés rendszerszinten magában foglalja a titkos információgyűjtés feltételeinek megteremtését, az alkalmazásukhoz szükséges rendszerek kiépítését, a végrehajtás eszközeinek rendelkezésre állását, valamint az alkalmazásukhoz elengedhetetlenül szükséges humán kapacitások, azaz a szakemberek biztosítását is. Az OSINT saját normarendszerében ugyanilyen követelmények megteremtését támasztja a nemzetbiztonsági szolgálatok felé.

A nemzetbiztonsági tevékenység egyik legfontosabb funkciója a titkos információgyűjtés. A tevékenység e lényegi eleme nem korlátlan, hiszen egy rendkívül szigorú feltételrendszer biztosítja, hogy az alkalmazás keretében mely cél elérése érdekében, milyen eszközöket, milyen időtartamban és kivel szemben lehet alkalmazni.[17] Az információgyűjtés aspektusai között minden esetben vizsgálni kell az ilyen csatornákon felvett adatfajták kezelését és feldolgozását is.

Ahogy arra történt utalás a nemzetbiztonsági szolgálatokról szóló törvényben, hiába keressük az OSINT-tevékenységre vonatkozó szabályokat. Fontos azonban rámutatni arra, hogy a nyílt forrásból történő információgyűjtés tárgyalása egy helyütt, az adatok beszerzését[18] szabályozó részében mégis helyet kapott a normaszövegben. Ilyen megközelítésben a jogszabály az adatfelvétel egyik lehetőségeként tekint rá, azonban részleteire, tartalmára és végrehajtásának módjára egyáltalán nem találunk részletszabályokat. Ennél a résznél találjuk még az érintett önkéntes, illetve a törvényben előírt kötelező adatszolgáltatását, a titkos információgyűjtést, valamint

[17] Finszter 1999, 18.
[18] Dezső–Hajas 2000, 242.

az adatkezelést végző szerv adatszolgáltatását is.[19] Itt is tetten érhető a korábban vizsgált elhatárolás. A fő irányelv tehát az, hogy a nemzetbiztonsági szolgálatok az adatkezelés során kötelesek az adott cél eléréséhez feltétlenül szükséges, ugyanakkor az érintett személyiségi jogait legkevésbé korlátozó eszközt igénybe venni. Nehezen vitatható, hogy a nemzetbiztonsági szolgálatok által az információszerzéssel érintett személy személyiségi jogait legkevésbé korlátozó eszköz ne a nyílt forrásból származó információgyűjtés lenne. Ez már a nemzetbiztonsági tevékenységre jellemző alapelvek területét érintő kérdés.

A szolgálatok nemzetbiztonsági cselekvőképességére egyre nagyobb hatást gyakorol a művelettámogató közeg. Az OSINT esetében az alkalmazás képességének megteremtése és a forrásokhoz történő hozzáférés biztosítása alapvető tényező. A források nyílt jellegét és a hozzáférés törvényes lehetőségeit minden esetben szükséges tehát vizsgálni, ezek nyújtanak ugyanis garanciát annak megfelelő alkalmazására.[20] Ugyanakkor a művelettámogató jelleget az OSINT esetében más szemszögből is érdemes megvizsgálni. Az OSINT jellegénél fogva ugyanis képes olyan információkat is felszínre hozni, amelyek már a titkos információgyűjtés eszközei, illetve módszerei alkalmazásához kötődnek. A jelenleg tapasztalható tendenciák alapján megállapítható, hogy a személyiségi jogok és személyes adatok kapcsán egyre markánsabban megjelenő jogi védelem miatt sokkalta nehezebb egyértelmű határvonalat húzni az OSINT tradicionális nyílt jellege és más, a már a titkos eszköz- vagy módszeralkalmazáshoz kötődő művelettámogató OSINT-funkciók között. Az OSINT alkalmazásának gyakorlatában egyre inkább összemosódhatnak azok a tevékenységek, amelyek tartalmi kérdésekben (például a személyes és különleges adatokhoz történő hozzáférést illetően), vagy az alkalmazott eszközök és eljárások legális volta tekintetében (zárt tartalmakba történő behatolás speciális informatikai eljárások segítségével) veszítenek nyílt jellegükből.

A nemzetbiztonsági tevékenység minden szakterületére igaz, hogy az ott megszerzett tudás nem általánosítható. Az OSINT esetén azért kiemelten fontos erre rámutatni, mert a nyílt forrásokat felhasználó, nemzetbiztonsági célból végzett tevékenység ugyanannak a szakmai közösségnek a privilégiuma, amelynek más, kifejezetten a szolgálatok számára törvényesen biztosított eszköz és módszer alkalmazását is lehetővé teszi. Ez pedig komoly felelősséggel jár. Az eszközök és módszerek alkalmazása, valamint az információszerzés forrásainak minél hatékonyabb alkalmazásai pedig mind közös célt szolgálnak: a döntéshozók munkájának támogatását. Ebben az OSINT-nak is egyre markánsabb szerep jut.[21]

Az OSINT és a döntéstámogatás

A magyar nemzetbiztonsági rendszer negyed évszázados történetének egyik legfontosabb területe a döntéshozatal támogatása. Olyan vívmány ez, amely az azt megelőző

[19] Dezső–Hajas 2000, 242.
[20] Dezső–Hajas 2000, 240–242.
[21] Lowenthal 2017, 178–183.

titkosszolgálati periódusban nem volt jellemző.[22] A nemzetbiztonsági szolgálatok eszköztárában lévő lehetőségeket aszerint is érdemes tehát megvizsgálni, hogy jellemzőik által milyen hatást gyakorolhatnak a döntéshozók munkájára. Ez az OSINT estében is szükségszerű. A szolgálatoknak itt az alkalmazási kockázatokra érdemes fókuszálniuk. Ez abból adódik, hogy a nyílt forrásokhoz történő hozzáférés esetén érvényesül legkevésbé az állam információs monopóliuma. Az OSINT esetében az információs autonómia nem kizárólag a szolgálatok sajátja, maga a döntéshozó is élhet a nyílt forrásokból megismerhető információk gyűjtésének lehetőségével, sokszor maga épít ki kapacitásokat ennek megvalósítására.

Az OSINT nem megfelelő alkalmazása ebből adódóan éppen a nemzetbiztonsági rendszer egyik legfontosabb funkcióját erodálhatja: a kormányzati tájékoztatást, azaz a döntéshozatalt. A legrosszabb forgatókönyv az, ha egyenlőségjel kerül egy nyílt sajtószemle és egy elemző-értékelő munka útján készült tájékoztató közé.

A döntéshozók szempontjából a nyílt információk hozzáférésének legfontosabb közege a média. Ez egyben az OSINT végrehajtásának egyik legelemibb közege is. A média és a nemzetbiztonsági szolgálatok alapvetően eltérő jogszabályi környezetben dolgoznak, így itt nem érvényesül a *fegyveregyenlőség elve.*[23] A szakszerű és eredményes nemzetbiztonsági tevékenység elképzelhetetlen nyílt – többségükben a célirányos OSINT-tevékenységből származó – adatok és információk felhasználása nélkül. Ezek az információk természetesen más közegen keresztül is eljuthatnak a döntéshozóhoz.

Alapvető elvárás a felhasználók részéről, hogy minden, a majdani döntéseik meghozatalához szükséges információ a lehető leggyorsabban álljon a rendelkezésükre. Nem vitás, hogy a kiemelt érdeklődésre számot tartó, azaz a döntéshozók hírigényébe tartozó információk esetében a nemzetbiztonsági szolgálatok a leghatékonyabb munkaszervezés és a legkorszerűbb technikai háttér biztosítása mellett sem képesek minden esetben felvenni a versenyt. Erre még akkor sincs lehetőségük, ha a titkos információgyűjtést végző szervezetek mindegyike a lehető leggyorsabb és legpontosabb munkavégzésre törekszik. A legkomolyabb humán és technikai kapacitásokkal rendelkező szolgálatok sem képesek maradéktalanul kezelni az információs tér dinamikáját, az információk értékének időbeni csökkenését.

Generálisan igaz, hogy a titkos információgyűjtés forrásaiból származó információk esetében jelentős annak az esélye, hogy a megszerzés időszakában szükségszerűen minősítettként kezelt információ a feldolgozás egy későbbi időszakában nyílt információvá válik és adott esetben a médiában is megjelenik. Az átalakulás folyamatának rendszerszintű rekonstruálása lehetetlen feladat. A titkos információgyűjtés eszközeinek és módszereinek alkalmazása útján megszerzett, minősített információknak az OSINT lehetőségeivel történő visszaellenőrzése pedig generálisan parttalan vállalkozás.

Az OSINT végrehajtásához minden szükséges forrással és az azokhoz kapcsolt hozzáférési formák mindegyikével érdemes rendelkezni. Az OSINT-kutatások alapját általában a korlátozott hozzáférésű nyílt források képezik, már amennyiben az elérhető adatok és információk válaszokat képesek találni a hírigény megfogalmazására

[22] Dobák–Kovács 2017, 195–196.; Vida 2015; Hetesy 2011.
[23] Lowenthal 2017, 493.

jogosult döntéshozó számára. A nyílt információk esetében is általános cél és elvárás, hogy a felhasználásra javasolt, relevánsnak tartott információ ne egyetlen, hanem lehetőleg több, hitelesnek tartott forrás által is megerősített legyen.[24] Súlyos hiba, és az OSINT alkalmazását is hitelteleníthetí, ha megerősítő információként az alapinformáció megismételt, duplikált verzióját használják fel.[25]

A döntéshozó által megfogalmazott, periodikusan ismétlődő kérdés esetén az OSINT mechanizmusa képes a leggyorsabban ellenőrizni a hasonló vagy azonos témakörben legutóbbi alkalommal elkészült tájékoztató anyag tartalmához képest bekövetkezett esetleges változásokat, összegyűjteni a pontosító, kiegészítő információkat.

Az OSINT végrehajtása során az adatszerzés és a feldolgozás fázisát strukturálisan és a végrehajtó állomány szempontjából is érdemes külön kezelni.[26] Amíg az adatszerző szakasznál a források felkutatására, kijelölésére, az információk beszerzésére és azok szelektálására kerül sor, addig a feldolgozás végrehajtását az elemző és értékelő tevékenység keretein belül célszerű elvégezni, hiszen ott már a nyílt forrásokon túl a titkos információgyűjtés eszközei és módszerei alkalmazása útján beszerzett adatok is rendelkezésre állnak.[27] A kizárólag csak az első stádiumra alapozó szakmai anyagok készítésének gyakorlata éppen olyan szakmai hibának minősül, mint a nyílt forrásokból származó információkat teljes mértékben figyelmen kívül hagyó elemző-értékelő tevékenység.

Az esetek döntő hányadában a döntéshozatalt támogató anyagon belül egyaránt felhasználásra kerül a nyílt és a titkos forrásból, az OSINT, illetve a titkos információgyűjtő tevékenységből származó információ.[28] Az elemző-értékelő tevékenység végeredményeként elkészülő dokumentumokat minden esetben a megfelelő minősítéssel kell ellátni. Ha az adott jelentés akár csak elemi részében is tartalmaz a minősítési jogkörrel rendelkező adatgazda által minősített információt, akkor azt a megfelelő szempontrendszer alapján kell ellátni minősítéssel, függetlenül attól, hogy annak tartalma nyílt forrásból származó és minőségét tekintve is nyílt információ. Az ilyen összetételű tartalmak félrevezetők lehetnek a döntéshozók számára, ezért felhasználásukhoz megfelelő segítséget kell biztosítani.

Nemcsak szakmai, hanem a döntéstámogatás szempontjából is megfontolandó lehet, hogy a nemzetbiztonsági munka megszervezése során az OSINT területe és az elemző-értékelő munka közege egymástól elkülönítve működjön. Ezzel a megoldással jelentős mértékben csökkenthető azoknak az információs termékeknek az aránya, amelyek tisztán nyílt források felhasználásával készülnek, és amelyek más csatornán is a döntéshozó rendelkezésére állhatnak.

---

24 Robertson 2007; Burke 2007.
25 Robertson 2007; Lowenthal 2017, 180.
26 Lowenthal 2017, 181.; Vida 2013a.
27 Jensen–McElreath–Graves 2017, 193.
28 Vida 2013a; Vida 2013b.

A nyílt forrásokat érintő tendenciák és lehetőségek

Az OSINT tevékenységi körébe tartozó jellemzőket számos nézőpontból szükséges és lehet vizsgálni. Az eddigiek során a hazai nemzetbiztonsági sajátosságokat és az OSINT normarendszerének illeszkedési problémáit, valamint a döntéshozatallal kapcsolatos tartalmakat tekintettük át. Láthattuk, hogy az OSINT merítési lehetősége, eszközrendszere és térbeli kiterjedése már napjainkban is reménytelenül széles, ezzel együtt folyamatosan bővül. Ahhoz, hogy a nyílt forrású információszerzést érintő tendenciákat érdemben lehessen vizsgálni, mindenképpen szükséges áttekinteni az OSINT források szerinti klasszikus felosztását.

Ezek az alábbiak:[29]

- A tradicionális média, ami alapvetően a nyomtatott sajtótermékeket és a sugárzott televízió- és rádióadókat foglalja magában, függetlenül a szolgáltatás technikai megvalósításától.
- A világháló, amelyet döntően egy elérési lehetőségként és keresőfelületként kell figyelembe venni.
- Az online kereskedelmi szolgáltatások, amelyek kereskedelmi alapon biztosítanak online tartalmakat vagy adathordozókat az előfizetők számára.
- A „szürke irodalom", amely egy meghatározott közönség számára biztosít hozzáférhető forrásokat.
- A szakértők és megfigyelők által készített összefoglalók, beszámolók és leírások, valamint a tapasztalásaikról szóló személyes interjúk, a kutatóintézetek által közzétett tartalmak.
- Az olyan, kereskedelmi műholdak által készített felvételek, amelyek egy szélesebb közönség számára is hozzáférhetők.

Habár az internet nem a legfontosabb területe az OSINT-tevékenységnek,[30] most mégis ennek a forrásként történő felhasználását érintjük. A nemzetbiztonsági tevékenység sikeres végrehajtásának szempontjából kiemelten fontos, hogy az OSINT területeire ne mint statikus elemekre tekintsünk. Aligha vitatható, hogy az OSINT az elmúlt három évtizedben, az internet alkalmazása következtében változott meg robbanásszerűen. Ma már nem kétséges, hogy a fenti klasszikus felosztást figyelembe véve az OSINT lehetőségeit kiaknázó szereplők, így a nemzetbiztonsági szolgálatok is rendszeresen hasznosítják az interneten keresztül elérhető forrásokat. Ehhez persze nem kizárólag az járult hozzá, hogy a világhálón egyre több információ vált hozzáférhetővé, hanem az, hogy az internet egyre inkább mint információs közeg, egyfajta közvetítő felület lett meghatározó.[31] Világos azonban, hogy ezzel együtt a világháló önmagában nem vált képessé az adatok, információk létrehozására. Az interneten fellelhető információk csupán az emberi tevékenység által létrehozott, összeállított, összegyűjtött, feldolgozott adatokat, tartalmakat közvetítenek, amelyekben a valós források megállapítása sem minden esetben egyértelmű. A közvetítő jelleg, illetve az ahhoz kapcsolódó technikai

[29] Lévay 2005, 35.; Vida 2013a; Jensen–McElreath–Graves 2017, 193.

[30] Lowenthal 2017, 180.

[31] Ez igaz a „mély webre" (deep web) is. A világhálónak az a tartománya, amelyet a keresők/keresőmotorok nem képesek indexálni.

közeg azonban más szempontból is megkerülhetetlenné vált. Az internet a szolgálatok számára a nyílt forrású információszerzés esetén mind fontosabbá váló metaadatok[32] beszerzésének lehetőségeit is képes biztosítani. Ez a terület az OSINT-hoz kapcsolódó művelettámogató funkció esetében lényeges.

Ami az internet primer információforrásként történő alkalmazását illeti, ott a nyíltan elérhető forrásokat döntően négy nagyobb csoportba lehet sorolni:

- mindenki által szabadon elérhető internetes oldalak (hírportál, blog, videómegosztók, személyes vagy szervezeti honlap stb.);
- mindenki által szabadon elérhető, de tartalmát tekintve regisztrációhoz kötött internetes oldalak (hírportál, blog, személyes vagy szervezeti honlap, a közösségi oldalak meghatározó része stb.);
- a kereskedelmi forgalomban megvásárolható zárt vagy korlátozottan hozzáférhető adattartalmak (hírportál, hírügynökségi zárt oldalak, adatbázisok, jogszabály- és dokumentumgyűjtemények stb.);
- kereskedelmi forgalomban nem megvásárolható, szervezeti tagság vagy más egyéb jogosultság alapján elérhető internetes oldalak (például zárt kormányzati adatbázisok).

A tapasztalatok alapján egyre több alkalommal fordul elő, hogy az érdeklődésre számot tartó, a hírigények kielégítését közvetlenül támogató nyílt információkat tartalmazó honlapok egy meghatározott szintig vagy egy próbaidőszakra szóló engedéllyel – mintegy figyelemfelkeltésként, hirdetésként – szabad hozzáférést biztosítanak a tartalom egy meghatározott részéhez, vagy éppen a kulcsszavakhoz. Ezen túlmenően a releváns információk csak anyagi ellenszolgáltatás megfizetése után válnak elérhetővé. A közelmúltban szerzett gyakorlati tapasztalatok azt támasztják alá, hogy az ilyen lehetőség útján hozzáférhető, zárt tartalmak mind nagyobb hányadukban tartalmaznak hiteles és gyakran ellenőrzöttnek tekinthető adatokat, feldolgozott információkat, de akár komplett elemzéseket is kínálnak. Nem kétséges, hogy a nemzetbiztonsági szolgálatok számára a zárt, valamint a jogosultságaik alapján elérhető tartalmak felhasználása élvez prioritást. Ebben az esetben természetesen magasabb költségekkel kell számolni.

Napjainkban a közösségimédia-felületek egyre gyorsabb ütemű használatával kapcsolatosan új lehetőségek és kihívások jelennek meg az információs térben. Az OSINT diverzifikációjának várhatóan a jövőben is tanúi leszünk. Ezek szinte mindegyike az internethez kötődik. A dinamikus fejlődés egyik következménye, hogy a döntések meghozatalához szükséges, alapvetően a nyílt forrásból megszerezhető információk összegyűjtésére fókuszáló OSINT-tevékenység más irányokban is „képességépítésbe" kezdett. Jó példa erre az alig másfél évtizede létező közösségi hálók információit érintő OSINT, amelyen belül mintegy leágazásként megjelent például a SOCMINT (Social Media Intelligence) [33] területe is.

---

[32] Dobák 2017.

[33] Holland 2012. Az OSINT-nak az a területe, amely során a közösségimédia-oldalakról történik az információgyűjtés. Két tényezőn, az eredeti közzétett tartalmak és a kapcsolódó metaadatok hozzáférésén alapszik.

Vannak az OSINT szempontjából komolyabb kihívást jelentő forráskategóriák is, amelyek feldolgozása komoly erőforrást igényel. Ezek kezelése optimálisan működő tudásmenedzsment[34] nélkül nehezen képzelhető el. A tudásmenedzsmentben az információra mint a nemzetbiztonsági szolgálatok erőforrására kell tekinteni.[35] Általában a rendelkezésre álló információhalmazból csak abban az esetben nyerhető ki használható tudás, ha a feldolgozást végző szakmai közegek rendelkeznek a megfelelő humán erőforrással és a szükséges információtechnológiai háttérrel.[36] A nyílt források közül az internet egyik meghatározó információs közegének, a videómegosztásnak a jellemzőit vizsgáljuk, mivel az ilyen úton közvetített tartalmak kinyerése több szempontból is nehézségekbe ütközik.

Az internet legismertebb és legtöbb felhasználó által látogatott internetes oldala a Youtube közösségi videómegosztó, ahová percenként mintegy 500 órányi anyagot töltenek fel. Ez jelenleg a világ internet-sávszélességének mintegy 11%-át foglalja le.[37] A felmérések szerint a legtöbben tanulásra, ismeretbővítésre használják, míg a tinédzserek „legjobb barátjukként" tekintenek rá. Szakértői vélemények szerint a 20 év alatti korosztálynál megfigyelhető, hogy a Facebookot egyre kevesebben használják, és egyre inkább áttérnek a Youtube-ra, az Instagramra és a Snapchatre.[38]

A legtöbb prognózis szerint a videómegosztók a jövőben a hagyományos televíziós csatornák szerepét is át fogják venni. A hagyományos műsorszórásban meghatározó társaságok már most rendelkeznek olyan videómegosztási lehetőséggel, ahol a feliratkozók üzenetet kapnak a legfrissebb feltöltésekről, amelyeket bármikor megtekinthetnek. A feltöltők nemcsak az általuk készített anyagot tehetik ilyen módon hozzáférhetővé, hanem élőben is közvetíthetnek tartalmakat. Ezeket a lehetőségeket egyre növekvő arányban használják ki NGO-k,[39] ismeretterjesztéssel foglalkozó oktatási intézmények, de politikai szervezetek is.[40]

A tudásmenedzsment szempontjából itt az a meghatározó, hogy a nyílt forrású információszerzés alkalmazási közege milyen komplexitású műveletek elvégzésére rendelkezik képességgel és ezen keresztül milyen információs termékeket, szolgáltatásokat képes nyújtani a feldolgozás folyamatában. A videómegosztókon közzétett nyílt forrású információk kezelése a teljesség igénye nélkül többek között az alábbi képességek megteremtését teheti szükségessé:

- a videótartalmak automatizált keresési feltételeinek megteremtése;
- a videók helyhez, időhöz, személyhez vagy eseményhez való kötése;
- az idegen nyelvű anyagok intelligens fordítási protokolljának megteremtése;[41]
- az ilyen módon kinyert tartalmak keresési feltételeinek megteremtése;
- a viselkedéskutatásra alkalmas szoftverek alkalmazása.

---

34 A szervezet teljesítményének és hatékonyságának növelése, az általa birtokolt tudás erőforrássá történő alakítása által.

35 Waltz 2003, 1.

36 Lowenthal 2017, 183.

37 Bruno 2019, 17.

38 Bruno 2019, 18.

39 Non-governmental organization – nem kormányzati szervezet.

40 A közelmúltban az európai parlamenti választásokon induló csúcsjelöltek vitáját is nyomon lehetett követni a Youtube videómegosztón.

41 Robertson 2017. Rámutat, hogy az OSINT egyik legnagyobb korlátját a nyelvi akadályok képezik.

A videómegosztó portálok azonban más aspektusból is figyelmet érdemelnek. Az egyre nagyobb nézőközönség révén különböző tartalmak megosztását, terjesztését, véleményeket közvetítenek, ezzel együtt pedig a befolyásolási lehetőség egyre szélesebb platformját képezik.[42] Ez a felismerés az OSINT szempontjából is tartalmaz lehetőségeket. Itt a már korábban érintett másik funkció, az OSINT művelettámogató képessége jelenik meg. Ez a lehetőség a befolyásoláshoz, azon belül is a közvélemény formálásához kötődik. Ha a hétköznapi befolyásolás legújabb trendjére vetünk egy pillantást, akkor azt találjuk, hogy a videómegosztók új és egyre inkább meghatározó elemeként megjelentek az influenszerek.[43] Az influenszer jelentése *másokat befolyásoló ember* vagy *véleményvezér.* Ennek megfelelően az influenszerek véleményét a megosztásra feliratkozók – leginkább a fiatalabb korosztály – jelentős hányada feltétlenül elfogadja. Influenszer bárki lehet, aki képes követőket szerezni és a figyelmüket folyamatosan fenntartani.

Tendenciaként látható, hogy az üzenetek célba juttatására bizonyos célcsoportok esetében már most ez a legalkalmasabb közeg. Ráadásul a felület éppen a működési mechanizmusa miatt – a kockázatot kezelő fél részéről – nehezen kontrollálható.[44]

A befolyásolásnak azonban van egy másik, stratégiai szintje is.[45] A befolyásolási tevékenységben az OSINT mint tevékenységi forma és mint műveleti közeg egyaránt szerepet kaphat. A véleményformálásra alkalmas ilyen nyíltan hozzáférhető felületek kihasználása komoly eszköz lehet.[46] A célzott befolyásolási műveletek előkészítési fázisában az OSINT aktívan képes támogatni a végrehajtót, ugyanakkor a kidolgozáshoz pótolhatatlan alap- és kiegészítő információkkal is képes támogatást nyújtani. Ugyanez vonatkozik a befolyásolási műveletek hatásainak nyomon követésére, az azzal kapcsolatos meghatározó információk folyamatos közvetítésére. [47]

Az OSINT és a biztonságtudatosság

A nyílt forrásokból beszerezhető információhalmaz egyik legfontosabb jellemzője, hogy egyaránt tetten érhetjük benne a társadalmi és a technológiai biztonság hiányára utaló körülményeket, ugyanakkor az információk nemzetbiztonsági szempontú besorolása már komoly akadályokba ütközik. Ezek a kockázatok elsősorban az egyén szintjén jelentkezhetnek. A hazai nemzetbiztonsági rendszerben is egyre komolyabb mértékben meghatározó az individuumra fókuszáló nemzetbiztonsági cselekvés.[48] Ennek a kontextusnak a középpontjában a nemzetbiztonsági szempontok alapján értelmezett biztonságtudatosság áll, amely tartalmazza annak kialakítását, fejlesztését és fenntartását. A biztonságtudatosság olyan magatartási normarendszer, amely

42 Lowenthal 2017, 182.
43 Bruno 2019, 18.
44 Problémát okozott legutóbb a Youtube számára, hogy az új-zélandi mészárláskor az elkövető élőben közvetítette tettét, amit a szolgáltató sokáig nem is tudott blokkolni, mivel a cselekmény elkövetése után rendkívüli mértékben terjedt a megosztások száma.
45 Gough 2003.
46 Lowenthal 2017.
47 Kovács 2017.
48 Dobák–Kovács 2017, 198.

elősegíti a mindennapi életünket befolyásoló kockázatok tudatos felismerését, megakadályozva a nemzetbiztonsági kockázatok kialakulását, illetve csökkentve a már bekövetkezett érdeksérelem negatív hatásait.[49]

Az OSINT metodikája és sajátosságai jelentős mértékben támogathatják a biztonságtudatos emberi magatartások kialakítását. Ez elsősorban az interneten végzett tevékenységre vonatkoztatható. A nemzetbiztonsági szolgálatok számára komoly kihívást jelent, hogy az emberek jelentős mértékben alábecsülik az online térben megjelenő, őket fenyegető biztonsági kockázatokat.[50] A nyílt források felhasználásával készült tájékoztatók, esettanulmányok segíthetik annak megértetését, hogy okoseszközeink vagy éppen az internet használata nem oka, hanem lehetősége a biztonsági kockázatok kialakulásának.

Az OSINT-források hitelesen képesek ráirányítani a figyelmet a feltárt biztonsági kockázatokra. Emellett segítenek eligazodni a megfelelő magatartásformákat illetően, és a biztonsági problémák bekövetkezése során is képesek segítséget nyújtani a kár mértékének enyhítésében.

Összefoglaló gondolatok

A tanulmány az OSINT-tevékenység magyar nemzetbiztonsági rendszerbe történő beillesztésének nehézségeire és alkalmazásának néhány sajátosságára kívánta felhívni a figyelmet.

Az OSINT-tevékenység önálló normarendszerrel rendelkezik, amely a titkos információgyűjtéssel együtt adja a szolgálatok cselekvőképességének gerincét. A nyílt és a titkos információgyűjtés akkor tudja mintaszerűen betölteni szerepét, ha azokra egymástól független, de egyenrangú információgyűjtési szabályrendszerként tekintünk. Ez biztosítja a törvényes alkalmazás kritériumait is.

Az általános gyakorlat alapján a nemzetbiztonsági tevékenységet végző szakterületek mindegyike használja a nyílt források által biztosított lehetőségeket. Minden nemzetbiztonsági szolgálatnak elemi érdeke tehát, hogy valamilyen módon birtokolja a nyílt forrásból történő információszerzés képességét. Az OSINT-tevékenységek végrehajtásának lehetőségeit egyformán behatárolják az aktuális technikai színvonal nyújtotta lehetőségek, a rendelkezésre álló anyagi erőforrások és a nemzetbiztonsági tevékenység sajátos biztonsági megfontolásai.

A nemzetbiztonsági szolgálatok számára az OSINT közege egy dinamikusan változó terület marad. Biztosra vehető, hogy a nyílt forrásokból kinyerhető információk aránya a közeljövőben sem fog csökkeni. Ezzel együtt az OSINT egyre hangsúlyosabb eszköze lesz a döntéstámogató tevékenységnek, ugyanakkor művelettámogató funkciók fejlesztésével is számolni kell.

A nyílt forrásból származó információk felhasználása komoly potenciált jelenthetne a biztonságtudatosság kialakításának területén.

[49] Szabó 2017.
[50] Jensen–McElreath–Graves 2017, 364.

A terület megértését a multidiszciplináris (polgári/katonai-humán/technikai) kutatási lehetőségek kiaknázása alapozhatja meg. E megközelítés a nemzetbiztonság egységes értelmezését is feltételezi. Az eszközök és módszerek alkalmazásával kapcsolatos témakör tanulmányozásának kiemelt célja, hogy azok eredményeit a szakmai gondolkodásban és a gyakorlatban, valamint az oktatásban is hasznosítani lehessen.

Felhasznált irodalom

Bruno, San (2019): Now playing, everywhere. *The Economist,* May 04 2019. 17–20.

Burke, Cody (2007): *Freeing knowledge, telling secrets: Open source intelligence and development.* CEWCES Research Papers. Paper 11.

Dezső Lajos – Hajas Gábor (2000): *A nemzetbiztonsági tevékenységre vonatkozó jogszabályok. Kommentár a gyakorlat számára.* Budapest, HVG-ORAC.

Dobák Imre – Kovács Zoltán András (2017): Korszakváltások a magyar nemzetbiztonsági intézményrendszerben. In Finszter Géza – Sabjanics István: *Biztonsági kihívások a 21. században.* Budapest, Dialóg Campus. 175–219.

Dobák Imre (2017): Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12. évf. 2. sz. Elérhető: http://hadmernok.hu/172_19_dobak.pdf (A letöltés dátuma: 2019. 04. 18.)

Finszter Géza (1999): Ismét a nemzetbiztonságról. Belügyi Szemle, 37. évf. 4–5. sz. 5–19.

Foucalt, Michel (2000): *A szavak és a dolgok.* Budapest, Osiris.

Gough, Susan L. (2003): *The Evolution of Strategic Influence.* U.S. Army War College. DOI: https://doi.org/10.1037/e427732005-001

Hetesy Zsolt (2011): *A titkos felderítés.* PhD-értekezés. Pécs, PTE ÁJK DI. Elérhető: http://ajk.pte.hu/files/file/doktori-iskola/hetesy-zsolt/hetesy-zsolt-vedes-ertekezes.pdf (A letöltés dátuma: 2018. 04. 20.)

Holland, Benjamin R.(2012): *Enabling Open Source Intelligence (OSINT) in private social networks.* Elérhető: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.9840&rep=rep1&type=pdf (A letöltés dátuma: 2019. 04. 18.)

Jensen, Carl J. – McElreath, David H. – Graves, Melissa (2017): *Bevezetés a hírszerzésbe.* Budapest, Antall József Tudásközpont.

Kovács Krisztián (2017): *A befolyásolás szerepe a modern hadviselésben.* Szakdolgozat. Nemzeti Közszolgálati Egyetem, Felsőfokú Nemzetbiztonsági Tanfolyam.

Lévay Gábor (2005): Az OSINT lehetőségei a katonai műveletek tervezésének támogatásában. *Felderítő Szemle,* 4. évf. 1. sz. 31–43.

Lowenthal, Mark M. (2017): *Hírszerzés: A titoktól a politikai döntésekig.* Budapest, Antall József Tudásközpont.

Robertson, Jeffrey (2007): *Detect and defeat – the complexities of accomplishing the HLS mission with existing intelligence collection practices.* Elérhető: https://calhoun.nps.edu/bitstream/handle/10945/3202/07Sep_Robertson.pdf?sequence=1&isAllowed=y (A letöltés dátuma: 2019. 04. 18.)

Szabó Károly (2017): *A katonai elhárítás elmélete.* PhD-értekezés kézirata. Budapest, NKE HDI.

Szentgáli Gergely (2015): Csendben szolgálni. A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 és 2014 között. 2. rész. *Hadtudomány,* 25. évf. 3–4. sz. 77–90. Elérhető: http://mhtt.eu/hadtudomany/2015/3_4/2015_3_4_8.pdf (A letöltés dátuma: 2019. 03. 28.) DOI: https://doi.org/10.17047/HADTUD.2015.25.3-4.77

Vida Csaba (2015): *A nemzetbiztonsági tevékenység szerepe a társadalomban.* Elérhető: http://real.mtak.hu/29936/1/19_VIDA_CSABA.pdf (A letöltés dátuma: 2019. 03. 28.) DOI: https://doi.org/10.17047/HADTUD.2015.25.E.221

Vida Csaba (2013a): Nyílt forrású adatszerzés (OSINT). In Kobolka István: *Nemzetbiztonsági alapismeretek.* Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó. 115–124.

Vida Csaba (2013b): *A hírszerző elemző-értékelő munka alapjai.* Elérhető: http://real.mtak.hu/14875/13/jav_real__2013-3.pdf (A letöltés dátuma: 2019. 03. 28.)

Waltz, Edward (2003): *Knowledge and Managment in the Intelligence Enterprise.* Boston–London, Arctech House.

Jogforrás

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99500125.TV#lbj28id2a4b (A letöltés dátuma: 2019. 03. 28.)

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 83–93. • DOI: 10.32561/nsz.2019.2.7

Dobák Imre[1]

OSINT – Gondolatok a kérdéskörhöz

OSINT – Thoughts on the Issue

Az OSINT mint hírszerzési ág napjainkra már széles körben kutatott, alkalmazása jelen van mind a gazdasági szereplők, mind a biztonságért felelős kormányzati szervek rendszerében. Számos alkalmazási előnnyel és korláttal rendelkezik, valamint a technológiai környezet jelentős hatást gyakorol az OSINT fejlődésére. Sajátos jellemzői rávilágítanak arra, hogy egyre összetettebb fejlődő területei a jövőben is meghatározóak maradnak.

Kulcsszavak: OSINT, hírszerzés, információgyűjtés, technológia, nemzetbiztonság

The OSINT as a branch of intelligence has been extensively researched nowadays, and its application is present in the sphere of both economic and government organisations responsible for security. It has many application advantages and limitations, and the technological environment has a significant impact on the development of OSINT. Its specific features highlight the fact that its more complex development areas will remain dominant in the future.

Keywords: OSINT, intelligence, information gathering, technology, national security

Jelen tanulmány az információgyűjtés egyik sajátos ágaként megjelenő nyílt forrásból történő információgyűjtés (OSINT – Open Source Intelligence) gyakran hangoztatott előnyei és hátrányai metszetében annak fejlődési kérdéseihez kíván gondolatokat megfogalmazni. A hírszerzési ág napjainkra már széles körben elterjedt, mind a gazdasági szereplők, mind a biztonságért felelős kormányzati szervek rendszerében. Mindazonáltal számos korlát és tisztán még nem látható fejlődési irány jellemzi a tevékenységet, amelyet közvetlenül befolyásol az infokommunikációs környezet rendkívül gyors fejlődése.

[1] Dr. Dobák Imre, Nemzeti Közszolgálati Egyetem. ORCID-azonosító: 0000-0002-9632-2914.

A fogalmi keret

Az angolszász rendszer hírszerzési ágai között megjelenő OSINT mint nyílt forrásból történő információgyűjtés fogalmának tudományos értékű tisztázására jelen tanulmány nem kíván részletesen kitérni, az általánosan ismert hazai és nemzetközi fogalmak néhány fő elemét azonban mindenképpen érdemes kiemelni. Ezek között jelenik meg a nyilvános forrásból történő *megszerezhetőség* elsődleges kritériuma, amely mellett az információgyűjtés összetett folyamatát (információk felkutatása, gyűjtése, szelektálása, elemzése-értékelése és felhasználása[2]), valamint egyes esetekben az információgyűjtés jogszerűségének kérdését szokták megemlíteni.[3]

Amíg Lévay definíciójában[4] megjelenik az információgyűjtés legális eszközökkel történő végzésének kérdése, a Vadász–Séllei szerzőpáros tanulmányában kiemeli, hogy az „angolszász szakirodalomban a jogszerűség általában kimarad, csak a mindenki számára történő elérhetőséget (publicly available) mint kritériumot adják meg”.[5] A kérdéskör hazai jogi oldalát tekintve Péterfalvy is rávilágít, hogy „a nyílt információgyűjtés nem egzakt jogi terminus abban az értelemben, hogy a jogforrásokban nem található olyan általános érvényű definíció, amely pontosan meghatározná a jelentését”.[6] Fenti megállapításokat elfogadva láthatóvá válik, hogy a két megközelítés (a nyílt forrású információgyűjtés jogi és hírszerzési célú OSINT-szakterminológia megközelítése) teljes egészében nincs átfedésben.

Amíg korábban a tevékenység elsősorban a különböző biztonsági szervekhez, titkosszolgálatokhoz kapcsolódott,[7] a század második felére a korábbi zárt állami jellegű felhasználásból kikerült a gazdasági, üzleti és egyéb szereplőkhöz. A kibertér térhódításával az információk tömeges jellegű, szabad elérhetősége biztosítottá vált, hiszen mint Szűts is megfogalmazza: „A mindenhol jelen lévő számítástechnika hatására az informatikai eszközök beépülnek környezetünkbe […] és ezzel együtt társadalmunkba is.”[8]

Nyílt jellege miatt az OSINT fejlődése rendkívül dinamikus és széles körű, egyedi és rendszerszintű információgyűjtési lehetőségei körül jelentős informatikai piacifejlesztői szegmens épült ki. Alkalmazási irányait, a világhálón keresztül elérhető adatok feldolgozhatóságának, felhasználásának témakörét szintén több tudományterület irányából, így például az informatika vagy akár a társadalomtudományok irányából kutatják. A témakörre is adaptálható Szűts informatika fejlődéséhez kapcsolódó megállapítása, miszerint a kutatók között „egyfajta felosztás alakult ki a munkát illetően: a hálózati kommunikációval foglalkozó mérnökök a jelenség technikai aspektusait vizsgálják, a kommunikációkutatók az információ átadásának folyamatát

2 Lévay 2006.
3 Lásd többek között a *Nemzetbiztonsági Szemle* jelen 2019/2. számában megjelenő Szabó Károly: *Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről*, vagy Solti István: *Az OSINT információgyűjtő eszközeiről* szóló tanulmányait.
4 Lévay 2006.
5 Vadász–Séllei 2017, 189.
6 Péterfalvy 2015, 17.
7 Schaurer–Störger 2010.
8 Szűts 2018, 53.

veszik górcső alá, míg a társadalomtudósok az egyénre és a közösségekre gyakorolt hatásokra kíváncsiak".[9]

Napjainkra az OSINT a köztudatban összeolvadt az interneten folytatott információszerzéssel, függetlenül annak egyedi vagy rendszerszintű megoldásaitól, témakörétől, vagy akár a megszerezhető adatok típusától, jellegétől. Az OSINT az elmúlt évtizedekben lényegében kinőtte a korábbi szűk fogalmi keretét, és kis jóindulattal szinte minden ide sorolható, ami nyílt forrásból elérhető és gyűjtője számára valamilyen relevanciával bír. A háttérben azonban a kibertér fejlődésével és a személyiségi jogok védelmével olyan szakmai viták is megfigyelhetők, mint az adatgyűjtési megoldások jogszerűsége, a nyílt információgyűjtés „határai", valamint a tömeges jellegű adatgyűjtések és feldolgozhatóság kérdése.

A kezdetben még a műsorszórásban megjelenő, majd később az interneten elérhető információk figyelése, monitorozása és az ott elhangzottak felhasználása egyre inkább nélkülözhetetlen információkat jelentett felhasználói számára. Az ICT[10]-környezet robbanásszerű fejlődésével azonban egyrészről átalakultak azon információs közegek, amelyek az OSINT számára a leginkább releváns forrásokat jelenthetik, másfelől átalakultak az információk megszerzésének és feldolgozásának módjai is. A felhasználói szokások változásával párhuzamosan így a nyílt információgyűjtés előterébe kerültek többek között a közösségi média különböző felületei, hiszen az itt megjelenő hírek számos esetben a biztonságra közvetlen hatást gyakorolnak (gondoljunk csak a terrorista hálózatok toborzó tevékenységére, vagy akár a nagyobb tömegek befolyásolásának szándékára).

Az OSINT jelene

Az OSINT mint sajátos hírszerzési ág, információgyűjtési terület jelenét tekintve mit is láthatunk?

- Az OSINT lehetőségeinek felhasználása érdekében számos alkalmazási területen saját információgyűjtő képességeket alakítottak ki, amelyek között a nemzetközi tevékenységek,[11] a kormányzati biztonsági szervek, az üzleti szféra, vagy akár a nem állami szereplők (NGO[12]) is megtalálhatók. Az OSINT-tevékenységek iránt jelentkező „megrendelői" igények kiszolgálására ugyanakkor számos olyan megoldás (például információbórkerek) is létrejött, amelyek internetre épülő adatgyűjtési megoldásaikkal, szolgáltatásaikkal, illetve szoftverfejlesztéseikkel tették professzionálissá a tevékenységet. Számos ország biztonsági szervei (rendőrség, nemzetbiztonsági szolgálatok) kezdték el az OSINT ellenőrzési és kutatási képességeit növelni, amelyek között megjelentek a nyílt interneten, a deep weben, a darkneten, valamint a közösségi oldalakon történő információgyűjtés lehetőségei. A megváltozott információmegosztási platformok folyamatosan alakították a kapcsolódó fejlesztések irányait is.

9 Szűts 2018, 127.
10 Information and Communications Technology.
11 Uri 2012.
12 Non-governmental organization – nem kormányzati szervezet, civil szervezet.

Lényegében az internet az ott megtalálható nyílt adatoknak köszönhetően adott teret az új tevékenységek kialakulásának.[13]

- Előtérbe kerültek az OSINT módszereinek jogszerűségéhez, annak határaihoz köthető szakmai viták. Információs társadalmunkban joggal merülhet fel a kérdés, hogy pontosan hol is húzódhat a kibertérben folytatott OSINT-tevékenység határa, és elsődlegesen a nyíltan elérhető forrásokat kell tekintenünk, vagy akár azon módszereket, amelyek – habár széles körben elérhetőek – speciális ismereteket igényelnek. Az OSINT-jellegű kutakodás kapcsán szinte biztosan felmerül a kérdés, hogy annak végzője számára az interneten megtalálható minden megoldás etikusnak, esetenként jogszerűnek tekinthető-e.[14] Igaz, számos esetben maguk a módszerek is *nyíltan* elérhetők, mindez azonban nem jelenti egyértelműen, hogy azok alkalmazása minden felhasználó számára *legálisnak* tekinthető. A nyílt információk és források jelentőségét felismerve több kutatóintézet és egyetem is kutatási irányai közé emelte az OSINT-tevékenységet, amelyek arra is rávilágítottak, hogy a *nyílt* információgyűjtés képessége számtalan (például jogi, etikai, gazdasági, technológiai) korláttal rendelkezhet. Gyakran hangoztatott előnyei (például költséghatékonyság, aktualitás, biztonságos alkalmazás – kockázatmentes „kutakodás" lehetősége), valamint hátrányai (például információdömping, nyelvi képességek szükségessége, időtényező) mellett kiemelten fontos szemponttá vált az információk megbízhatóságának[15] kérdése.
- Az OSINT eszközei és módszerei nyilvánossága kapcsán szembesülhetünk az alkalmazott eszközök *átláthatóságának*[16] és az adatszerzés *mélységének* kérdésével. Fejlődő technológiai környezetünkben nap mint nap jelennek meg azon új megoldások, amelyeket például egy-egy közvetlenül nem értelmezhető információ megjelenítéséhez rutinszerűen felhasználunk.[17] Az eszköz *nyílt elérésénél* azonban már kérdésként merülhet fel, hogy mitől lesz az információ értelmezését segítő megoldás is nyílt egy olyan kibertérben, ahol számtalan forrásból akár a hackertechnikák szürke zónájához sorolható megoldások is szabadon elérhetők. Az OSINT kapcsán fontos hangsúlyozni, hogy az információ megszerzésére amellett, hogy a megjelenő információ nyíltan elérhető, csak passzív módon, legális eszközökkel kerülhet sor, egyéb megoldások már akár a hackingtevékenységek irányába mutathatnak. A biztonsági struktúrák,

---

13 https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security- private-sector-public-safety/ (A letöltés dátuma: 2019. 02. 10.)

14 A témával foglalkozó egyik áttekintett szakirodalom sajátos példaként veti fel például az interneten „kiszivárogtatott" állami szintű minősített információk nyílt internetes felületen történő elérésének problematikáját. Hassan–Hijazi 2018, 1.

15 A hiteles információkhoz történő hozzájutást segíthetik a professzionális OSINT-megoldások mellett a különböző állami és nem állami szereplők által kezelt adatbázisok (például tudományos adatbázisok). Ugyanezen kategóriába sorolhatók a gazdasági, pénzügyi élet területein alkalmazott megoldások (példaként a tőzsdei információk azonnali, illetve késleltetett elérése közti különbség említhető), amelyek a gyors gazdasági döntéseket segíthetik.

16 Wells 2016.

17 Gondoljunk egyszerűen egy olyan adatra, amely csak egy szabadon, bárki által letölthető nyílt programmal válik számunkra értelmezhetővé. Ebben az esetben mind a forrás, mind az annak értelmezéséhez szükséges megoldás nyíltan elérhető (eltekintve attól, hogy alkalmazása esetleg már speciális tudást feltételez).

nemzetbiztonsági szervezetek esetében azok állami célú feladatellátása és jogszabályi lehetőségei mentén azonban ezen eszközök és módszerek szélesebb körben értelmezhetők.

- Gyakran hangoztatott szempont az OSINT költséghatékonysága, amely a többi információgyűjtési terület forrásigényét feltételezve valóban egyértelműnek tűnik, hiszen relatíve kis költséggel rendkívül nagy számú információt érhetünk el.[18] A megfelelő, professzionális szakmai képesség (idesorolva az OSINT professzionális informatikai megoldásait és a szükséges szakértői, elemzői bázist) kialakítása azonban akár már jelentősebb forrásokat igényelhet. Ennek eleme a hozzáértő, egyre inkább az informatikai megoldások iránt nyitott szakmai állomány alkalmazása, amely a magas szintű OSINT-képesség működtetésének egyik kulcstényezője. Itt természetesen az alapszintű OSINT-tevékenységen túlmutató ismeretek megszerzése (idesorolva a lehetséges ágazati jellegű ismereteket, például üzleti, gazdasági, rendvédelmi ismeretek) azonban időt, felkészülést és nem utolsósorban a változások folyamatos nyomon követését igénylik. Szót kell ejteni a speciális tudásra és képességekre épülő információbrókerekről is, akik már adott anyagi ellenszolgáltatásért biztosíthatják az információmegrendelő számára azon szükséges információkat, amelyek megszerzésére az adott félnek sem szakmai képessége, sem eszközrendszere nem áll rendelkezésre. Ugyanide sorolhatók egyes fizetős adatbázisok változatai is, ahol az alapvetően nyíltan elérhető adatok mentén az anyagi korlátok megléte szabhat gátat az információk elérésének. Azt gondolhatnánk, hogy ezek forrásigénye elhanyagolható, azonban ha csak a jelentősebb nemzetközi tudományos adatbázisok jogszerű, folyamatos online elérésére gondolunk, akár jelentős költségek is felmerülhetnek. Ennek egyszerűbb példái azon tőzsdei mozgásokat megjelenítő megoldások is, amelyeknek például csak időben késleltetett változatai érhetők el ingyenesen.
- Az idővel való versengés az OSINT egyik legfontosabb elemévé vált, amely az egyéb szempontoknak történő megfelelés (például hitelesség, ellenőrzöttség) esetén a gyors döntéshozatal nélkülözhetetlen tényezője. A globális média korában az úgynevezett CNN-effektust szokták említeni, hiszen a média is a rendkívül gyors, aktuális információk megszerzésében és közzétételében érdekelt. Mint Botz 2000-ben közzétett írásában kifejti, „az OSINT […] részben a hírszerzés válasza a »CNN-effektusra«, azaz a professzionális hírszolgáltatók versenyére, amely nemcsak a közvélemény, hanem a döntéshozók kegyeinek megnyeréséért is folyik”.[19] Véleményem szerint máig igaznak tekinthetők megállapításai, miszerint a mérleg a hírszerzés oldalára dől, amely „szakmai kvalitásai alapján megbízhatóbb, tárgyilagosabb, tényszerűbb, mélyebbre hatoló, jobban a felhasználói igényekhez igazított, rendszerezőbb, szakszerűbb és vezethetőbb, mint a szenzációhajhász, manipuláló és manipulálható média”.[20]

[18] Bányász 2015, 24.
[19] Botz 2000, 27.
[20] Botz 2000, 27.

- Az OSINT-források mentén szembesülhetünk az álhírek/információk[21] jelenségével, „az online hamis hírek előrejelzett növekedésével”.[22] Mindez hamar a kutatók látókörébe került, amely az OSINT oldaláról az egyes adatok, illetve információk hitelességének kérdését és a mögöttes vélt vagy valós megtévesztési szándékokat vetheti fel. Nemzetbiztonsági szempontból a propaganda, szándékos megtévesztés, információs műveletek digitális formáinak korszakában mindennek rendkívüli jelentősége van. A történelem korábbi példáihoz viszonyítva az eltérés talán csak annyi, hogy napjaink megtévesztési műveleteinek elsődleges színterei az elektronikus média különböző megjelenési formáira tevődtek át. A digitális közösségi média térhódításával, az egyének által generálható hírek gyors terjedésével hatásuk fokozottan jelenik meg, és ellenőrzöttség hiányában rendkívül gyorsan válhatnak akár a hitelesnek vélt források részeivé is. A biztonságot befolyásoló, az adott állam szuverenitását, működésének megzavarását okozó hatásuk miatt jelentőségük és ezáltal kiszűrésük feladata vitathatatlan. (A közösségi oldalakon és egyéb internetes médiafelületeken megjelenő hatalmas információmennyiségből a felhasználók számára szinte lehetetlen a hamis hírek kiszűrése, amely még az információgyűjtésre, elemzésre-értékelésre szakosodott szerveket is komoly feladat elé állíthatja.)
- Előremutató kérdésként jelenik meg az interneten nyíltan elérhető adatok tömeges jellegű kereshetőségének, megszerzésének, feldolgozhatóságának problematikája, amely lehetőségét szintén a fejlődő technológiai környezet hozta létre. Gondoljunk csak a napjainkban már globálisan elterjedt üzleti célú adatgyűjtésre (például trendelemzés), amelyek akár életvitelünkbe, szokásainkba, érdeklődési körünkbe is betekintést engedhet. A közösségi oldalakhoz köthető az elmúlt években kirobbant, már említett adatvédelmi botrány (Cambridge Analytica[23]) is, amely jól jelzi, hogy a nyílt információgyűjtés határán létrehozhatók olyan személyes jellegű adathalmazok, metaadatok, amelyek tömeges feldolgozása már szenzitív kumulált adathalmazként értelmezhetőek.[24] Végeredményként a különböző adatbázisokban elérhető egyedi adatok összevetése révén akár minőségileg új, az eredeti rendeltetési céljától eltérő adatkoncentráció jöhet létre. Az adatbázisokban történő keresés kapcsán érdekes gondolatot vet fel a Vadász–Séllei szerzőpáros is, miszerint nehéz a valóságban pontos határt vonni a nyílt forrású információkeresés és

[21] Gyakran használt kifejezés az úgynevezett „fake news”, amely kapcsán a szakirodalmak bővelkednek a meghatározásokban, ezek közös elemeként jelenik meg, miszerint olyan valótlan információkról beszélhetünk, amelyekkel egy adott cél érdekében egyéneket, vagy szélesebb közösségeket kívánnak megtéveszteni. Irányait tekintve a politikai jellegű álhírektől kezdve, a gazdasági-üzleti irányokig számtalan megoldásával találkozhatunk.

[22] Hassan–Hijazi 2018.

[23] Lásd: www.europarl.europa.eu/news/hu/headlines/society/20181005STO15108/facebook-botrany-tobbet-kell-tenni-az-adatvedelmi-torveny-ervenyre-juttatasaert (A letöltés dátuma: 2019. 02. 10.)

[24] Szinte közhelynek tekinthető, hogy a kibertér össztettsége révén a legkörültekintőbb akarattal is mindenki olyan digitális nyomokat hagy maga után, amelyek nyílt elérése révén információk keletkeznek életére, szokásaira, preferenciáira nézve. Ezek tudatos felhasználása, amellett, hogy névtelenül lecsupaszítva az üzleti célú felhasználást segíthetik, a politika oldalán akár befolyásolási lehetőségeket is megalapozhatnak az egy adott csoport irányába (profilozás lehetősége, kapcsolati hálók).

a tágabban értelmezhető *információkeresés* között. A témakör hazai kereteit vizsgáló szaktanulmány fontos megállapítást tesz: „Ismereteink szerint a nyílt forrású adatok keresése nem kell, hogy célhoz kötötten történjen. Más szavakkal: nem tiltott a tömeges információkeresés (bulk search).”[25]

- Az OSINT üzleti-vállalati és kormányzati megoldásainak fejlesztése ma már önálló piaci szegmensként jelenik meg. Mint a Market Research Future ötéves (2018–2023) OSINT piaci előrejelzéséről szóló tájékoztatójában rámutat, a globális OSINT piaca folyamatosan – a 2017-es 2865,9 millió dollárról 2023 végére várhatóan 7047,7 millió dollárra – növekszik.[26] A kutatási jelentésről szóló rövid ismertetőben hangsúlyozzák, hogy számos OSINT technikai megoldás és irány jelent meg (big data adatszoftverek, videóelemzés, szövegelemzés, vizualizációs megoldások, kiberbiztonság, webelemzés, közösségi médiaelemzés), amelyek egyre bővülő piaccá növik ki magukat,[27] és ahol technológiai szempontból a kiberbiztonság tekinthető a vezető szegmensnek. Egy másik, a témával foglalkozó előrejelzés[28] szintén a globális szintű nyílt forráskódú hírszerzési piac növekedését – 2018 és 2026 között várhatóan 23,7%-kal – vetíti előre. „A globális OSINT-piac élvonalában Észak-Amerika van. […] A piac növekedése nagyrészt a felhőtechnológia és az IoT[29] egyre növekvő elfogadásából származik a régióban.” [30] Növekszik a Webint[31] és a Social Media Monitoring piaca is,[32] hiszen ezen források a nyílt adatokra alapozva szinte azonnal adatokat szolgáltathatnak, a kormányzati vagy akár gazdasági szereplők számára.

A jövő kérdései

- Az OSINT-megoldások számos előnnyel és hátránnyal rendelkeznek, amelyek közül leginkább a dinamikusan változó ICT-környezetben történő szabad fejlődés lehetősége emelhető ki. Mindez előrevetíti az alapvetően nyíltként aposztrofált OSINT folyamatosan változó sajátosságait: információtechnológiai környezet fejlődése, a mesterséges intelligencia egyre szélesebb körben történő alkalmazása, vagy akár az adat és szövegbányászati technológiák, vagyis maga az információk elérésének sajátos formái. A fejlődés mögött a szabad fejlesztési lehetőségek, az egyre bővülő, nyíltan, digitális formában elérhető szabad források, valamint az OSINT-képességek iránti jelentős piaci kereslet

---

25 Vadász–Séllei 2017, 189.

26 www.marketresearchfuture.com/press-release/open-source-intelligence-market (A letöltés dátuma: 2019. 02. 10.) (Megj.: jelen tanulmány szerzőjének a teljes előrejelzés tanulmányozására nem nyílt lehetősége.)

27 www.marketresearchfuture.com/press-release/open-source-intelligence-market (A letöltés dátuma: 2019. 02. 10.)

28 www.businesswire.com/news/home/20181214005137/en/2018-Open-Source-Intelligence-Market-Global-Analysis (A letöltés dátuma: 2019. 02. 10.)

29 Internet of Things – „dolgok internete”.

30 *Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023*, 2018.

31 Web Intelligence.

32 https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security-private-sector-public-safety/ (A letöltés dátuma: 2019. 02. 10.)

húzódik meg.[33] Mindez érthető, hiszen a gazdasági élet szereplői jelentős arányban fektetnek be olyan OSINT-képességekbe, amelyekkel hatékonyságukat növelhetik, piaci szerepüket erősíthetik. Vezető szerepet a belbiztonsági szegmens tölt be, míg a katonai és védelmi terület várhatóan a leggyorsabban növekvő szegmens lesz.[34]

- Az adatvédelmi és etikai kérdésekhez fontos megemlíteni, hogy a nyílt forrásokból származó adatok összegyűjtése a jövőben is felszínen tartja az adatvédelmi és jogi kérdéseket.[35] Ennek egyik elemének tekinthető a GDPR általános adatvédelmi rendelet, amely a személyes adatok mentén érinti a kérdéskört. A sokféle nyílt formában elérhető adat „kategóriájában" azonban talán kevésbé tudatosulnak az egyes metaadatként megjelenő, anonim adatokat tartalmazó adathalmazok, amelyek meghatározott szempontú feldolgozást követően akár „értékes" részelemeket is tartalmazhatnak.
- A jövőben a rohamosan fejlődő technikai képességek mentén az OSINT és az azon túlmutató képességek között továbbra is meghatározó marad az a „szürke zóna", amely megfelelő szaktudás és technikai képesség birtokában túlmutathat a nyílt források legális felhasználásának lehetőségén.[36]
- Az álhírek kapcsán felértékelődő kérdés lesz, hogy hogyan lehet kiszűrni a téves/hamis információkat, azok típusától, illetve megjelenési platformjától függetlenül. Az álhírek kapcsán a témakörben áttekintett több forrás is felhívja a figyelmet a hitelesség biztosításának nehézségére, ahol az információmennyiség nagyságrendjéből és összetettségéből adódóan a humán elemzési tényezők mellett különös jelentőségek kaphatnak a jövőben a *mesterséges intelligencia* képességei. A hatalmas mennyiségű, internetes felületen elérhető adathalmazok gépi keresésének, ellenőrzésének során nagyobb valószínűséggel derülhet fény az egyes álhírek ellentmondásaira, segítve ezzel a hitelesség megállapítását.[37] Ugyanakkor szakértők fontosnak tartják[38] a szabadság és emberi jogok, valamint a társadalmat érintő fenyegetések egyensúlya mentén a big data elemzésekhez kapcsolódó OSINT-tevékenység további vizsgálatainak szükségességét is.
- A technológiai környezet fejlődésével, az egyre mélyebb informatikai és adatbázisfeldolgozói ismereteket igénylő OSINT-tevékenység mentén bizonyos szakmai ágak jelentős fejlődés előtt állnak (így például az adatfeldolgozás, -értékelés, -elemzés területei). Mindez azonban a nemzetbiztonsági szervezetek humán erőforrásának fejlesztési igényét is előrevetíti, hiszen „a hírszerzői lehetőségek kihasználását illetően számos szakértő azon a véleményen van, hogy a szolgálatok a megfelelő képzettség hiányában nem képesek az ipar

33 *Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023,* 2018.
34 *Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023,* 2018.
35 Gibson 2016.
36 Boda–Dobák 2015.
37 www.cobwebs.com/fake-news-challenges-for-osint/ (A letöltés dátuma: 2019. 02. 10.)
38 Staniforth 2016.

által kínált új technikai lehetőségeket felhasználni, például az elemzés, az események követése és a kommunikáció területén".[39]

- A szabadon elérhető szoftverek, valamint azok nyílt környezetben történő fejlesztésének lehetősége a jövőben még inkább lehetővé teszik, hogy a nyíltan elérhető adathalmazok vagy akár adott események OSINT-feldolgozását szabadon bárki elvégezhesse és elemzéseket készítsen.[40] A biztonságért felelős területeken vélhetően erősödni fog az OSINT azon előnye is, miszerint „szabadon hozzáférhető adatok miatt az együttműködés lehetőségét biztosítja külső szakértőkkel".[41]
- Mint Akhgar kifejti a tanulmányában,[42] a big data és az OSINT, illetve a tömeges adatállományok elemzési képessége, a jövőben egyedülálló lehetőséget biztosítanak a biztonsági szolgálatoknak a különböző veszélyek feltárására. Nemzetbiztonsági szempontból a fő cél, hogy az OSINT-megoldások járuljanak hozzá, segítsék a bűnüldöző szervek és a biztonsági szolgálatok információgyűjtési képességeit, támogassák a különböző információkon alapuló döntéshozatalt.[43] Szakértői tanulmány szerzője[44] hívja fel a figyelmet a big data alkalmazásának gondos mérlegelésére és fokozatosságára, hiszen ellenkező esetben (például túlterjeszkedve) az állam és polgárai közötti kapcsolat megromlásához vezethet. Mindez kétségtelenül megköveteli a meglévő hírszerzési modellek, a kapcsolódó rendszerek és folyamatok áttekintését.[45]
- Összességében a kibertérhez köthető nyílt forrásokból történő információgyűjtés jelentősége a jövőben még inkább meghatározó lesz, ide sorolva a 21. század nemzetbiztonsági célú feladatrendszereit és szervezeteit is, ahol a szolgálatok „sajátos szakmaiság mentén egyre kifinomultabb megoldásokkal törekszenek a számukra értékes információk gyűjtésére, elemzésére, értékelésére".[46] Tendenciaként egyrészről a személyiségi jogok további védelme kerülhet előtérbe, másrészről a metaadatként értelmezhető részadatok tömeges, akár mesterséges intelligenciával támogatott feldolgozása nyithat új, eddig ismeretlen területeket. Mint Nihad A. Hassan és Rami Hijazi kifejti könyvében, a jövőben elterjedő IoT-eszközökből származó hatalmas mennyiségű metaadatok bonyolult analitikai megoldásokat igényelnek majd, és „a mesterséges intelligencia és a gépi tanulási technológiák fejlődése ismét átalakítja az OSINT-ot az elkövetkező években".[47]

---

39 Kis-Benedek 2013, 109.

40 www.datasciencecentral.com/profiles/blogs/exploring-the-vw-scandal-with-graph-analysis (A letöltés dátuma: 2019. 02. 10.)

41 Bányász 2012, 157.

42 Akhgar 2016.

43 Az OSINT vs. nemzetbiztosági szervezetek relációban nem feledkezhetünk meg arról sem, hogy az OSINT megközelítése kettős, hiszen egyrészről az információgyűjtési lehetőségek maximális kihasználásában, másrészről a hozzájuk kapcsolható információk védelmében vagy éppen megfelelő alakításában érdekeltek.

44 Staniforth 2016, 18.

45 Staniforth 2016.

46 Boda–Dobák 2015, 22.

47 Hassan–Hijazi 2018, 342.

Felhasznált irodalom

Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds. (2016): *Open Source Intelligence Investigation, From Strategy to Implementation*. Springer. DOI: https://doi.org/10.1007/978-3-319-47671-1

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. évf. 2. sz. 21–36.

Bányász Péter (2012): A közösségi média szerepe a 21. század hadseregeiben. *Hadtudomány,* 22. évf. 1–2. sz. 152–161.

Boda József – Dobák Imre (2015): A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században In: *A nemzetbiztonság technikai kihívásai a 21. században.* Budapest, NKE Szolgáltató Nonprofit Kft. 16–22.

Botz László (2000): A Katonai Felderítő Hivatal feladatai a NATO-csatlakozás után. *Külpolitika,* 6. évf. 1–2. sz. 22–36.

David, Robert – Vivas, Steele (2004): *Special Operation Forces Open Source Intelligence (OSINT) Handbook.* Oakton. OSS International Press.

Gibson, Helen (2016): Acquisition and Preparation of Data for OSINT Investigations. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds.: *Open Source Intelligence Investigation, Advanced Sciences and Technologies for Security Applications*. Springer International Publishing AG. DOI: https://doi.org/10.1007/978-3-319-47671-1_6

Hassan, Nihad A. – Hijazi, Rami (2018): *Open Source Intelligence Methods and Tools, A Practical Guide to Online Intelligence*. Berkeley, Apress Media. DOI: https://doi.org/10.1007/978-1-4842-3213-2

Kis-Benedek József (2013): A nemzetbiztonsági szolgálatok együttműködése. *Hadtudomány,* 23. évf. 1–2. sz. 100–114.

Kleinsmith, Erik (2016): *Fake News and Data Mining: Mapping Today's Media for Intel Analysis*, December 13, 2016. Elérhető: https://inhomelandsecurity.com/fake-news-data-mining-intel/

Lévay Gábor (2006): *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Egyetemi jegyzet. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

McKeown, Sean – Maxwell, David – Azzopardi, Leif (2014): *Investigating People: A Qualitative Analysis of the Search Behaviours of Open-Source Intelligence Analysts*. Regensburg, Germany. DOI: https://doi.org/10.1145/2637002.2637023

Péterfalvy Attila (2015): Néhány gondolat a nyílt információgyűjtés és a személyes adatok védelmének összefüggéseiről. In: *A nyílt információgyűjtés fejlődő területei*. Nemzetközi Tudományos-Szakmai Konferencia Tanulmánykötet. Budapest, Belügyi Tudományos Tanács.

Schaurer, Florian – Störger, Jan (2010): *The evolution of Open Source Intelligence.* OSINT Report 3/2010, International Relations and Security Network (ISN), ETH Zurich. Elérhető: www.research-collection.ethz.ch/bitstream/handle/20.500.11850/25221/eth-2238-01.pdf (A letöltés dátuma: 2019. 02. 10.) DOI: https://doi.org/10.3929/ethz-a-006251404

Staniforth, Andrew (2016): *Open Source Intelligence and the Protection of National Security.* In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds.: *Open Source Intelligence Investigation.* Advanced Sciences and Technologies for Security Applications. Springer International Publishing AG. DOI: https://doi.org/10.1007/978-3-319-47671-1_2

Szűts Zoltán (2018): *Online – Az internetes kommunikáció és média története, elmélete és jelenségei.* Budapest, Wolters Kluwer Hungary.

Vadász Pál – Séllei Márton (2017): Az információkeresés magyar jogi környezete. *Hadtudomány,* 27. évf. 1–2. sz. 178–191. DOI: https://doi.org/10.17047/HADTUD.2017.27.1-2.178

Uri László (2012): *A rendőri tanácsadó misszió és a nyílt forrású információgyűjtés.* Elérhető: http://mhtt.eu/hadtudomany/2012/2012_elektronikus/2012_e_Uri_Laszlo.pdf (A letöltés dátuma: 2019. 02. 10.)

Wells, Douglas (2016): Taking Stock of Subjective Narratives Surrounding Modern OSINT. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds.: *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications.* Springer International Publishing AG. DOI: https://doi.org/10.1007/978-3-319-47671-1_5

Internetes források

Fake News Challenges for OSINT (2018). Elérhető: www.cobwebs.com/fake-news-challenges-for-osint/ (A letöltés dátuma: 2019. 02. 10.)

https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security-private-sector-public-safety/ (A letöltés dátuma: 2019. 02. 10.)

Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023 (2018). Elérhető: www.marketresearchfuture.com/reports/open-source-intelligence-market-4545 (A letöltés dátuma: 2019. 02. 10.)

The 2018 Open Source Intelligence Market: Global Analysis & Forecast Through 2016–2026 (2018). Elérhető: www.businesswire.com/news/home/20181214005137/en/2018-Open-Source-Intelligence-Market-Global-Analysis (A letöltés dátuma: 2019. 02. 10.)

www.datasciencecentral.com/profiles/blogs/exploring-the-vw-scandal-with-graph-analysis (A letöltés dátuma: 2019. 02. 10.)

www.europarl.europa.eu/news/hu/headlines/society/20181005STO15108/facebook-botrany-tobbet-kell-tenni-az-adatvedelmi-torveny-ervenyre-juttatasaert (A letöltés dátuma: 2019. 02. 10.)

www.marketresearchfuture.com/press-release/open-source-intelligence-market (A letöltés dátuma: 2019. 02. 10.)

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 94–108. • DOI: 10.32561/nsz.2019.2.8

Gesztei László[1]

Az alapjogok nemzetbiztonsági szempontból történő korlátozása és az alapjogok korlátozásának alkotmánybírósági értelmezési gyakorlata I.[2]

The Restriction of Fundamental Rights for National Security and Its Interpretation by the Constitutional Court of Hungary I.

Az alapjogok korlátozásának a kérdése egyidős maguknak az alapjogoknak az állam által történő elismerésével és védelmével. Azonban felmerült a kérdés, hogy az egyes alapjogoknak hol húzódik a határa, meddig érvényesülhetnek, illetve mikortól szükséges és kívánatos a korlátozásuk. Az alapjogok korlátozásának speciális esetét jelentik a nemzetbiztonsági érdekek. Az alapjogok korlátozásával kapcsolatos vitának új lendületet adott a Nyugat-Európát sújtó terrorizmus elleni védekezés, ezzel kapcsolatban előtérbe kerültek a nemzetbiztonsági érdekek és ezek alkotmányjogi vonatkozásai. Magyarországon az alapjogok tartalmának megállapításában és alakításában az Alkotmánybíróság kiemelkedő szerepet töltött és tölt be. A jogértelmező tevékenységének kiemelt területe az alapjogok korlátozásának a kérdése és gyakorlata. A tanulmány első része az Alkotmánybíróság értelmező, jogfejlesztő szerepét tekinti át az alapjogok tartalmának konkretizálásával összefüggésben, továbbá az alapjogok korlátozásának indokait, céljait, illetve az alapjogok korlátozásával kapcsolatos alkotmánybírósági gyakorlatot.

Kulcsszavak: alapjogok, alapjogok korlátozása, Alkotmánybíróság, nemzetbiztonsági szempontok

[1] Dr. Gesztei László doktorandusz, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. ORCID-azonosító: 0000-0002-7255-4112.

[2] Az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg az alábbi tanulmány. 2018.

The question of restricting fundamental rights is coeval with the recognition and protection of fundamental rights by the state. However, the question arises as to where the limitations of each fundamental right lie, for how long they can take effect, and when their restriction is necessary and needed. National security interests are a special case of restricting fundamental rights. The debate on the restriction of fundamental rights has been given new impetus by the defence against terrorism in Western Europe, with this debate national security interests have come to the fore, as its constitutional aspects. In Hungary, the Constitutional Court has played primary role in establishing and shaping the content of fundamental rights. One of the priority areas of its interpretative activity is the question and practice of restricting fundamental rights. The first part of the study considers the role of the Constitutional Court as an interpretative and legal development in the context of concretising the content of fundamental rights. Furthermore, the reasons and objectives of the restriction of fundamental rights, and the case law of the Constitutional Court relating to the restriction of fundamental rights.

Keywords: fundamental rights, restriction of fundamental rights, Constitutional Court of Hungary, interest of national security

Az alapjogok tartalma és az Alkotmánybíróság értelmező szerepe

Az alkotmányok a társadalom működésével kapcsolatos érdekek és célok gyűjteményei, az állam működésének szabályozása mellett rögzítik az adott állam által elismert és védett alapjogokat is. Az alapjogok elismerésének és védelmének célja bizonyos esetekben az, hogy a természetes és jogi személyeket megóvja az állam hatalmától. Az állam esetében az a látszólag paradox helyzet áll fenn, hogy állami szerv aktív védelme szükséges egy másik állami szerv túlkapása vagy jogsértése ellen, részben ezt a helyzetet kell az alkotmánybíróságoknak és az ombudsmannak feloldania. Az alkotmányok védelmének legfőbb szervei tipikusan a rendes bíróság szervezetétől elkülönülten felállított alkotmánybíróságok,[3] hasonlóan ahhoz, ahogy ezt az Alkotmánybíróságról szóló 2011. évi CLI. tv. (a továbbiakban: Abtv.) 2. §-a is kimondja. „Az Alkotmánybíróság az Alaptörvény védelmének legfőbb szerve. Feladata a demokratikus jogállam, az alkotmányos rend és az Alaptörvényben biztosított jogok védelme, a jogrendszer belső összhangjának megőrzése, valamint a hatalommegosztás elvének érvényre juttatása."[4] Az Alkotmánybíróság kiemelten fontos feladata az absztrakt módon megfogalmazott alapjogok területén azok tartalmának kibontása általánosságban, illetve

[3] Bizonyos országokban a történelmi hagyományokat fenntartva az alkotmánybíráskodás feladatkörét nem elkülönült alkotmánybíróság látja el, hanem a rendes bírósági struktúrán belül a legfelsőbb bírósági szint foglalkozik ezzel a feladattal.

[4] www.alkotmanybirosag.hu (A letöltés dátuma: 2018. 10. 15.)

az egyedileg szabályozott életviszonyok tekintetében.[5] „Az Alkotmánybíróság ugyanis az alapvető jogok Alkotmányba foglalt katalógusát nem tekinti zárt rendszernek, mivel az egyes nevesített alapjogok értelmezése során kibontja az Alaptörvényben deklarált jogok – adott tényállásra vonatkoztatható – aspektusait: az alapjog lényeges tartalmát, funkcióját, más alapjoghoz való viszonyát, korlátait és biztosítékait."[6] Az alapjogok esetében további feladat az alapjogi kollízió feloldása és a jogalkotó által szabályozás alá vont életviszonyok esetében felmerülő alapjogkorlátozás alkotmányosságának vizsgálata. Az alkotmányok funkciójukból kifolyóan az alapjogokat röviden és elvi szinten deklarálják, az egyes alapjogok esetében az alkotmányok az adott alapjog érvényesülésének szabályait törvényi szintű jogalkotásra bízzák, amennyiben ez nem így lenne, akkor az alkotmányok terjedelmük miatt áttekinthetetlen és alkalmazhatatlan joganyagok lennének. Magyarországon a sarkalatos törvények kihangsúlyozzák egy adott életviszonyra vonatkozó szabályozás kapcsán annak fontosságát, kiemelt szerepét. „Fontos azonban megjegyezni, hogy egyrészt minősített többség/egyszerű többség szerinti differenciálás nem tételez fontossági sorrendet az alapjogok között, hanem inkább azt szolgálja, hogy az alapjogi szabályozás lehetőleg ne váljon politikai kompromisszumok tárgyává."[7] Az elvont elvek tartalommal való megtöltése elsődlegesen a jogalkotó feladata, az alkotmányos keretek tiszteletben tartását jogállami keretek közt az Alkotmánybíróság védelmezi. Felmerül a kérdés, hogy az alapjogok tartalma miért képezi vita tárgyát, miért van szükség egyáltalán a fogalmak jelentésének az Alkotmánybíróság általi vizsgálatára. „Az alapvető jogok vonatkozásában ennek egyik oka, hogy e jogoknak továbbra is absztrakt etikai-filozófiai jellegük van, és az egyes alapjogok az absztraktságuk, puszta etikai meghatározottságuk és jogdogmatikai konkretizálhatóságuk fokában nagy eltéréseket mutatnak, aminek következtében cizelláltságuk és kimunkáltságuk is kívánnivalót hagy maga után."[8] Az egyes fogalmak jogilag konkretizálható jelentéstartalmának bizonytalanságai mellett számos más összetettebb probléma merül fel az alapjogok gyakorlati alkalmazhatósága kapcsán. „Ez közelebbről azt jelenti, hogy a hatályos alaptörvény bár – rövid deklarációkban – egymás után felsorolja a nemzetközileg elfogadottá vált alapvető jogokat, de esetükben legtöbbször tartalmi bizonytalanság áll fenn. Nem egyértelmű, hogy az Alkotmányba foglalt egyes alapvető jogok milyen konkrét jogosultságokat jelentenek, illetve milyen részjogosítványok vezethetők le belőlük. Az sem mindig világos, hogy kit köteleznek és mire: elegendő-e a megvalósulásukhoz, hogy az állam tiszteletben tartja e jogokat, illetve nem avatkozik be, vagy többről van szó, azaz védelemben kell-e részesítenie őket, illetve aktív módon elő is kell mozdítania érvényesülésüket."[9] Az Alkotmánybíróság az Abtv. 38. §-ában foglaltak szerint a törvényben meghatározott személyek indítványára konkrét alkotmányjogi probléma összefüggésén keresztül jogosult az Alaptörvény rendelkezéseinek értelmezésére.

[5] Ennek alapján megkülönböztetjük az alapjogok szubjektív oldalát, ami egy konkrét személy ügyében, élethelyzetében jelenik meg, illetve az objektív oldalát, ami magának a védendő alapjognak a lényegében, általános értékében manifesztálódik.

[6] Chronowski et al. 2013, 23.

[7] Chronowski 2005, 207.

[8] Pokol 1993, 53.

[9] Chronowski et al. 2013, 19–20.

A 38. § (2) bekezdése szerint állami szerv jogállásával, működésével vagy feladat- és hatáskörével összefüggésben felmerülő alkotmányjogi probléma esetében, ha az az Alaptörvénnyel összhangban történő működést, illetve feladat- és hatáskörgyakorlást ellehetetleníti, illetve az értelmezési bizonytalanság a jogbiztonságot veszélyezteti. Hangsúlyozni kell, hogy az Alkotmánybíróság nemcsak a 38. §-ban meghatározott feladatának ellátása során végzi az Alaptörvény rendelkezéseinek az értelmezését, hanem a többi feladat- és hatáskörébe tartozó eljárások, különösen az előzetes és utólagos normakontroll során is. Az Alkotmánybíróság a rendszerváltást követő időszakban jelentős mértékben hozzájárult a hazai jogfejlődéshez és az alapjogok tartalmának, korlátainak, valamint érvényesülési feltételeinek konkretizálásában. Ezt részben a jogfejlesztő, alkotmányértelmező tevékenységével, másrészt az Alkotmányos rendelkezéseket sértő jogszabályi rendelkezések megsemmisítésével érte el. Az Alkotmánybíróság aktivizmusát és annak a jogfejlődésre gyakorolt hatását sokan kritizálták. A kritikák alapját az jelentette, hogy az Alkotmánybíróság tevékenységével kvázi jogalkotói szerepet vindikált magának, ami ellentétes a hatalommegosztás elvével. A túlzott aktivizmus veszélyei miatt merülhetett fel az a kérdés, hogy a túlságosan elvontan megfogalmazott normaszöveg homályos tartalma miatt elkerülhetetlenül szükséges értelmezés esetében meddig beszélhetünk a jogalkalmazáshoz szükséges mértékű és mélységű értelmezésről, és mikortól áll fenn a tényleges veszélye annak, hogy az Alkotmánybíróság átcsúszik a jogalkotói szerepbe.[10] „Az értelmezés célja ugyanis nem az eredeti alkotmányi rendelkezés jelentésváltozásának elérése, hanem a felmerült alkotmányjogi konfliktusnak a rendezése, mégpedig az alkotmányozó által megállapított normatartalom alapján."[11] Az Alkotmánybíróság kezdetben rendkívül széles jogköre miatt mégis érintetté vált a napi politikában, amihez kapcsolódott főleg Dr. Sólyom László elnöksége alatti aktivista felfogás, amit egyes, akkor „kormánypárti" politikusok kimondottan nehezményeztek. „Az Alkotmánybíróságnak ráadásul a politikai folyamatokban való akaratlan részvétele miatt bírálatok mellett szembe kellett néznie a jogtudomány egyes képviselői részéről az »alapjogi aktivizmus« és a jogalkalmazás területére való illetéktelen beavatkozás vádjával."[12] A Halálbüntetést Ellenzők Ligájának indítványa alapján meghozott 23/1990. (X. 31.) AB határozat párhuzamos indokolásában Dr. Sólyom László alkotmánybíró összefoglalta az Alkotmánybíróságnak a saját határozata kialakításához való szabadságát és annak korlátait: „Ebben az értelmezésben az Alkotmány egésze a kiindulópont. Az Alkotmánybíróságnak folytatnia kell azt a munkáját, hogy értelmezéseiben megfogalmazza az Alkotmány és a benne foglalt jogok elvi alapjait, és ítéleteivel koherens rendszert alkot, amely ma még gyakran napi politikai érdekből módosított Alkotmány fölött, mint láthatatlan alkotmány, az alkotmányosság biztos mércéjéül szolgál; és ezért várhatóan a meghozandó új alkotmánnyal vagy jövőbeli alkotmányokkal sem

[10] A problémafelvetés nem egyedi, az Európai Unió Bírósága kapcsán egyre gyakrabban merül fel a „vád", hogy az aktivista szemléletmódjával a tagállami szuverenitást érintő kérdésekben rendre a szupranacionális intézményrendszer javára dönt, ezzel is elvonva a tagállami hatásköröket. Az EUB ezeket a hatásköröket vagy azok bizonyos részeit jogértelmezés útján tereli az uniós intézményekhez a szerződések homályos vagy pontatlan megfogalmazását kihasználva.

[11] Petrétei 2011, 136.

[12] Csapody 1996, 28.

kerül ellentétbe. Az Alkotmánybíróság ebben az eljárásában szabadságot élvez, amíg az alkotmányosság fogalmának keretén belül marad."

A láthatatlan Alkotmány fikciója jelentette az alapot ahhoz, hogy az Alkotmánybíróság az egyes elveket és alapjogokat tényleges tartalommal kezdje el megtölteni, az értelmező tevékenységének csak saját önmérséklete, az Alkotmány világos rendelkezései és az alkotmányozó szándékai szabtak határt. A láthatatlan alkotmánnyal kapcsolatban sokan fogalmazták meg fenntartásaikat: „Az alkotmánybírák döntései során létrejövő és az ezekben megtestesülő »láthatatlan alkotmány« az írott alkotmány felett álló igazi alkotmány téziseként az alkotmányozó hatalom nyílt elvételét jelenti az adott ország sokmilliós közösségétől. Az alkotmánybírák sehol sem mondták még ezt ki ilyen nyíltan, mint hazánkban."[13] Dr. Sólyom László a párhuzamos indokolásában maga is elveti az Alkotmánybíróságnak az alkotmányértelmezésen keresztül megvalósuló kvázi jogalkotó vagy alkotmányozó szerepét: „Az alkotmányos jogok igen absztrakt megfogalmazásában nem fedezhető fel semmilyen jele annak, hogy a törvényhozó ezen jogok egy adott értelmezése mellett kötelezte volna el magát. De ha így is lett volna, ez az Alkotmánybíróság számára nem lehetne kiindulópont: az Alkotmánybíróság független a törvényhozó szándékától, de egyébként is aggályos lenne arra hivatkozni, hogy az eltelt egy év alatt olyan társadalmi változások játszódtak le, amelyek túlhaladottá tették az alkotmányozó eredeti koncepcióját. Ez ugyanis azt jelentené, hogy az Alkotmánybíróság megváltoztatni kénytelen az Alkotmány értelmét. Az Alkotmánybíróságnak nem erre van hatásköre." Sólyom maga is elismeri, hogy az Alkotmánybíróság az alkotmányértelmezés során alakítja magának az értelmezésnek a mércéjét is, ezért hangsúlyozza, hogy az adott fogalomnak több releváns és legális értéktartalma lehetséges, a választás ezek között az alkotmánybíró feladata és felelőssége. Amikor értékválasztásról beszélünk, akkor végső soron az alkotmányos norma tartalmának a meghatározását értjük ez alatt, ami bizonyos esetekben jócskán túlmutat a szükséges jogértelmezés hatókörén. „Az alkotmányértelmezésnek az értelmezendő jogok fogalmából kell kiindulni, mint semleges kategóriából, amelynek határaira nézve nagyfokú konszenzus állapítható meg, tartalmára nézve viszont több, eltérő értéktartalmú koncepcióval is kitölthető. Ha így járunk el, akkor az Alkotmány tág definíciói megannyi morális kérdésfeltevést (is) tartalmaznak. A pluralista társadalom lényegéhez tartozik, hogy ezekre a kérdésekre többféle válasz adható, vagyis a jogok többféle értéktartalommal kitölthetők úgy, hogy közben a jogok egész alkotmányos rendszere koherens és működőképes marad. Az Alkotmánybíróságnak a határesetekben kell beavatkoznia, azt a vonalat meghúznia, amelyen túl egy adott tartalmi koncepció (válasz) már az Alkotmány egész rendszerével (alapelveivel) nem hozható összhangba. […] Szembe kell néznünk tehát azzal, hogy az alkotmányos jog fogalmának egyik lehetséges értelme válik kötelezővé (amelyet esetleg az Alkotmánybíróság későbbi ítélkezése korrigálhat vagy a desuetudo ronthat le)."[14]

A fentiek alapján is világos, hogy az Alkotmánybíróság döntése mindig szubjektív és egy adott történelmi időszak értelmezését hordozza magában, ami nem

[13] Pokol 2017, 40.

[14] Dr. Sólyom László alkotmánybírónak a 23/1990. (X. 31.) AB határozathoz fűzött párhuzamos indokolásából, ABH 1990/88.

szakadhat el a társadalmi folyamatoktól vagy a tágabb nemzetközi környezettől, és mint ilyen, a döntések és a meghozatalukhoz felhasznált érvek, értékek is felülvizsgálat tárgyát képezhetik. Az Alaptörvény elfogadását követően újra fellángolt a láthatatlan alkotmány létjogosultsága körüli vita: „A magyar Alkotmánybíróság alkotmánymagyarázó gyakorlata az úgynevezett »láthatatlan alkotmány« elvein alapul 1989 óta. A láthatatlan alkotmány elve jelenti a korábbi történeti »íratlan« alkotmány örökségének tagadását, de ugyanakkor a kommunista alkotmány törvényes (legitim) alkotmányként való elfogadását; jelenti a hatályos alkotmány szövege megváltoztatásának hatalmát az Alkotmánybíróság által; jelenti a kettős mérce alkalmazásának elfogadását, korlátlan monetarizmus engedését; továbbá az Alkotmánybíróság által követett »értéksemleges« filozófiát. Ez a relativizmus és az antagonizmus filozófiája."[15] Az alapjogok értelmezése körül az Alkotmánybíróság álláspontja ugyan jelentős, de nem kizárólagos, az Európai Unióban az alapjogok értelmezése, fejlesztése az uniós intézményekben, uniós szerződésekben és nem utolsósorban az Emberi Jogok Európai Bíróságának joggyakorlatában jelenik meg. Az alapjogok hazai fejlődése, értelmezése nem szakad és nem is szakadhat el az uniós trendektől és irányoktól, ezt bizonyítja, hogy a tagállamok alkotmányos elvei és értékei közelednek egymáshoz, részben az alkotmányokban való megjelenési formájuk, de inkább az érvényesülésük és egységes tartalomértelmezésük során. Ezt áttételesen az Alkotmánybíróság az 57/2001. (XII. 05.) AB határozat indokolásában is megerősítette, eszerint az Alkotmánybíróság az alapvető jog korlátozásának vizsgálatánál meghatározó jelentőségűnek tekinti azokat a nemzetközi kötelezettségeket, amelyeket Magyarország nemzetközi egyezményekben vállalt. „Az alapjogok értelmezése és védelme terén látványos egységesítési folyamat mutatható ki, a nemzeti (elsősorban Alkotmánybíróságok), valamint a nemzetközi bíróságok bírái az összehasonlító jog segítségül hívásával homogenizálják az alapjogvédelem kereteit. Az alapjogok szabályozása és érvényre juttatása értékmérőként jelenik meg, ez alapján lehet értékítéletet mondani arról, hogy egy országban a jogállamiság veszélyben van vagy sem."[16] A tagállamokban működő alkotmánybíróságok egységesülő értelmezésével kapcsolatban felmerül annak a veszélye, hogy az alkotmányok kialakulásában meghatározó szerepet játszó egyedi nemzeti sajátosságok fokozatosan háttérbe szorulnak. Az Európai Unión kívülre tekintve az alapjogok deklarációja mellett látható az alapjogok érvényesülésének látványos, az aktuális hatalmi szempontoknak történő alárendelése, ezt pedig csak részben magyarázhatjuk az eltérő kulturális hagyományokkal. A nyugati értékek mint a jogállamiság, a demokrácia vagy egyes alapjogok tisztelete bizonyos országokban teljesen más jelentéstartalmat kaphatnak. Az alapjogok esetében az értelmezés politikai determinalizációja következtében a politikai változásoknak való kitettség miatt hosszú távon az alapvető jogok és azok jelentéstartalma sincs kőbe vésve, hanem időről időre értelmezés és gyakran átértelmezés tárgyává válnak. Ennek megfelelően az egyes alapjogok esetében a korlátozásuk mértéke és annak indokai is jelentősen módosulhatnak bizonyos társadalmi szintű változásokkal, elvárásokkal összhangban, akár rendkívül rövid idő alatt.

[15] Tóth 2013.
[16] Trócsányi 2014, 30.

Az alapjogok korlátozása

Amikor az alapjogok tartalmáról beszélünk, akkor kiindulópontként az alkotmányokban megjelenő normaszövegre tekintünk, viszont amikor már a fogalmaknak a tartalmáról beszélünk, akkor már más a helyzet, nem is beszélve az anyajogból levezetett egyéb alapjogok tartalmáról. Ilyenkor már nemcsak a normaszöveget vesszük figyelembe, hanem a mögöttes jelentéstartalmakat is, ebben az értelmező személy világnézetének, jogfelfogásának befolyásoló hatása mellett az adott korszak tágan vett politikai környezete, illetve erkölcsi értékítéletei is megjelennek. „Az alapvető jogoknak azonban nincs egységes, pontos és általánosan elfogadott meghatározása, mert e fogalom tartalmának jelentése, megalapozása vitatott, különösen azokon a fogalmaktól – mint természetes jogoktól, az emberi jogoktól, az alkotmányos jogoktól az alapvető szabadságoktól stb. – történő elhatárolásuk nem egyértelmű és világos."[17] Az egyes alapjogok tartalma körüli bizonytalanság az érvényesülésük akadályát képezheti. Azonban az alapjogok érvényesülésének további konkrétabb és racionálisabb gátjai is vannak, mivel az alapjogok alkotmányos deklarációja nem jelentheti ezeknek a jogoknak a korlátlan és feltétlen érvényesülését. „Az alapvető jogok garantálásának nem lehet az a következménye, hogy az egyén jogosult lenne alapvető joga korlátlan gyakorlására. Minden alapvető jognak a dolog természetéből adódóan kényszerítő módon – a terjedelme – tárgyi hatótávolsága (védelmi területe) tekintetében korlátozottnak kell lennie, vagyis az alapvető jogok rendkívül kevés kivételtől eltekintve – nem korlátlan és nem is korlátozhatatlan jogot jelentenek."[18] Az alapjogi katalógus látványos bővülésének köszönhetően egyre többször jelennek meg azok a pontok, ahol az egyes alapvető jogok közt átfedések jönnek létre, bizonyos esetekben pedig szembekerülnek egymással, ezeket nevezzük alapjogi kollíziónak. „Az alapjogok a mindennapokban elkerülhetetlenül konfliktusba kerülhetnek egymással és más alkotmányos értékekkel, célokkal. E természetes alapjogi konfliktusokat az államnak, a törvényalkotónak a lehetősége feloldani, sőt kötelessége is rendezni, márpedig az ütköző jogoknak és értékeknek az egymás javára történő korlátozása útján."[19] A probléma kezelése az állam részéről aktív fellépést igényel, aminek ugyanakkor kellő önmérséklettel kell párosulnia. A fenti érvek alapján látható, hogy a legtöbb alapjog esetében legitim és megengedhető a korlátozásuk. Ilyen például az 58/1994. (X. 10.) AB határozat, ami kimondta a tulajdonjog korlátozásának alkotmányosságát, amennyiben arra egy másik jog védelme vagy érvényesülése, illetve egyéb alkotmányos cél más módon nem érhető el, és a korlátozás arányban áll az elérni kívánt cél fontosságával. De a 30/1992. (V. 26.) AB határozat is kimondta például, hogy a véleménynyilvánítás és a sajtószabadság is korlátozható a gyűlöletbeszéd visszaszorítása érdekében. Az alapjogok tartalmi korlátozására az önmérséklet mellett számos jogállami garanciát léptettek életbe az egyes államokban, a legfontosabb ezek közül a törvényalkotás tevékenységének az Alkotmánybíróságok általi ellenőrzése és felügyelete, de emellett számos más megoldás is létezik. Többek közt

[17] Petrétei 2011, 414.
[18] Petrétei 2011, 450–451.
[19] Halász 2013, 186.

ilyen az alkotmányozás és az alkotmánymódosítás elfogadásához szükséges speciális parlamenti többség, eljárásmód vagy a törvényi szinten megjelenő alapjog-korlátozás elfogadásához szükséges minősített többség előírása. Az alkotmányok megváltoztatásának nehézsége megakadályozza az egyes alkotmányos értékek és alapjogok devalválódását, mivel az alkotmányok gyakori, napi ügyekre reflektáló módosítása pontosan ennek a veszélyét rejtené magában. Az alapjogok érvényesülésének másik nyilvánvaló korlátját jelenti magának a jogalkotónak az akarata. Gyakran láthatjuk, hogy egyes alapjogok érvényesülésének feltétele egy másik jog vagy esetenként jogoknak a korlátozása. „Erre tekintettel meghatározhatók ún. »általános korlátok«: az általános korlátok mások hasonló jogainak védelme (érvényesülése), továbbá az alkotmányban meghatározott, illetőleg meghatározandó egyéb jogi értékek megfelelő érvényesülésére, megvalósulására, illetőleg funkcionálása, valamint az alapjogok véletlenszerű, kiszámíthatatlan és ezáltal súlyos hátránnyal járó kollíziójának megelőzése érdekében tehetik lehetővé az alapjogok korlátozását."[20]

Egyes alapjogok tartalmának korlátozása megjelenhet törvényi szinten vagy akár magukban az Alkotmányokban is. A korábbi Alkotmány is tartalmazta az alapjogok korlátozásával kapcsolatos fontos garanciális elemként a törvényi szintű szabályozás szükségességét. A hazai jogrendszerben további különleges garanciát jelent egyes alapjogok szabályozásával kapcsolatban a minősített többséggel elfogadott úgynevezett kétharmados törvények, sarkalatos törvények köre.[21] Az egyes alapjogok kapcsán a szükséges szabályozási szint kérdésében az Alkotmánybíróság világosan kifejtette az álláspontját, és határozataiban megerősítette a törvényi szintű szabályozásnak a szükségességét, ugyanakkor kimondta azt is, hogy közvetett és távoli összefüggések esetében a rendeleti szintű szabályozás önmagában nem minősül alkotmányellenesnek. „Valamely alapjog tartalmának meghatározása és lényeges garanciáinak megállapítása csakis törvényben történhet, törvény kell továbbá az alapjog közvetlen és jelentős korlátozásához is. Közvetett és távoli összefüggés esetében azonban elegendő a rendeleti szint is. Ha nem így lenne, mindent törvényben kellene szabályozni. Ebből az következik, hogy mindig csak a konkrét szabályozásról állapítható meg, hogy – az alapjoggal való kapcsolata intenzitásától függően – törvénybe kell-e foglalni vagy sem."[22] Az alapjogok korlátozásának esetében kiemelten fontos szerep hárul az Alkotmánybíróság alkotmányt védelmező szerepére, ami szorosan összefügg az egyes alapjogok tekintetében az értelmező, tartalmat meghatározó tevékenységgel. Az Alkotmánybíróság tevékenysége ugyanakkor nem konkurálhat a jogalkotóéval, az alkotmánybírói aktivizmus nem veheti el a jogalkotó kitüntetett szerepét az alapjogok tartalmának kialakítása terén. Az Alkotmánybíróság a 64/1991. (XII. 17.) AB határozat indokolásában is világosan kifejtette, hogy az állam kötelezettsége az egyes alapjogok megvalósításához szükséges jogszabályi környezet

[20] Petrétei 2011, 453.

[21] Az Alkotmánybíróság a 4/1993. (II. 12.) AB határozat indokolásában behatóan foglalkozott az alapjogokról szóló törvények elfogadásához szükséges minősített többség kérdésével, ebben megerősíti, hogy az alapjog érvényesítéséhez szükséges részletszabályokat egyszerű többségű törvény határozza meg, továbbá eldöntötte azt a vitát is, miszerint a minősített többséggel megalkotott törvényt egyszerű törvénnyel nem lehet módosítani.

[22] 64/1991. (XII. 17.) AB határozat indokolásából, ABH 1991/297.

kialakítása és az így kialakuló jogrendnek a feladata, hogy az egyes alapjogok legkedvezőbb érvényesülését és az alapjogok összhangját megteremtse. Az Alkotmánybíróság fennállásának a kezdetétől szembesült az alapjogok korlátozásának alkotmányosságával kapcsolatos kiemelt feladatával. Abban nem volt vita, hogy bizonyos esetekben az alapjogokat korlátozni lehet és kell, a kérdéshalmazzal kapcsolatos alapvetését az Alkotmánybíróság az alábbiak szerint fogalmazta meg: „Valamenynyi alkotmányos alapjog tekintetében fontos kérdés, hogy azokat lehet-e és milyen feltételekkel megszorítani, korlátozni, kollíziójuk esetén milyen szempontok alapján kell a prioritást meghatározni. […] Az alapjog korlátozásának alkotmányosságához tehát önmagában nem elegendő, hogy az másik alapjog vagy szabadság védelme vagy egyéb alkotmányos cél érdekében történik, hanem szükséges, hogy megfeleljen az arányosság követelményeinek: az elérni kívánt cél fontossága és az ennek érdekében okozott alapjogsérelem súlya megfelelő arányban legyen egymással. A törvényhozó a korlátozás során köteles az adott cél elérésére alkalmas legenyhébb eszközt alkalmazni. Alkotmányellenes a jog tartalmának korlátozása, ha az kényszerítő ok nélkül, önkényesen történik vagy ha a korlátozás súlya az elérni kívánt célhoz képest aránytalan."[23] Az alapjogok korlátozásának létezik egy végső akadálya a fenti, gyakran szubjektív szempontokon túl, ez pedig az úgynevezett abszolút jogok kategóriája. „A korlátozhatatlan vagy más megfogalmazásban abszolút jogok alatt azokat a jogokat értjük, amelyekkel szemben más alapjog vagy alkotmányos cél, egyéb alkotmányos előírás nem mérlegelhető. Az abszolút jogokból nem lehet visszavenni más szempontok érvényesülése érdekében, nincs olyan jog vagy érdek, amely miatt engedniük kell (amely miatt korlátozhatók)."[24] A 23/1990. AB határozathoz fűzött párhuzamos véleményében Dr. Sólyom László alkotmánybíró a fentieket megerősítve hangsúlyozta, hogy az alapjogok korlátozhatóságának az Alkotmány maga szabott határt azzal, hogy lényeges tartalmukat alapvetően elvonta az állam jogalkotása alól. További garanciális elem, hogy a legfontosabb alapjogok gyakorlását még a kivételes állapot bevezetése esetén sem lehet felfüggeszteni vagy korlátozni. Ilyen kiemelt alapjogok az élethez és az emberi méltósághoz való jog, mivel ezek – véleménye szerint – fogalmilag korlátozhatatlanok, itt a jog jelenti magát a tartalmat is egyben, ezért az állam nem rendelkezhet felette. Ezeknek a jogoknak a kiemelt szerepét mutatja, hogy minden más alapjognak a részét képezik, azok forrásai és feltételei is egyben, emellett az alapjogok korlátozhatóságának abszolút határait is jelentik.

Az Alaptörvény I. cikk (3) bekezdésében szereplő meghatározás értelmében „alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható".[25] Az Alkotmánybíróság gyakorlatából az Alaptörvénybe átültetett szükségességi és arányossági

[23] 30/1992. (V. 26.) AB határozat indokolásából, ABH 1992/167.

[24] BALOGH 2011, 5.

[25] Az Alkotmány 8. § (2) bekezdése a szükségesség és arányosságra való utalás nélkül tartalmazott rendelkezést az alapjogok korlátozásának szabályára: „A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg, alapvető jog lényeges tartalmát azonban nem korlátozhatja." A 8. § (4) bekezdése pedig taxatíve felsorolta azokat az alapvető jogokat, amiknek a gyakorlását még rendkívüli állapot, szükségállapot vagy veszélyhelyzet idején sem lehet felfüggeszteni vagy korlátozni.

teszt fontos alkotmányos garanciát jelent az alapjogok korlátozásának tekintetében, ez egyszerre jelent értelmezési módszert és mértéket is. „Az alapjogi konfliktusokat hordozó jogviták életbevágóan fontos kérdésekről szólnak, feloldásuk azonban a legritkább esetben magától értetődő. Nagy a helyes döntés tétje, ha az Alkotmánybíróság vagy más bíróság nem a megfelelő következtetésre jut, mindenképpen valamilyen alapjog elfogadhatatlan mértékű korlátozását kockáztatja. A döntés azért sem könnyű, mert sok esetben nem egyértelmű, hogy milyen módszerrel tárható fel egy alapjog védett és még korlátozható jogi tartalma."[26] Az Alkotmány 8. § (2) bekezdésében szereplő fordulat, miszerint alapvető jog lényeges tartalma nem korlátozható, további értelmezés után kiáltó megfogalmazása miatt merült fel az a kérdés, hogy az egyes alapvető jogok tartalmi kiüresedésének elkerülése érdekében hol húzódik az adott esetben releváns *lényeges tartalom* határa. „A lényeges tartalom európai emberi jogi dokumentumok számára nem ismeretlen fogalom. Az intézményt a Grundgesetz vezette be a közjogi gondolkodásba 1949-ben: az 1989-es magyar Alkotmány, valamint az Alaptörvény jogkorlátozási klauzulája számára is mintaként szolgáló szabály csak a lényeges tartalom (Wesengehalt) védelmét fogalmazza meg az alapjogkorlátozás tartalmi korlátjaként."[27] Tértől és időtől függetlenül általánosan alkalmazható, egységes zsinórmérték nem áll rendelkezésre, ezért az alkotmánybíróságok feladata, hogy kidolgozzák azt a dogmatikai rendszert, ami alapján meg tudják ítélni, hogy a jogalkotó által megalkotott jogi norma alkotmányba ütközik-e vagy sem. Az alkotmánybíróságok tevékenységük megkönnyítése, uniformalizálása és egységes mérce kialakítása érdekében a feladat- és hatáskörükbe utalt eljárások során különféle teszteket dolgoztak ki. Az alapjogok korlátozásának alkotmányossági vizsgálatára szolgáló tesztek célja, hogy olyan általánosan alkalmazható értelmezési keretet biztosítsanak, ami megbízható fogódzót jelent annak az eldöntésére, hogy az adott alapjogot vagy alapjogokat korlátozó konkrét jogszabály vagy annak valamelyik rendelkezése megfelel-e az alkotmányosság követelményének.[28] Ennek az eldöntése talán abban az esetben a legnehezebb, amikor a jogalkotó alapjogi kollízió feloldása vagy más alapjog, alkotmányos érték hatékonyabb érvényre juttatása érdekében korlátoz egy adott alapjogot. Az Alkotmánybíróság idejekorán felismerte az általános alapjogi teszt alkalmazhatóságának a határait, ezért további kiegészítő módszerek bevezetésére volt szüksége. Az adott alapjog lényeges tartalmának alkotmányellenes korlátozását főszabályként az általános alapjogi teszt, a szükségesség, alkalmasság[29] és arányosság tesztje mutatja meg, de egyes alapjogok esetében a korlátozás alá kerülő lényeges tartalmat az alapjog egyedi természetéhez igazodó speciális tesztek

[26] Pozsár-Szentmiklósy 2016, 9.

[27] Pozsár-Szentmiklósy 2016, 208–209.

[28] Az alapjogi tesztek alkalmazásának a célját tekintve megkülönböztethetjük: 1. A formális megközelítést: a tesztek célja, hogy általánosan elfogadott módszert kínáljanak az alapjogokat korlátozó jogi normák alkotmányosságának az eldöntéséhez. 2. A tesztek funkciójának tartalmi vizsgálata során értelmet nyer az egyes korlátozásoknak az érvényre juttatni kívánt alkotmányos értékeket felerősítő funkciója, mint például a közérdek vagy a jogállamiság védelme.

[29] Az alapjog-korlátozás esetében az alkalmasság vizsgálata fokozatosan háttérbe szorult és lényegében a szükségesség vizsgálatának vált a részévé. Eredetileg az egyes alapjog korlátozás kapcsán az elérendő cél és a megválasztott eszköz (jogkorlátozás) kapcsolatának vizsgálatát jelentette.

is segítenek feltárni.[30] Az alapjogi tesztek közül az arányossági tesztek jelentik a kiindulási alapot, ezt a Német Szövetségi Köztársaság Alkotmánybírósága alakította ki a munkáját segítő eszközként. A teszt alapmodellje kétlépcsős vizsgálati rendszert alakított ki, először megvizsgálták, hogy az adott jogszabályi rendelkezés megsérti-e ténylegesen valamelyik alkotmányos alapjogot. Ezt követően kezdődött a tartalmi vizsgálat, ami során a jogalkotói célkitűzés indokoltságát, a célkitűzést előmozdító jogkorlátozás alkalmasságát és végül a jogsérelem mértékét állították szembe az elérendő cél társadalmi hasznosságával a jogkorlátozás arányosságának vizsgálata során. „A magyar Alkotmánybíróság gyakorlata az alapjogi teszt szerkezetét tekintve a klasszikus megközelítést követi, amelynek megfelelően a jogalkotói célkitűzés értékelését, a jogalkotói célkitűzés és a jogkorlátozás eszköze között kimutatható kapcsolat vizsgálatát, valamint a jogkorlátozás eszközének minősítését követően kerül sor az arányosság vizsgálatára."[31] A 6/1998. (III. 18.) AB határozat indokolásában az Alkotmánybíróság saját állandósult gyakorlatára hivatkozva kimondta, hogy valamely alapjog lényeges tartalmát az a korlátozás sérti, ami más alapvető jog vagy alkotmányos cél érdekében nem elkerülhetetlenül szükséges. A társadalmilag igazolható, elérni kívánt célnak pedig arányban kell lennie a szükséges alapjog-korlátozással megvalósuló jogsérelemmel. Az általános alapjogi teszt alkalmazása esetében az Alkotmánybíróság rávilágított, hogy „egyes alapjogok esetében az Alkotmány maga tartalmaz további kritériumokat, amelyek egyrészt ezt az általános mércét az illető jog tartalmához igazítva konkretizálják, másrészt amelyek konkrét voltukban sokkal inkább állandó és saját tartalmi ismérvekkel határozzák meg az adott alapjog lényeges tartalmát a viszonyítással dolgozó általános szabály helyett". Az általános alapjogi teszt egy elvont módszertan annak érdekében, hogy bármilyen alapjog-korlátozás esetén alkalmazható legyen, de éppen emiatt korlátozott is a használhatósága, mivel az egyes alapjogok védett tartalma esetenként eltérő. Ehhez kapcsolódik, hogy az alapjog-korlátozás alkotmányosságát megalapozó legitim társadalmi célok sokszínűsége miatt az arányosság kérdésének tisztázása is nehézségekbe ütközik. Emiatt van szükség az egyes alapjogok lényeges tartalmát egyedi módon megállapító speciális tesztekre, amelyek bármely korlátozással szemben ugyanazt a határt jelölik ki. Ezzel a módszerrel az egyedi alapjogok korlátozásának abszolút határa is kijelölhető, illetve az adott esetben alkalmazni kívánt korlátozás alkotmányosságának saját, külön ismérvek alapján történő mérlegelése is lehetségessé válik. Végső soron a speciális tesztek alkalmazásával bizonyos alapjogok lényeges tartalma sokkal mélyebben, konkrétabban és egyértelműbben határozható meg, mint az általános alapjogi teszttel. A különféle alapjogi tesztek pozitív megítélése mellett azonban használhatóságukkal kapcsolatban számos kritikát is megfogalmazott a jogásztársadalom. „A világszerte népszerű mérlegelést a kezdetektől fogva bírálatok érik. A magyar változat alapjául szolgáló német megközelítéssel (Güterabwaegung) kapcsolatban […] Habermas azt fogalmazta meg, hogy a jogkorlátozási teszt nem biztosít racionális mércét, ezért

[30] A speciális tesztek az adott alapjog egyedi aspektusaihoz alakítva vizsgálják a jogkorlátozás alkotmányosságát, ilyen például a speciális közérdekűségi teszt, ami az állami beavatkozás megengedett területét, a korlátozás alkotmányosságát a közérdek biztosításához köti, vagy a kommunikációs jogok esetében a reális veszély tesztje.

[31] Pozsár-Szentmiklósy 2016, 138.

a döntések szükségképpen önkényesek és ellenőrizhetetlenek. Eredményét tekintve pedig az alapjogok így elveszítik elsőbbségüket a különféle közcélokhoz képest, összeomlik az egyéni jogok és a különféle politikai célok közötti fal."[32] Az alapjogkorlátozás legitimitását mind jogi, mind politikai szempontból az adja, hogy egy másik alapjog védelme, annak érvényesülése vagy más alkotmányos cél előmozdítása másként nem biztosítható. Ennek a gyakorlati megfogalmazását láthatjuk az Alaptörvény I. cikk (3) bekezdésében. Ez a korlátozás azonban csak szükséges mértékű lehet, az igazi nehézséget a szükséges mérték meghatározása és megtalálása jelenti. Az alapjogok korlátozása tekintetében új kihívást jelent az új típusú globális terrorizmus és az ellene való védekezés módszereinek kialakítása, mivel a terrorizmus elleni küzdelem jogi szempontból kimondottan a jogkorlátozás területe. A bűnüldözéssel és a terrorizmus elleni harccal kapcsolatos intézkedések kapcsán komoly morális kérdések merülnek fel, amelyek a jogkorlátozás szükséges mértékének helytelen felméréséből fakadnak. „[T]együk a rosszat, hogy a jó következzék belőle!"[33]

Az Alkotmánybíróság korábbi határozatainak kötőereje

Az Alkotmány *Alapvető jogok és kötelezettségek* című fejezetével összehasonlítva az Alaptörvény szövegében a módosításoknak köszönhetően egyre gyarapodik az alapjogok korlátozására irányuló rendelkezéseknek a száma. Az alkotmányozás során fontos kérdés volt, hogy az Alkotmány hatályon kívül helyezését követően mi lesz az Alkotmánybíróság korábbi határozatainak a sorsa. Magyarország rendszerváltást követő alkotmányfejlődésében kiemelkedő szerepe volt az Alkotmánybíróság alkotmányt értelmező és jogfejlesztő tevékenységének. Az egyes alapvető jogok tartalmának kibontása és az egyes jogszabályok vizsgálata során meghozott határozatok esetében az indokolásban szereplő okfejtéseknek is meghatározó jelentősége volt a későbbi jogalkotásra. Az Alaptörvény záró és vegyes rendelkezéseinek 5. pontja alapján: „Az Alaptörvény hatálybalépése előtt meghozott alkotmánybírósági határozatok hatályukat vesztik. E rendelkezés nem érinti az ezen határozatok által kifejtett joghatásokat."[34] A jogalkotó (alkotmányozó hatalom) eredeti célja az volt, hogy az Alaptörvény rendelkezései az Alkotmánytól függetlenül kerüljenek *új* értelmezésre, valamint a jogalkotó ezzel egyértelművé tegye, hogy az Alkotmánybíróság nincs kötve az Alkotmány értelmezése során hozott határozataihoz. A korábbi határozatok hatályának kérdését árnyalja, hogy a fenti rendelkezés nem zárta ki, hogy az Alkotmánybíróság az Alaptörvény értelmezésekor a korábbival megegyező tartalmú határozatot hozzon. A jogalkotó célja ugyanakkor annak a jogszabályi lehetőségnek a biztosítása volt, hogy hasonló kérdésben az Alkotmánybíróság az Alaptörvény értelmezése során a korábbihoz képest eltérő vagy akár ellentétes tartalmú határozatot is hozhasson. Ezzel a jogalkotó ki kívánta tágítani az Alkotmánybíróság értelmezési szabadságát, ennek a szabadságnak azonban korlátját jelentik az Alkotmánybíróság korábbi tevékenysége során

[32] Tóth 2009, 203.
[33] Rómabeliekhez írt levél 3. fejezet 3:8.
[34] A T/9929. számú Magyarország Alaptörvényének módosításáról szóló eredeti javaslatban a szövegezés egyértelműbben fogalmazott: „Az Alaptörvény hatálybalépése előtt meghozott alkotmánybírósági határozat és annak indokolása az Alaptörvény értelmezése során nem vehető figyelembe."

kikristályosodott alapelvek és értelmezési keretek,[35] ez különösen igaz az egyes alapjogok tartalmának megítélése kapcsán. Az alkotmányozás során a jogalkotó az Alaptörvénybe emelte az alkotmánybírósági gyakorlat néhány elemét, ezek közül a legjelentősebb, hogy a *Szabadság és felelősség* című rész I. cikk 3. bekezdése beépítette és lényegében alkotmányos rangra emelte az Alkotmánybíróság eddigi tevékenysége során alkalmazott gyakorlatot: a szükségességi és arányossági tesztet. Más megközelítésben alkotmányos szinten került szabályozásra az egyes alapjogok és alkotmányos értékek érvényesülése érdekében az alapjogok korlátozásának lehetősége. A korlátozás határát a már hivatkozott szükségesség és arányosság követelményei, valamint a korlátozásra kerülő alapjog lényeges tartalmának tiszteletben tartása jelenti. Amikor az Alaptörvény kijelenti, hogy az egyes „alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg", akkor az alapjogok többsége esetében, az abszolút vagy korlátozhatatlan jogok kivételével,[36] a gyakorlásuk és érvényesülésük feltételeinek a szabályozásáról beszélünk, ezek már önmagukban korlátozást jelentenek. Nemcsak törvényi szinten, hanem az Alaptörvényben is találhatunk olyan rendelkezéseket, amik egyes alapjogok korlátozását jelentik. Erre szemléletes példa a hetedik Alaptörvénymódosítás során elfogadott *Szabadság és felelősség* rész VI. cikk (1) bekezdésének kiegészítése, ami a véleménynyilvánítás szabadságának és a gyülekezési jog gyakorlásának állít korlátot mások magán- és családi életének, illetve otthonának kiemelt védelmével. De megemlíthetjük a jelentős médiavisszhangot kiváltó, a hajléktalanságot „kriminalizáló", XXII. cikk (3) bekezdését is, ami szerint

[35] Az Alkotmánybíróság a 13/2013. (VI. 17.) AB határozatának indokolásában ABH 2013/440. foglalt állást a korábbi határozataiban foglaltak érvényességét illetően a jogbiztonság érvényre juttatása érdekében: „[30] Az Alaptörvény hatálybalépését követően az Alkotmánybíróság a korábbi alkotmányon alapuló határozatai tekintetében kimondta, hogy az újabb ügyekben felhasználhatja az Alaptörvény hatálybalépése előtt hozott határozataiban szereplő érveket, ha „az Alaptörvény konkrét – az előző Alkotmányban foglaltakkal azonos vagy hasonló tartalmú – rendelkezései és értelmezési szabályai alapján ez lehetséges. […] A korábbi Alkotmányon alapuló határozatokban kifejtett elvi jellegű megállapítások felhasználása tehát megkívánta az előző Alkotmány és az Alaptörvény megfelelő szabályainak tartalmi összevetését és mérlegelését az Alaptörvény értelmezési szabályaira is tekintettel".
[32] A hazai és európai alkotmányjogi fejlődés eddig megtett útja, az alkotmányjog szabályszerűségei szükségképpeni hatással vannak az Alaptörvény értelmezésére is. Az Alkotmánybíróság az újabb ügyekben vizsgálandó alkotmányjogi kérdések kapcsán felhasználhatja a korábbi határozataiban kidolgozott érveket, jogelveket és alkotmányossági összefüggéseket, ha az Alaptörvény adott szakaszának az Alkotmánnyal fennálló tartalmi egyezése, az Alaptörvény egészét illető kontextuális egyezősége, az Alaptörvény értelmezési szabályainak figyelembevétele és a konkrét ügy alapján a megállapítások alkalmazhatóságának nincs akadálya, és szükségesnek mutatkozik azoknak a meghozandó döntése indokolásába történő beillesztése.
[33] Az Alkotmánybíróság – a fenti feltételek vizsgálata mellett – a hatályát vesztett alkotmánybírósági határozat forrásként megjelölésével, a lényegi, az adott ügyben felmerülő alkotmányossági kérdés eldöntéséhez szükséges mértékű és terjedelmű tartalmi vagy szövegszerű megjelenítéssel hivatkozhatja vagy idézheti a korábbi határozataiban kidolgozott érveket, jogelveket. Az indokolásnak és alkotmányjogi forrásainak ugyanis a demokratikus jogállamban mindenki számára megismerhetőnek, ellenőrizhetőnek kell lennie, a jogbiztonság igénye az, hogy a döntési megfontolások átláthatóak, követhetőek legyenek. A nyilvános érvelés a döntés indoklásának létalapja." Párhuzamos indokolásában Dr. Pokol Béla ezzel szemben azt hangsúlyozta, hogy a korábbi határozatok hatályon kívül helyezésével azok érvei, döntési formulái és megállapításai elveszítették normativitásukat, a későbbi döntéseket meghatározó autoritásukat, és a továbbiakban csak az alkotmányjogi gondolkodás szabad gondolati kincseit jelentik.

[36] Ilyen korlátozhatatlan jog például az emberi méltóság, az Alaptörvény *Szabadság és felelősség* részének II. cikke kimondja, hogy az emberi méltóság sérthetetlen.

tilos az életvitelszerű közterületen való tartózkodás.[37] Az utóbbi kérdéskör jól példázza, hogy jogvédő szervezetek és az ellenzéki pártok miért nehezményezik azt a jogalkotói gyakorlatot, ami arra irányul, hogy az Alkotmánybíróság által korábban vitatott jogszabályi megoldásokat magába az Alaptörvénybe szerkesztik bele, annak módosítása során. Így a napi politikai érdekeknek megfelelően szabadon bekerülhetnek az Alaptörvénybe *nem alkotmányos jelentőségű* szabályok. Azonban, ha ezek a módosítások elérnek egy kritikus mennyiséget, akkor óhatatlanul lerontják az Alaptörvényt. Ezzel a jogalkotási gyakorlattal az Alkotmánybíróság elveszti annak lehetőségét, hogy az adott, Alaptörvényben szabályozott (korlátozott) életviszonyra vonatkozó szabályozást felülvizsgálhassa. Az *Állam* című rész 24. cikkének (5) bekezdése értelmében az Alkotmánybíróság az Alaptörvényt és annak módosítását csak a megalkotására és kihirdetésére vonatkozó, az Alaptörvényben foglalt eljárási követelmények tekintetében vizsgálhatja felül.[38] Tehát az Alaptörvény vagy annak módosítása tartalmának vizsgálatára nem terjed ki az Alkotmánybíróság jogköre. Ha nem így lenne, akkor előállhat az a sokak által vizionált helyzet, hogy az Alkotmánybíróság *negatív* jogalkotóként megsemmisíthetné az Alaptörvény egyes rendelkezéseit vagy módosítását. Ezzel összefüggő kérdés, hogy az Alkotmánybíróságnak lehetősége van *összefüggés* okán bizonyos ügyek megvizsgálására.

Felhasznált irodalom

Balogh Zsolt (2011): *Alapjogok korlátozása az új alkotmányban.* Budapest, Pázmány Law Working Papers, 19. sz.

Chronowski Nóra (2005): *„Integrálódó" alkotmányjog.* Budapest–Pécs, Dialóg Campus.

Chronowski Nóra – Drinóczi Tímea – Petrétei József – Tilk Péter – Zeller Judit (2013): *Magyar Alkotmányjog III.* Budapest–Pécs, Dialóg Campus.

Csapody Tamás (1996): *Ne az én nevemben!* Budapest, Constitutional Legislative Policy Institute.

Halász Iván (2013): *A Magyar Köztársaság Alkotmányától Magyarország Alaptörvényéig. Alkotmányozás Magyarországon Anno Domini 2011.* Kijev, Uridicna Dumka.

Petrétei József (2011): *Az alkotmányos demokrácia alapintézményei.* Budapest–Pécs, Dialóg Campus.

Pokol Béla (2017): *A jurisztokratikus állam.* Budapest, Dialóg Campus.

Pokol Béla (1993): A német alkotmányjogi bíráskodás jogelméleti kérdései. In Pokol Béla: *Pénz és politika.* Budapest, Aula.

[37] Az Alkotmánybíróság 38/2012. (XI. 14.) számú határozatában ABH 2012/185. egyértelműen állást foglalt a hajléktalanság kriminalizálásának témájában: „[51] […] nem állapítható meg az az ok, az a védeni kívánt érdek, ami indokul szolgált arra, hogy az Alaptörvény XIX. cikkében szabályozott állami feladatvállalás alapján az Sztv.-ben a szociális ellátás körébe vont élethelyzetet a törvényhozó társadalomra veszélyes, kriminális magatartássá nyilvánítson."

[38] Az Alkotmánybíróság hatáskörének szélesebb körű és lényegesen szubjektívabb alapokon nyugvó *ideiglenes* korlátozását jelentik az Alaptörvény 37. cikk (4) bekezdésében szabályozott, az államadósság elleni küzdelem érdekében hozott rendelkezések. Ameddig az államadósság a teljes hazai össztermék felét meghaladja, addig az Alkotmánybíróság bizonyos pénzügyi tárgyú jogszabályok esetében nem vizsgálhatja azok Alaptörvénnyel való összhangját kivéve, ha a kifogásolt szabályozás összeegyeztethetetlen az élethez és az emberi méltósághoz való joggal, a személyes adatok védelméhez való joggal, a gondolat, a lelkiismeret és a vallás szabadságához való joggal vagy a magyar állampolgársághoz kapcsolódó jogokkal.

POZSÁR-SZENTMIKLÓSY Zoltán (2016): *Alapjogok mérlegen.* Budapest, HVG-ORAC.
SZABÓ Máté (2011): *Emberi jogok – Alapvető jogok?* Budapest, Kairosz.
TÓTH Gábor Attila (2009): *Túl a szövegen.* Budapest, Osiris.
TÓTH Zoltán József (2013): Egyes észrevételek az Alaptörvény értelmezéséhez. *Polgári Szemle,* 9. évf. 1–3. sz. Elérhető: https://polgariszemle.hu/archivum/109-2013-majus-9-evfolyam-1-3-szam/a-tarsadalom-es-tudomanya/520-egyes-eszrevetelek-az-alaptoerveny-ertelmezesehez (A letöltés dátuma: 2018. 10. 15.)
TRÓCSÁNYI László (2014): *Az alkotmányozás dilemmái.* Budapest, HVG-ORAC.

Internetes forrás

www.alkotmanybirosag.hu (A letöltés dátuma: 2018. 10. 15.)

Jogforrások

2011. évi CLI. törvény az Akotmánybíróságról
13/2013. (VI. 17.) AB határozatának indokolása
1990/88. AB határozat
1991/297. AB határozat
38/2012. (XI. 14.) AB határozat
4/1993. (II. 12.) AB határozat
64/1991. (XII. 17.) AB határozat indokolása
6/1998. (III. 18.) AB határozat indokolása

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 109–127. • DOI: 10.32561/nsz.2019.2.9

Szászi Ivett[1]

A humánbiztonság koncepciója és mérésének lehetőségei

The Concept of Human Security and Its Possible Measurement Methods

Hogyan érheti el az ENSZ a humánbiztonság területén kitűzött céljait 2030-ra? A fenntartható fejlesztési célok teljesítéséről szóló eredmények azt mutatják, hogy a különböző területek eltérő prioritást élveznek, ezáltal más-más intenzitással fejlődnek, egyaránt mutatnak javuló és romló tendenciákat. A választ a társadalmi fejlettségi mutató koncepciója adja, amely a gazdasági prosperitás helyett a kormányok szociális erőfeszítéseitől teszi függővé a társadalmi jólét növekedését. A humánbiztonság tehát nem az országok GDP-jének növekedésén fog múlni, hanem azon, hogy a kormányok milyen törvényeket hoznak a társadalom fejlődésének érdekében, például korszerű egészségügyi ellátáshoz és oktatáshoz való hozzáférés biztosítása terén.

Kulcsszavak: humánbiztonság, biztonság, Social Progress Index, ENSZ, UNDP

How is the UN capable of achieving its goals in the field of human security till 2030? The reports on the fulfilment of the sustainable development goals show that the significance of the SDGs can be interpreted differently in every region. The answer is in the Concept of Social Progress Index. In order to increase human well-being, the SPI focuses more on the social efforts of the national governments rather than economic prosperity. Therefore, human security does not depend on the growth of the countries' GDP, but on the laws that governments put in place for the development of society, such as access to modern health care and education.

Keywords: human security, security, Social Progress Index, United Nations, UNDP

[1] Szászi Ivett, Tempus Közalapítvány, Budapest, okl. nemzetközi biztonság- és védelempolitikai szakértő. (Tempus Public Foundation. Certified international security and defence expert.) ORCID-azonosító: 0000-0003-1591-1918.

Bevezetés

A hidegháború és a Szovjetunió felbomlása után a posztbipoláris korban megindult globalizáció és a megváltozott nemzetközi kapcsolatok hatására új, többdimenziós biztonsági kihívásokkal, veszélyekkel és fenyegetettséggel kellett szembenézni a világnak. Ezért az ENSZ fejlesztési programja (United Nations Development Programme – UNDP) egy új koncepció kidolgozásával próbálta és próbálja mind a mai napig felvenni a versenyt, amely a humánbiztonságra helyezi a fő hangsúlyt. A koncepció alapjait az 1994-es Humán Fejlődés Jelentés rakta le.[2] A humánbiztonság az egyének biztonságát tűzi ki célul, amely a szegénység felszámolásától az oktatás elérésén át a fenntartható környezetig terjed. Az emberi biztonság erősítésének újabb mérföldkövének tekinthetők a világszervezet által kidolgozott Millenniumi Fejlesztési Célok (Millenium Development Goals – MDG), és az ezt követő Fenntartható Fejlesztési Célok (Sustainable Development Goals – SDG). Mindkét program célkitűzéseiben követi a humánbiztonság koncepciójának alapelveit. A tanulmány arra keresi a választ, hogy minek a segítségével érheti el az ENSZ a maga elé kitűzött célokat 2030-ra a humánbiztonság területén? Látni fogjuk, hogy bár a fenntartható fejlesztési célok megvalósításának vannak hasznos részeredményei, a humánbiztonság globális állapotának javítása azonban mégis kérdéses marad, mert átfogó jellege miatt nehéz konkrétan értelmezni, alkalmazni, valamint a változásokat mérni. A cikk másik fő kérdése, hogy el tudjuk-e érni ennek ellenére a kitűzött fejlesztési célokat? Már a millenniumi fejlesztési célok teljesítésének értékelése során világossá vált, hogy önmagában a gazdasági növekedéssel nem lehetséges a fejlődés megfelelő mérése, ezért új megközelítésre van szükség. Írásomban arra teszek kísérletet, hogy bizonyítsam, a humánbiztonság újfajta megközelítésével, a társadalmi fejlettségi mutató bevezetésével talán ez a cél megvalósítható lesz.

A humánbiztonság koncepciója

A modern politikai elképzelés szerint a biztonság hagyományosan a modern állami szuverenitás részét képezi. Ha az állam nem biztonságos, akkor a politikai rend és végső soron a polgárok veszélybe kerülnek. A biztonság jelentéstartalmát mindazonáltal erőteljesen vitatják. A viták nagy része az államon kívüli biztonság kiterjesztésével foglalkozik.[3] A hidegháború alatt főleg katonai kihívásokkal kellett megbirkózniuk az államoknak. Azonban az 1973-as és 1979-es olajválságok, valamint a nemzetközi fórumokon napirendre kerülő szén-dioxid-kibocsátás miatti üvegházhatás megmutatták,[4] hogy nem csak katonai események okozhatnak komoly problémákat és fenyegethetik az államokat. A bipoláris világ megszűnésével még jobban egyértelművé vált, hogy újra kell gondolni, mit is jelent a biztonság, milyen új veszélyek fenyegetik az államokat és hogyan lehet fellépni ezekkel szemben. Barry Buzan az új biztonsági

[2] Teke 2018.
[3] Stern–Öjendal 2010, 14.
[4] Gazdag–Tálas 2008, 4.

kihívásokat öt különböző szektorban látta megjelenni, amelyeket katonai, politikai, társadalmi, gazdasági és környezeti szektorokba sorolt.[5] A nemzetállami rendszerben hiányoznak azok az eszközök, amelyekkel küzdeni tudnának a mai fenyegetésekkel, ideértve a terrorista hálózatokat, a nemi erőszakot, az erőszakos etnikai diszkriminációt, a globális járványokat és az éghajlatváltozást.[6] Így *a nemzeti biztonságról áthelyeződött a hangsúly a humánbiztonságra*, ami azt jelenti, hogy a nemzetközivé eszkalálódott problémákat a kialakulási helyükön kell megoldani, tehát a fókusz a megelőzésre[7] került.

A biztonságpolitika központi kérdése az, hogy hogyan csökkenthető a konfliktusok száma. Ennek a problémának a megoldására dolgozta ki a világszervezet a humánbiztonság koncepcióját, amely először 1994-ben került az ENSZ Fejlesztési Program napirendjére. Ez az elmélet úgy tartja, hogy az állam biztonsága (a katonai védelem, az államérdek és a területbirtoklás) helyett az egyének biztonságára (jólétére, ételhez, oktatáshoz, munkához való hozzáférésére)[8] kell helyezni a hangsúlyt, mert megváltoztak a fenyegetések típusai. A hidegháború alatt külső, az állam biztonságát fenyegető veszélyekkel kellett felvenni a harcot, de a világrend megváltozása után a fő problémát a *belső konfliktusok és a gazdasági fejletlenség* okozzák.[9] A fejlődő világban a térségek elmaradottsága nagyon sok esetben visszavezethető a szabadság és biztonság hiányára.[10] Így ha az egyéneket érő kockázatokat próbálják elhárítani, azzal csökken a konfliktusok száma, és nagyobb stabilitás érhető el. A fejlett államok belátták, hogy a humánbiztonság segélyeken keresztüli megerősítése stabilitást eredményezhet, és az államon belüli fegyveres konfliktusok kialakulását is csillapíthatja.[11]

A humánbiztonság és a nemzeti biztonság egymással nem versengő, hanem egymást kiegészítő fogalmak, úgymond szimbiózisban működnek. A humánbiztonság az egyénnel és a közösséggel foglalkozik, nem pedig az állammal. Az emberek biztonságát fenyegető veszélyek közé tartoznak olyan fenyegetések is, amelyek nem minősülnek veszélynek az állami biztonság szempontjából. A humánbiztonság fókuszában álló szereplők köre túlnyúlik magán az államon, míg a nemzeti biztonság hatásköre csak az államra összpontosul. A humánbiztonság nemcsak az emberek védelmét foglalja magában, hanem az emberek felkészítését is arra, hogy képesek legyenek magukat megvédeni. Az 1. táblázat összefoglalja, hogy milyen hatáskörökkel bír a humánbiztonság és a nemzeti biztonság, valamint hogy mely területeken egészítik ki egymást.[12]

5 Gazdag–Remek 2018, 21–24.
6 Stern–Öjendal 2010, 15.
7 Remek 2017, 222–224.
8 Paris 2001, 89.
9 Paris 2001, 89.
10 Hampson 2008, 229–232.
11 Péczeli 2011, 1–3.
12 Owen 2008, 118.

1. táblázat

A humánbiztonság és a nemzeti biztonság egymást kiegészítő elemei

Humánbiztonság	Nemzeti biztonság
Az egyénnel és közösséggel foglalkozik.	Az állammal foglalkozik.
Vannak olyan tényezők, amelyek az egyéneket veszélyeztetik, de az államot nem.	
Hatásköre túlnyúlik az állam határain, mert a humánbiztonság univerzális jellegű.	Hatásköre alá az állam tartozik.
Feladata az emberek védelme és felkészítése arra, hogy ne legyenek kitéve a fenyegetéseknek.	Feladata az emberek védelme.

Forrás: Owen 2008, 118. alapján a szerző szerkesztése.

A humánbiztonsági koncepció jelentősen megváltoztatta a biztonsággal kapcsolatos felfogást, új alapelveket fogalmazott meg, például a nemzetbiztonságról áthelyeződött a hangsúly az egyének biztonságára, a döntéshozatal és a források biztosítása pedig az államról átkerül olyan nemállami szereplőkre, mint a nemzetközi szervezetek, a civil szervezetek és a helyi közösségek. A humánbiztonság stratégiájának megszervezése és végrehajtása olcsóbb és egyszerűbb, mert a *megelőzésen* alapul. A prevenció különösen fontos az egészségügy területén, hiszen a járványok megelőzése csak a higiénia fejlesztésével, kórházak és szakképzett orvosok telepítésével, valamint megfelelő gyógyszerek biztosításával lehetséges, nem szabad megvárni, amíg a fejlődő térségekből a világ többi részére is eljutnak a pusztító járványok.[13] Továbbá a humánbiztonság magában foglalja még a gazdasági fejlődést, a társadalmi igazságosságot, a demokratizálódást, a leszerelést, az emberi jogok tiszteletben tartását és a jogállamiságot.[14]

A humánbiztonságot fenyegető veszélyek listája hosszú, de a legtöbbet a következő *hét fő kategóriába* lehet sorolni: gazdasági biztonság, élelmiszer-biztonság, egészségügyi biztonság, környezeti biztonság, személyi biztonság, közösségek biztonsága és politikai biztonság.[15]

A humánbiztonság definícióját a szakirodalom, a politikai szereplők és maga az ENSZ is sokféleképpen megfogalmazta már, számos fogalom létezik, amelyek attól függnek, hogy a definiáló szűk vagy széles értelemben vizsgálja-e az emberre irányuló veszélyeket és fenyegetéseket. *A szűk értelmezés* az erőszakkal – különösen a szervezett politikai erőszakkal – kapcsolatos fenyegetésekre fókuszál, amelyet az ENSZ Humánbiztonsági Hálózata *(Human Security Network, HSN)*[16] használ, és alapját képezi a humánbiztonsági jelentések elkészítésének. Ezek a jelentések a humánbiztonságot a *szervezett erőszaktól mentes szabadságként* nevezik meg. A szervezett erőszakot

[13] Péczeli 2011, 1–3.
[14] Annan 2001.
[15] United Nations Development Programme (UNDP). *Human Development Report* 1994, 23.
[16] A (HSN – Human Security Network) hálózat 1999-ben jött létre 12 ország társulásával. Célja a humánbiztonság koncepciójának terjesztése. www.austria.org/the-human-security-network/ (A letöltés dátuma: 2019. 03. 11.)

egy azonosítható személy/szervezet követi el, és nem véletlenszerű, hanem előre megtervezett.[17]

A tág értelmezés az *emberi sebezhetőségre* összpontosít, ezért a fenyegetések összes típusát magában foglalja. Tehát a szűk koncepcióban elismert szervezett politikai erőszak mellett az erőszak más formáit is érinti, továbbá a természeti katasztrófák, a betegségek, a környezetromlás, az éhínség, a munkanélküliség és a gazdasági visszaesés veszélyeit is tartalmazza.[18]

Az UNDP definíciója (szűk értelmezéshez közelít) szerint a humánbiztonság két fő célt szolgál: először is megszünteti a krónikus fenyegetéseket, mint az éhínség és a járványok, másodszor pedig védelmet nyújt a mindennapi életből eredő hirtelen és káros zavarok és veszélyek ellen, amelyek akár az otthonokban, akár a munkahelyeken vagy a közösségekben érhetik az embereket.

Az ENSZ Humánbiztonsági Bizottság (Commission on Human Security – CHS) definíciója (tág értelmezéshez közelít) szerint az emberi élet létfontosságú elemeinek védelmét kell biztosítania olyan módon, amely növeli az emberi szabadságot és az emberi kiteljesedést.[19]

Sadako Ogata, ENSZ egykori menekültügyi főbiztosa (1990–2001) szerint humánbiztonságról több kulcselem együttes megléte esetén beszélhetünk. *Az első kritérium szerint* humánbiztonságról csak akkor beszélhetünk, ha minden polgár békében és biztonságban élhet saját országának határain belül. Ez magában foglalja az államok és a polgárok azon képességét, hogy a konfliktusokat megelőzzék, illetve békés és erőszakmentes módon megoldják, illetve a konfliktus vége után képesek legyenek megbékélésre. *A második alapelv* szerint biztosítani kell az emberek számára a hátrányos megkülönböztetés nélküli életet, minden olyan joggal és kötelezettséggel – beleértve az emberi, politikai, társadalmi, gazdasági és kulturális jogokat is –, amelyek egy államhoz tartoznak. *A harmadik elem* a politikai, társadalmi és gazdaságpolitikai folyamatokhoz való egyenlő hozzáférés, valamint az egyenlő előnyök kivívása. *A negyedik irányelv* a jogállamiság és az igazságszolgáltatás függetlensége. A társadalom minden egyes tagja ugyanolyan jogokkal és kötelezettségekkel kell, hogy rendelkezzen. A törvény előtti egyenlőségen alapuló alapvető garanciák hatékonyan enyhítik az önkényesség kockázatát, amely gyakran diszkrimináció, visszaélés vagy elnyomás formájában nyilvánul meg.[20]

A humánbiztonságnak nincs egyetemesen elfogadott definíciója. Az előbbiekben bemutatott ötféle megközelítésből látszik, hogy a szerzők a humánbiztonság fogalmát különféle tartalmi leírással határozták meg, és mind helytállónak bizonyult. Roland Paris[21] szerint a humánbiztonság fogalma azért ennyire tág, hogy a középhatalmak, fejlesztési szervezetek és civil szervezetek eltérő érdekei mind érvényesülni tudjanak. Emiatt azonban a fogalmat nehéz hasznosítani egy egyetemi kutatáshoz vagy politikai

17 Fukuda-Parr–Messineo 2012, 5.
18 Fukuda-Parr–Messineo 2012, 7.
19 Owen 2008, 118.
20 Különböző definíciók a humánbiztonságról, Definitions of Human Security: www.gdrc.org/sustdev/husec/Definitions.pdf (A letöltés dátuma: 2019. 03. 11.)
21 Roland Paris politológus és nemzetközi tanulmányok szakértő: Roland Paris CV www.rolandparis.com/cv (A letöltés dátuma: 2019. 03. 11.)

döntéshozatalhoz.[22] A tágan értelmezett fogalom könnyebb átláthatóságának érdekében a 2. táblázat összefoglalja a humánbiztonság definíciójának elemeit.

2. táblázat

A humánbiztonság fogalmának elemei

4 jellemző[23]	5 alapelv[24]	6 tág értelmezés szerinti fenyegetés[25]	6 szűk értelmezés szerinti fenyegetés[26]
általános érvényű	emberi jogok elsődlegessége	kontroll nélküli népességnövekedés	gazdasági és társadalmi fenyegetések (szegénység, fertőző betegségek, környezeti állapotromlás)
interdependencia	legitim politikai láthatóság	globális szintű jövedelemkülönbségek	államközi konfliktusok
megelőző jellegű	multilateralizmus	növekvő nemzetközi migráció	a belső konfliktusok
emberközpontú	alulról felfelé történő megközelítés	környezetrombolás	népirtás
	regionális fókusz	kábítószer-kereskedelem	nukleáris, radiológiai, vegyi és biológiai fegyverek
		nemzetközi terrorizmus	terrorizmus és transznacionális szervezett bűnözés

Forrás: a szerző szerkesztése a táblázatban megjelölt források alapján.

Ha a humánbiztonság koncepcióját fent akarják tartani az ENSZ rendszerében, akkor két kihívással kell megbirkóznia a szervezetnek. Meg kell fogalmaznia egy általánosan elfogadott fogalmat, amihez egyrészt továbbra is meg kell tartania a koncepció központi elemének az egyént, másrészt szigorúan körül kell határolnia, mely egyén elleni fenyegetések tartoznak bele a humánbiztonságba, és melyek nem. Ha ez nem fog megvalósulni, akkor egyszerűen a tág fogalom elhagyását és a *szűk értelmezés előnyben részesítését* ajánlják a kutatók. A humánbiztonság fogalmának megalkotóinak fel kell ismerniük, hogy nincs különbség az áradás, a fertőző betegség vagy a háború okozta halál között: az összes megelőzhető kár veszélybe sodorhatja az embert. A meghatározásnak szelektívnek kell lennie a fenyegetések körével kapcsolatban is, anélkül hogy bármely nagyobb emberi csoportot érintő veszély elhárításának kárára válna.[27]

22 Paris 2001, 88.
23 Péczeli 2011, 1–3.
24 Kaldor 2007, 182–197.
25 Péczeli 2011, 1–3.
26 Owen 2008, 119.
27 Owen 2008, 123.

A fejlesztés és a biztonság nexusa

A fejlesztés és a biztonság két szorosan összefüggő fogalom. A két fogalom egy olyan meghatározott földrajzi területen belül értelmezhető, mint az állam vagy egy térség, mint például az Európai Unió. A *fejlődés feltételei* (mint például a gazdasági növekedés, a demokratizálódás és a szociális jólét) megkövetelik, hogy az állam erős eszközrendszerrel rendelkezzen és magas szintű politikai legitimitást élvezzen, vagyis megkövetelik a *biztonság feltételeinek* érvényesülését.[28]

Az így megértett kapcsolat ideális esetben kettős kötést eredményez, ahol a biztonság és a fejlesztés kölcsönösen erősítik egymást. Azonban abban az esetben, amikor sem a biztonság, sem a fejlődés feltételei nem érvényesülnek, a kölcsönösség összeomlik. A fejlődő világban ezek a feltételek többségében nem teljesülnek, ezért ha van is valamilyen egymásrautaltság, a kapcsolat nem képes kielégítően működni, így az államok gyengén látják el feladataikat, vagy működésképtelenné válnak.[29] A bipoláris rendszer felbomlását és a Szovjetunió bukását követően a nemzetközi tér és annak problémái is megváltoztak. Fejlesztés nélkül nincs biztonság és biztonság nélkül nincs fejlesztés. A fejlesztés nem lehet hatékony instabil államokban, ezért a donorországoknak érdekében áll a békeépítés és az államépítés a törékeny államokban. Ez az állítás visszafelé is igaz, miszerint béke- és államépítés nélkül nem lehet hatékony a fejlesztés sem.[30] A fejlesztéspolitika és a biztonságpolitika több területen is összekapcsolódott, komoly kockázatokat is hordoz.[31]

A bipoláris világrendszer felbomlása után azon fejlődő országok, amelyekre a két szuperhatalom korábban kiterjesztette befolyását, például Szomália[32] és Afganisztán,[33] nem voltak elég erősek ahhoz, hogy önálló államiságuk legyen. Ezekben a törékeny államokban diktatúra jött létre és polgárháborúk robbantak ki. Nagy részük bukott állammá vált, mert a hatalom nem rendelkezett olyan eszközökkel, amelyekkel képes lett volna kielégíteni egy állam szükségleteit. Törékeny biztonság, gyenge gazdaság és működésképtelen politikai intézményrendszer jellemezte ezen államokat. A gyengeségük lehetőséget adott arra, hogy az idővel globális problémákká duzzadó fenyegetések, mint a terrorizmus, megvessék a lábukat. Törékeny biztonsági rendszerük azért ad okot az aggodalomra, mert így nem tudják biztosítani a lakosság védelmét, továbbá arra sem képesek, hogy megfelelő ellenőrzés alatt tartsák a határaikat. Ráadásul, mivel a modern nemzetközi jogrend alapján egy másik állam szuverenitásának megsértése jogellenes, a világ nem tudja hatékonyan megakadályozni az itt kialakuló veszélyek terjedését.[34]

[28] Stern–Öjendal 2010, 18.
[29] Stern–Öjendal 2010, 18.
[30] Horváthné Angyal 2013, 102.
[31] Hampson 2013, 279–295.
[32] Erdős 2011, 6.
[33] Solymos 2010, 18.
[34] Paragi–Szent-Iványi–Vári 2007, 27–43.

A hirtelen megnövekedett népesség is igen nagy kockázatot rejt magában. A népességnövekedés a fejlődő világban ment végbe. Ez azért probléma, mert a fejletlen infrastruktúrával, egészségüggyel, oktatással és munkalehetőségekkel rendelkező területeken még valószínűbbé vált az éhezés, a járványok és az ételért vagy munkáért kialakuló viszályok előfordulása, valamint az ezek következtében meginduló migráció. Egy törékeny államból meginduló migrációs hullám például nagyon leterhelheti a régióban lévő szomszédos fejlődő államot, valamint a fejlett államokat is. Sokszor a menekültek már saját kontinensükön sem képesek megélni, és kénytelenek a fejlett világ segítségét kérni. Az államok bukásából eredő társadalmi konfliktusok pedig táptalajt jelentenek a terrorszervezeteknek, ugyanis ilyen körülmények között könnyen tudnak toborozni maguknak tanulatlan, földönfutó embereket, akik tartozni akarnak valahova és könnyen manipulálhatók.[35] A környezetpusztulás, az éghajlatváltozás és a környezetszennyezés következtében az emberek nagy csoportjainak helyzete kritikussá vált. A globális felmelegedés hatására az ivóvízkészlet egyre fogyóban van. A szárazság terméketlenné teszi a földeket. A környezetszennyezés pusztítja az élővilágot, és egymás után halnak ki a különböző fajok.[36] Egyre növekszik az energia iránti igény, főként a kőolajért és a földgázért megy a verseny az államok között. Azonban ezen energiahordozók fogyóban vannak, de nincs meg a megfelelő technológia sem arra, hogy a földben maradt mennyiséget kitermeljék.[37]

A fejlődő államokban a fejlesztés és a biztonság úgy jelenik meg, hogy a nagyobb donorállamok (például az Egyesült Államok, Nagy-Britannia vagy Franciaország) pénzügyi támogatással, szakértők és önkéntesek munkájával próbálják újjáépíteni a törékeny államokat, továbbá békét és biztonságot teremteni. A fejlesztés egyben hatékony eszköz lehet arra is, hogy így harcoljanak az országukat és lakosaikat leginkább fenyegető terrorizmussal, aminek forrása éppen ezekben a fejlődő államokban (például a már említett Afganisztánban) található.[38] Az ENSZ elképzelése szerint a fejlesztés jó eszköz arra, hogy a kritikus területeken a liberális kormányzást és a demokratikus eszméket terjesszék, segítsék a gazdaság és a piac liberalizációját, hogy ezzel elindítsák a várt fejlődést, ami ha megvalósul, számításaik szerint automatikusan magával hozza a biztonságot. Ennek következtében a fejlődő világ kevésbé lesz veszélyes.[39]

A 3. táblázat összefoglalja a humánbiztonság és a fejlesztés hatáskörébe tartozó feladatok közötti különbségeket és hasonlóságokat.

35 Kéri Nagy 2005, 57.
36 Ürmösi 2012, 176.
37 Hegedűs 2009, 68.
38 Birik 2014, 7–10.
39 Paragi–Szent-Iványi–Vári 2007, 102.

3. táblázat

A humánbiztonság és a fejlesztés közötti különbségek és hasonlóságok

Humánbiztonság	Fejlesztés
Különbségek	
Célja az, hogy minden ember számára biztosítsa a létfontosságú képességeket.	Célja az létfontosságú képességek biztosításán túl más, nem maguktól értetődő kihívások megoldása.
Közvetlenül vizsgálja a fenyegetés kimenetelét, mint az erőszakot vagy a gazdasági visszaesést.	A fenyegetés kialakulását vizsgálja.
Inkább a sürgős helyzetek kezelésére koncentrál.	Hosszabb távú tervei vannak, mint az intézmények kialakítása.
Hasonlóságok	
Az egyén áll a középpontban.	
Multiszektorális és többdimenziós.	
Hosszú távú terveik vannak az egyének személyes kiteljesedésével és elégedettségével kapcsolatban.	
Közvetlenül foglalkoznak a krónikus szegénységgel.	

Forrás: Owen 2008, 121–123. alapján a szerző szerkesztése.

Az összehasonlítás felszínre hozza azt a problémát, hogy néhol ellentmondanak egymásnak a jellemzők attól függően, hogy a humánbiztonság fogalmát szűken vagy tágan értelmezzük. Ha a nagyon szűk meghatározást vesszük alapul, akkor a kettő között kevés átfedés van, de ha a széles fogalommeghatározást alkalmazzuk, mint az ENSZ Humánbiztonsági Bizottsága *(Commission on Human Security – CHS),* akkor mindhárom különbségnél találkozunk ellentmondással.

A fejlesztést ért *kritikák* között fogalmazódik meg az a vád, hogy a fejlesztésért tett erőfeszítések csak még inkább fokozzák az elmaradottságot, az „új háborúk”[40] is a biztonságot bizonytalansággal, erőszakkal és fenyegetéssel váltják fel. Tehát pont olyan problémákat teremt a nexus, mint amiket meg kellene oldania.[41] Ha elfogadjuk a nemzetközi fejlesztést a nemzetközi biztonság letéteményeseként, akkor könnyen kialakulhat egy *beavatkozási* kultúra, ami azt jelenti, hogy a donorállamok a nemzetközi biztonságra hivatkozva beavatkozhatnak más államok belügyeibe, és ez komolyan felvetette a szuverenitás megsértésének kérdését. Ezért sok fejlődő állam tiltakozott a humánbiztonság összetettebb mérése ellen, mert attól féltek, hogy a humán válságokról szóló korai figyelmeztetési funkció bevezetésével figyelemmel kísérnék az olyan mutatókat, mint az egyenlőtlenség, az emberi jogok megsértése, a szegénység, az etnikai konfliktusok és a katonai kiadások, amivel a világ figyelme olyan működésképtelen országokra összpontosulna, mint Afganisztán, Haiti, Szudán vagy Zaire.[42] A fejlesztés területén az elvárt célok méréséhez az UNDP iránymutatást és segítséget ad.

40 A háborúk klasszikus elveinek már-már szabályszerű ignorálása és az aszimmetrikus hadviselés elemeinek előtérbe kerülése megváltoztatta a hadviselés egész képét, a hadviselési formákat, jelentősen előtérbe helyezve a háborúk „civil” jellegét, azaz a nem reguláris erők harcát nem reguláris erők ellen (lásd etnikai konfliktusok), illetve a civil lakosság közvetlen háborúba emelését (civil lakosság mint célpont, emberi pajzs stb.). Szíjj 2010.

41 Stern–Öjendal 2010, 22–25.

42 Stern–Öjendal 2010, 22–25.

A fenntartható fejlesztési célok jövője

2012-ben Rio de Janeiróban megtartották az ENSZ fenntartható fejlődésről szóló konferenciáját *(United Nations Conference on Sustainable Development),* a Rio +20-at. A június 20–22. között megtartott konferencián felállították a nyolc millenniumi fejlesztési célra épülő tizenhét fenntartható fejlesztési célt.[43]

A világ humán problémái nagyon összetettek. Minden siker ellenére sok kihívással kell szembenézni, amelyek nemcsak a fejlődő, hanem a fejlett országokat is sújtják. Ilyen például a nélkülözés, a nemek közötti egyenlőtlenség, a szélsőségek időszakos megerősödése, a vízhiány, a természeti katasztrófák, az éghajlatváltozás következményei és a gyors urbanizáció. Annak ellenére, hogy a szegénység felszámolásában hatalmas sikereket értek el, még mindig 385 millió gyermek él 1,9 dollár alatt naponta, és a szegénység növekszik a fejlett országokban is.[44] *Az új, emberközpontú globális fejlesztési program 2015 és 2030 között érvényes.* Az Agenda 2030 az emberi történelem során először emeli ki, hogy a világ nemzetei egyetértenek egy átfogó vízióval, világos célokkal és célkitűzésekkel a Föld bolygón élő civilizációnk fejlődése érdekében.

2018-ban a gyors éghajlatváltozás, a konfliktusok, az egyenlőtlenségek, a tartós szegénység, az éhínség, az ivóvízhiány, a gyors urbanizáció, valamint a források rossz elosztása jelentik a legnagyobb kihívást az országok számára, hogy elérjék a fenntartható fejlesztési célokat 2030-ra. A 2018-as Fenntartható Fejlődési Célokról szóló jelentés[45] alapján a konfliktusok és az éghajlatváltozás jelentősen hozzájárultak ahhoz, hogy egyre több ember éhezik és kényszerül elhagyni a lakóhelyét, valamint nem jutnak hozzá az alapvető vízellátáshoz és a higiéniai szolgáltatásokhoz sem. Több mint egy évtizede most először növekedett, és nem csökkent az éhező emberek száma. 1990-től 2015-ig az alultápláltak száma a felére csökkent. 2015-ben 777 millió fő éhezett, azonban ez az adat 2016-ra 815 millióra emelkedett.

Ugyanakkor a 2018-as jelentés[46] megállapította, hogy több ember él jobb életkörülmények között, mint egy évtizeddel ezelőtt. 2000 óta arányaiban jelentősen csökkent azon munkavállalók száma is, akik családjukkal napi 1,9 dollárnál kevesebb pénzből élnek – számuk 2000 óta 26%-ról 2017-re 9,2%-ra csökkent. Az ötéves kor alatti halálozási ráta csaknem 50%-kal csökkent, a legkevésbé fejlett országokban pedig a villamosenergia-hozzáféréssel rendelkező lakosság aránya több mint kétszeresére nőtt 2000 és 2016 között. Azonban 2015-ben 2,3 milliárd ember még mindig nem ért el alapszintű higiéniai szolgáltatást, és 892 millió ember továbbra sem rendelkezett beltéri mellékhelyiséggel. 2016-ban 216 millió ember fertőződött meg maláriaval, szemben a 2013-as adattal, amikor 210 millió esetet jegyeztek fel. Továbbá közel 4 milliárd ember maradt szociális védelem nélkül 2016-ban.[47] Ezekből a folyamatokból láthatjuk, hogy a fejlődés nemcsak földrajzilag mutat eltérő jegyeket, de célonként sem egységesek, és vannak olyan területek, amik ha sokáig

[43] https://sustainabledevelopment.un.org/rio20 (A letöltés dátuma: 2019. 03. 11.)
[44] *The Sustainable Development Goals Report* 2018.
[45] *The Sustainable Development Report* 2018.
[46] *The Sustainable Development Report* 2018.
[47] Background on the goals: www.undp.org/content/undp/en/home/sustainable-developmentgoals/background.html (A letöltés dátuma: 2019. 03. 11.); *The Sustainable Development Report* 2018.

egyenletes javulást is mutattak, most mégis visszaestek. A fenntartható fejlesztési célok elérésében az egész világ érdekelt, ezért minden ENSZ-tagország dolgozik érte.

A humánbiztonság szavatolása érdekében a nemzetközi közösségnek el kell érni a fenntartható fejlesztési célokat. A legfontosabb mérőszám az, hogy egy állam mennyit költ szociális politikájának[48] megvalósítására. Ha azt a tézist vesszük alapul, hogy a fejlődés feltétele a gazdasági prosperitás, akkor értelemszerűen a GDP-vel (Gross Domestic Product – bruttó hazai termék) tudjuk mérni az országok fejlődését. Azonban nem a gazdasági növekedés lesz a fejlesztési célok elérésének megoldása, hanem a meglévő források átcsoportosítása és jobb elosztása az ország rendelkezésére álló javaiból a szociális politikák megvalósítására.

Társadalmi fejlődési mutató

Simon Kuznets[49] *Nemzeti jövedelem 1929–1932 (National Income 1929–1932)* című műve alapján az országok teljesítményét a mai napig a GDP szerint mérjük. Sokáig az országok fejlettségét is a gazdasági növekedéssel tették egyenlővé. Ennek ellenére ma már számos olyan példát tudunk felhozni, amelyek azt bizonyítják, hogy a gazdaság erőssége és a humánbiztonság fejlettsége nem mindig egyenesen arányos, például Brazíliának alacsonyabb az egy főre jutó GDP-je Oroszországnál, mégis többet fordít a szociális politika fejlesztésére (lásd 5. táblázat). A GDP a gazdasági teljesítmény mérésére szolgáló eszköz és nem a jólétünk mértéke, ezért ez nem szolgálhat útmutatásként minden döntéshozatalhoz. Ennek ellenére mégis minden ország a nagyobb és nagyobb GDP-mutatók eléréséért küzd, ez mozgatja a világ gazdaságát. GDP-vel nem lehet a boldogságot, a biztonságot, az elegendő ételt, a megfelelő oktatási rendszert vagy az igazságosságot mérni. A GDP a 20. században feltalált mérési eszköz, amely az akkori kihívások kezelésére jött létre. A 21. században már olyan új kihívásokkal szembesülünk, mint a társadalom elöregedése, az elhízás vagy az éghajlatváltozás. Ezen kihívásoknak való megfelelés érdekében új mérési eszközökre, vagyis az előrehaladás értékelésének új módjaira van szükségünk.[50]

Michael Porter, a Harvard Egyetem professzora hozta létre 2013-ban a ma már az Európai Bizottság által is használt *társadalmi fejlődési mutatót (Social Progress Index – SPI)*.[51] Az SPI előtt már voltak olyan indexek, amelyek megpróbálták meghaladni a GDP-t, mint például a *humán fejlettségi index*[52] és a *boldogságindex.*[53] De egyik sem fordított kellő figyelmet az olyan társadalmi és környezeti kérdésekre,

48 Az államnak, közigazgatási, politikai és társadalmi testületeknek mindazon tevékenységei, amelyek az emberiség társas életének szabályozására, különösen pedig annak javítására vannak irányozva. www.kislexikon.hu/szocialis_politika.html#ixzz5iWkjHDqQ (A letöltés dátuma: 2019. 03. 11.)

49 Kuznets. *National Income and Capital Formation, 1919–1935* (1937). 61–90. www.nber.org/chapters/c5455.pdf (A letöltés dátuma: 2019. 03. 11.)

50 Green 2014.

51 *Michael Porter unveils new health and happiness index* 2013; *European Commission agrees to investigate using social progress tool alongside GDP* 2015.

52 Humán fejlettségi index (Human Development Index): http://hdr.undp.org/en/content/human-development-index-hdi (A letöltés dátuma: 2019. 03. 11.)

53 Az ENSZ 2012 óta minden év márciusában közzéteszi a Világ Boldogság Jelentést (World Happiness Report). 2019-es jelentés: https://worldhappiness.report/ed/2019/ (A letöltés dátuma: 2019. 03. 11.)

mint az iskolához való hozzáférés, az egészségügyi ellátás, a tiszta környezet, a higiénia és a táplálkozás. Az ötlet a Világgazdasági Fórum egyik munkacsoportjától indult, amelynek tagjai a GDP-től eltérő módon akarták értelmezni a fejlettséget. Eredményeiket három közgazdász, Amartya Sen, Douglass North és Joseph Stiglitz gondolatai inspirálták.[54]

Michael Green közgazdász vezeti a Társadalmi Fejlődési Kötelezettségek[55] elnevezésű nonprofit szervezetet, ami az SPI népszerűsítésére jött létre. *Az SPI a társadalom jólétének mércéje, amely teljesen elkülönül a GDP-től.* Az index leírja a jó társadalmat, amelyet három dimenzióban vizsgál. Az első szempont, hogy rendelkezik-e mindenki a túlélés alapvető szükségleteivel: élelmiszerrel, vízzel, menedékkel és biztonsággal? A második kérdés, hogy van-e hozzáférése mindenkinek az életük javításához szükséges építőelemekhez, mint az oktatás, az információ, az egészség és a fenntartható környezet? A harmadik feltétel pedig, hogy megvan-e az esélye minden embernek arra, hogy céljait és álmait akadályoktól mentesen követhesse? Ezek együttesen alkotják a három dimenzió tizenkét összetevőjét (lásd 4. táblázat), amikhez még számos indikátor kapcsolódik, amelyekkel az országok teljesítményét mérik. A különbség a GDP és az SPI között az, hogy az SPI nem azt méri, hogy a kormány mennyit költ egészségügyre, vagy hogy milyen törvényeket hoz a diszkrimináció ellen, hanem azt, hogy milyen hosszú és minőségű egy ember élete, valamint hogy szenvednek-e diszkriminációban vagy sem.[56]

Az SPI szerint a feltörekvő gazdaságok közül *Brazília áll az élen*, megelőzve Oroszországot, Kínát és Indiát. Oroszország természeti erőforrásokban gazdag, de sok a szociális probléma. Kína gazdasága ütemesen fejlődik, de nem sok előrelépést tesz az emberi jogok és a környezetvédelem területén. Indiának űrprogramja van, de millióknak még rendes illemhelyisége sincs. Másrészről vannak országok, amelyek a GDP-jükhöz mérten túlteljesítenek a társadalmi fejlődésben. Costa Ricában az oktatás, az egészség és a fenntartható környezet elsődleges ügyek, így ők elég magas szintre tudtak jutni a társadalmi fejlődésben, igen alacsony GDP mellett.[57] Ha összevetjük az Egyesült Államok és Új-Zéland adatait, láthatjuk, hogy bár az USA gazdasága jóval erősebb, a társadalmi fejlődési index Új-Zélandnál mégis magasabb. Tehát Új-Zéland annak ellenére, hogy gazdaságilag gyengébb sokkal, nagyobb figyelmet fordít a szociális problémák megoldására. Kuvait azokhoz az országokhoz tartozik, ahol sok a GDP, de nagyon alacsony az SPI, ami azt jelenti, hogy annak ellenére, hogy az ország gazdaságilag erős, a szociális gondok megoldására egyáltalán nem fordít figyelmet. 2018-ban a legjobban teljesítő ország Norvégia 90 ponttal, a legrosszabbul teljesítő pedig a Közép-afrikai Köztársaság 26 ponttal.[58] Az 5. táblázat mutatja összefoglalva a fentebb említett országokat GDP- és SPI-mutatók alapján.

---

54 *Social Progress Beyond GDP* 2013.

55 Index to Action to Impact: Social Progress Imperative: www.socialprogress.org/ (A letöltés dátuma: 2019. 03. 11.)

56 Green 2014.

57 Green 2015.

58 Norway 2018 Social Progress Index.

4. táblázat

A társadalmi fejlődési index mutatói[59]

Alapvető emberi szükségletek	A jólét alapjai	Lehetőségek
Táplálkozás és alapvető orvosi ellátás	*Hozzáférés az alapvető tudáshoz*	*Személyes jogok*
Alultápláltság, anyai halálozási arány, a gyermekhalandóság aránya, gyermekek fejlődési lehetőségeinek kiaknázatlansága, fertőző betegségekben elhalálozás	Felnőttkori írástudás aránya, általános iskolába beiratkozottak száma, középiskolai beiratkozás, nemek közötti egyenlőség a gimnáziumban, hozzáférés a minőségi oktatáshoz	Politikai jogok, szólásszabadság, az igazságszolgáltatáshoz való hozzáférés, vallásszabadság, nők magántulajdonjoga
Víz és higiénia	*Hozzáférés az információkhoz és a kommunikációhoz*	*Személyes szabadság és választás joga*
Hozzáférés az ivóvízhez, a vezetékes vízhez, legalább az alapvető higiéniai létesítményekhez, hozzáférés angol WC-hez	Mobiltelefon-előfizetések, internethasználók, ügyfélkapuhoz és független médiához való hozzáférés	Veszélyeztetett foglalkoztatás, korai házasság, megfelelő fogamzásgátlás iránti igény, korrupció
Menedék	*Egészség és jólét*	*Egyenlő bánásmód*
Hozzáférés a villamos energiához, a villamosenergia-ellátás minősége, a háztartási légszennyezés okozta halálesetek	A várható élettartam 60 év, korai halálozások nem fertőző betegségektől, az alapvető szolgáltatásokhoz való hozzáférés, minőségi egészségügyi ellátáshoz való hozzáférés	A melegek és a leszbikusok elfogadása; a kisebbségekkel szembeni megkülönböztetés és erőszak; a politikai hatalomból való egyenlő részesedés nemek szerint; a politikai hatalomból való egyenlő részesedés szocio-gazdasági pozíciók között; a politikai hatalomból való egyenlő részesedés társadalmi csoport szerint
Személyes biztonság	*Környezetminőség*	*Hozzáférés a felsőoktatáshoz*
Gyilkossági arány, politikai gyilkosságok és kínzások, lakosság által érzékelt bűnözés, közúti halálesetek	A kültéri levegőszennyezésből eredő halálesetek, szennyvíz kezelése, üvegházhatást okozó gázok kibocsátása, biome-védelem	A felsőoktatás évei, nők átlagos évei az iskolában, globálisan rangsorolt egyetemek, a globálisan rangsorolt egyetemeken beiratkozott felsőoktatási hallgatók aránya

Forrás: 2018 Social Progress Index: Methodology alapján a szerző szerkesztése.

[59] *2018 Social Progress Index, Methodology.*

5. táblázat

Bizonyos országok egy főre jutó GDP-je és SPI-je 2018-ban

Ország	Egy főre jutó GDP dollárban (helyezés)	SPI-pontozás: 100 pont a maximum (helyezés)
Norvégia	64 000 (5/146)	90 (1/146)
Közép-afrikai Köztársaság	647 (144/146)	26 (146/146)
Új-Zéland	34 000 (25/146)	89 (10/146)
Amerikai Egyesült Államok	53 000 (8/146)	84 (25/146)
Brazília	14 000 (62/146)	72 (49/146)
Oroszország	24 000 (39/146)	70 (60/146)
Kanada	43 238 (17/146)	88 (14/146)
Japán	38 000 (22/146)	89 (6/146)
Magyarország	25 000 (38/146)	80 (36/146)
Lengyelország	26 000 (36/146)	81 (32/146)
Ausztria	44 000 (14/146)	86 (20/146)

Forrás: Norway 2018 Social Progress Index alapján a szerző szerkesztése.

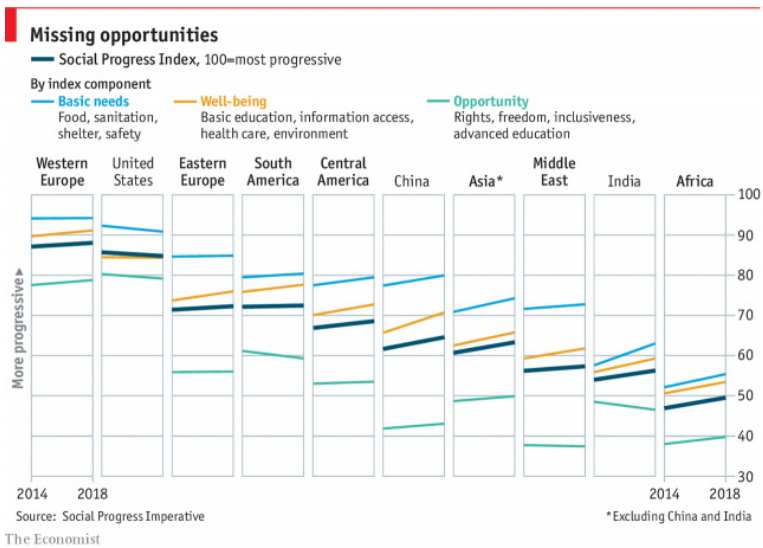
A 2018-as SPI alapján Magyarországot Lengyelországgal és Ausztriával hasonlítom össze a három fő szempont szerint (alapvető emberi szükségletek, jólét, lehetőségek), hogy érzékeltessem az index humánbiztonságot mérő lehetőségeit. Az alapvető emberi szükségletek biztosításában Ausztria vezet 96 ponttal, ezzel a 8. helyen áll, majd Lengyelország 92 ponttal a 27. helyen és Magyarország 90 ponttal a 32. helyen. Az alapvető emberi szükségleteken belül a személyes biztonságban például a világ országai közül Ausztria a 11., Lengyelország a 21. és Magyarország a 27. helyen áll. A jólét biztosításában ugyanez a sorrend, Ausztria 91 ponttal a 11. helyen áll, Lengyelország 85 ponttal a 31. helyen és Magyarország 81 ponttal a 39. helyen. A lehetőségeknél már megváltozik a rangsor, Ausztria 72 ponttal a 24. helyen áll, őt Magyarország követi 68 ponttal a 32. helyen, végül pedig Lengyelország 65 ponttal a 37. helyen. A három ország közötti sorrend az egy főre jutó GDP alapján is ugyanazt a tendenciát mutatja, mint az SPI-mutatók alapján felállított sorrend. A három ország közül Ausztria áll az első helyen, őt követi Lengyelország, majd Magyarország. A két utóbbi ország GDP-je közelít egymáshoz, míg Ausztria GDP-je (44 490 USA dollár)[60] majdnem kétszer akkora, mint Lengyelországé (26 100 USA dollár)[61] vagy Magyarországé (25 600 USA dollár).[62]

Az SPI és az éves tendenciák kiszámítására Michael Green nonprofit szervezete a Deloitte[63] csapatát kéri fel minden évben. A 2018-as eredmények alapján, ha összesítjük minden ország pontszámát a népességgel súlyozva, akkor átlagértékként 63 pontot kapunk. Ez azt jelenti, hogy ma egy átlagember a társadalmi fejlődés olyan szintjén él, mint Botswanában és a Fülöp-szigeteken. 2014 óta a világátlag-pontszám

60 *Austria 2018 Social Progress Index.*
61 *Poland 2018 Social Progress Index.*
62 *Hungary 2018 Social Progress Index.*
63 Deloitte Magyarország: Magas színvonalú könyvvizsgálati, tanácsadási, valamint adótanácsadási vállalati kockázati és jogi szolgáltatásokat nyújtunk ügyfeleinknek. www2.deloitte.com/hu/hu.html (A letöltés dátuma: 2019. 03. 11.)

1,66 ponttal javult 61,80-ról 63,46-ra. 133 ország (az összes vizsgált ország 91%-a) fél ponttal vagy annál nagyobb mértékben erősödött: 111 ország egy vagy több ponttal javult, és 19 ország pedig három vagy több ponttal fejlődött. 2014 óta mindössze hat ország pontjai csökkentek, ezek Brazília, Mauritánia, Thaiföld, Törökország, az Egyesült Államok és Jemen.[64]

Az USA mezőgazdasági minisztériuma 2014-ben 3,1%-ra tette a világ átlagos gazdasági növekedését az elkövetkező 15 évben, ami azt jelentené, hogy 2030-ra az egy főre jutó GDP összege 23 ezer dollár körül lenne. Ha ilyen mértékben gazdagodunk, hogy alakul a társadalmi fejlődés? A számításokat 2014-ben a Deloitte csapata végezte, és azt mondták, hogy ha a világ átlagos gazdagsága évi 14 ezer dollárról 23 ezer dollárra nő (csak a gazdasági növekedést figyelembe véve), akkor a társadalmi fejlődés mutatószáma 61-ről 62,4-re változik.[65] Ennek ellenére már láttuk, hogy a 2018-as érték 63 pont, tehát több, mint amennyit 2030-ra jósoltak. Ez azt mutatja, hogy ha csak a gazdasági növekedésre támaszkodunk, akkor nem fogunk eredményeket elérni a társadalmi fejlettség terén. *Arra van szükség, hogy a kormányok – gazdasági erejüktől függetlenül – a társadalom fejlesztésére irányuló politikát alkalmazzanak.*



1. ábra

2014 és 2018 közötti SPI-trendek

Megjegyzés: Színmagyarázat: Világoskék: alapvető szükségletek. Sárga: jólét. Zöld: Lehetőségek. Sötétkék: SPI: 100 = leginkább progresszív

Forrás: The Economist: Citizens' basic needs are being met, but they lack opportunities. Elérhető: www.economist.com/graphic-detail/2018/09/20/citizens-basic-needs-are-being-met-but-they-lack-opportunities (A letöltés dátuma: 2019. 03. 14.)

64 2018 Social Progress Results *2018.* www2.deloitte.com/global/en/pages/about-deloitte/articles/social-progress-index-results.html (A letöltés dátuma: 2019. 03. 11.)

65 Green 2015.

Az 1. ábra összefoglalóan bemutatja, hogy az SPI három kategóriája szerint az elmúlt négy évben milyen regionális változások történtek. A táblázat nem említi külön Közép-Európát vagy Közép- és Kelet-Európát, így számunkra a kelet-európai oszlop adatai relevánsak. Látható, hogy az alapvető emberi szükségletek biztosítása terén nincs változás 2014 és 2018 között, bár a jólét általában növekedett, a lehetőségek tekintetében a társadalom „befagyott", nem látható változás egyik irányba sem. Bár nem sok változás mutatkozik, de összességében elmondható, hogy az SPI-ben kisebb előrelépés történt. A nemzetközi összehasonlításból még két térséget emelnék ki, az Egyesült Államokat és Afrikát, amelyek eredményei szintén mutatják az SPI erejét. Az USA-ban mindhárom indikátornál romlás mutatkozik, míg Afrikában mindegyik indikátornál egyenletes javulást értek el.

Összefoglalás

A fejlesztés alapkoncepciója az, hogy a gazdasági növekedéssel a társadalmi jólét is növekszik. Az egyenlőtlen fejlődésről szóló tényadatok azonban megcáfolják azt az elképzelést, miszerint az országok gazdasági erősödésével a fenntartható fejlesztési célkitűzéseket meg lehet valósítani a megadott időn belül. A kérdésre, miszerint el tudjuk-e érni ennek ellenére a kitűzött fejlesztési célokat, a választ a társadalmi fejlettségi mutató koncepciója adja, amely a gazdasági prosperitás helyett a kormányok szociális erőfeszítéseitől teszi függővé a társadalmi jólét növekedését. Társadalmi Fejlődési Kötelezettségek *(Social Progress Imperatives)* nonprofit szervezet és a Deloitte kutatásai alapján a fenntartható fejlesztési célok elérhetőek 2030-ra, csak ez nem az országok GDP-jének növekedésén fog múlni, hanem azon, hogy a kormányok milyen törvényeket hoznak, és milyen feltételeket biztosítanak a társadalom fejlődése érdekében, különösen a jólét és a fejlődési lehetőségek területén. A humánbiztonságot fejlesztő jó kormányzáshoz pedig az összetettebb mérési lehetőségek (mint például a társadalmi fejlődési mutató) széles körű alkalmazását kell erősíteni.

Felhasznált irodalom

Birik, Shamsa (2014): Increasing Securitization of Development Post 9/11: Implications For Human Security and Aid. *Political Science Quarterly,* Vol. 116, No. 4. 585–610. Elérhető: www.academia.edu/10852255/The_Increasing_Securitization_of_Development_Post_9_11_Implications_For_Human_Security_and_Aid

Fukuda-Parr, Sakiko – Messineo, Carol (2012): *Center for Research on Peace and Development. Human Security: A critical review of the literature.* CRPD Working Paper No. 11. Elérhető: https://soc.kuleuven.be/crpd/files/working-papers/wp11.pdf. (A letöltés dátuma: 2019. 03. 11.)

Gazdag Ferenc – Remek Éva (2018): *A biztonsági tanulmányok alapjai.* Budapest–Pécs, Dialóg Campus. Elérhető: https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_EKM_Biztonsagi_tanulmanyok_alapjai.pdf (A letöltés dátuma: 2019. 03. 11.)

Gazdag Ferenc – Tálas Péter (2008): A biztonság fogalmának határairól. *Nemzet és Biztonság,* 1. évf. 1. sz. Elérhető: www.nemzetesbiztonsag.hu/cikkek/gazdag_ferenc__talas_peter-a_biztonsag_fogalmanak_hatarairol.pdf (A letöltés dátuma: 2019. 03. 11.)

Green, Michael (2014): *What the Social Progress Index can reveal about your country.* Elérhető: www.ted.com/talks/michael_green_what_the_social_progress_index_can_reveal_about_your_country/transcript (A letöltés dátuma: 2019. 03. 11.)

Green, Michael (2015): *Ted Talks London. How we can make the world a better place by 2030.* TED Talk. Elérhető: www.ted.com/talks/michael_green_how_we_can_make_the_world_a_better_place_by_2030/transcript (A letöltés dátuma: 2019. 03. 11.)

Hampson, Fen Osler (2008): Human Security. In Williams, Paul D. ed.: *Security Studies.* New York, Routledge. 229–232. DOI: https://doi.org/10.1093/oxfordhb/9780199560103.003.0031

Hegedűs Henrik (2009): A biztonság fogalmának tágabb és szűkebb értelmezése. A humánbiztonság, avagy egy konferencia tanulságai. *Hadtudományi Szemle,* 2. évf. 1. sz. 65–76.

Horváthné Angyal Boglárka (2013): *A nemzetközi segélyezés mint globális közjószág: civil szervezetek Afganisztánban.* PhD-értekezés. Budapest, Corvinus Egyetem. Elérhető: http://phd.lib.uni-corvinus.hu/743/1/Angyal_Boglarka.pdf (A letöltés dátuma: 2019. 03. 11.) DOI: https://doi.org/10.14267/phd.2014006

http://epa.oszk.hu/02400/02463/00004/pdf/EPA02463_hadtudomanyi_szemle_2009_1_065-076.pdf (A letöltés dátuma: 2019. 03. 11.)

Kaldor, Mary (2007): *Human Security – Reflections on Globalization and Intervention.* Cambridge, Polity Press. 182–197.

Kéri Nagy Zsolt (2005). A Magyar Köztársaság és a magyar nemzet biztonságát, stabilitását befolyásoló kockázatok és kihívások elemzése a nemzeti biztonsági stratégia továbbfejlesztése tükrében. Doktori disszertáció. Budapest, Nemzeti Közszolgálati Egyetem. Elérhető: http://m.ludita.uni-nke.hu/repozitorium/handle/11410/9750 (Letöltés dátuma: 2019. 03. 11.)

Owen, Taylor (2008): *UNESCO, The uncertain future of human security in the UN.* Elérhető: www.taylorowen.com/Articles/2008%20Owen%20%20UN%20and%20HS%20chapter.pdf (A letöltés dátuma: 2019. 03. 11.)

Paragi Beáta – Szent-Iványi Balázs – Vári Sára (2007): *Nemzetközi fejlesztési segélyezés.* Budapest, TeTT Consult Kft. Elérhető: www.grotius.hu/doc/pub/uhqifb/paragi_szentivany_vari_nemzetkozi_fejlesztesi_segelyezes.pdf (A letöltés dátuma: 2019. 03. 11.)

Paris, Roland (2001): Human Security. Paradigm Shift or Hot Air? University of Colorado, Boulder. *International Security,* Vol. 26, No. 2. 87–102. DOI: https://doi.org/10.1162/016228801753191141

Péczeli Anna (2011): *A humán biztonság elmélete és gyakorlata, Kanada és Japán példáján.* Elérhető: www.grotius.hu/doc/pub/ESLRKT/2011_243_peczeli_anna_a_human-biztonsag_elmelete_es-gyakorlata.pdf (A letöltés dátuma: 2019. 03. 11.)

Remek Éva (2017): Az EBESZ válságkezelő tevékenysége (intézmények, működési elv, eredmények), különös tekintettel a válságkezelés elméleti és fogalmi hátterére.

Hadtudományi Szemle, 10. évf. 4. sz. 222–224. Elérhető: http://real.mtak.hu/85314/1/17_4_bp_remek.pdf (A letöltés dátuma: 2019. 03. 11.)

Solymos András (2010): *Afganisztáni háborúk*. Budapest, Magyar Hadtudományi Társaság. Elérhető: http://mhtt.eu/hadtudomany/2010/2010_elektronikus/2010_e_28.pdf (A letöltés dátuma: 2019. 04. 28.)

Stern, Maria – Öjendal, Joakim (2010): Special Issue on the Security–Development Nexus Revisited. Mapping the Security–Development Nexus: Conflict, Complexity, Cacophony, Convergence? *Security Dialogue,* Vol. 41, No. 1. DOI: https://doi.org/10.1177/0967010609357041

Szíjj Dóra (2010): Az „új" háborúk hozadéka: a gyerekkatonaság modernkori formái. *Nemzet és Biztonság,* 3. évf. 4. sz. 27–38. Elérhető: www.nemzetesbiztonsag.hu/cikkek/szijj_dora-az___34_uj__34__haboruk_hozadeka__a_gyerekkatonasag_modernkori_formai.pdf (A letöltés dátuma: 2019. 03. 11.)

Teke András (2018): Az emberi biztonság és a „klasszikus biztonságfelfogás" viszonyrendszere. In Gaál Gyula – Hautzinger Zoltán szerk.: *Pécsi Határőr Tudományos Közlemények, XX.* Pécs, MHT HTSZ. Elérhető: www.pecshor.hu/periodika/XX/teke.pdf (A letöltés dátuma: 2019. 04. 28.)

The Sustainable Development Report 2018 (2018). https://unstats.un.org/sdgs/report/2018/overview/ (A letöltés dátuma: 2019. 03. 11.)

United Nations Development Programme (UNDP). Human Development Report (1994). New York, Oxford University Press. Elérhető: http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf (A letöltés dátuma: 2019. 03. 11.)

Internetes források

2018 Social Progress Index Results. Elérhető: www2.deloitte.com/global/en/pages/about-deloitte/articles/social-progress-index-results.html (A letöltés dátuma: 2019. 03. 11.)

2018 Social Progress Index, Methodology. Elérhető: www.socialprogress.org/index/methodology (A letöltés dátuma: 2019. 03. 11.)

2018 Social Progress Index, Norway. Elérhető: www.socialprogress.org/?tab=2&code=NOR (A letöltés dátuma: 2019. 03. 11.)

2018 Social Progress Index, Austria. Elérhető: www.socialprogress.org/?tab=2&code=AUT (A letöltés dátuma: 2019. 03. 11.)

2018 Social Progress Index, Hungary. Elérhető: www.socialprogress.org/?tab=2&code=HUN (A letöltés dátuma: 2019. 03. 11.)

2018 Social Progress Index, Poland. Elérhető: www.socialprogress.org/?tab=2&code=POL (A letöltés dátuma: 2019. 03. 11.)

Annan, Kofi (2001): *Towards a Culture of Peace.* 2001. augusztus 22. www.gdrc.org/sustdev/husec/Definitions.pdf (A letöltés dátuma: 2019. 03. 11.)

European Commission agrees to investigate using social progress tool alongside GDP (2015). Elérhető: www.theguardian.com/sustainable-business/2015/apr/09/social-progress-gdp-economic-growth-european-commission (A letöltés dátuma: 2019. 03. 11.)
https://sustainabledevelopment.un.org/rio20 (A letöltés dátuma: 2019. 03. 11.)
Michael Porter unveils new health and happiness index (2013). Elérhető: www.theguardian.com/sustainable-business/michael-porter-health-happiness-index (A letöltés dátuma: 2019. 03. 11.)
Social Progress Beyond GDP (2013). Elérhető: www.economist.com/feast-and-famine/2013/04/18/beyond-gdp (A letöltés dátuma: 2019. 03. 11.)
Social Progress Imperative: Index to Action to Impact, 2018 Social Progress Index. Elérhető: www.socialprogress.org/ (A letöltés dátuma: 2019. 03. 11.)
The Sustainable Development Goals Report 2018. hwww.un.org/development/desa/publications/thesustainable-development-goals-report-2018.html (A letöltés dátuma: 2019. 03. 11.)
www.austria.org/the-human-security-network/ (A letöltés dátuma: 2019. 03. 11.)
www.gdrc.org/sustdev/husec/Definitions.pdf (A letöltés dátuma: 2019. 03. 11.)
www.kislexikon.hu/szocialis_politika.html#ixzz5iWkjHDqQ (A letöltés dátuma: 2019. 03. 11.)
www.undp.org/content/undp/en/home/sustainable-development-goals/background.html (A letöltés dátuma: 2019. 04. 28.)
www2.deloitte.com/hu/hu.html (A letöltés dátuma: 2019. 03. 11.)

NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 128–129. • DOI: 10.32561/nsz.2019.2.10

Regényi Kund Miklós[1]

Könyvismertető

Szabó Szilárd: *Az Osztrák–Magyar Monarchia központi katonai és polgári hírszerző és elhárító szervezete 1850–1918* című könyvéről

Az Osztrák–Magyar Monarchia titkosszolgálatainak kutatója, a Debreceni Tudományegyetem oktatója, Szabó Szilárd egy kismonográfiával járult hozzá a téma iránt érdeklődő szakmai közönség – no meg minden érdeklődő – épüléséhez. A mű *Az Osztrák–Magyar Monarchia központi katonai és polgári hírszerző és elhárító szervezete 1850–1918* címmel, 242 oldal terjedelemben, a Debreceni Egyetemi Kiadó gondozásában jelent meg 2019-ben. A könyv színvonaláról sokat elárul, hogy két lektora is volt, Szakály Sándor és Parádi József, akik szakmai teljesítménye önmagában garancia az igényességre és a részletességre.

A mű, bevallott önkorlátozással, az intézménytörténetre fókuszál, ott viszont a teljességre törekszik. Igazi történészhez méltóan levéltári forrásokon (is) alapul. Erényei között kiemelendő a hazai, illetve osztrák szakirodalom részletes, kritikai vizsgálatokkal kiegészített, és a művek egymáshoz való viszonyát is tárgyaló bemutatása. A szerző ugyanezt az osztrák levéltári források vonatkozásában is elvégezte, ezzel a téma többi kutatóját abba a kényelmes helyzetbe hozta, hogy az eddiginél sokkal fókuszáltabban, ezáltal hatékonyabban kutathatnak. (Erre a lehetőségre, mintegy felhívásként, a szerző utal is.)

Másik nagy erénye a műnek, hogy a nemzetbiztonsági intézményrendszernek nemcsak a katonai szárnyára összpontosít, amely védhető lett volna, hiszen a vizsgált kor biztonsági és államfelfogásában az Evidenzbüro és utódszervei általános feladatokat ellátó szervezet volt(ak). A szerző vizsgálódásait kiterjesztette a közös külügyminisztérium keretén belül működő, mai terminológiával polgári hírszerzésnek nevezhető Informationsbürora is.

Ezen túlmenően bemutatja azt a széles körű kormányzati együttműködést is, amely az állam, a nemzet biztonsága érdekében az eső világháború előtt és alatt kialakult. Ezzel a szerző túl is lépett az önmaga által meghatározott határokon, hiszen ez a fajta együttműködés már szakmai szempontokból is vizsgálható, magyarázatot adva arra, hogy tudott az Evidenzbüro, illetve a két világháború között a magyar

[1] Dr. Regényi Kund Miklós egyetemi adjunktus, Nemzeti Közszolgálati Egyetem. ORCID-azonosító: 0000-0003-1833-9523.

állambiztonsági szervezetrendszer oly kis létszámmal oly komoly feladatokat ellátni, azaz, hogy tudta a szakmai munkát oly hatékonyan szervezni és elvégezni.

Összefoglalva elmondható, hogy a kismonográfia az első lépés kell, hogy legyen a dunai monarchia állambiztonsági tevékenységének tudományos, szakmai vagy akár ismeretterjesztő célú vizsgálata során.