NEMZETBIZTONSÁGI SZEMLE
10. évfolyam (2022) 4. szám 65–76. • DOI: 10.32561/nsz.2022.4.5

Vida Csaba[1]

Szanitizáció – A források és az adatok védelme az elemző-értékelő munka során

Sanitization – Protection of Sources and Data during Intelligence Analysis

A szerző a tanulmányában megvizsgálta a szanitizáció fogalmi rendszerét és funkcióját a nemzetbiztonsági rendszeren belül. Előtte azonban áttekintette a szanitizáció fogalmát a különböző tudományágakban. Bemutatja a nemzetbiztonsági szolgálatoknál alkalmazott szanitizáció célját, illetve a vele szemben támasztott követelményeket és annak gyakorlati megvalósítását. Rámutat a források és a szenzitív adatok fokozottabb védelmének fontosságára, mivel azok hiánya közvetlen veszélyt jelent a nemzet biztonságára. A szanitizáció történhet a források, az információ metaadatainak és információtartalmának védelme érdekében. A tanulmány végén felvázolja a szanitizációnak azt a fajtáját, amikor politikai vagy szakmai célokból a minősített dokumentumokat nyilvánosságra akarják hozni, amelyet meg kell előznie a dokumentum szanitizációjának.

Kulcsszavak: *nemzetbiztonság, elemzés-értékelés, szanitizáció, tájékoztatás, információ*

The author in his study examined the conceptual system and function of sanitization within the national intelligence system. Before that, he had reviewed the concept of sanitization in different scientific disciplines. He presents the purpose, the requirements and the practical implementations of sanitization used in the framework of the intelligence services. He points to the importance of enhanced protection of sources and sensitive data, as their absence poses a direct threat to national security. Sanitization can be done in order to protect sources, as well as metadata and content of information. At the end of the study, he outlines the type of sanitization when classified documents are made public for political and professional purposes, which must be preceded by the sanitization of the document.

Keywords: *intelligence, intelligence analysis, sanitization, dissemination, information*

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, e-mail: vida.csaba@uni-nke.hu

Bevezetés

Egy ország nemzetbiztonsági rendszerének legfontosabb értékei a nemzetbiztonsági szolgálatok forrásai, függetlenül attól, hogy azok melyik adatszerzési ághoz tartoznak. A források biztosítják a szolgálatok számára azokat az adatokat és információkat, amelyekből az adatfeldolgozást és az elemzés-értékelést követően a nemzetbiztonsági szolgálatok végrehajtják az állami politikai és katonai vezetés tájékoztatását a döntés-előkészítés érdekében, illetve támogatják a sikeres nemzetbiztonsági műveleteket. A nemzetbiztonsági szolgálatok teljesítményét ezáltal a rendelkezésre álló forrásaik határozzák meg, így a szolgálatok egyik legfontosabb törekvése azok védelmének maximalizálása, mivel elvesztésük veszélyezteti tevékenységük sikerességét. A nemzetbiztonsági szolgálatok forrásai – a nemzetbiztonsági rendszer törvényi felhatalmazása alapján – a külső engedélyhez kötött és nem kötött titkos,[2] illetve nem titkos információgyűjtés keretében biztosítják a szükséges adatokat és információkat. Így a források nagyon szenzitívek, és sok esetben bizalmi elven működnek, ezért maximális mértékben kell biztosítani azok védelmét. A források esetleges beazonosítása azok azonnali megszűnéséhez vezethet, ami nemcsak a nemzetbiztonsági szolgálatok számára jár rövid és hosszú távú károkkal, hanem a források számára is, mivel az egyes esetekben – főleg a hírszerzés külföldi forrásai számára – életveszélyt is jelenthet. A hosszú távú károkhoz tartozik a szolgálattal – országgal – szemben kialakult általános bizalmatlanság, amelynek közvetett hatása van az ország értékeinek védelmére és érdekeinek érvényre juttatására.

A források védelme tehát létszükséglet a szolgálatok számára. A védelem szükségessége független az adatszerzési ágaktól, mert a források lehetnek személyek vagy technikai rendszerek is, így bármelyik elvesztése problémát okoz. A védelem erős pillérei a minősített adatok védelméről szóló jogszabályok,[3] amelyek garantálják a források és az azoktól származó adatok és információk egyfajta védelmét. A jogszabályok az információvédelmen keresztül biztosítják a források védelmét. Az információk védelme a jogszabályok alapján uniformizált, vagyis nem egyedi, hanem általános, így nincs mindig lehetőség a források egyedi és speciális védelmére. Általában a forrás védelmének kell a legmagasabb szintűnek lennie, mint a forrás által biztosított (szállított) információé. A jogszabályok szellemisége alapján, ha egy dokumentum több elkülönülő információt tartalmaz, akkor védelmének mindig a legmagasabb védelmet igénylő információval kell azonosnak lennie, így az alacsonyabb védelmet igénylő információkat is magasabb védelemmel látják el, mivel sokszor technikailag nem lehet szétválasztani az adatokat és az információk különböző elemeit.[4] A magasabb minősítésű információ kezelése azonban sokkal bonyolultabb, így azok felhasználása is nehezebb, valamint egyes adatok esetében túlminősítés[5] is fennállhat. Ezért szük-

[2] Például Magyarországon a 1995. évi CXXV. törvény 53–58. §-ban meghatározott eljárások.

[3] Magyarországon a 2009. évi CLV. törvény a minősített adatvédelemről, de más országokban is külön jogszabály szabályozza a területet. Például Szlovákiában a 215/2004. számú törvény a minősített adatok védelméről (Zákon č. 215/2004. Z.z. o ochrane utajnových skutočnosti).

[4] Magyarországon a 2009.évi CLV törvény 5. § (10) bekezdése is erre utal.

[5] A túlminősítésre akkor kerül sor, amikor a közérdek által védendő adatot a szükségesnél magasabb minősítéssel látják el, ezáltal korlátozzák a hozzáférését.

séges sokszor szétválasztani a forrást és az információt, vagyis a különböző szintű védelmet igénylő adatelemeket.

A források tehát legtöbbször a legmagasabb – sokszor a jogszabályok által nyújtott garanciákon túli – védelmet igénylik, ezért a jogszabályokon kívüli további védelmi mechanizmusokat is megkövetelnek. A fokozottabb védelemnek több lehetősége van, ezek közé tartozik a „need to know"-elv, valamint a „szanitizáció".

„Need to know" elv

A „need to know" elv alapvetően azt jelenti, hogy „azt kell tudni, ami szükséges", de különböző tudományágakban és intézményrendszerekben más-más jelentése van. Talán ez az egyik olyan idegen kifejezés, amelyet a szakértők is sokszor félreértelmeznek. A fogalom általában a „szükséges ismeretet", a „feltétlenül szükséges megismerni" fogalmat, a „szükséges mértékű ismeretet" jelenti,[6] de a „legkisebb jogosultság"[7] értelmezése is ismert. A nemzetbiztonsági rendszerben ugyanakkor a „need to know" elv azt takarja, hogy az adott személy (nemzetbiztonsági munkatárs/vezető) csak azokat az adatokat vagy információkat ismerheti meg, amelyek a munkájának, a feladatainak végrehajtásához szükséges. Ez is segíti a szenzitív információk védelmét azzal, hogy korlátozza az információk megismerőinek körét. Biztosítja továbbá, hogy illetéktelen, vagyis olyan személyek ne ismerjék meg az adott információt, akik nem jogosultak, vagy nincs szükségük rá. Sok esetben nem a jogosultság kérdése, hanem a praktikusságé, mert felesleges olyan információkkal terhelni a munkatársakat/felhasználókat, amelyekre nincs szükségük a munkavégzésükhöz. Az elv alkalmazása az élet számos más területén (az üzleti szférában, az iparban, de még a szervezett bűnözésnél vagy éppen a terrorszervezeteknél) is érvényesül, mivel egyfajta védelmet biztosít az adott tevékenységnek vagy munkafolyamatnak.[8]

A nemzetbiztonsági rendszerben a „need to know" elv nemcsak a szolgálatokon belül működik, hanem a nemzetbiztonsági tájékoztatók felhasználóira (döntéshozókra) is vonatkozhat, mivel számukra csak azokat az információkat kell továbbítani, amelyre a döntéseik meghozatalához szükségük van. Ezt tekintik a szolgálatok tájékoztató tevékenységében többek között a vertikálisan és horizontálisan differenciált tájékoztatásnak. Ez szintén nem feltétlenül arra vonatkozik, hogy az adott állami vezető nem jogosult az információ megismerésére, hanem arra, hogy azokra nincs szüksége a döntéseihez, így felesleges annak megismerése. A felhasználók esetében is változatlanul magáról az információról, és nem a forrásról van szó, mivel a döntéshozó számára az adott információ a fontos, és csak ritka esetben releváns, hogy az adott információ milyen forrásból származik. Az információ esetében a döntéshozók számára

---

6 Az eur-lex.europe.eu adattárban szereplő meghatározások. Lásd: www.linguee.hu/angol-magyar/forditas/on+a+need+to+know+basis.html

7 Mihály (é. n.)

8 A nemzetbiztonsági rendszerben létezik a „need to share" elv, amely azt jelenti, hogy mindent, amit lehet, meg kell osztani az illetékesekkel, vagyis minél több információt hozzáférhetővé kell tenni. Ez részben szemben áll a „need to know" elvvel, de a „need to share" nem az információk védelmére vonatkozik, hanem inkább a nemzetbiztonsági rendszeren belüli együttműködés erősítésére. A rendszer sikeres működése érdekében meg kell találni a két elv alkalmazása közötti egyensúlyt.

annak valódisága (igazságtartalma) a legfontosabb. Természetesen vannak olyan esetek, amikor a forrás is meghatározó, ha például üzenetről van szó, vagy olyan jellegű információról, amelynek értékét a forrás határozza meg. Sokszor ezekben az esetekben is szükséges a források kiemelt, fokozottabb védelme, tehát nem lehet mindig konkrétan megnevezni.

Megállapítható ugyanakkor, hogy a „need to know" elv nem mindig biztosít megfelelő garanciát a forrás védelmére, ezért főleg a döntéshozók tájékoztatása során, de a nemzetbiztonsági rendszeren belül is egy másik mechanizmust kell alkalmazni. Ezzel kapcsolatban a dilemma a döntéshozók tájékoztatásának hatékonysága és a nemzetbiztonsági szolgálatok forrásainak védelme közötti hangsúlyon van. A probléma egyik megoldása az információk „szanitizálása", amely a nemzetbiztonsági szektorban az információk felhasználása során a források és az eljárások védelmét biztosítja.

A „szanitizáció" értelmezése a különböző tudományágakban

A „szanitizáció" nagyon ismerős, de mégis ismeretlen fogalom, mivel használata során számos félreértéssel lehet találkozni. A különböző tudományágakban sokszor eltérő értelmezésben használják, amelyekben ellentmondásokat is fel lehet fedezni. A „szanitizáció" mint idegen fogalom annyira „idegennek" tekinthető, hogy az Akadémiai Kiadó által hivatalosnak tekinthető, az *Idegen szavak és kifejezések szótár*ának átdolgozott második kiadása[9] sem tartalmazza annak magyarázatát. Az átdolgozott és felújított szótár 30 000 címszót tartalmaz,[10] amelybe nem fért be a vizsgált fogalom. Szintén nem található a fogalom az Akadémiai Kiadó által hivatalosnak minősülő *Magyar értelmező kéziszótár*ban",[11] amely szintén aktualizált és 75 000 címszót tartalmaz.[12]

Tehát a fogalom magyarázatát az adott tudományágaknál kell keresni, ami nem egyszerű, mivel a legnépszerűbb internetes keresőlapon[13] a „szanitizáció" és a „szanitizálás" – magyar nyelvű fogalmakra – összesen 124 és 70 találat volt. A találatok többsége az informatika és az egészségügy területére vonatkozott. Az egészségügyben általában tisztítás/csírátlanítás/fertőtlenítés egyfajta változataként azonosítják. Az informatika területén általában adattörlést vagy adatmegsemmisítést jelent. Kovács László fogalmazott meg egy komplexebb definíciót, amely szerint „a szanitizálás az információnak a forrástól való elválasztását jelenti, ami kizárja, hogy az információ forrására vagy annak különböző paramétereire vonatkozó következtetéseket lehessen levonni".[14] A fogalmat a kiberbiztonsággal kapcsolatban alkalmazza annak érdekében, hogy az incidenskezelés során az illetékesek megkaphassák a szükséges információkat. A találatok közül csak néhány tartozik a nemzetbiztonság elméletéhez (kiemelten a hírszerzéshez, felderítéshez). Egyik egy korábbi tanulmányom szövegében

9 Bakos 2002
10 Bakos 2002: hátsó borító.
11 Pusztai 2003
12 Pusztai 2003: hátsó borító.
13 A Google internetes keresőrendszer (www.google.com), amely több mint 20 milliárd tétel közül keresi a megfelelő egyezést.
14 Kovács 2018: 49. 25. lábjegyzet szövege.

található,[15] amely a hírszerző elemző-értékelő munkával foglalkozik, míg a többi találat a rádióelektronikai felderítéssel (SIGINT[16]) kapcsolatos.[17]

A legnépszerűbb internetes keresőben a „szanitizáció" angol nyelvű változatára *(sanitization/sanitisation)* már jóval több, 178 millió találat van, amelyek közül a nemzetbiztonság vonatkozásában 5 280 000 találatot lehet azonosítani. Így a nemzetközi szakirodalomban már sokkal részletesebb fogalmi rendszere van a „szanitizációnak", amely szintén számos tudományágban fogalmaz meg definíciókat. Általában fertőtlenítést és egy terület megtisztítását jelenti, de sokkal tágabb fogalmi rendszere van. Az információs elméletekkel kapcsolatban is szélesebb fogalomkör található, mivel megjelenik az adattisztítás, vagyis a törölt adatok helyreállításának megakadályozása, továbbá a nem biztonságos informatikai elemek eltávolítása, de az információcenzúra vonatkozásában az információk nyilvánosságra hozatalának tiltása is az értelmezéséhez tartozik. Viszonylag széles szakirodalma van az információtechnológiában az adatok „szanitizációjának", amely alapvetően a különböző memóriaeszközökön tárolt adatok végleges törlésére irányul, vagyis visszafordíthatatlanul eltávolítják vagy megsemmisítik az adatokat, hogy ne maradjanak használható maradványok vagy utalások se a megszüntetett adatokról.[18]

A nemzetközi szakirodalom külön foglalkozik a minősített információk szanitizációjával kapcsolatban, amelynek központi eleme az információkból az érzékeny elemek eltávolítása.[19]

A „szanitizáció" fogalma a nemzetbiztonsági rendszerben

A nemzetbiztonsági szektorban a „szanitizáció" fogalmi rendszere alapvetően az információkkal kapcsolatos, vagyis az információ egyes elemeinek védelmére, törlésére vagy korlátozott hozzáférésére vonatkozik. Ez alapján – a nemzetbiztonsági rendszerben – a „szanitizáció" fogalma: az adatszerzők által különböző eljárásokkal és módszerekkel összegyűjtött nemzetbiztonsági információk olyan mértékű – a valóságtartalom módosítása nélküli – átalakítása, hogy ne lehessen visszakövetkeztetni az eredeti információk egyes szenzitív részeire, kiemelten a forrásaira.[20] Tehát többek között az eredeti információt megfosztják azoktól az elemektől, amelyek alapján beazonosíthatók az információ védendő részei.[21]

A nemzetbiztonsági információs rendszerben több célra használják a „szanitizációt", mivel nemcsak a források, hanem annak metaadatai vagy részeinek védelmére is alkalmazzák. A legfontosabb a forrás védelme, vagyis információ olyan módon történő megjelenítése, hogy rejtve maradjon a valódi forrás. Emellett szükségessé válhat az információ megfosztása a metaadataitól, például a megszerzés módjától, valamint

15 Vida 2017: 121.
16 Signal intelligence.
17 Balogh Péter tudományos publikációiban alkalmazta a fogalmat mint a SIGINT-tevékenység egyik elemét. Például Balogh 2013.
18 International Data Sanitization Consortium: www.datasanitization.org/
19 Például UNODC 2011
20 Vida 2017
21 Balogh 2018: 148.

arra való bármilyen utalástól, hogy milyen módon szerezték meg a nemzetbiztonsági szolgálatok az adott nyers adatot. Az információtartalom vonatkozásában is vannak további védendő adatelemek. Ezek közé tartozhatnak a személyiségi adatok, valamint a szenzitív, de információtartalom alapján nem releváns adatok is.

Alapkövetelmények

A „szanitizációval" szemben több olyan követelmény van, amelyek betartása és megvalósítása létfontosságú annak érdekében, hogy megfelelő módon be tudja tölteni funkcióját.

Mindenképpen úgy kell megvalósítani, hogy nem módosulhat az eredeti információtartalom, egyedüli lehetőség az információtartalom csökkentése/korlátozása. A „szanitizált" adat nem térhet el tartalmában az eredeti nyers adattól.

Szükség szerinti mértékben kell elvégezni, mert amennyiben a kelleténél több információt törölnek, akkor az sértheti a felhasználó érdekeit, amennyiben pedig a szükségesnél kevesebb információt törölnek, a tevékenység funkciója, vagyis az információ (kiemelten a forrás) speciális védelme nem valósul meg.

Az információ adattartalmának csökkentését az információ birtokosának – vagyis titokvédelmi szempont szerint a minősítőjének – kell elvégeznie, mivel ő van tisztában az információ egyes elemei mögötti tényekkel, az információ részletes metaadataival és a teljes eredeti információval.

A fentiek nem zárják ki azt, hogy az adatokba betekintéssel rendelkező személy szükséges esetben nem ismerheti meg a teljes nyers adatot, erre azonban többségében – az információ birtokosától – külön felhatalmazás kell. Tehát csak egyedi esetekről lehet szó.

Lehetővé kell tennie, hogy csökkenteni lehessen az információk védelmét, így az a felhasználók minél szélesebb köréhez eljuttatható, mert sokszor a fokozottabb védelem akadályozza meg, hogy az információ eljusson a megfelelő számú felhasználóhoz.

Meghatározott szabályozók[22] alapján kell elvégezni, attól eltérni nem szabad, mert akkor feleslegessé válhat az egész tevékenység, és sérülhet a forrás védelme és a nemzetbiztonsági tevékenység.

Gyakorlati megvalósítása az információelméletben

Az információelméletben a „szanitizáció" általános gyakorlati eljárásai közé tartozik az adat fizikai megsemmisítése, az adat visszaállítható törlése, az adat titkosítása (rejtjelezése), valamint az adat elfedése.[23]

[22] A tanulmány második részében található.
[23] Data sanitization: www.imperva.com/learn/data-security/data-sanitization/

Az *adat fizikai megsemmisítése* a legdrasztikusabb változata a „szanitizációnak", amelynek a célja, hogy a törölt adatot ne lehessen visszaállítani mások által. A megsemmisítés történhet illetéktelenek kezébe jutásának megakadályozása érdekében, vagy hogy az adat egyszeri megismerését követően ne lehessen azt továbbítani vagy sokszorosítani (vagyis többször megismerni).

Az *adat visszaállítható törlése* az illetéktelenek kizárását támogatja, tehát csak azok ismerhetik meg az adatot, akiknek jogosultsága van arra, amennyiben illetéktelenekhez kerül az adat, akkor például törlődik az információ. A visszaállítható törlés jelentheti azt, hogy csak azok számára törlődnek a szenzitív adatelemek, akik nem jogosultak megtekinteni azokat.

Az *adat titkosítása* során az adatok egyes elemeinek olyan jellegű rejtjelezését végzik el, amelynek következtében a szenzitív rész korlátozott hozzáférést biztosít, tehát csak azok ismerhetik meg az adatot, akik ismerik a rejtjelek, kódok kulcsát. Így csak azok rendelkeznek a megoldással, akik jogosultak megismerni az adott titkosított adatot/információt.

Az *adatok leplezése* során az adatok szenzitív elemeit kicserélik más (sokszor megtévesztő) adatokkal, így csak azok számára értelmezhetők az adatok szenzitív elemei, akik ismerik az eredeti adatot vagy a behelyettesített adatok megfelelőjét.

A fenti információelméleti „szanitizációs" eljárásokat a nemzetbiztonság elméletében is alkalmazzák, de azoknak egyfajta módosított és különleges megoldásait.

Megvalósítása a nemzetbiztonsági tevékenységben

A nemzetbiztonsági rendszerben a „szanitizációt" a szolgálatok esetében minden szervezeti elemnek alkalmaznia kell, amelyek köre az adatszerzőktől, a műveleti elemektől az elemző-értékelőig tart, valamint a nemzetbiztonsági tájékoztatókban is meghatározó szerepük van. A „szanitizáció" mögött mindig konkrét céloknak kell állnia, amelyek a nemzetbiztonsági rendszer képességeinek fenntartása és lehetőség szerinti bővítése a források, valamint a megszerzett információk megfelelő kezelése által. Tehát a „szanitizáció" ebben az értelmében nemzetbiztonsági tevékenységet támogató elem, amelynek meghatározott – rendkívül fontos – funkciója van a nemzetbiztonsági rendszerben, így mindennapos annak alkalmazása.

A nemzetbiztonsági rendszer működésében a „szanitizáció" történhet:[24]

- a forrás védelme érdekében;
- a nyers adatok/információk metaadatainak védelme érdekében;
- az adatszerzési módok, eljárások védelme érdekében;
- a személyes adatok védelme érdekében;
- a szenzitív adatok védelme érdekében.

A forrás védelme érdekében történő „szanitizáció" a nemzetbiztonsági rendszerben leggyakrabban alkalmazott eljárás, amelynek a célja az információk forrásának leplezésére és oltalmazására irányul, hogy ne lehessen visszakövetkeztetni a pontos

[24] UNODC 2011: 27–28.

forrásra. A forrás „szanitizációjának" többfajta megoldása van, amelyek más-más szinten és munkafolyamatban valósulnak meg. A források első szintű „szanitizációja", hogy a forrásokat kódokkal vagy jelekkel leplezik, így a pontos forrás csak azok számára beazonosítható, akik ismerik a kódok és a jelek mögötti valós forrást, valamint közvetlen kapcsolatban állnak a forrásokkal. Így mások számára csak a forrás általános jellege ismerhető meg. Az általános jellegéhez tartozik az adatszerzés általános módja (műveleti, nyílt vagy hazai és nemzetközi együttműködés), a forrás hitelességének szintje, valamint a forrás által biztosított információ valószínűsége, megbízhatósága. Védelem alá kell helyezni az adatszerzés pontos idejét és helyét, az adatszerzést végző szervezetet, az adatszerzés pontos módszerét, mert ezekhez az információkhoz a nemzetbiztonsági rendszer néhány szereplője férhet hozzá, akik jogosultak a szenzitív információk megismerésére, többek között az elemző-értékelők, akik további „szanitizációs" eljárásokat alkalmaznak, amelyek a forrás további védelmét biztosítják, így az elemzett-értékelt információból (a nemzetbiztonsági tájékoztatókból) már nem lehet visszakövetkeztetni a pontos forrásra. Az elemző-értékelők a tájékoztatókban nem a forrásokra, hanem az azok által megszerzett információra helyezik a hangsúlyt, így a szenzitív adatelemek nem jelennek meg, valamint csak abban az esetben utalnak azokra, ha végképp szükséges, de akkor is leplezetten.

Az információ metaadatainak „szanitizációja" szintén a forrás védelmére irányul, amely során nem közvetlenül a forrást védik, hanem minden olyan adatot, amelyből vissza lehet következtetni a forrásra. Ezekhez tartozik a forrás által biztosított információ megszerzésének helye és ideje, valamint a forrás tevékenysége. A metaadatok „szanitizációja" az elemző-értékelő munka keretében történik meg, amelynek során az elemző-értékelők alapvetően az információ tartalmának értékelésére-elemzésére helyezik a hangsúlyt, így az információ metaadatai csak kiegészítő információkat biztosítanak, amelyek egyáltalán nem vagy nagyon korlátozottan jelennek meg a döntéshozók tájékoztatóiban. Csak abban az esetben szükséges a metaadatokra (például a megszerzés idejére vagy esetleg helyére) utalni a tájékoztatókban, ha azok abszolút fontosak az információ megértéséhez. Az elemzés-értékelés során nem az információ megszerzésének időpontja, hanem az információhoz köthető időpont a releváns, vagyis például mikor történt az az esemény, amelyről az információ szól. A helyszín vonatkozásában is inkább az esemény helyszíne és nem az információ megszerzésének a helye a fontos. Tehát az elemzés-értékelés során a metaadatoktól viszonylag könnyen meg lehet fosztani az információt, ami általában nem csökkenti az információ értékét a nemzetbiztonsági tájékoztatókban.[25]

Az információ megszerzési módjának „szanitizációja" a nemzetbiztonsági tevékenység védelmének egyik legfontosabb eleme, mert ugyan a titkos információszerző lehetőségeket a jogszabályok tartalmazzák, de a részletes információszerző eljárások már védendő információnak minősülnek. Az információszerzési ágak[26] saját infor-

[25] A nemzetbiztonsági tájékoztatók a nemzetbiztonsági szolgálatok termékei, amelyekből megtörténik a döntéshozók megfelelő információkkal való ellátása.

[26] Információszerző ágakhoz tartozik többek között az emberi erőforrással folytatott hírszerzés (human intelligence, HUMINT), a rádióelektronikai felderítés (signal intelligence, SIGINT), a képi felderítés (imagery intelligence, IMINT), a nyílt forrású információszerzés (open sources intelligence, OSINT), a kiberhírszerzés (cyber intelligence, CYBINT), illetve a közösségi médiából folytatott információszerzés (social media intelligence, SOCMINT).

mációszerzési eljárásokkal és technikákkal rendelkeznek, amelyek célja a szükséges információk összegyűjtése. Az információszerzés körülményei elemző-értékelő szempontból kevésbé relevánsak, mert az elemző-értékelő főleg az információ tartalmával és nem annak megszerzési módjával foglalkozik. A megszerzés módja csak abból a szempontból fontos, hogy megítélje a megszerzett információ jellegét és valóságtartalmát.[27] Tehát a döntéshozók tájékoztatásához nem szükséges az információ megszerzési módjának a megjelenítése. Maximum annak jelzése szükséges, hogy megerősített vagy megerősítésre szorul az információ, illetve műveleti vagy nyílt forrásból származott, továbbá, milyen mértékben védendő információról van szó. Megerősítettnek tekinthető az az információ, amelyet több forrás is megerősített, míg a megerősítésre szoruló információ olyan jellegű, amelynek valószínűsége fennáll, de még nem sikerült több forrásból megerősíteni. A műveleti információk közé sorolhatók a titkos információszerző tevékenységből származó információk. Az információ megszerzési módjának „szanitizációjával" magát a hírszerzési ágat is védik, vagyis, hogy az adott információ melyik adatszerzési terület terméke.

Az információtartalom „szanitizáció"-jához tartozik az információ személyes adatoktól való megfosztása, amely a személyiségi jogok törvényi védelméhez köthető.[28] Az információtartalmat az elemző-értékelő munka keretében feldolgozzák, elemzik és értékelik, illetve azt követően valósul meg a döntéshozók számára a tájékoztatók elkészítése. Az információtartalom felhasználásának szabályaihoz lehet sorolni, hogy az információból minden olyan elemet (tényt és adatot), így a személyes adatot, ki kell venni, amelyből következtetni lehet a forrás kilétére. Ezenfelül eltávolítanak minden másra vonatkozó személyes adatot, amely az információ megértése szempontjából nem lényeges. Az információ megfosztása az érzékeny személyes adatoktól azt is jelenti, hogy bővíthető azok köre, akik megismerhetik azt. Tehát a személyes adatok a döntéshozók tájékoztatóiban csak abban az esetben használhatók fel, ha az információtartalom azt megköveteli. Ide sorolható a célszemélyek profilozása.

Az információtartalom „szanitizációja" a nem releváns szenzitív információk elhagyása, amelynek alapvető célja, hogy az elemző-értékelők a döntéshozó számára csak azokat az információkat továbbítják, amelyek szükségesek az adott tájékoztató (témakör) megértéséhez. A nem releváns, felesleges információk csak megzavarják vagy félrevezetik és túlterhelik a döntéshozót, ezért alapvető fontosságú, hogy a tájékoztatóba csak azokat az információkat kell belefoglalni, amelyek segíti annak megértését.[29] Tehát csak abban az esetben szabad a szenzitív információkat belehelyezni a tájékoztatóba, ha valóban szükség van az adott témakörben a döntéshozó tájékoztatására. Ez nem jelenti azt, hogy a döntéshozó nem jogosult az adott információ megismerésére, hanem, hogy felesleges terhelni az irreleváns információkkal. Ezen túl a rendkívül szenzitív információk „szanitizációja" megvalósulhat az elemzés-értékelés folyamatában is, mivel összforrású elemzés-értékelés zajlik, így a többi információval közösen elvegyülve, valamint a különböző információelemző eljárásokkal is csökkenthető a szenzitivitás mértéke. A fentiek nem jelenthetik azt, hogy a szenzitív információkról

27 Vida 2016
28 NMHH 2018
29 Önmagában azért nem kell belerakni egy információt a tájékoztatóba, mert rendelkezésre áll.

nem tájékoztatják a döntéshozókat, hanem a tájékoztatás olyan formában történik meg, amely megerősíti a szenzitív információk védelmét.

A „szanitizáció" gyakorlati megvalósítása a nemzetbiztonsági tevékenységben nagyon pontos és precíz munkát követel meg az elemző-értékelőktől és más szervezeti elemek munkatársaitól, hogy maradéktalanul teljesüljenek a követelmények, amelyek központi tényezője, hogy – az információk és azok forrásának védelme mellett – a döntéshozók mindig megkapják a szükséges információt, és a tájékoztatásuk csak valós információkkal történhet meg. A „szanitizáció" nem károsíthatja az információt és annak értékét.

A „szanitizáció" szerepe a minősített információk nyilvánosságra hozatalában

A „szanitizáció" meghatározó szerepet tölt be, amikor politikai vagy szakmai okokból egy minősített információt hivatalosan nyilvánosságra akarnak hozni, mivel a szélesebb kör általi megismerését például társadalmi érdekek megkövetelik. Ebben az esetben szükséges a minősített információt megfosztani azoktól az adatoktól, amelyek szenzitívek és változatlanul közérdek által védendőnek minősülnek. A dokumentumok ilyen jellegű „szanitizációjának" általában politikai vagy bűnüldözési céljai vannak. Ezáltal egyfajta általános presszió van, hogy minél kevesebb adatot töröljenek (vagyis minél kevesebb adat esetében tartsák fenn a védelmet). A „szanitizációt" ebben az esetben az információ birtokosa, vagyis annak minősítője végezheti el,[30] mert ő tudja megítélni, melyek azok a szenzitív információk, amelyeket mindenképpen védeni kell (általában a személyes adatok).

Az adatok effajta „szanitizációjának" megvalósítása különbözik a papíralapú vagy az elektronikus dokumentumok vonatkozásában. A papíralapú dokumentumok esetében viszonylag egyszerű, mivel a dokumentumban ki kell takarni azokat az adatokat, amelyek változatlanul védettek maradnak. Ez a takarás jelenthet fekete színnel való besatírozást vagy jelenthet leragasztást is. A cél, hogy a védendő adatokat úgy kell kitörölni, hogy azokat ne lehessen a dokumentum olvasói számára megismerni, valamint a nyomtatott anyagon ne lehessen az eredeti adatokat ismét láthatóvá tenni. Az elektronikus dokumentumok vonatkozásában már sokkal nehezebb, mert a dokumentumból úgy kell kitörölni az adatokat, hogy azokat semmiféleképpen ne lehessen visszaállítani. Az elektronikus dokumentumok esetében, ha befényképezett nyomtatott dokumentumokról van szó, akkor a nyomtatott dokumentumban a törléseket a fényképek esetében se lehessen visszaállítani. Az általában PDF-formátumú fájloknál már sokkal nagyobb erőfeszítésre van szükség az adatok eltörlésére, mivel azok egyszerű (szabványos eljárású) törlés esetén visszaállíthatók, így speciális módszerekre van szükség (például a meghatározott karakterek többszöri felülírására).

[30] Ebben az esetben a szanitizáció a minősített adat felülvizsgálatának tekinthető. A 2009. CLV. törvény a minősített adatvédelemről 8. paragrafusa alapján történik Magyarországon.

Az amerikai Nemzetbiztonsági Ügynökség (NSA[31]) például külön útmutatót adott ki,[32] hogyan lehet a „szanitizációt" gyakorlatilag végrehajtani PDF- és Word-fájlformátumú dokumentumok esetében.

Összefoglalás

Amennyiben a nemzetbiztonsági rendszerben a „szanitizáció" háttérbe kerül, vagy alkalmazása során nem megfelelően járnak el, akkor komoly problémák léphetnek fel a források és az információk védelme területén, ami csökkenti a nemzetbiztonsági rendszer hatékonyságát és feladatainak végrehajtását, közvetve pedig veszélyt jelent az adott ország biztonságára. A források esetleges dekonspirációja nemcsak a nemzetbiztonsági rendszer számára jelent problémát, hanem esetenként a forrás életét is veszélyeztetheti. A dekonspiráció nemcsak egy-egy forrásra, hanem a nemzetbiztonsági rendszer jövőjére is hatással van, mert amennyiben a nemzetbiztonsági rendszer nem tudja megvédeni a forrásait, akkor egyre inkább csökken a rendelkezésre álló információk száma, és új források sem keletkeznek. Tehát a „szanitizáció" a nemzetbiztonsági rendszer egyik lételeme, amely szükséges ahhoz, hogy hatékonyan működjön az ország biztonsága érdekében.

Felhasznált irodalom

BAKOS Ferenc (2002): *Idegen szavak és kifejezések szótára.* Budapest: Akadémiai Kiadó

BALOGH Péter (2013): A szövetségi felderítő rendszer korszerűsítése, avagy néhány gondolat a NATO földfelszíni felderítő rendszerének megteremtéséről. *Felderítő Szemle,* 12(3–4), 126–138.

BALOGH Péter (2018): Rádióelektronikai felderítés (SIGINT). In RESPERGER István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest: Dialóg Campus, 142–154.

BUCKLEY, John (2014): *Managing Intelligence – A Guide for Law Enforcement Professionals.* London: CRC Press – Taylor & Francis Group. Online: https://doi.org/10.1201/b15515

College of Policing: Intelligence report. Online: www.college.police.uk/app/intelligence-management/intelligence-report

Intelligence Community Directive Number 208. – Write for maximum utility. Online: www.dni.gov/files/documents/ICD/icd_208.pdf

KOVÁCS László (2018): *Kiberbiztonság és -stratégia.* Budapest: Dialóg Campus

LAUFER Balázs (2020): A nemzetbiztonság veszélyeztetésének megjelenési formái az egyes jogszabályokban. *Nemzetbiztonsági Szemle,* 8(3), 3–18. Online: https://doi.org/10.32561/nsz.2020.3.1

MIHÁLY Tamás (é. n.): *A legkisebb jogosultság elv betartásának támogatása, elsősorban üzleti alkalmazásoknál.* Előadás. Online: https://eoq.hu/szakb/11/ea180924.pdf

31 National Security Agency – az Amerikai Egyesült Államok egyik nemzetbiztonsági szolgálata.
32 NSA 2005

National Security Agency (2005): *NSA I333-015R–2005 Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF.* Online: https://sgp.fas.org/othergov/dod/nsa-redact.pdf

NMHH (2018): *Mitől személyesek a személyes adatok, és hogyan védi őket a jog?* Online: https://nmhh.hu/cikk/194671/Mitol_szemelyesek_a_szemelyes_adatok_es_hogyan_vedi_oket_a_jog

PUSZTAI Ferenc (2003): *Magyar értelmező kéziszótár.* Budapest: Akadémiai Kiadó

RANGAN, Keerthi (2022): What is Data Sanitization? *G2.com,* 2022. május 4. Online: www.g2.com/articles/data-sanitization

UNODC (2011): *Criminal Intelligence – Manual for Analysts.* New York: United Nations. Online: www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

VIDA Csaba (2016): A hírszerzési ágak elemző-értékelő megközelítése. *Felderítő Szemle,* 15(3), 77–93.

VIDA Csaba (2017): Az elemző-értékelő munka termékei – nemzetbiztonsági tájékoztatók készítése. *Felderítő Szemle,* 16(3–4), 112–128.

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. Online: https://net.jogtar.hu/jogszabaly?docid=99500125.tv

2009. évi CLV. törvény a minősített adatvédelemről. Online: https://net.jogtar.hu/jogszabaly?docid=a0900155.tv

Zákon č. 215/2004. Z.z. o ochrane utajnových skutočnosti. Online: www.zakonypreludi.sk/zz/2004-215