II. RÉSZ

A villamosenergia-rendszer egyes szervezeteinek OSINT-tudatossága és aktuális védelmi képességei

Vákát

Bevezetés

Az elmúlt időszakban számos kibertámadás ért villamosenergia-rendszereket, az egyik legjelentősebb az ukrán villamosenergia-rendszer elleni 2016. decemberi támadás volt. Az elemzések azt valószínűsítik, hogy a támadókat nyílt forrású információk is jelentősen segíthették tevékenységük végrehajtásában. Ennek megfelelően a biztonságos villamosenergia-ellátás összetett feltételrendszerét szükséges egy új elemmel bővíteni, mégpedig a nyílt forrású információk körével.

A nyílt forrású információszerzés (*open source intelligence,* OSINT) alapvetően a nyílt forrású információk gyűjtését jelenti. A nyílt forrású információk kifejezésre számos különböző fogalmat találunk, ezek közül az egyik legpontosabb megfogalmazás az Információs Hivatal honlapján érhető el. E szerint

> „a nyílt forrású információk a bárki számára hozzáférhető, nyilvános és legális eszközökkel megszerezhető információk, amelyeknek forrásai az elektronikus média, az írott sajtó, az internetes oldalak, az ingyenes és kereskedelmi adatbázisok lehetnek. Ezek szisztematikus gyűjtése és feldolgozása révén hírszerzési szempontból releváns információk keletkeznek."[1]

A *NATO Open Source Intelligence Handbook*ban szintén megfogalmaztak egy OSINT-fogalmat. Ez a 2001-ben publikált könyv a nyilvánosság számára szabadon elérhető, célja, hogy a nyílt forrású hírszerzés tárgyában alapvető oktatási segédlet legyen az egyesített és a szövetséges képzések alkalmával. A könyv megfogalmazása szerint

> „az OSINT olyan információ, amelyet tudatosan megszereztek, kiválasztottak, kivonatoltak és felterjesztettek egy kiválasztott felhasználói körnek, általában a parancsnok és közvetlen beosztottja számára, speciális kérdések megvizsgálása céljából. Az OSINT más szóval a hírszerzés bevált eljárási módszereit alkalmazza a sokféle nyílt forrású információ gyűjtése során, ami értesülések megszerzéséhez vezet."[2]

[1] Információs Hivatal.

[2] „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: 2–3. Az idézet a szerzők fordítása.

A nyílt forrású információszerzés definícióját hazánkban először Lévay Gábor határozta meg a hírszerzéstől és a katonai felderítéstől elkülönített formában. E definíció szerint az *OSINT*

> „[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*".[3]

Jelen tanulmányban bemutatjuk azokat az eredményeket, amelyeket az MVM Energetika Zártkörűen Működő Részvénytársaság, valamint a Nemzeti Közszolgálati Egyetem között kötött együttműködési megállapodás alapján végrehajtott kutatások szerint állítottak fel a résztvevők. A kutatás során a szakértők és a hallgatók a villamosenergia-rendszerek kiberbiztonsági képességének fokozása érdekében azt vizsgálták, hogy az OSINT, vagyis a nyílt forrású információszerzés tekintetében milyen tapasztalatok jellemzőek a magyar villamosenergia-rendszerre. A tanulmányban bemutatjuk a jelenleg rendelkezésre álló, hatályos uniós és hazai szabályozói környezetet, valamint az interjúk alapján a hazai villamosenergia-szektor szereplőinek OSINT-tudatossági szintjét, illetve képességeit.

A tanulmány 2021-ben készült, ám csak megerősíthetjük, hogy a nyílt forrású információszerzés mint tevékenység vizsgálata az azóta eltelt mintegy két évben még relevánsabb terület lett. A jelenleg is zajló orosz–ukrán háború okán a villamosenergia-rendszerek védelmével különösen érdemes foglalkozni a lehető legtöbb nézőpontból. Ezért is ajánljuk jó szívvel az Olvasónak gondolatainkat.

Tóth András

[3] Lévay 2006: 6.

1. A nyílt forrású információszerzés eszközei

A nyílt forrású információszerzés során számos különböző eljárást alkalmazhatnak a gyűjtési tevékenységet folytató személyek. A legjellemzőbb eljárási módszereket Deák Veronika *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* című cikkében foglalta össze. Ezek a következők:

- telefonos információgyűjtés;
- hagyományosan publikált anyagok;
- megfigyelés;
- internetes információgyűjtés;
- kukaátvizsgálás;
- rádió- és televíziós adások, médiahírek;
- személyes megkeresés.[4]

A fenti felsorolásból is látható, hogy nem feltétlenül az interneten keresztül történő információgyűjtés az egyetlen módszere a nyílt forrású információk gyűjtésének. Erre hívja fel a figyelmet Solti István is *Az OSINT információgyűjtő eszközeiről* című cikkében, amelyben azt írja, 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."[5]

Szintén ő mutatja be azokat a személyeket, szolgáltatókat és módszereket, amelyek hozzájárulhatnak az információk megszerzéséhez. Az első ilyenek az online kereskedelmi szolgáltatók, akiknél alapvető lehetőségként merül fel, hogy az általuk létrehozott, gyűjtött, feldolgozott és tárolt tartalmakat és adatbázisokat ellenszolgáltatás fejében biztosítják partnereik számára. Ebben az esetben

[4] Deák 2018: 391–402.
[5] Solti 2019: 11.

sem feltétlenül játszik szerepet az internet, nagyon sok esetben előfordul, hogy a szükséges információkat valamilyen adathordozón vagy például nyomtatott formában osztják meg. A következő lehetséges módszer a szürke irodalom előállításának és megszerzésének köre. A szürke irodalom olyan dokumentumokat takar, amelyek nyílt információkat tartalmaznak, azonban csak egy jól meghatározott szűk kör számára készülnek, a széles nyilvánosság számára nem feltétlenül publikálják őket. Idesorolhatók 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 szürke irodalmat legtöbbször előállító szervezetek és intézmények:

- a nemzeti kormányok és kormányzati szervek;
- a politikai pártok;
- a kutatóintézetek;
- az egyetemek;
- az akadémiák;
- a kereskedelmi társaságok.[6]

A szürke irodalom minden esetben nyilvános adatokat tartalmaz, a minősített adatok ebbe a körbe semmiképpen nem vonhatók be, és magának az OSINT-tevékenységnek sem képezik részét.

A különböző OSINT-technikákon keresztül végzett, folyamatos iterációkat elemezni és értelmezni kell, hogy értékes információkat nyerjenek. A szakirodalomban egyre több elemzési technika létezik ennek a feladatnak a végrehajtására.[7] Az alábbiakban kiemeljük a nemzetközi szakirodalomban feldolgozott technikákat és csoportosításokat:

- Lexikai elemzés: A nyers adatokat meg kell vizsgálni, hogy az információt és az összefüggéseket ki lehessen vonni a szövegből. Alapvető fontosságú, hogy ha többnyelvű forrásokat használunk, azokat lefordítsuk az OSINT-vizsgálatban használt nyelvre,[8] és szűrjük.
- Szemantikai elemzés: Az adatok megértésének céljából manapság természetes nyelvfeldolgozó algoritmusokat alkalmaznak.[9] Ezenkívül

[6] Lévay 2006: 8.
[7] Liu–Zhang 2012: 415–463.
[8] Ranade et al. 2018: 238–243.
[9] Noubours–Pritzkau–Schade 2013: 1–7.

a hangulatelemzési technikák lehetővé teszik a szubjektív hozzászólások vagy vélemények kontextusba helyezését a szerző érzelmi állapotának osztályozásával (például pozitív, negatív vagy semleges). Végezetül az igazságfeltáró eljárások azzal a kihívást jelentő feladattal foglalkoznak, hogy feloldják a konfliktusokat a több forrásból származó adatok között, amelyek ugyanabban a témában ellentétes álláspontokat képviselnek.[10]

– Földrajzi elemzés: A közösségi médiából, eseményekből, érzékelőkből vagy IP-címekről gyűjtött adatokat érdemes helyalapú szempontból elemezni. Ebben az értelemben a térképek vagy grafikonok használata megkönnyíti az adatok ábrázolását és megértését, valamint értelmes összefüggések feltárását az események vagy személyek között.[11]
– Közösségimédia-elemzés: A modern közösségi média által nyújtott szolgáltatások lehetővé teszik a kutatók számára, hogy mélyreható elemzést végezzenek a felhasználókról. Ilyen helyzetben a közösségimédia-adatok elemzése lehetővé teszi a téma körüli kapcsolatok, interakciók, helyek, viselkedések és ízlések hálózatának létrehozását.[12]

A fent említett technikák bevezetésének eredményeit kimeneti információnak tekintjük, és három fő csoportba soroljuk:

– A személyes adatok összegzik azon személyazonossági adatokat, amelyek főként a valódi névből, e-mail-címből, felhasználónévből, közösségi médiából és keresőmotorokból származnak.
– A szervezeti információkat azon személyek adatai alkotják, akik egy csapatban vagy vállalatnál vannak. Lényegében a közösségi média, keresőmotorok, helyadatok, domainnév és IP-cím-adatok segítségével határozzák ezeket meg.
– A hálózati információk a rendszerek és a kommunikációs topológiák technikai adatait tartalmazzák, amelyeket általában hely-, tartománynév- és IP-cím-információval valósítanak meg.

[10] Li et al. 2015: 1–16.
[11] Vopham et al. 2018.
[12] Stieglitz et al. 2018: 156–168.

2. Az OSINT előnyei és kihívásai

Az OSINT alkalmazási területei sokfélék, és az e paradigma alapján fejlesztett megoldások köre egyre bővül. A módszertan mögött azonban sokszor olyan kompromisszumos lehetőségek állnak, amelyekkel a fejlesztőknek és a mérnököknek meg kell birkózniuk. Amint az első táblázatban láthatjuk, az OSINT számos előnnyel jár, de néhány kihívással is foglalkozni kell, amennyiben ezt a technológiát szeretnénk használni. Ezeket az előnyöket, illetve kihívásokat a következőkben részletezzük.

1. táblázat: Az OSINT előnyei és kihívásai

Előnyök	Kihívások
Hatalmas mennyiségű rendelkezésre álló információ	Az adatkezelés összetettsége
Nagy számítási kapacitás	Strukturálatlan információk
Big data és gépi tanulás	Téves információk
Kiegészítő adatok	Az adatforrások megbízhatóságának kérdésköre
	Erős etikai/jogi kérdések

Forrás: a szerzők szerkesztése Bányász 2015: 22–24. alapján

2.1. Az OSINT előnyei

A nyílt forrású információszerzés alkalmazásának számos előnye létezik, amelyek közül jelen tanulmányban csak az alábbiakat elemezzük:

- hatalmas mennyiségű rendelkezésre álló információ;
- nagy számítási kapacitás;
- *big data* és gépi tanulás;
- kiegészítő adatok.

2.1.1. Hatalmas mennyiségű rendelkezésre álló információ

Jelenleg nagy mennyiségű értékes nyílt forrású adat áll rendelkezésre, amely elemezhető és összekapcsolható.[13] Idetartoznak többek között a közösségimédia-platformok, a kormányzati dokumentumok és jelentések, az online multimédiás tartalmak, az újságok, sőt a deep és dark web tartalmai is.[14] Valójában mind a *deep web,* mind a *dark web* (utóbbi az előbbin belül található) még több információt tartalmaz, mint a *surface web* (azaz a legtöbb felhasználó által ismert internet).[15] Ahhoz, hogy hozzáférhessünk ezekhez a hálózatokhoz, speciális eszközöket kell használni, mivel tartalmukat a hagyományos keresőmotorok nem indexelik.

2.1.2. Nagy számítási kapacitás

A számítógépes architektúra, a processzorok és a GPU-k (*graphics processing unit:* grafikus feldolgozóegység) fejlődése lehetővé teszi az erőforrás biztosítását a gyűjtésre, feldolgozásra, elemzésre és tárolásra egyaránt. Ezeknek az eszközöknek a segítségével lehetőségünk van az OSINT alkalmazására, tekintettel arra, hogy nagy mennyiségű nyilvános információt kell feldolgozni, és ezen információk kapcsolatát és mintáit is kezelni kell.

2.1.3. Big data és gépi tanulás

Az adatelemzési és adatbányászati technikák, valamint a gépi tanulási algoritmusok növekvő elterjedése is elősegíti az OSINT használatát. A gépi tanulás automatizálhatja és intelligensebbé, továbbá hatékonyabbá teheti a vizsgálati és döntéshozatali folyamatokat.[16] Lehetővé teszi olyan összetett összefüggések észlelését, amelyek az emberek számára kiszámíthatatlanok. Ez a pont kiemelt jelentőségű lesz az OSINT jövőbeni használatában, mivel meg fognak jelenni az emberi és a mesterséges intelligencia által vezetett kutatások közötti különb-

[13] Wong 2016: 167–185.
[14] Kalpakis et al. 2016: 111–132.
[15] Bergman 2001.
[16] Gandomi–Haider 2015: 137–144.

ségek. E technikák beépítésével a gyűjtés és elemzés folyamata végérvényesen javulni fog, ezáltal pontos, célunkhoz közeli vizsgálatokat eredményezve.[17]

2.1.4. Kiegészítő adatok

Lehetőség van az OSINT-vizsgálatok kiegészítésére más forrásból származó adatokkal, ezáltal tovább pontosítva e műveletek eredményeit. A legtöbb OSINT-rendszer belső felépítése kellően nyitott ahhoz, hogy olyan adatokat is feldolgozzon, amelyeket valójában nem nyílt forrásból szereztek be. Ez a tény azt jelenti, hogy az OSINT még hatékonyabb lehet, ha képesek vagyunk külső információkat hozzáadni a vizsgálatok kiegészítéséhez.[18]

2.2. Az OSINT kihívásai

Az OSINT-nak az előnyök mellett természetesen számos kihívása is van, amelyek közül jelen tanulmányban az alábbiakat elemezzük:

- az adatkezelés összetettsége;
- strukturálatlan információk;
- téves információk;
- az adatforrások megbízhatóságának kérdésköre;
- erős etikai/jogi kérdések.

2.2.1. Az adatkezelés összetettsége

Az adatok mennyisége óriási, következésképpen nehéz őket hatékonyan és eredményesen kezelni. Előnyös, ha az OSINT-folyamatok a lehető legtöbb információt feldolgozzák. Ehhez azonban fejlett technika és jelentős erőforrások kellenek, hogy a magas színvonalú gyűjtés, feldolgozás és elemzés biztosítva legyen.[19]

[17] Barnea 2019: 433–447.
[18] Day–Gibson–Ramwell 2016: 133–152.
[19] Fleisher 2008: 852–866.

2.2.2. Strukturálatlan információk

Az interneten elérhető nyilvános információk eredendően tömegesen strukturálatlanok. Ez azt jelenti, hogy az OSINT által gyűjtött adatok annyira heterogének, hogy ez megnehezíti a releváns kapcsolatok és ismeretek kinyerése érdekében történő osztályozásukat, összekapcsolásukat és vizsgálatukat. Ebben az értelemben az OSINT a strukturálatlan információk homogenizálásához, annak érdekében, hogy fel tudják használni azokat, olyan mechanizmusokat igényel, mint az adatbányászat, a természetesnyelv-feldolgozás (*natural language processing,* NLP) vagy a szövegelemzés.

2.2.3. Téves információk

A közösségimédia-platformokat és a kommunikációs médiumokat elárasztják a szubjektív vélemények, az álhírek.[20] Ezért az OSINT-mechanizmusok használatakor figyelembe kell venni a pontatlan információk meglétét. Az OSINT-tevékenységnek mindig megbízható információkon kell alapulnia, és megbízható kutatási irányokat kell követnie a pozitív és meggyőző eredmények biztosítása érdekében.[21]

2.2.4. Az adatforrások megbízhatóságának kérdésköre

Az információk megbízhatósága és valódisága valóban a sikeres OSINT-vizsgálatok kulcsa.[22] Ideális esetben az összegyűjtött adatoknak hiteles, ellenőrzött és autentikus forrásokból (hivatalos dokumentumok, tudományos jelentések, megbízható kommunikációs médiumok) kell származniuk. A gyakorlatban az OSINT-folyamatok szubjektív vagy nem hiteles forrásokat is fel fognak használni, például a közösségimédia-platformok tartalmát. Annak ellenére, hogy az ilyen típusú források hajlamosabbak a félretájékoztatásra, valójában sok tudást lehet kinyerni belőlük az emberek, csoportok vagy vállalatok vizsgálatához.[23]

[20] Bello-Orgaz–Jung–Camacho 2016: 45–59.
[21] Mármol–Pérez–Pérez 2014: 32–40.
[22] Gong–Cho–Lee 2018: 5428–5435.
[23] Zago et al. 2019: 98–104.

2.2.5. Erős etikai/jogi kérdések

Az OSINT fejlesztésével számos aggály merül fel a magánélet tisztelete és a személyes integritás tekintetében. Egyrészt, bár nyilvánosan hozzáférhető a felhasznált adatok köre, az OSINT képes olyan információkat felfedni, amelyek nincsenek kifejezetten közzétéve az interneten. A feltárt eredményeknek tiszteletben kell tartaniuk a felhasználók magánéletét, és nem szabad felfedniük intim és személyes adatokat, figyelembe véve a vonatkozó szabályozásokat (például GDPR). Ebből a szempontból az internetről kikövetkeztethetők olyan adatok, mint a szexuális irányultság, a vallási meggyőződés, a politikai hovatartozás. Másrészt az OSINT-alapú keresések hatókörét értelemszerűen a nyílt adatforrásokra kell korlátozni. A tudás kinyerése érdekében semmilyen körülmények között nem lehet megkerülni a hozzáférés-vezérlést vagy a hitelesítési módszereket.[24]

3. Jogszabályi háttér

Ebben a fejezetben a nyílt információszerzés jogszabályi hátterét ismertetjük. A felhasznált módszerektől függetlenül, általánosságban elmondható, hogy minden tevékenység, amely adatszerzéssel, adatfeldolgozással vagy adatelemzéssel kapcsolatos, meg kell feleljen a jogszabályi alapoknak. A nyílt jellegű információszerzés esetén nem szabad abba a tévedésbe esni, hogy csupán azért, mert az adat nyíltan elérhető, a gyűjtése, felhasználása jogszerű. E fejezetnek ez a kulcskérdése, a jogszabályi elemzéseinkkel erre a kérdésre kívánunk választ adni. Számos információ nyíltan, ráadásul a közösségi médiával átszőtt világunkban relatíve könnyen és olcsón hozzáférhető. Ugyanez igaz a telefonos applikációkon belül történő adatgyűjtésre. Viszont amennyiben ez az adat személyes adatnak minősül, hiába nyílt, egyértelmű hozzájárulás nélkül nem felhasználható. Ez nem csupán a jogkövetkezmények, hanem a szervezet jó hírneve miatt is kifejezetten fontos. A közelmúltban a legjelentősebb botrány a Cambridge Analyticához kapcsolódott, pedig a felhasználók adatait a közösségi médián

[24] Kandias et al. 2013: 98–110.

keresztül és hozzájárulással gyűjtötték és dolgozták fel. A szervezetet ebben az esetben azért érte komoly médiakritika, mert ugyan a felhasználók engedélyt adtak az adataik kezelésére, de nem volt egyértelmű, hogy mit gyűjtenek, és azt mire használják fel.

A jogszabályi háttér bemutatása során az Európai Unióban és Magyarországon releváns jogszabályokat elemezzük. Az Európai Unióban legjelentősebb az Európai Parlament és a Tanács (EU) 2016/679-es rendelete (GDPR), Magyarországon pedig az Alaptörvény és a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).

Elemzésünk kulcskérdése a személyes adat kérdésköre lesz, mivel mindkét jogforrás abban az esetben válik hatályossá, ha személyes adat kezelése történik. A GDPR esetében először egy keretszerű tájékoztatást adunk, majd pedig a személyes adatok jogszabályi definícióját tisztázzuk. A magyar jogforrásoknál a GDPR vonatkozásában releváns azonosságokat és jogszabályi szűkítéseket mutatjuk be, szintén a személyes adat kérdésével kapcsolatban. A jogszabályi háttér ismertetésének így az a célja, hogy segítsen a szervezetnek mérlegelni, érdemes-e személyes adatokat kezelnie (tisztázva azt, hogy ténylegesen mi is a személyes adat) és a következő lépcsőben megvalósítania a jogszabályoknak való megfelelést, vagy sem.

3.1. Az Európai Parlament és a Tanács (EU) 2016/679-es rendelete (GDPR)

Az Európai Parlament és a Tanács (EU) 2016/679-es rendelete (más néven: GDPR, adatvédelmi rendelet) számos változást hozott az adatkezelők számára. Ez a nyílt információ szerzése (és ezen adatok feldolgozása, elemzése) szempontjából is kifejezetten időszerű. A GDPR-t az OSINT vonatkozásában nem úgy kell kezelni, hogy ez egy jogszabály, amely ellehetetleníti a nyílt információból történő adatszerzést, hanem szigorú szabályozásként, amely az egyének védelme érdekében szűkíti vagy bizonyos esetekben engedélyhez köti az adatokkal kapcsolatos tevékenységet. Az OSINT alkalmazásában a GDPR hozott érezhető változásokat,[25] viszont a tényleges hatása szervezettől és OSINT-jellegtől függő. Az adatvédelmi rendeletnek alapvetően nem az a célja, hogy lehetetlenné tegye a személyes adatok feldolgozását, hanem sokkal inkább az egyensúly

[25] Shere 2020: 429–448.

megteremtése az adatcsere szükségessége, valamint a polgárok magánélethez való alapvető joga között. A GDPR egyensúlyt teremt e jog és más jogok között azáltal, hogy a személyes adatok feldolgozását olyan esetekre korlátozza, amikor erre jogalap van (6. cikk). Hat különböző jogalapot sorol fel, amelyek közül három potenciálisan releváns az OSINT-tevékenység szempontjából, ezek: a hozzájárulás [6. cikk (1) bekezdés *a)* pont], a jogi kötelezettség [6. cikk (1) bekezdés *c)* pont] és a jogos érdek [6. cikk (1) bekezdés *f)* pont].

A rendelet tisztázza a jogszabály célját:

> „A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez."[26]

A fentiek alapján a cél a személyes adatok védelme, amely vonatkozásában OSINT-szempontból két részre szükséges bontani az adatgyűjtést. Az egyik rész a személyes adat, a másik rész a személyekhez nem köthető adatok köre. A GDPR csak a személyes adatok gyűjtésére vonatkozik, így az adatkezelőnek csupán ezek esetében kell a jogszabályban foglaltakat betartania. A személyes adatok nyílt információból való gyűjtése nem kizáró ok, viszont e tevékenység végzéséhez megfelelő tájékoztatás és hozzájárulás szükséges. Ez az OSINT szempontjából egy erős limitációt jelent: egy szervezet – még ha jó szándékkal is (például saját biztonságának növelése érdekében) – az érintettek hozzájárulása nélkül nem gyűjthet személyes adatot nyílt forrásokból. Ez fundamentálisan viszont alá tudja ásni egy szervezet OSINT-céljait, hiszen amennyiben az érintett dolgozók tudnak arról, hogy mit és miért fognak gyűjteni róluk, maga az adatgyűjtés okafogyottá és értelmetlenné válhat. Az idézett első bekezdés kiemelten fontos, mivel egyértelműsíti, hogy a jogszabály elsődleges célja leszögezni, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Nem az adatgyűjtők, hanem az egyének szemszögéből közelíti meg a kérdést, és így elsődlegesen az érintettek érdekeit védi és képviseli. A jogszabály alapelveit tiszteletben kell tartani a természetes személyek lakóhelyétől és állampolgárságától függetlenül – mondja

[26] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (1) bekezdés.

ki az Európai Unió –, mivel ez az alapja a közösség gazdasági és társadalmi fejlődésének. Ellensúlyként megfogalmazza a rendelet, hogy:

> „[a] személyes adatok kezelését az emberiség szolgálatába kell állítani. A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal."[27]

Az OSINT-tevékenységek során a megismert kutatásban a fő cél a szervezet biztonságának növelése, amely így része az energiabiztonság növelésének. Ezáltal a felmerülő jogviták elkerülhetőek, és az is egy relatív kérdés, hogy milyen az arányosság mértéke a személyes adat korlátozása és felhasználása esetén, továbbá ez hogyan viszonyul a társadalmi érdekhez. Kiegészítésként meg kell állapítanunk, hogy bizonyos szabadságelveket még így sem lehet megsérteni. Ezek a következők:

- a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához,
- a személyes adatok védelméhez,
- a gondolat-, a lelkiismeret- és a vallásszabadsághoz,
- a véleménynyilvánítás és a tájékozódás szabadságához,
- a vállalkozás szabadságához,
- a hatékony jogorvoslathoz és a tisztességes eljáráshoz,
- a kulturális, vallási és nyelvi sokféleséghez való jog.

Értelmezésünkben ez azt jelenti, hogy ha még a biztonság érdekében történik is nyílt információszerzés, és ez arányos a társadalmi érdekekkel, a személyes adatok védelméhez való jog akkor sem sérthető meg. Tehát ha a felhasználó védeni kívánja a személyes adatait, ezt a jogot nem lehet korlátozni, és a nyílt információszerzés szempontjából ez egy erős limitáció. Előzetesen megismertük azt, hogy amennyiben nyílt forrásból szerzünk információt, és ebben személyes adatok érintettek, akkor a felhasználónak erről előzetesen tudnia kell, és bele kell egyeznie. Ezzel a ponttal együtt értelmezve a szervezet nem kényszerítheti olyan helyzetbe az érintettet, hogy az a személyes adatok védelmének jogáról lemondjon. Azaz ha nem járul hozzá, hogy az adatai OSINT tárgyává váljanak, akkor az ő esetében még társadalmi érdekre hivatkozva sem korlátozható ez.

[27] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (4) bekezdés.

Továbbá a (6) bekezdés lehetővé teszi a személyes adatok cseréjét (a nemzetek között), és a hatóságok tevékenységét is elismeri.

> „A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét."[28]

OSINT-tevékenységek szempontjából ez az egyik legfontosabb és legkiemelkedőbb rendelkezés. A kérdéskört a rendelet nem a szolgáltatók vagy az állam, hanem az érintettek, egyének szemszögéből közelíti meg, és az is érezhető, hogy az ő érdekükben fogalmazták meg, az ő döntéseiket is figyelembe véve. A biztonság növelése céljából folyamatosan az aktuális technológiai kihívásokra kell választ adnunk: a felhasználók új platformokon élnek virtuális életet, illetve folyamatosan új eszközöket használnak. A rendeletet úgy érdemes értelmeznünk, hogy az figyelembe veszi, hogy egyre több személyes adat válik elérhetővé. Ez a nyílt információból történő adatszerzés kulcsa, ami kapcsán ugyanakkor a rendelkezés védelmet kíván nyújtani. Az információszerzés szempontjából ez nem kibővíti a lehetőségeket, hanem leszűkíti. Ha a két kiemelt rendelkezést együtt értelmezzük (a személyes adatoknak az emberiség szolgálatába állítása és a személyes adatok megosztása), akkor érezhető, hogy a védelem sokkal erősebben jelenik meg, mint a társadalmi érdek. Ebből eredően egy szervezetnek nem elegendő csakis önmagában a (4) bekezdésben foglalt társadalmi érdekre hivatkoznia. A GDPR a címében[29] tartalmaz olyan ellensúlyt, amely megerősíti azt, hogy ez egy adatvédelmi rendelet. Más érdekek alárendelődnek az adatvédelemnek. Bármiféle nyílt információgyűjtést, adatfeldolgozást (személyes adatokra vonatkozóan) csak arra alapozni, hogy az a későbbiekben társadalmi érdeket fog szolgálni, nem szabad, mivel a jogszabály ezt az opciót ellensúlyozza

[28] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (6) bekezdés.

[29] Cím alatt nem a jogszabály tényleges címét, hanem a bevezető rendelkezéseket értjük a szövegben.

erősen. Országok közötti diverzifikációra[30] pedig nincs sok lehetőség, az adatvédelmet az unió egész területén biztosítani és érvényesíteni szükséges.

Kutatásunkban egy másik kérdéskör az automatizáció szerepe. A GDPR az automatizált és a manuális adatgyűjtést is taglalja:

> „A komoly szabály-kerülési kockázat veszélyének elkerülése érdekében a természetes személyek védelmének technológiailag semlegesnek kell lennie és nem függhet a felhasznált technikai megoldásoktól. A természetes személyek védelme a személyes adatok automatizált eszközök útján végzett kezelése mellett a manuális kezelésre is vonatkozik, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni. Olyan iratok, illetve iratok csoportjai, és azok borítóoldalai, amelyek nem rendszerezettek meghatározott szempontok szerint, nem tartoznak e rendelet hatálya alá."[31]

Gyakorlati szempontból ez azt jelenti, hogy nem releváns maga az adatgyűjtés módja, ha az automatizáltan vagy manuálisan történik. Nem szabad abba a tévedésbe esnünk, hogy csupán azért, mert automatizált és nagy mennyiségű az adatgyűjtés, nem esik a GDPR hatálya alá. Ez nem képez kivételt a törvény alól, mondván, hogy a nyílt adatok az automatizáltságból és a nagy mennyiségből eredően személytelenné válnak. A GDPR ezt a kiskaput itt bezárja: a rendeletet nem lehet és nem is érdemes úgy megkerülni, hogy a szervezet a technológiai megoldáson keresztül hoz létre jogalapot az OSINT-tevékenységének, mivel a jogszabály technológiasemlegességet mond ki. Az automatizáltságról továbbá meg kell jegyezni, hogy amennyiben az érintett igényli, gépi formátumban kell rendelkezésére bocsátani az adatot, és joga van azt más adatkezelőnek is továbbítani.[32] Az adatkezelés helye sem releváns ilyen szempontból, amit a (22) bekezdés taglal: azzal sem kerülhetőek meg a rendelkezések, hogy az adatkezelés és -tárolás az EU-n kívül történik. Amennyiben az alanyok az EU állampolgárai, akkor az adatkezelőnek a rendeletben foglaltakat be kell tartania.

Technológiai szempontból felmerülő kérdés a személyes adat személytelenítése vagy álnevesítése. Álnevesítésre viszont lehetőséget nyújt a rendelet, amely ezt szintén az egyén szemszögéből közelíti meg, és nem az adatgyűjtő érdekeit veszi figyelembe. Ennek a célja az, hogy az egyéneknek pluszvédelmet nyújthasson a szolgáltató, nem pedig az, hogy a meglévő személyes adatokat álnevesítsék, majd felhasználják. Továbbá a (30) bekezdés a technológiai

[30] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (10) bekezdés.
[31] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (15) bekezdés.
[32] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (68) bekezdés.

aspektust és a személyeket összekapcsolja: a rendelet elismeri, hogy technológiai szempontból egy egyén beazonosítható az eszköze adatain keresztül is (például IP-cím, cookie-azonosító). OSINT-tevékenység során erre kifejezetten figyelnie kell a szervezetnek, hogy ha egyedi eszközadatokat gyűjt be, amelyek alapján a felhasználó beazonosítható, akkor szintén hozzájárulás szükséges. Egyedi azonosítók akár nyílt információból (például nyílt wifihálózaton látható eszközök) való begyűjtése és elemzése, ahogy az ezekkel kapcsolatos adatoké is, így hozzájáruláshoz kötött. Az adatkezelőnek ezért létre kell hoznia olyan technológiai megvalósítást, amely lehetővé teszi azt, hogy az érintettek jogainak és szabadságainak érvényesülését bizonyítani tudja.[33] Ennek érdekében nyilvántartást is kell vezetnie, illetve az adatvédelmi incidens bekövetkezése esetén megfelelő tájékoztatást kell adnia.

A nemzetbiztonsággal kapcsolatos teendők a GDPR hatályán kívül esnek,[34] így a szervezet akkor gyűjthet személyes adatokat nyílt forrásokból, ha tevékenysége ugyanebbe a halmazba tartozik. De ez esetben, amennyiben nemzetbiztonsági alapja van az adatgyűjtésnek, az egész jogszabályi kérdéskör megváltozik. Ezt a speciális esetet itt, a jogszabályi háttér elemzésénél nem kívánjuk feltárni, mivel nem kapcsolódik szorosan a nyílt információszerzéshez. Hasonlóan mentesülést határoz meg a rendelet hatósági, bűnmegelőzési és bűnfelderítési tevékenység végrehajtása esetén is.

Az adatkezeléssel kapcsolatosan szigorú szabályokat fogalmaz meg a törvény:

> „Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez. Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak. A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni. Ha az érintett hozzájárulását elektronikus felkérést követően adja meg,

[33] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (77)–(78) bekezdés.
[34] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (16) bekezdés.

a felkérésnek egyértelműnek és tömörnek kell lennie, és az nem gátolhatja szükségtelenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kérik."[35]

A rendelet egyértelműen kimondja: ahhoz, hogy személyes adatot gyűjtsenek vagy dolgozzanak fel, az érintett konkrét tájékoztatás birtokában adott hozzájárulása szükséges. Ennek a módja lehet digitális is, viszont az egyértelműségnek ott is meg kell jelennie. Egy applikáció esetében például lehetőség van arra, hogy a felhasználó hozzájáruljon az adatkezeléshez, de önmagában egy hozzájárulás gomb nem elegendő, megfelelő tájékoztató tartalmat kell megjeleníteni. Ez az applikációkból történő nyílt információszerzést elő tudja segíteni, és így a felmerülő jogviták elkerülhetők. Továbbá, mivel a jogszabály a gyermekek személyes adatait kifejezett védelem alá helyezi, amennyiben feltételezhető, hogy gyermekek is alanyaivá válhatnak az adatgyűjtésnek, ennek elkerülése érdekében érdemes életkor szerinti ellenőrzést elhelyezni az applikációban. Az adatkezelőnek emellett tudnia kell bizonyítani azt a későbbiekben, hogy az érintett hozzájárult az adatkezeléshez. Digitálisan így nem elegendő csupán egy „ellenőrző pont" felállítása, hanem ténylegesen rögzíteni kell a felhasználó engedélyét. Az önkéntes hozzájárulást illetően jogakadályként jelenik meg a közhatalmi aszimmetria esete. A (43) bekezdés egyértelműen kimondja, hogy még ha az érintett engedélyt is adott, azonban az adatkezelő és az érintett között egyenlőtlen viszony áll fenn, akkor a hozzájárulás nem tekinthető önkéntesnek. Erre kifejezetten oda kell figyelni azért, hogy ne legyen esély arra, hogy a felhasználó az egyenlőtlen viszonyból eredő helyzete miatt adja beleegyezését. A hozzájárulás ebből következően nem köthető más tevékenységek elvégzéséhez, kivéve, ha szorosan kapcsolódik ahhoz. Általánosságban így elmondható, hogy a szervezet biztonságának növelése mint cél nem tartozik szorosan ide. Jogalap szempontjából tehát az adatkezelést külön hozzájárulással szükséges intézni, mert a munkakörhöz, pozícióhoz kapcsolása jogszerűen nehezebb, és így nem merülhet fel a hatalmi aszimmetria kérdése.

Összességében kijelenthető, hogy a hozzájárulás kulcsszerepet játszik az adatgyűjtés esetében. A hozzájárulásnak:

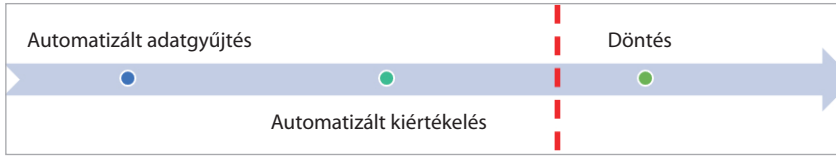
- az egyén szempontjából
  - önkéntesnek,
  - egyértelműnek,
  - hatalmi pozíciótól függetlennek, míg

[35] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (32) bekezdés.

– a szervezet szempontjából
  - arányosnak,
  - etikusnak,
  - szükségesnek,
  - tisztességesnek,
  - átláthatónak kell lennie.

A hozzájárulástól függetlenül az egyénnek joga van az elfeledéshez, azaz az egyén kérése esetén a kifejezetten az online környezetben szerzett adatokat is törölni kell.[36] Az applikációkban erre a felmerülő jogviták elkerülése és a felhasználók GDPR-ban rögzített jogai biztosítása érdekében érdemes lehetőséget biztosítani.

Az OSINT-on alapuló adatgyűjtés a biztonság növelése céljából felveti a teljes automatizálás kérdését. Teoretikusan nézve nyílt információból való adatszerzéskor előfordulhat olyan eset, hogy az érintett nyíltan olyan adatokat ad meg magáról, amelyek a szervezeten biztonsági rést ütnek. Ezt akár egy automatizált OSINT-alapú rendszer ki tudná szűrni, és ez alapján releváns döntéseket lehetne hozni. Viszont erre ilyen tisztán a GDPR-ban foglaltak fényében nincs lehetőség: a megfogalmazás szerint ha személyes jellemző érintett, akkor nem lehet ez a folyamat döntéssel együtt automatizált.[37] Első olvasatra úgy tűnhet, hogy ellenkező esetben azonban engedélyezett ez a megoldás. Viszont (később ismertetjük, hogy) a személyes adat személyes jellemzőkből áll össze. Gyakorlati szempontból így elmondható, hogy ha a GDPR alapján történik a személyes adatok kezelése, akkor (főszabály szerint) teljes automatizmus nem valósulhat meg.



1. ábra: GDPR és a személyes adatok kezelése

Forrás: a szerzők szerkesztése Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (1)–(68) bekezdése alapján

[36] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (66) bekezdés.
[37] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (71) bekezdés.

Az előbbiekben bemutatott rendelkezések a cím részét képezik és a jogalkotó szándékát fejezik ki. Összességében keretet adnak a GDPR-ban foglalt határozatoknak, viszont a jogszabályi elemzés szempontjából nem eshetünk abba a hibába, hogy ezeket a bevezető pontokat átugorjuk, mert ezek prezentálják igazán a jogalkotó szándékát. A tényleges elbírálásban és értelmezésben ez jelentős szerepet játszik.

Röviden megfogalmazva érdemes az OSINT vonatkozásában egymással szembehelyezni a korlátozó és erősítő tényezőket.

2. táblázat: Az OSINT-tevékenységeket erősítő és korlátozó tényezők

Erősítő tényezők	Korlátozó tényezők
Társadalmi érdekből végzett tevékenység	Személyes adatok védelméhez fűződő jog
Nemzetbiztonsággal kapcsolatos tevékenységek	Személyes adatok védelméhez fűződő jog védelme
Digitális hozzájárulás lehetősége	Automatizált adatgyűjtés esetén azonos védelem
	Technológiai semlegesség elve
	Személyek készülékazonosítókhoz kapcsolásának alapelve
	Közhatalmi aszimmetria esete
	Teljes automatizáció (a döntést is beleértve) tilalma
	Részletes nyilvántartás vezetése az adatkezelés módjáról

Forrás: a szerzők szerkesztése Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I–III. fejezetének egésze alapján

A rendelet a bevezetőt követően összesen 11 fejezetre tagozódik, ebből OSINT-szempontból az első három a releváns: az Általános rendelkezések, az Elvek és az Érintettek jogai. Az általános rendelkezésekben a törvény tárgyát, tárgyi hatályát, területi hatályát és a releváns fogalmak meghatározását taglalják. A rendelet tárgya röviden megerősíti a címben foglalt célokat:

> „(1) Ez a rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.
> (2) Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

> (3) A személyes adatok Unión belüli szabad áramlása nem korlátozható vagy tiltható meg a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból."[38]

A tárgy jelentése számunkra az, amit a címben lefektetett alapvetéseknél is értelmeztünk. A rendelet célja az érintettek személyes adatainak védelme, és ezt az érintettek szemszögéből kívánja érvényesíteni. Így az OSINT-tevékenység szempontjából elmondható, hogy ha a GDPR alapján személyes adatokat fog kezelni, akkor azt úgy érdemes felépíteni, hogy figyelembe vegye a felhasználó nézőpontját. A jogszabállyal való hasonulás érdekében előnyös, ha a szervezet az ilyen nyílt információgyűjtésen alapuló tevékenységét úgy fogalmazza meg és hajtja végre, hogy az nem csupán az ő, hanem az egyének adatainak védelmében is történik.

A második cikk a rendelet tárgyi hatályát rögzíti. Röviden négy pontban taglalja azokat a fő eseményeket (kritériumokat), amelyek során az adatkezelőnek a rendeletben foglaltakat kötelező érvényűen be kell tartania.

> „(1) E rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni."[39]

A kulcsfogalom a tárgyi hatály értelmezésénél a személyes adat, erre épül a tárgyi hatály. Ha nem személyes adat kezelése történik, akkor a rendelet nem kötelező érvényű. Ezt a gondolatot a címben foglalt alapvetésekből már megismertük. A nyílt információszerzés szempontjából azt kell értelmeznünk, hogy személyes adatot kezelünk, vagy sem. A címben rögzített alapvetések itt is visszaköszönnek, tehát maga a technikai mód, hogy automatizált (és, mondjuk, ebből eredően nagy mennyiségű), nem jelent kibúvót a jogszabály tárgyi hatálya alól.

A rendelet területi hatálya komplexebb, és értelmezéséhez szükséges a teljes szövegét látnunk:

[38] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 1. cikk (1)–(3) bekezdés.

[39] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 2. cikk (1) bekezdés.

„(1) E rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.
(2) E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:
a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó.
(3) E rendeletet kell alkalmazni a személyes adatoknak a nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó."[40]

A területi hatálynál is megerősíti a rendelet azt, hogy nem az adatkezelők szemszögéből közelíti meg az adatvédelmi kérdést, hanem az érintettek felől. Mindhárom pontban előjön az, hogy ha az alany egy bizonyos kritérium alá tartozik, és személyes adatot gyűjtenek, akkor a területi hatály érvényes. Ez a technikai kiskapu kihasználásának lehetőségét kizárja, azaz lényegtelen, hogy az adatkezelőnek jelen esetben nincs európai székhelye, hogy az adatokat nem egy EU-s ország területén kezeli és tárolja, amennyiben a tevékenységi hely uniós. Ez az érintettek jogvédelme szempontjából előnyös, viszont ha az OSINT-tevékenység felől nézzük az egészet, akkor elmondhatjuk, hogy a területi hatály érvényesül. A kulcskérdés itt is az, hogy személyes adatnak minősül-e az adat, de arra, hogy mi számít annak, később tér ki a rendelet.

Az első bekezdés azt mondja ki, hogy ha az adatkezelőnek vagy -feldolgozónak az Európai Unió területén tevékenységi helye van, akkor függetlenül attól, hogy az érintettek uniós állampolgárok, vagy sem, személyes adat kezelése esetén érvényes a rendelet. Ami itt hiányosság, az az, hogy a tevékenységi helyet mint fogalmat nem tisztázzák. A tevékenységi központot viszont igen, amely a rendelet szerint a központi ügyvitele a tevékenységi helyeknek. Így utóbbit ebből a fogalomból tudjuk csak levezetni: bármilyen tevékenység, amely az EU érintettségi területén történik, az itteni tevékenységi helynek minősül. A második bekezdés szerint szintén ha személyes adatot kezelnek, akkor az érintett uniós területen belül való tartózkodása területileg hatályossá teszi a rendeletet. A b) pont pedig megerősíti azt, hogy nem csupán szolgáltatás nyújtása esetén érvényesül a jogszabály, az is elegendő, hogy a tevékenység megfigyelési célt szolgáljon, ebben

[40] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 3. cikk.

az esetben azonban az érintett megfigyelendő viselkedésének az unió területén belül kell jelentkeznie. Arra a kérdésre, hogy a tevékenységi hely telefonos applikációból gyűjtött nyílt információk esetén elkülöníthető-e, akkor „nem" a válasz, ha az érintett, akinek a viselkedését megfigyelik, már nem az EU területén tartózkodik, és ezt egy szoftver geolokációs adatok alapján felismeri, mert akkor sem gyűjthető személyes adat az érintettről GDPR-kompatibilitás hiányában, ha az első pont szerinti tevékenységi területe változatlan.

Az egész rendelet kulcskérdését, azaz a személyes adat fogalmát a fogalommeghatározásoknál ismertetik:

> „1. »személyes adat«: azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;"[41]

illetve a címben foglalt alapvetés szerint

> „[a] természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, valamint egyéb azonosítókkal, például rádiófrekvenciás azonosító címkékkel".[42]

Az eddigi jogszabály-értelmezésben visszatérő elemként nevezik meg a személyes adat kifejezést, és az OSINT-tevékenységek szemszögéből általánosan úgy értékelik, hogy valószínűleg személyes adat lesz a gyűjtött információ. Ez a címben megismert tág értelmezésből következik. A legegyszerűbb megfogalmazás ez esetben az, hogy minden olyan egyedi azonosító vagy akár jellemző információ, amelyből egy személy kiléte levezethető, személyes adatnak minősül. Ami a konkrét behatárolást jelentősen megnehezíti, az az, hogy a jogszabály példálózó jellegű. A „különösen" szó azt jelenti, hogy ezekben az esetekben kifejezetten érvényesül, de nem kizárólag ezekben az esetekben. Emiatt nagyon nehéz arra a kérdésre választ adni, hogy mi minősül személyes adatnak, mert az kimondottan függhet a szervezetnél dolgozók sajátosságaitól is. Így olyan jellemzők

[41] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 4. cikk.
[42] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (30) bekezdés.

(gyűjtött adatok) is személyes adattá tehetik az adathalmazt, amelyekről elsőre nem gondolnánk. Például ha a vállalat nyílt információt gyűjt az applikációba való bejelentkezési időről, azaz arról, hogy a felhasználó milyen gyorsan adja meg a jelszavát (hogy így határozzák meg a megfelelő időzárhosszt a biztonság növelése érdekében), az elsőre nem tűnhet személyes adatnak. De ha van egy érintett a csoporton belül, akiről tudják, hogy lassan gépel, akkor így már beazonosíthatóvá válik, és személyesadat-kezelésnek minősül a tevékenység. Az egész kérdéskör nagyon komplex, és a tág fogalommeghatározás jelentősen megnehezíti annak egyértelmű meghatározását, hogy mi nem minősül személyes adatnak. Ez nagymértékben szervezet- és személyfüggő, és ahogy az a rendelet kulcseleméből is látható („bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon"),[43] maga a személyes adat nagyon sok esetben konkrétan nem meghatározható.

A tényleges kihívás az OSINT-tevékenység szempontjából az, hogy ne minősüljön személyes adatnak a gyűjtött információ. De a rendelet szerint bármilyen információ annak számíthat, ha akár közvetett módon is beazonosítható általa az érintett. Nem magyarázzák meg, hogy a közvetlenség alatt mit ért a törvény, így még nehezebb egyértelmű behatárolást megfogalmazni a kérdéskör értelmezésénél. A legegyszerűbb köznyelvi szinten úgy lehetne ezt kifejezni, hogy bármilyen adat, amelyből az érintett személye kikövetkeztethető – módtól, tevékenységtől, adatmennyiségtől – függetlenül a személyes adatok halmazába esik.

Az is igen lényeges elem, ha az eszközök azonosítóit a személlyel kapcsolják össze. Tehát ha egy eszköz azonosító adatát kezelik, és ebből beazonosítható az érintett, akkor az is személyes adatnak minősül. A „különösen" határozószóval bevezetett részben ezeket taglalja a rendelet, amelyek közül számunkra a helymeghatározó adat és az online azonosító a releváns és hangsúlyos. A helymeghatározó adat mint kifejezés erősen függ az értelmezéstől, így az, hogy ezt nem definiálják, szintén megnehezíti a személyes adat fogalmának szűkítését. Ez utóbbi definíciójának első feléből az szűrhető le, hogy a helymeghatározó adatot is a közvetett identifikáció lehetősége teszi személyessé. Az online azonosító aránylag egyértelműnek hangzik, viszont ezt sem határozza meg a rendelet, ami szintén tágítja a fogalom értelmezését. Az online azonosító nemcsak a felhasználónév és a hozzá kapcsolódó jelszó lehet, hanem bármilyen adat, amely az adott személyt beazonosítja. A bevezető cím teszi egyértelművé

[43] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) I. fejezet 4. cikk.

azt, hogy ezeket az azonosítókat tágan kezeli a rendelet, ezért kiemelten fontos a címben foglaltakat is értelmezni. Itt megnevezik az IP-címet (amely akár több érintett/eszköz esetében is azonos lehet[44]) és a cookie-azonosítókat is, szintén példálózó jelleggel.

Összefoglalva: ha OSINT-tevékenység során bármilyen olyan eszközadatot is rögzítünk, amely alapján az érintett identifikálható, akkor a GDPR szabályai érvényesek. A személyes adat definíciója így igen tágan értelmezhető, és ez jelentősen szűkíti az OSINT-lehetőségeket. De nem zárható ki az ilyen tevékenység, hiszen a címben (és később szabályozásban is) taglaltak alapján hozzájárulás esetén végezhető. Ugyanakkor ha az érintett értesül az adatgyűjtésről, akkor maga az OSINT-tevékenység gyengülhet. A személyes adatoknál esetenkénti értelmezés szükséges, hogy az adott információ alapján beazonosítható-e ténylegesen valaki. Lényegében az adat jellege, mennyisége, minősége, akár átfedés az adatokban nem releváns, csak az, hogy ha hozzárendelhető egy érintett, akkor az személyes adatnak minősül.

Amennyiben személyes adatot kezelünk, az alábbi elveket szükséges követnünk:[45]

- jogszerűség,
- tisztességes eljárás,
- átláthatóság,
- célhoz kötöttség,
- adattakarékosság,
- pontosság,
- korlátozott tárolhatóság,
- integritás és bizalmas jelleg elve.

Ezek az alapelvek kötelező jelleggel érvényesek a személyesadat-kezelés teljes egészére. Fontos eleme a rendeletnek, hogy nem az adatkezelésre mint tevékenységre vonatkozóan határozza meg ezeket az elveket, hanem a személyes adatok kezelésére. Ez a különbség azt jelenti, hogy az egyenkénti információknak, amelyek személyes adatnak minősülnek, kell megfelelniük ezeknek a kritériumoknak. Ez például az adattakarékosság elvénél jelenik meg igazán, amely azt jelenti, hogy csak a releváns és szükséges adatokat lehet gyűjteni. Tehát az OSINT-tevékenység vonatkozásában nem felel meg az adattakarékosság elvének az, ha

[44] IPv4 esetén.

[45] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) II. fejezet 5. cikk.

különféle, nagy mennyiségű adatot gyűjtenek (hozzájárulás birtokában), és azt ténylegesen nem használják fel, nem elemzik. A „később még jól jöhet" mint cél a személyes adatok esetében nem jöhet szóba, mert az ilyen tevékenység sem az adattakarékosság, sem pedig a célhoz kötöttség elvének nem tesz eleget. A korlátozott tárolhatóság elve is ezt erősíti meg, amelynek értelmében az adat csak a cél eléréséig őrizhető meg. Ezeknek az alapelveknek csak akkor lehet megfelelni, ha a tervezett tevékenységet előzetesen konkrétan tisztázták, a gyűjteni kívánt adatfajtákat egyértelműen meghatározták, és mindegyikhez világosan hozzákapcsolható a kezelési cél, illetve a szükséges tárolási idő. „Szórt" jellegű nyílt információ (személyes adat) gyűjtésére nem ad lehetőséget a rendelet, még akkor sem, ha az érintett hozzájárul.

Az adatkezelés jogszerűségét mint alapelvet a 6. cikkben taglalják részletesen. Hat esetet határoz meg a rendelet, amelyek közül ha csak egy is érvényesül, az adatkezelés jogszerűnek minősül. Ezektől eltérésre lehetőség nincs. Az esetek röviden és egyszerűen a következők:

- az érintett hozzájárult;
- a szerződés teljesítéséhez szükséges;
- az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- létfontosságú érdek védelme miatt történik;
- közérdekű vagy közhatalmi adatkezelés;
- harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

Számunkra a releváns ezek közül az érintett hozzájárulása, amelynek feltételeit a 7. cikk taglalja, és a címben is tesznek említést erre vonatkozóan. A hozzájárulással kapcsolatban négy esetkört fogalmaz meg a rendelet:

- az adatkezelés alapja a hozzájárulás, amelynek meglétét tudnia kell igazolni az adatkezelőnek;
- összevont hozzájárulások esetén egyértelmű elkülönítés szükséges;
- a hozzájárulás bármikor visszavonható;
- az önkéntes hozzájárulás esete.

A címben taglalt jelölőnégyzetes módot itt nem említik, de az (1) bekezdés nem zárja ki ennek a lehetőségét, ha összevetjük az alábbi, címben foglalt gondolatokkal:

> „Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat

> hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi."[46]

A cím és a rendelkezés összevetése során világossá válik, hogy a rendelet maga a hozzájárulás módját tágan kezeli, a hangsúly azon van, hogy a felhasználó egyértelműen tájékozódhasson arról, mihez járul hozzá, illetve a hozzájárulását később visszavonhassa. A technikai megoldás nem releváns, ami jelentősen egyszerűsítheti a nyílt információs adatgyűjtési eszközök viszonyát. Felmerül, hogy technikai megoldás keretében lehet-e álnevesíteni és így megkerülni a hozzájárulás és a személyes adat komplex kérdéskörét. Ebben a rendelet címében megismert eset az irányadó, külön fejezet nem tárgyalja az álnevesítés lehetőségét. Ezt egyébként egy biztonsági lépésnek titulálja a GDPR, nem pedig egy lehetőségnek, amellyel megkerülhető a rendelet. A gyakorlatban ez azt jelenti, hogy az adatkezelő a birtokában lévő személyes adatokat álnevesíti, így biztosítva azt, hogy ha később történne egy adatvédelmi incidens, és az adatok részben vagy egészben elérhetővé válnának, akkor az érintettek ne legyenek azonosíthatóak. Arra viszont, hogy olyan technikai megoldással, amelynek keretében a gyűjtött adatot automatikusan álnevesíti a rendszer, megkerülhető-e a hozzájárulás, a válasz az, hogy nem. Azért nem, mert személyes adatnak minősül minden olyan adat, amely alapján az érintett közvetlenül vagy közvetetten identifikálható, az adott szervezeten belül pedig így a közvetett beazonosítás lehetősége fennáll.

Az érintettnek továbbá joga van a helyesbítéshez és a törléshez is:

> „Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését."[47]

Hat esetben jogosult az érintett kérni a róla rögzített személyes adatok törlését:

- az adatgyűjtési cél már nem áll fenn;
- az érintett visszavonta a hozzájárulását, és nincs más jogalap;
- személyes ok miatt;
- jogellenes az adatkezelés;

[46] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) (32) bekezdés.
[47] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) III. fejezet 16. cikk.

– más jogszabály miatt törölni kell;
– online térben gyűjtött adatról van szó.

A rendelet azt nem határozza meg, hogy ezt miként kell megvalósítania az adatkezelőnek, és erre hogyan kell lehetőséget nyújtania. Viszont az átláthatóság alapelvének érvényesülése érdekében ezt érdemes a hozzájáruláshoz hasonló módon biztosítani. Tehát egy applikáció, egy eszköz esetében célszerű azon az opción belül, ahol a személyes adatok gyűjtéséről szóló tájékoztatás olvasható, megadni a lehetőségét (vagy megnevezni a módját) annak, hogy a felhasználó az adatokat pontosíthassa, vagy az adatkezeléshez való hozzájárulást visszavonhassa.

Automatizált döntéshozatalra, ahogy a címben is említik, nincs lehetőség:

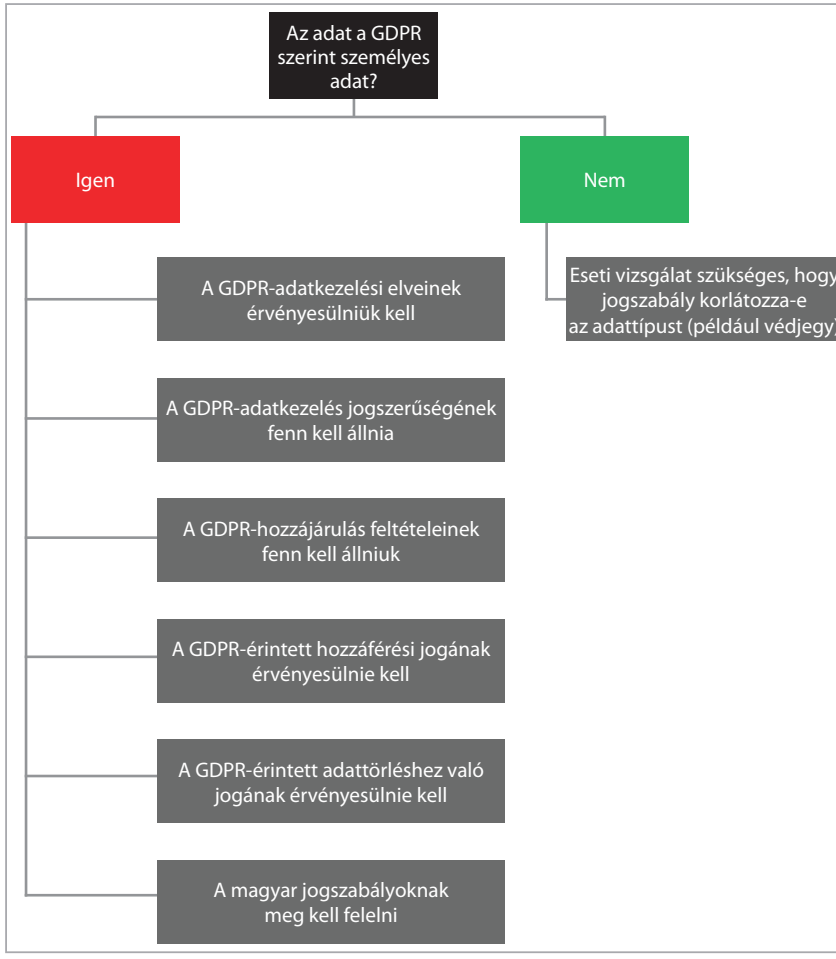
> „Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené."[48]

Főszabály szerint nem lehet nyílt információból személyes adatot gyűjteni, és ennek alapján egy automatizált rendszer révén hátrányos döntést hozni még bizonyos kritériumok fennállása esetén sem szabad. A címben megismertek fényében a döntésnek magának egyedinek kell lennie.

Az adatkezelőre és adatfeldolgozóra vonatkozó szabályokat ebben a tanulmányban nem taglaljuk, mivel túlzottan szervezetspecifikus az értelmezésük. Jogszabályelemzésünk során bemutató jelleggel értelmeztük a GDPR vonatkozásait, amelyek az OSINT-tevékenység megkezdése előtt relevánsak a jogszabályi megfelelés szempontjából.

Az OSINT-tevékenységgel kapcsolatosan így első lépésként minden esetben azt kell megvizsgálnunk, hogy az adatvédelmi rendelet szerint a gyűjteni kívánt adatok személyes adatnak minősülnek-e. Amennyiben igen, lépcsőzetes keretszerű megfelelést kell előzetesen végrehajtanunk.

[48] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) III. fejezet 22. cikk (1) bekezdés.



2. ábra: Lépcsőzetes keretszerű megfelelés

Forrás: a szerzők szerkesztése Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) alapján

Összességében elmondható, hogy az OSINT-tevékenységet elsődlegesen az előzi meg, hogy az annak során gyűjteni kívánt adat az Európai Parlament és a Tanács (EU) 2016/679-es rendelete szerint személyes adatnak minősül-e, vagy sem.

Az, hogy az adat nyíltan elérhető, vagy automatizált gyűjtéssel szerzik, nem releváns a rendelet szempontjából. Az viszont kifejezetten fontos, hogy először meg kell vizsgálnunk, az érintett adatok személyes adatnak számítanak-e. Ezen jogszabályi elemzésünkkel ennek a kérdésnek a tisztázását kívánjuk megalapozni. Az, hogy milyen adattípusok esnek pontosan ebbe a kategóriába, erősen személy- és szervezetfüggő. Ugyanakkor elmondható, hogy a megszerezni kívánt információ nagy eséllyel személyes adatnak minősül, így a szabályozás összetettségéből eredően olyan tényezők gyűjtését javasoljuk, amelyekből egy személy még közvetett módon sem azonosítható be egyértelműen. Ez a gyakorlatban azt jelenti, hogy általános jellegű OSINT-tevékenység valósítható meg, így az egyén nem tud fókuszba kerülni. Az általános jellegre egy példa az értelmezés vonatkozásában: az érintett szervezet fel kívánja mérni azt, hogy a szolgálati okostelefonokon a felhasználók milyen alkalmazásokhoz (például névjegyzék, kamera, üzenetek, naptár) milyen mértékű hozzáférést adnak más applikációknak. Ez egy biztonsági kockázat, amely legitimálni tudja a nyílt információs felmérés célját. Amennyiben ezeket az információkat egy applikáció csak mennyiségileg továbbítja, nem minősülnek személyes adatnak, azonban ha ezekhez eszközadatot is hozzárendel, akkor már igen. Ez pedig egy nagy dilemmát vet fel, amelyet a szervezetnek kell eldöntenie az OSINT-tevékenység előtt: érdemes-e a személyes adatok kezelésének útjára lépnie, vagy sem. A tevékenység akkor is hatékony lehet, ha megmarad az általános jelleg, a vállalat kiberhigiéniájának felméréséhez és oktatási anyagok létrehozásához nagyon nagy segítséget tud nyújtani. A súlyos, kiugró végletek, amelyek tényleg veszélyeztetik az intézmény biztonságát, azonban így nem beazonosíthatóak és nem szankcionálhatóak. Ha pedig a szervezet a személyes adatok kezelése mellett dönt, akkor a megismert jogszabály alapján neki kell mérlegelnie, hogy megéri-e a plusz jogi lépéseket a biztonsága. Még egy óriási hátulütője a rendelet alkalmazásának, hogy a benne foglalt adatkezelési szabályoknak meg kell felelni, de ezt a specifikussága miatt a jogszabály-értelmezésünkben nem taglaljuk.

3.2. A Magyarországon releváns jogszabályi háttér

Ebben a fejezetben a Magyarországon releváns jogszabályokat mutatjuk be és értelmezzük a nyílt információs adatgyűjtés szempontjából. Számunkra két jogforrás az, amely kulcsfontosságú: Magyarország Alaptörvénye és a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

Az Alaptörvény nem taglalja részletesen a kérdéskört, a VI. cikkében szól a személyes adatokról:

> „(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák. A véleménynyilvánítás szabadsága és a gyülekezési jog gyakorlása nem járhat mások magán- és családi életének, valamint otthonának sérelmével. […]
> (3) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.
> (4) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi."[49]

Az Alaptörvény is a GDPR-ból megismerthez hasonló nézőpontot képvisel az adatkezelést illetően: szintén az egyén felől közelíti meg a kérdéskört. A számunkra releváns adatkezelés kérdésével csak a VI. cikkben foglalkozik, tehát itt sem valósul meg az, hogy szervezeti szempontokból vizsgálják a tevékenységet. Ez sem előnyös a nyílt információból történő adatgyűjtés esetében. Az első bekezdésben megfogalmazott kritérium először nem tűnik relevánsnak, de fontos, mert esetünkben azt fejezi ki, hogy maga a tevékenység, azaz az adatok gyűjtése, feldolgozása, kielemzése, értékelése során nem fordulhat elő olyan helyzet, amely az egyénre nézve sértő. A harmadik pontban az Alaptörvény meghatározza azt, hogy mindenkinek joga van a személyes adatai védelméhez. Ez a kifejezés kulcsfontosságú: az egyéneknek nem egyszerűen az adataik, hanem a személyes adataik védelméhez van joguk. Ez nagyon hasonlít az európai adatvédelmi rendelet szemléletéhez, és a magyar jogszabályi háttér esetében itt rajzolódik ki, hogy a személyes adatnak minősülés irányából kell megközelíteni a kérdéskört.

Az Alaptörvény VI. cikkéhez kapcsolódik a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.). Ezt maga a törvény is megerősíti a bevezetőjében:

„Az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokról, valamint az ezen szabályok ellenőrzésére hivatott hatóságról az Alaptörvény végrehajtására, az Alaptörvény VI. cikke alapján a következő törvényt alkotja".[50]

[49] Magyarország Alaptörvénye VI. cikk (1), (3)–(4) bekezdés.
[50] 2011. évi CXII. törvény.

E törvény bevezetőjének értelmezése is releváns számunkra, igaz, hogy a magyar jogban ez jóval rövidebb, de ez mutatja meg a jogalkotó tényleges szándékát és célját a jogszabállyal. A hazai törvény célja pedig teljesen azonos az EU adatvédelmi rendeletéével: mindkettő a személyes adatok védelmére irányul. Ezért a magyar jogszabályok esetében is az egyén felől kell megközelítenünk a kérdést, mert így tudjuk biztosítani a megfelelést. Az első szakasz megismétli a törvény célját:

> „E törvény célja a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák […].”[51]

Gyakran felbukkanó gondolat, és már lassan önismétlő hatást is kelt, de ennyiszer visszatérő elem és ennyire nyomatékos adatkezelési szempontból, hogy ez a jogszabály az érintettek szemszögét érvényesíti. Itt újra megerősítik azt a feltevést, hogy a cél az, hogy a természetes személyek magánszféráját tiszteletben tartsák az adatkezelők. Semmi olyat nem fogalmaznak meg, hogy bizonyos kivételes esetekben (például a biztonság növelése) az érintettek szféráját akár egy vállalat érdekei alá kell rendelni. A nyílt információs adatgyűjtésnél és adatkezelésnél mindig ezt kell szem előtt tartanunk, de még előnyösebb, ha a tevékenységbe belevonható az egyének érdekeltsége is.

A jogszabályi megfelelés kiemelt célja a párhuzamos tevékenység létrehozása. Az Infotv. hatálya szintén nagyon hasonló a GDPR hatályához: „[…] minden olyan adatkezelésre kiterjed, amely személyes adatra, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik”[52]. A magas szintű hasonulás a jogszabályi megfelelésből ered: az adatvédelemmel kapcsolatos magyar jogszabályoknak is eleget kell tenniük az uniós szabályozásnak, így az abban foglaltakhoz hasonló feltételeket szabnak. Az adatkezelőknek ettől függetlenül mind a hazai, mind az uniós rendeleteket be kell tartaniuk. A kulcskérdés az előbbinél is a személyes adat fogalma, hiszen a jogszabály csak arra az esetre vonatkozik, amikor személyes adatot kezelnek. A törvény hatályánál ezt definiálják, és egy az egyben a GDPR-ban használt meghatározást veszik át, illetve megerősítik azt, hogy a GDPR-ban foglaltak kötelező érvényűek attól függetlenül, hogy az Infotv. hatályos-e, vagy sem. Ez azt jelenti, hogy ha egy kérdéskör az adatvédelem

[51] 2011. évi CXII. törvény 1. §.
[52] 2011. évi CXII. törvény 2. §.

vonatkozásában nem szabályozott a hazai jogrendben, de a GDPR-ban igen, akkor az ott rögzített meghatározás kötelező érvényű. Ez nem előírt része egy jogszabálynak, viszont számunkra azt jelenti, hogy a magyar jogalkotó megerősíti és elismeri a felettes jogforrásban foglaltakat.

Az értelmező rendelkezésekben egy kicsit eltérően újra megfogalmazza a jogszabály a személyes adat definícióját, illetve bevezet egy új fogalmat, a különleges személyes adatot.

> „2. személyes adat: az érintettre vonatkozó bármely információ;
> 3. különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,
> 3a. genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;
> 3b. biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;”[53]

A GDPR értelmezéséhez képest a személyes adatot itt egyszerűbben fogalmazzák meg, viszont ez jelentésbeli eltérést nem hozott a képbe. A különbség a különleges adat megjelenésénél érződik. Ez semmivel sem más, mint a GDPR-ban rögzített személyesadat-fogalom, valójában nem bővült a definíció, csupán két részre bontották. A különleges adatok közül számunkra az egyedi azonosítást célzó biometrikus adat válhat relevánssá. A gyakorlatban OSINT-tevékenység során nagyon kevés esetben, esetleg telefonos applikációnál a képernyőzár módjának és adatainak gyűjtésekor merülhet fel a kérdéskör. Egy későbbi értelmezésben kiemeljük, hogy ez miért nem megvalósítható jogi szempontból. Ezek a definíciók viszont csupán magyarázóbb leírásai a GDPR személyesadat-kritériumának.

Az Infotv. is megfogalmaz személyes adatok kezelésére vonatkozó alapelveket:[54]

– jogszerű és tisztán meghatározott célú kell hogy legyen;

[53] 2011. évi CXII. törvény 3. §.
[54] 2011. évi CXII. törvény 4. §.

– csak az adatkezelés céljával összefüggő személyes adatok kezelhetők;
– adatkapcsolat elve – mindaddig személyes adat marad az információ, ameddig kapcsolódik az érintetthez;
– adatok pontosságának elve;
– adatok védelmének elve.

Ezen alapelvek szintén követik az európai uniós jogszabályban foglaltakat, és általánosságban elmondható, hogy az észszerű és jóhiszemű adatkezelést biztosítják. Itt is kirajzolódik, hogy az érintettek érdekét képviseli a jogszabály, nincs olyan pont és lehetőség, amely az adatkezelő szemszögéből közelíti meg a jogosultságot. Az alapelveknél is szem előtt kell tartani ezt, hogy nem a szervezet érdeke a létfontosságú, sőt, az semmilyen módon nem jelenik meg mint személyesadat-kezelésre feljogosító esetkör. Emiatt itt is csak a hozzájárulás függvényében történhet személyesadat-kezelés, amelynek jogalapja (és általános feltételei) a jogszabály szerint a következők:[55]

– ha törvény elrendeli;
– ha az adatkezelő törvényben meghatározott feladataihoz szükséges, és az érintett hozzájárult;
– létfontosságú érdek védelméhez kapcsolódik, és ezzel arányos;
– az érintett a személyes adatát kifejezetten nyilvánosságra hozta, és az adatkezelés ezzel arányos.

A különleges adatok kezelését illetően pedig a törvény még szigorúbb kritériumokat fogalmaz meg: azok lényegében törvényben meghatározott érdekek esetén használhatók. Az automatizált adatkezelés vonatkozásában szintén keményebb feltételeket szab a jogszabály: döntéssel együtt csak akkor engedélyezett, ha azt az érintett kifejezetten kéri, vagy az adatkezelőnek európai uniós jogi aktust kell végrehajtania. Az általános követelményekből sokkal szigorúbb kritériumrendszer rajzolódik ki, mint a GDPR-ban. A GDPR hozzájárulással lehetőséget ad az adatkezelésre, de ezt az Infotv. jelentősen szűkíti. A beleegyezés itt önmagában nem elegendő, hanem az is szükséges, hogy valamilyen egyedi feltétel fennálljon. Ez lehet az adatkezelő törvényi kötelezettsége vagy speciális létfontosságú érdek (például testi épség, vagyoni javak védelme). A különleges adat kezelésének lehetőségei pedig így még korlátozottabbak.

[55] 2011. évi CXII. törvény 5–7. §.

A nyílt információs személyes adatok kezelését, gyűjtését a jogszabály ezzel erősen visszaszorítja. Hogy az megvalósítható legyen, kritikus érdeknek és hozzájárulásnak kell mögötte állnia, amelyet a szervezetnek kell mérlegelnie és megvizsgálnia az esetkör előtt. Ez az OSINT-tevékenységre nézve nagy érvágás, de küzdeni ellene nem érdemes, mert abból később jogviták lehetnek. Ha személyes adatát kezelik, az érintettnek számos joga van, ezeknek az érvényesülését is biztosítani kell. A jogok röviden:[56]

- előzetes tájékozódáshoz való jog: az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről tudomást szerezzen;
- hozzáféréshez való jog: az adatkezelőnek az illető kérelmére rendelkezésére kell bocsátania a tárolt személyes adatait;
- az adatok helyesbítéséhez való jog;
- az adatkezelés korlátozásához való jog;
- az adatok törléséhez való jog.

Ezek szintén hasonlítanak a GDPR-ban megfogalmazottakhoz, ahogy a jogok érvényesülésének biztosításáról szóló rész is, amelynek értelmében az adatkezelő:

- mind műszakilag, mind szervezéssel biztosítsa, hogy az érintett jogai érvényesüljenek;
- ingyenesen lássa el az érintett jogaival kapcsolatos tevékenységét;
- előzetesen tájékoztassa az érintettet az adatvédelemmel kapcsolatos releváns információkról (például az adatkezelő, az adatvédelmi tisztségviselő személye, az adatkezelés célja és időtartama, az adatkezelés jogalapja);
- segítse elő az érintett adatokhoz való hozzáférését;
- biztosítsa a helyesbítéshez való jogot az érintettnek.

Ezek a jogok megerősítik azt, hogy az egyén van a törvény középpontjában, és az ő érdekében történik az adatkezelés. A jogszabály „hatalmat" ad az érintettnek az adatai fölött, így bármikor kérhet törlést, helyesbítést vagy módosítást. Ez szintén szűkíti az OSINT-tevékenységek lehetőségeit, mivel így a háttérben történő, felmérő jellegű személyesadat-kezelést nem lehet megvalósítani. Az adatkezelés szervezetre vonatkozó szabályait nem elemezzük ebben a tanulmányban, mivel azok túlzottan szervezetspecifikusak, hanem az OSINT-tevékenység jogi alapjára kívánunk itt választ adni.

[56] 2011. évi CXII. törvény 14–24. §.

Összességében elmondható, hogy a magyar jogszabály is szigorú a személyes adat kezelését illetően, sőt, a GDPR-hoz képest tovább szűkíti annak lehetőségeit. A megismert jogszabályi háttér fényében a ténylegesen hatékony és megvalósítható OSINT-tevékenységek alapja a nem személyes adatok kezelése. Arra kell kifejezetten figyelnie a szervezetnek, hogy az információk ne minősüljenek személyes adatnak, mert ha annak minősülnek, akkor az Infotv. és a GDPR szabályainak szigorúan meg kell felelniük, és ez a két rendelet jelentősen csökkenti bármilyen személyes adat kezelésének lehetőségét. A megismert szabályozás alapján szerintünk érdemesebb ezt a tevékenységet általános jelleggel folytatni és a személyspecifikus adatgyűjtést, személybeazonosíthatóságot mellőzni, mert abban az esetben jogszabályi felhatalmazásra van szükség a hozzájárulás mellett, ami a ténylegesen végezhető cselekvések körét jelentősen szűkíti.

4. A villamosenergia-vállalatok OSINT-tudatossága és képességei

Ebben a részben a mellékletben vázolt interjúkérdésekből leszűrt eredményeket tekintjük át. Az egyes témaköröket a kapott válaszok alapján külön ismertetjük az általános jellemzők és az alkalmazott gyakorlatok bemutatásával.

4.1. Miért van szükségük a vállalatoknak a nyílt forrású információszerzésre?

A nyílt forrású hírszerzés legnagyobb előnyei közé tartozik a korai adatszivárgás észlelése, ugyanis az OSINT-elemzők a keresőmotorok, weboldalak eltemetett adatai navigálásának szakértői, így hihetetlen gyorsasággal össze tudják szedni a szükséges információkat. A szivárgások korai detektálása és megállapítása a vállalat márkájának és hírnevének védelmére is szolgálhat, amely védelem az ügyfelek, vevők véleményének eldugott fórumokon vagy akár a *surface* vagy *deep weben* való felkutatásával is megvalósítható. Mindezek mellett a hírszerzés a gyors közvélemény-kutatással elősegítheti a kríziskommunikációt, és akár egy

felbecsülhetetlen értékű eszköz lehet a megalapozottabb döntések meghozatalához, ráadásul alacsony költséggel jár.

4.1.1. Az általános ismeretek felmérése

Kutatásunk során először a vállalatok OSINT-ról való általános ismereteit mértük fel, továbbá egy átfogó képet alkottunk a folyamataikról. Ezeket az alábbi kérdések tették lehetővé:

1. *Hogyan definiálja az OSINT-ot?*

2. *Véleménye szerint az OSINT a szervezetére nézve inkább lehetőség vagy kockázat?*

3. *Milyen, az OSINT-tal kapcsolatos normatív szabályzókat ismer?*

4. *Végeznek-e nyílt forrású információgyűjtést?*

Minden válaszadó tisztában volt az OSINT fogalmával, vagyis azzal, hogy az legális keretek között végzett, nyílt, bárki által hozzáférhető adatokból való információgyűjtés. A válaszadók feltűnően az OSINT támadó oldalát vették figyelembe a kitöltés során, vagyis azt a típusú hírszerzést, amellyel más cégekről gyűjthetnek össze a saját vállalatukat valamilyen kompetitív előnyhöz juttató információkat. A válaszokból rendre kihagyták az OSINT elleni védekezést, azaz a vállalatról kikerülő információk figyelését és kontrollálását.

A lehetőség és kockázat témakörében kettős kép rajzolódott ki: megközelítőleg azonos gyakoriságúnak tartották a pozitív és a negatív kimeneteleket. A képet azonban árnyalja, hogy bár látták a lehetőségeket, ezeket nem tartották teljes mértékben kihasználhatónak, különböző hiányosságokra hivatkozva. A kockázatok között megjelent a reputációs és az informatikai kockázat is, míg a lehetőségeket a válaszadók nem pontosították.

Normatív szabályzóknál a vállalati belső kommunikációs szabályzat és a magyar törvények jelentek meg, de több válaszadó üresen hagyta ezt a területet. Általánosságban kijelenthető, hogy a szervezet életében nincsen kiemelt szerepe az OSINT-műveletek során a különböző szabályzatoknak és törvényeknek. Árnyalja a képet, hogy minden válaszadó tudott példát mondani cégcso-

porton belüli informatikai biztonsági tudatosságnövelő képzésekre, valamint vállalati titkokat érintő és védő szabályokra. Ezek nem kizárólag az OSINT-tal foglalkoznak, de mindenképpen érintik a területet.

Összességében megállapítható, hogy a kitöltő vállalatok szisztematikus, folyamatkövető nyílt forrású hírszerzést akár anyagi, akár humánerőforrás-hiány miatt nem folytatnak. Sokkal elterjedtebb az eseti megkeresések alapján történő információgyűjtés. Ellenben nagy eltérés tapasztalható a vállalatok között: van olyan, amely ezt kizárólag csoportszintű feladatnak tartja, de olyan is, amely munkája során ennek a területnek stratégiai fontosságú szerepet adna, és a jövőbeli terveinek is része a képesség további fejlesztése. Ez nagyjából egybeesik a várakozásainkkal, miszerint a legtöbb piaci szereplő jelenleg nem foglalkozik operatív szinten OSINT-tal. A válaszok között megjelenik a sajtófigyelés is, amely manapság az ilyen hírszerzés legelterjedtebb típusa. A reputációs veszteségek megelőzése külső szolgáltató segítségével vagy megvásárolható szoftver útján könnyen definiálható és számszerűsíthető eredményt hoz, épp emiatt a vállalati szintű OSINT egyik népszerű formája. Ugyanakkor a cégcsoport dolgozói által a közösségi oldalakon végzett tevékenységek és a megosztott tartalmak figyelése, a támadások kivédése céljából nem jelenik meg. Pedig az így nyilvánossá tett adatok és információk elősegítik mind a *social engineering,* mind a tradicionális hackertámadások kivitelezését.

A vállalatok OSINT-ról való általános ismeretének szintje válaszaik alapján megnyugtató. Ideális esetben cégcsoportra vonatkozóan kell létrehozni szabályzatokat és folyamatokat, amelyekkel minden vállalatnak tisztában kell lennie, így közösen magasabb szintű tevékenységet tudnak végezni, és a kinyert információ jobban áramolhat a tagok között.

4.1.2. A kapacitás felmérése

A második kérdéskör a vállalatok jelenlegi és tervezett OSINT-kapacitását járja körül. Választ kerestünk rá, hogy amennyiben nem, miért nem végeznek információgyűjtést, továbbá mi hiányzik ahhoz, hogy széles körű és mélyebb hírszerzést folytassanak.

Ezt a területet az alábbi négy kérdés fedte le a kérdőívben:

5. *Ha nem végeznek, akkor szeretnének-e kialakítani ilyen képességet?*

6. *Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:*
   a) *szükséges technológiai erőforrás beszerzése;*
   b) *szükséges humán erőforrás biztosítása;*
   c) *szükséges szaktudás biztosítása?*

7. *Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?*

8. *Ha végeznek nyílt forrású információgyűjtést, annak lépései mennyire dokumentáltak?*

Mindössze egy kitöltő állította, hogy kétséget kizáróan végeznek OSINT-tevékenységet, egy másik vállalat pedig, bár nem lát el ilyet, a jelenlegi eljárásaival teljesen elégedett volt. A többi cégnél nincsen folyamatban a képesség kialakítása, bár akár csoportszintű kérés, akár lehetőség esetén érdeklődőek és nyitottak lennének rá.

A kitöltők egyhangúlag a szükséges humán erőforrás biztosítását jelölték meg mint kritikus hiányzó tényezőt. A válaszokból az derül ki, hogy vagy pluszfőt igényelnének a csapatukba, vagy azt szeretnék, hogy a kollégák kapjanak időt erre. Továbbá többen is megjelölték a szaktudás hiányát. Mivel az ilyen jellegű feladathoz szükséges a vállalatcsoport működésének ismeretén túl a specializált technológiai szaktudás, új munkatárs felvétele vagy egy meglévő átképzése esetén jelentős időt vesz igénybe, hogy az megtanulja a helyi működést vagy megszerezze az OSINT-ismereteket.

Egy kivételével semelyik kérdőív nem fogalmaz meg további akadályt a képesség kialakítását illetően. A humán erőforrás biztosításán kívül az egyetlen felmerülő tényező az erre a területre fordítható keret lehet: költséghatékonyság miatt jelenleg nem opció a folyamattal való kísérletezgetés, és nincs szabad befektetési tőke új technológiák megvásárlására. Erre a problémára megoldást jelenthet az olyan eszközökbe való csoportszintű befektetés, amelyek mindegyik vállalat számára segítséget tudnak nyújtani.

A korábbi válaszoktól függetlenül az OSINT-tevékenység nem dokumentált módon működik. Elsősorban ad hoc projektek, kérések és megkeresések a jel-

lemzőek, már ahol egyáltalán van ilyen tevékenység. Ezeket előzmény alapon (a múltban nyilvánosan megjelent információkat kutatva) végzik el, a szerzett információkat pedig külön nem tárolják vagy dolgozzák fel. A módszertan nem egységes, inkább célorientáltan történik a keresés.

Az világos, hogy új kollégák felvételére, új ismeretek elsajátítására és technológiák, eszközök megvásárlására mindenképp költeni kell. Azonban, ahogy a többi kérdésből látszik, ezt meg kell hogy előzze a célok és módszerek pontos definiálása és dokumentálása. Természetesen a jelenlegi állapotban is vannak még rejtett tartalékok, elsősorban vállalati szinten, azonban a vállalatcsoport esetében ez kizárólag úgy tud érvényesülni, ha a kitöltők egy csoportszintű, definiált és strukturált folyamat részesei, ami lehetővé teszi a tevékenység visszakövetését, reprodukálását és a kinyert eredmények többszöri és több célból történő felhasználását.

A kérdőíveket kiegészítő szóbeli interjún elhangzottak alapján két terület tovább nehezíti a gyors kiépítést. Az egyik a kizárólagos hosszú távra tervezés, ami megakadályozza, hogy egy-egy projektet indítsanak ezen a téren a vállalatok. A másik pedig a feladatkiosztás megváltozása a vállalatstruktúra átalakulása során: korábbi központi feladatok eltűntek, a cégek pedig nem tudják beépíteni a képességet a szolgáltatásportfólióba. Erre a konkrét példa a különböző akvizíciókat vagy üzleti döntéseket megelőző vezetői összefoglaló készítése volt, amely korábban nagymértékben támaszkodott OSINT-technikákra, azonban jelenleg már semelyik kitöltő vállalat nem foglalkozik ilyen területtel.

4.1.3. Hol és mivel végeznek OSINT-tevékenységet?

A következő kérdéscsoport azt mérte fel, hogy pontosan hol, tehát milyen felületeken, honlapokon, nyílt adatbázisokban keresnek a kitöltők elérhető információkat, továbbá hogy amikor ilyen kutatást végeznek, akkor azt milyen eszközökről teszik. Alapvetően az OSINT definíciója miatt nem feltétlenül szükséges ezeket az eszközöket túlságosan korlátozni, mivel nyíltan hozzáférhető és legálisan gyűjtött információról beszélünk. Azonban az adatok felhasználása, tárolása és osztályozása miatt, megfelelve a GDPR-nak és további informatikai biztonsághoz köthető szabályozásoknak, szabványoknak és törvényeknek, senki nem lehet elég óvatos, így OSINT-tevékenység végzése esetén mindenképpen javasolt a hétköznapi felhasználásúnál zártabb rendszerek használata.

9. Milyen felületeken, platformokon végeznek nyílt forrású információgyűjtést?

A válaszadók közül felületszinten az OSINT mindössze egy vállalatnál jelent meg széleskörűen, amelyre hagyományos webes keresőmotorok (például Google), közösségi oldalak (például Facebook) és még a célzottan OSINT-tevékenységre specializálódott Maltego[57] használata is jellemző volt. A Maltego egy nyílt forráskódú hírszerző és grafikus kapcsolatelemző eszköz, egy Java-alkalmazás, amely Windows, Mac és Linux rendszereken fut, és nyomozati feladatokhoz szükséges információk gyűjtésére és összekapcsolására szolgál. Sokan használják, a biztonsági szakemberektől kezdve a törvényszéki nyomozókon át az oknyomozó újságírókig és kutatókig.

Ezenkívül mindössze egy kitöltő jelezte, hogy a cége valamilyen szinten formalizáltan céloz különböző platformokat. Ők a nyomtatott és az online sajtóból szereznek információkat. A többi vállalat elmondása alapján feladatfüggően, ad hoc folytat gyűjtést, olyankor pedig inkább célorientáltan, bármilyen felületet felhasználva.

10. Külön rendszeren végzik a nyílt forrású információgyűjtést, vagy ugyanazt a rendszert használják, mint amelyet a napi munkavégzésre is?

Egy kitöltő használ a hétköznapi munkavégzéstől elkülönülő rendszert információgyűjtésre, mindenki más az ügyviteli rendszerüket alkalmazza erre. A korábbi megállapítással azonosan igazából nem elképzelhetetlen az OSINT működése, de mindenképpen könnyebb a formalizált munkavégzés és a szabályzóknak való megfelelés, ha az OSINT-ot végző rendszerek elkülönülnek a többitől, legalább eszköz-, de akár hálózati szinten is.

11. Virtualizációt használnak?

Semelyik válaszadó nem használ virtualizációt.

„A virtualizáció olyan technológia, amely egyesíti vagy felosztja a számítási erőforrásokat, hogy egy vagy több operációs környezetet hozzon létre, olyan módszerek segítségével, mint a hardver- és szoftverparticionálás vagy -összevonás, részleges vagy teljes gépszimuláció, -emuláció, időmegosztás stb. A virtualizációs technológiáknak számos területen vannak fontos alkalmazásai, mint például

[57] Lásd: www.maltego.com.

a szerverkonszolidáció, biztonságos számítási platformok, több operációs rendszer támogatása, rendszermag-mentesítés, szerver- és szerveralapú kiszolgálás, hibakeresés és fejlesztés, rendszermigráció stb. Legtöbbjük hasonló működési környezetet kínál a végfelhasználónak, azonban nagymértékben különböznek az általuk alkalmazott absztrakciós szintek és a mögöttes architektúra terén."[58]

Az OSINT esetében azért használunk virtualizációt, hogy csökkentsük a saját rendszereink megfertőzésének veszélyét. Akár kézi, akár automatizált eszközöket alkalmazunk munkánk során, nem tudjuk elkerülni azt, hogy a talált és megnyitott dokumentum potenciálisan fertőző legyen, esetleg kifejezetten kibervédelmi mézesbödönként álljon előttünk.

Amennyiben virtualizációt használunk, jelentősen, szinte nullára csökkenthetjük annak az esélyét, hogy az ilyen fenyegetések elérjék az éles rendszereinket, és kárt tudjanak tenni bennük. A virtualizált rendszer ugyanis hálózatilag is elkülönülten tud futni, és ideális esetben egy kártevőnek köszönhetően kizárólag az aznapi munkát lehet elveszíteni.

12. Automatizáltan vagy manuálisan folytatnak információgyűjtést?

Felmérésünkben megvizsgáltuk, hogy a vállalatok az információgyűjtés folyamatát manuálisan vagy pedig automatizációs szoftverek segítségével végzik. Az interjúk során megállapítottuk, hogy ahol nyílt forrásból szereznek adatokat, azt manuálisan teszik. Ugyan túlnyomórészt így gyűjtik össze az információt, alkalmanként használják a Maltego nevű alkalmazást. De számos más program és szoftver is segíti és gyorsítja az adatgyűjtés folyamatát, például az OSINT Framework[59] vagy a Shodan[60]. A Google a legismertebb és legnépszerűbb böngésző, azonban a Shodan, más keresőmotorokkal ellentétben, a biztonsági szakemberek számára sokkal érthetőbb és könnyebben értékelhető eredményeket biztosít. Az OSINT Framework pedig a nyílt forrású hírszerzésre használt eszközök összegyűjtésére készült keretrendszer, amelynek célja, hogy segítsen az embereknek megtalálni az ingyenes OSINT-forrásokat.

[58] Nanda–Chiueh 2005: 1. Az idézet a szerzők fordítása.
[59] Lásd: https://osintframework.com.
[60] Lásd: www.shodan.io.

13. Amennyiben manuálisan folytatják a nyílt forrású információgyűjtést, milyen gyakorisággal teszik? Mennyi humánerőforrás-időt igényel naponta/hetente?

Vizsgálatunk során megállapítottuk, hogy a folyamat formalizálatlansága, valamint a projektszerű és megrendelésalapú működés következtében a kérdésre nem tudtak a vállalatok pontos válasszal szolgálni.

14. Milyen keresőmotort használnak jellemzően?

Az interjúk során kapott válaszok alapján a vállalatok által használt egyetlen keresőmotor a Google, amelynek számos hasznos kiegészítő funkciója van. Ezek között szerepel például a *deep web search,* amelynek segítségével a *deep weben* is kereshetünk. Ez a funkció a Google Chrome megnyitása után az Alt + Shift + F billentyűkombináció lenyomásával érhető el és használható. Továbbá talán egyik legismertebb előnye a Google Dorks és a Google Hacking Database, amelyekkel szűkíthetjük és pontosíthatjuk, irányíthatjuk a keresést. A Google Dorks segítségével kereshetünk fájlkiterjesztésekre, URL- és weblapcímekre is. A Google Hacking Database elérhető az exploit.db nevű oldalon, valamint folyamatosan frissítik. Ezenfelül a Google-nak létezik képkereső funkciója, amellyel hasonló képeket lehet keresni, vagy felkutathatjuk az eredetit is, de egy adott személyről készült felvételekre is rátalálhatunk. Erre a legalkalmasabb, bár kevésbé ismert oldal a PimEyes[61] arcfelismerő eszköz, amelynek felületén napi 10 keresés ingyenesen lefuttatható.

15. Használnak-e rejtett kommunikációt?

Vizsgálatunk során megállapítottuk, hogy a vállalatok egyike sem használ rejtett kommunikációt. Annak érdekében, hogy értelmezni tudjuk az információgyűjtés és -szerzés célját, módszereit, lépéseit, illetve a folyamatok elleni védekezést, vagyis az információk védelme érdekében tett intézkedéseket, elengedhetetlen, hogy tisztában legyünk az alapvető fogalmakkal és jelenségekkel. A hírszerzés típusától függetlenül elsőként szükséges tisztázni, hogy mire irányulnak ezek az információs tevékenységek, tehát mi a művelet tárgya. Konkrétan az általunk vizsgált témakörben a lényegi kérdés az információk és adatok gyűjtése, majd azok felhasználása.

[61] Lásd: https://pimeyes.com/en.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rögzíti, hogy az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. A jogszabály leszögezi, hogy az információ bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában közölt tapasztalat, megfigyelés vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét átalakítja, megváltoztatja, illetve befolyásolja, továbbá bizonytalanságát csökkenti vagy megszünteti.

Az említett források közé tartoznak a nyilvánosan elérhető adathordozók, ilyenek az általános módon publikált anyagok, kötetek, könyvek, folyóiratok, konferencia-előadások, közösségimédia-tartalmak. Az OSINT tárháza szinte végtelen, viszont manapság az internet fejlődésének és a globalizációnak köszönhetően ez a módszer mondható a legjobbnak a cél elérése érdekében.

16. Milyen elérhető források között keresnek?

A kérdőívet kitöltő vállalatoknál az elérhető források kihasználtsága széles skálán mozog. Az erre a kérdésre adott válaszokból is tisztán látszik, hogy melyek azok a cégek, amelyek jelenleg is használnak OSINT-eszközöket, vagy legalább a közeljövőben kívánják kihasználni a tevékenység nyújtotta lehetőségeket.

17. Mire keresnek jellemzően?

A kutatásban érintett szereplők a tevékenységüktől függően jelölik ki azokat a témaköröket, amelyekben adatokat, jobb esetben pedig információt kívánnak gyűjteni.

18. Melyek azok a kulcsszavak, információk, amelyek az OSINT szempontjából lényegesek a vállalata számára?

A kérdésre adott válaszok eltérőek voltak. Itt is megjelent a vállalatokra jellemző profil, amely az egyes válaszadóknál megegyezett a keresett témakörrel. Ezzel szemben láthattunk példát a versenytársakra, illetve olyan nyíltan elérhető adatokra történt irányított, kulcsszavas keresésekre, amely információk magukban foglalják a cégekhez köthető e-mail-címeket, más esetben vállalati felhasználóazonosítókat, informatikai rendszereket és azok elérhetőségeit.

19. Igénybe veszik-e külső, harmadik felek (beszállítók, alvállalkozók, tanácsadók) segítségét az OSINT bármelyik állomása során?

Három érintett adott igenlő választ, akik közül kettő ugyanazt a médiafigyelő szolgáltatót nevezte meg mint harmadik felet, a harmadik pedig egy, az adott vállalaton belül működő szervezeti egységet jelölt meg mint támogató elemet. A többiektől nemleges választ kaptunk.

20. Hogyan dolgozzák fel a találatokat? Használnak-e szabadszavas keresőt?

Két esetben használnak szabadszavas keresőt az érintettek, egy szereplő pedig a manuális adatfeldolgozást preferálja.

21. Hogyan és meddig tárolják az információgyűjtés során szerzett nyers adatokat?

Egy válaszadó konkrét törvényi szabályozásra (Infotv.) hivatkozott, míg a többiek úgy nyilatkoztak, hogy az információgyűjtés témájától függően tárolják az adathalmazokat (például intranet). Egy kirívó esetben az adatgyűjtést végző munkatársra bízták az adatok megőrzésének időtartamát, ami egy kevésbé kötött belső szabályozási környezetre utal.

22. A mobilalkalmazások adatait felhasználják-e nyílt információszerzéshez?
A kérdésre az összes kitöltő nemleges választ adott.

23. A nyílt információgyűjtésbe bevonják-e az alkalmazottak közösségimédia-profiljait is, és ha igen, milyen mélységben?

Napjainkban egyre népszerűbb és hangsúlyosabb a közösségimédia-portálokon történő aktivitás, kommunikáció, jelenlét, azonban sokan nem ismerik fel az ezekben a felületekben rejlő veszélyeket. A koronavírus miatt a mindennapos kommunikáció is eltolódott az online térbe, hiszen annak egyik elsődleges forrását a karantén alatt a közösségimédia-oldalak jelentették, ami jelentősen növelte a felhasználók digitális lábnyomát. Ez azon nyomok, információk összessége, amelyeket az internetezők online tevékenységük és jelenlétük után hagynak, és amelyek alapján aktivitásukról következtetéseket lehet levonni. Az online térben történő nyílt forrású hírszerzés is felhasználja ezeket a nyomokat, hogy

átfogó, részletes és informatív profilt alkosson egy adott személyről. Az ilyen eredetű információkkal visszaélve küldhetnek célzott adathalászleveleket, vagy egy kibertámadáshoz használhatják fel az adatokat. Ezért egyre több vállalat bővíti ki információbiztonság-tudatosítási tréningjét a közösségimédia-portálok megfelelő használatával.

Vegyük például a LinkedInt, a világ legnagyobb professzionális hálózatát. Segítségével a felhasználók megtalálhatják a megfelelő állást vagy szakmai gyakorlatot, szakmai kapcsolatokat alakíthatnak ki és ápolhatnak, valamint elsajátíthatják a karrierjükhöz szükséges készségeket. A LinkedIn elérhető asztali számítógépről, mobilalkalmazásból, mobil webes élményből vagy a LinkedIn Lite Android-applikációból. Számos előnye mellett viszont nagyon sok veszélyt is rejt magában, hiszen e felületen keresztül megkereshetőek egy adott szervezet alkalmazottai, az ő profiljukból, képességeikből pedig kiszűrhetőek a cég által használt technológiák, vagy a vállalat álláshirdetéséből, a szükséges technikai készségek révén. Ezenfelül képek megosztására is van lehetőség, ami szintén veszélyes lehet, ha a fotót a belépőkártyával a nyakában készíti a felhasználó, vagy egy olyan monitorral a háttérben, amelyen érzékeny adatok olvashatóak, esetleg egy ráragasztott cetlire írva a dolgozó jelszava.

Az interjú során megfigyeltük, hogy a vállalatok gyűjtenek-e információt nyílt forrásból az alkalmazottaikról. A felmérés keretében elsősorban a közösségimédia-portálokon keresztül történő adatgyűjtést vizsgáltuk. Az első kérdés ez volt: A nyílt információgyűjtésbe bevonják-e az alkalmazottak közösségimédia-profiljait, és ha igen, milyen mélységben? Az interjú eredményeit három csoportba soroltuk: a vállalat nem végez, csak mérsékelten végez, illetve végez ilyen adatgyűjtést.

Az első csoport esetében a cégek nem folytatnak semmiféle információgyűjtést. A második kategóriába tartozó szervezetekre jellemző bizonyos mértékű nyílt forrású adatgyűjtés. Itt az elsődleges közösségimédia-portálok a Facebook, LinkedIn, Instagram, Twitter, YouTube, valamint társkereső oldalak. A harmadik csoport tagjai a leírtak szerint is végeznek nyílt forrású információgyűjtő tevékenységeket, nemcsak passzív módon, hanem akár aktív interakcióba is kezdenek az alkalmazottakkal, egy baráti felkérés vagy üzenetküldés által. Ennek oka a biztonságtudatosság felmérése, továbbá a jövőbeli oktatási anyagok összeállításához történő információgyűjtés. Az ilyen interaktív vizsgálatot végző szervezetek viszont az adatokat semmilyen más módon nem használják fel.

24. Végeznek-e profilalkotást a kinyert információk alapján? Ha igen, ezt hogyan és meddig tárolják?

Ezt az előző kérdéshez szorosan kapcsolódva az ott felosztott csoportok közül csupán a második és harmadik esetében vizsgáltuk. A második kategóriába tartozó vállalatok nem csinálnak profilalkotást, csupán szűrő jelleggel végzik ezeket a tevékenységeket, az információkat nem is tárolják. A harmadik csoport tagjai csak a *social engineering auditok* keretében, közösségimédia-fókusszal összegyűjtött információk alapján készítenek anonim – azaz konkrét természetes személyhez nem köthető – értékeléseket és elemzéseket a későbbi oktatási anyagok összeállításához. Így profilalkotás ebben az esetben sem történik.

25. Történt-e a szervezetükben olyan információbiztonsági incidens, amelynek hátterében OSINT-tevékenység állhatott?

A támadóképességek mellett a védekezőképességeket is felmértük kutatásunk során, és ez volt az első erre vonatkozó kérdésünk. A vállalatokat, mint ahogy minden céget vagy magánszemélyt, szintén érték adathalász-támadások, amelyek a nyílt forrású hírszerzés felhasználási lehetőségeinek egyikét jelentik. Ezenfelül a szervezetek úgy vélik, hogy az ügyfélszolgálati honlapjukon történő visszaélések hátterében is OSINT-tevékenység állhat, ez azonban nehezen bizonyítható. Tehát a vállalatokat is érintik a ma már mindennaposnak számító adathalászkampányok, ugyanakkor más OSINT-akcióból származó incidensről nem tudnak.

26. Ha igen, ezt hogyan követték vissza?

A következő kérdésünk az előzőben megfogalmazott, OSINT-tevékenységből eredő incidensek visszakövetésére vonatkozott, ami a biztonsági terület feladata. Mivel az adathalász-támadásokon kívül más nyílt forrású hírszerzéssel kapcsolatban álló incidens nem történt, nem vizsgáltuk tovább ezt a kérdést.

27. Az egyes incidenseket besorolják-e veszélyességi szintek szerint?

Kitértünk egy kérdés erejéig az egyes incidensek biztonsági szintbe sorolására, amelyet a társaságok információbiztonsági szabályzataiban rögzítenek, és amely az ott meghatározott szintek alapján történik. A vállalatoktól kapott

válaszok szerint minden esetben az információbiztonsági szabályzatban foglaltak szerint járnak el.

28. Milyen jogi lépéseket tettek az incidenskezelést követően?

A támadásokra vonatkozóan az adott jogi lépésekre kérdeztünk rá. Ezek megtétele a biztonsági és jogi terület feladat- és hatáskörébe tartozik. A vállalatok legjobb bevett gyakorlata, hogy az incidens okozóját a feltárt és általa előidézett kockázat megszüntetéséről szóló nyilatkozattételre kérik fel. Azonban nyílt forrású hírszerzési tevékenység nyomán történt incidens esetében jelen állás szerint nem került sor jogi lépésekre. Ennek oka az előzőleg leírtak alapján az, hogy a villamosenergia-rendszer vállalatait ért egyetlen OSINT-tevékenységből származó támadástípus, amely igazolhatóan bekövetkezett, az adathalászat volt.

29. Lehetséges-e Ön szerint az OSINT-ot alkalmazni a reputációs veszteségek csökkentésére?

E kérdés esetében is az előzőleg kialakított három csoport alapján értékeltük az interjúk eredményét. Az első csoportnál, ahol a vállalatok nem végeznek semmiféle információgyűjtést, a válasz semleges volt, míg a második tagjai, amelyek aktív adatgyűjtést folytatnak, úgy vélik, hogy lehetséges a reputációs veszteség. Ugyanígy gondolják a harmadik kategória cégei, amelyekre szintén jellemző a nyílt forrású információgyűjtés és azon túl az aktív kapcsolatfelvétel is. Elképzelhetőnek tartják azt, hogy ha egy megfelelően konfigurált, automatizált OSINT-eszköz a vállalatcsoportot érintő, negatív tartalmú információról ad riasztást, akkor a kommunikációs területtel együttműködve – az információ széles körű elterjedése előtt – megelőző intézkedéseket lehet hozni. (A válaszadók minden esetben a vállalatról a közösségi platformokon megjelent hírek, bejegyzések, hozzászólások vizsgálatát tartották szem előtt, nem az alkalmazottakra vonatkozó kereséseket.)

30. Milyen megelőző intézkedéseket tesznek, hogy a vállalat működése során a dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek?

31. Ha nem tesznek ilyen megelőző intézkedéseket, akkor szeretnének-e a jövőben ilyen képességet kialakítani?

A vállalatok a tudatosítást tartják a legjobb módnak arra, hogy biztosítsák, a dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek. Ha a munkavállalók megértik, milyen kockázatai vannak a nyilvános adatmegosztásnak, akár a magánéletük tekintetében, maguk is érdekeltté tehetőek az adatok védelmében. A jövőre nézve pedig fontos a tananyagok folyamatos modernizálása, aktualizálása, ezzel tovább segítve a megelőzést. A témakört szabályozó adminisztratív intézkedések meghozatalát is jó módszernek vélik.

32. Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:
a) *szükséges technológiai erőforrás beszerzése;*
b) *szükséges humán erőforrás biztosítása;*
c) *szükséges szaktudás biztosítása?*

33. Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?

A képességek kialakítása esetében a legnehezebbnek a szükséges humán erőforrás megtalálását tartják, ezt pedig a szükséges szaktudás és technológiai erőforrás biztosítása követi.

34. Szerveznek-e rendszeres sérülékenységvizsgálatot? Ennek a fingerprinting/reconnaissance, vagyis a teszteket megelőző információgyűjtési fázisának része-e a vállalatukról online hozzáférhető információk vizsgálata? Ha igen, hogyan kezelik az esetleges találatokat?

Arra is kíváncsiak voltunk, hogy a megkérdezett cégek szerveznek-e sérülékenységvizsgálatot. Erre többféle válasz érkezett, de általánosságban elmondható, hogy többféle információbiztonsági tesztet végeznek. Egy válaszadó úgy nyilatkozott, hogy szolgáltatásként is nyújtanak sérülékenységvizsgálatot, majd javaslatokat tesznek a megrendelőnek a feltárt kockázatok kezelését illetőleg. Ezek a javaslatok minden partner esetében vállalatspecifikusak, a kockázat

mértékéhez igazodnak. Náluk *social engineering auditra, social media reconra, rubber duckyra* (billentyűzetet emuláló pendrive), illetve *phishingre* is lehetőség nyílik. A kitöltők közül volt, aki *black box* jellegű sérülékenységvizsgálatot szokott kérni, azonban a rendszerelemzések mindig célzottak, sosem általános behatolási kísérletek. Egy válaszadó nyílt forrású információgyűjtést is végez, amelynek eredményeit a vállalat későbbi vizsgálatai során is felhasználják.

35. Ön szerint OSINT-támadások elleni védelem esetén meddig tud eljutni egy támadó, azaz van-e olyan pont (és azt lehetséges-e meghatározni) a szervezetben, amelyen semmilyen esetben sem hatolhatnak át?

Összességében elmondható, hogy nem definiálható ilyen pont. A válaszadók véleménye szerint ha a munkavállalók betartják az előírásokat, akkor nem juthat be a támadó, valószínűleg elakad vagy felderítik.

36. A szervezetre irányuló, felderítő célú OSINT-tevékenységek naplózási adatait elemzik-e?

37. Védekezés és támadás tekintetében használnak AI-alapú módszert, vagy van-e tervben ilyesmi alkalmazása a jövőben?

38. Foglalkoznak-e nyílt információgyűjtésre alkalmas szoftver fejlesztésével? Ha igen, mikor kezdték meg ezt, illetve milyen hatékonysággal működik?

A megkérdezettek közül csak egyetlenegynek vannak információi a szervezetre irányuló, felderítő célú OSINT-tevékenység naplózásáról. Továbbá védekezés és támadás esetén nem használnak AI-alapú technológiát, és nem is foglalkoznak nyílt forrású információgyűjtésre alkalmas szoftver fejlesztésével.

39. Rendelkezik-e a terület valamilyen szabályozással? Van-e eljárásrend releváns találat esetén esemény eszkalálására?

A megkérdezetteknél nincs ilyen, vagy nem foglalkoznak esemény eszkalálásával kapcsolatos eljárásrenddel. Egy válaszadó említette az információbiztonsági szabályzatot, amelyben szerepel eszkalációs rend, azonban nyílt forrású információgyűjtésre vonatkozót nem tartalmaz.

40. Milyen jogi akadályokba ütköznek, amelyek a hatékony és szükséges információgyűjtést gátolják?

41. Ön szerint milyen hazai és/vagy nemzetközi jogi szabályozásra vagy változtatásra lenne szükség?

Az interjú során kitértünk a nyílt forrású hírszerzés jogi korlátaira is. Ilyeneket nem azonosítottak a vállalatok, azonban egy megkérdezett pont a normatív eszközök hiányát említette mint legnagyobb akadályt. A kitöltők szerint szükség lenne egy hazai és/vagy nemzetközi szabályozásra, amely meghatározza az OSINT-tevékenység kereteit és határait, főleg az internet mint információforrás tekintetében. Itt ugyancsak fontos a nagyobb közösségi oldalak és keresőmotorok (például Facebook, Google, Twitter, Instagram) részletesebb szabályozása.

42. Hogyan értékeli szervezete OSINT-képességét (1–10-es skálán, ahol az 1-es a leggyengébb, a 10-es a legjobb)?

Erre a kérdésre eltérő válaszokat kaptunk. Az egyik megkérdezett 2-esre értékelte magukat, mert a szervezetükben maximum egy terület végez ilyen jellegű tevékenységet.

43. Önnek milyen javaslatai lennének szervezete OSINT-fejlesztésére?

Végezetül pedig kíváncsiak voltunk, milyen ötleteik vannak arra, hogy szervezetük OSINT-tevékenységét javítsák. Egy válaszadó szerint ezt célszerű lenne a központi biztonsági terület által meghatározott és végrehajtott formában végezni. Egy másik egy olyan automatizált OSINT-eszköz beszerzését javasolta, amely nemcsak a biztonsági, hanem az üzleti folyamatok támogatására is alkalmas (például üzleti hírszerzés).

4.2. Javaslatok

Az interjúk alapján javasoljuk a felhasználói jogosultságokkal és felelősségi körökkel arányos oktatás és a biztonságtudatosság fenntartását, valamint a közösségi média megfelelő használatának e tananyagokba való integrálását. Azért tartjuk fontosnak az optimális közösségimédia-használat oktatását,

hogy a vállalatok a lehető legkevesebbre csökkentsék az interneten fellelhető olyan információk számát, amelyeket a támadók felhasználhatnak egy későbbi adathalász-kísérletre vagy a cég hírnevének károsítására.

Tanácsoljuk továbbá az automatizált eszközök bevezetését, valamint a jelenleg használt keresőmotorok kibővítését, a kutatásunk során korábban említett programok alkalmazását. Például ajánljuk az OSINT Framework használatát, amely az ingyenes eszközökből vagy forrásokból történő információgyűjtésre összpontosít. A célja az, hogy segítsen az embereknek megtalálni az ingyenes nyílt információs forrásokat. Előfordulhat, hogy egyes webhelyek regisztrációt igényelnek, vagy további adatokat kínálnak magas áron, azonban a keretrendszer segítségével a vállalatok képesek lehetnek arra, hogy a rendelkezésre álló információk legalább egy részét hatékonyan és díjmentesen szerezzék be. Javasoljuk továbbá a Shodan platform használatát, amely révén nemcsak az ismert hálózat figyelhető meg, hanem hálózati eszközök megtalálására is alkalmas az interneten. Észlelheti az adatszivárgásokat a felhőben, adathalászwebhelyeket detektálhat, és veszélyeztetett adatbázisokat tárhat fel, ami elősegíti a vállalatok hírnevének védelmét, valamint lehetőséget biztosít az internethez csatlakoztatott összes eszköz megfigyelésére. Természetesen a listáról nem maradhat le a Paterva fejlesztette Maltego sem, amely mára már a Kali Linux – sérülékenységvizsgálatokra, külső és belső hálózati betöréstesztekre és biztonsági auditokra fejlesztett operációs rendszer – beépített eszközévé vált, de Windows operációs rendszerre is elérhető. A Maltego számos beépített transzformáció lefuttatásával segít jelentős és átfogó felderítést végezni (valamint lehetővé teszi egyedi módosítások implementálását is). Van egy úgynevezett *community,* azaz közösségi verziója, amelynek használata ingyenes, de funkcióiban korlátozott a fizetős verzióhoz képest.

Az előbb említett két pont mellett fontosnak tartjuk az információgyűjtés formalizálását, dokumentálását egy kidolgozott szabályzat elkészítésével, amely tartalmazza a folyamat lépéseit, hatályát, alkalmazott és releváns jogszabályi környezetét, valamint a vállalatok által használt módszertanokat és eszköztárat. Végezetül pedig javasoljuk az I-Intelligence-től az *Open Source Intelligence Tools and Resources Handbook 2020,* valamint Heather J. Williams és Ilana Blum *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* című tanulmányának feldolgozását az OSINT-képességek fejlesztése és fontosságának megértése érdekében.

Felhasznált irodalom

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

Barnea, Avner (2019): Big Data and Counterintelligence in Western Countries. *International Journal of Intelligence and CounterIntelligence,* 32(3), 433–447. Online: https://doi.org/10.1080/08850607.2019.1605804

Bello-Orgaz, Gema – Jung, Jason J. – Camacho, David (2016): Social Big Data: Recent Achievements and New Challenges. *Information Fusion,* 28, 45–59. Online: https://doi.org/10.1016/j.inffus.2015.08.005

Bergman, Michael K. (2001): White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing,* 7(1). Online: https://doi.org/10.3998/3336451.0007.104

Day, Tony – Gibson, Helen – Ramwell, Steve (2016): Fusion of OSINT and Non-OSINT Data. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser (szerk.): *Open Source Intelligence Investigation. From Strategy to Implementation.* Cham: Springer, 133–152. Online: https://doi.org/10.1007/978-3-319-47671-1_9

Deák Veronika (2018): A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során. *Hadmérnök,* 13(3), 391–402.

Fleisher, Craig S. (2008): Using Open Source Data in Developing Competitive and Market Intelligence. *European Journal of Marketing,* 42(7–8), 852–866. Online: https://doi.org/10.1108/03090560810877196

Gandomi, Amir – Haider, Murtaza (2015): Beyond the Hype: Big Data Concepts, Methods, and Analytics. *International Journal of Information Management,* 35(2), 137–144. Online: https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gong, Seonghyeon – Cho, Jaeik – Lee, Changhoon (2018): A Reliability Comparison Method for OSINT Validity Analysis. *IEEE Transactions on Industrial Informatics,* 14(12), 5428–5435. Online: https://doi.org/10.1109/TII.2018.2857213

Információs Hivatal: *A hírszerzés forrásai.* Online: www.mkih.hu/a-hirszerzes-forrasai.html

Kalpakis, George – Tsikrika, Theodora – Cunningham, Neil – Iliou, Christos – Vrochidis, Stefanos – Middleton, Jonathan – Kompatsiaris, Ioannis (2016): OSINT and the Dark Web. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser (szerk.): *Open Source Intelligence Investigation. From Strategy to Implementation.* Cham: Springer, 111–132. Online: https://doi.org/10.1007/978-3-319-47671-1_8

Kandias, Miltiadis – Mitrou, Lilian – Stavrou, Vasilis – Gritzalis, Dimitris (2013): Which Side Are You On? A New Panopticon vs. Privacy. In *Proceedings of the*

10th International Conference on Security and Cryptography (SECRYPT). Setúbal: SciTePress, 98–110. Online: https://doi.org/10.5220/0004516500980110

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

Li, Yaliang – Gao, Jing – Meng, Chuishi – Li, Qi – Su, Lu – Zhao, Bo – Fan, Wei – Han, Jiawei (2015): A Survey on Truth Discovery. *ACM SIGKDD Explorations Newsletter,* 17(2), 1–16. Online: https://doi.org/10.1145/2897350.2897352

Liu, Bing – Zhang, Lei (2012): A Survey of Opinion Mining and Sentiment Analysis. In Aggarwal, Charu C. – Zhai, ChengXiang (szerk.): *Mining Text Data.* Boston: Springer, 415–463.

Mármol, Félix Gómez – Pérez, Manuel Gil – Pérez, Gregorio Martínez (2014): Reporting Offensive Content in Social Networks: Toward a Reputation-Based Assessment Approach. *IEEE Internet Computing,* 18(2), 32–40. Online: http://dx.doi.org/10.1109/MIC.2013.132

Nanda, Susanta – Chiueh, Tzi-cker (2005): *A Survey on Virtualization Technologies.* Online: www.computing.dcu.ie/~ray/teaching/CA485/notes/survey_virtualization_technologies.pdf

NATO: *NATO Open Source Intelligence Handbook* (2001): Norfolk: [k. n.]. Online: https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up

Noubours, Sandra – Pritzkau, Albert – Schade, Ulrich (2013): NLP as an Essential Ingredient of Effective OSINT Frameworks. In *2013 Military Communications and Information Systems Conference (MCC 2013).* Piscataway: IEEE, 1–7.

Ranade, Priyanka – Mittal, Sudip – Joshi, Anupam – Joshi, Karuna (2018): Using Deep Neural Networks to Translate Multi-Lingual Threat Intelligence. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI 2018).* [H. n.]: IEEE, 238–243. Online: https://doi.org/10.1109/ISI.2018.8587374

Shere, Anjuli R. K. (2020): Now You [Don't] See Me: How Have New Legislation and Changing Public Awareness of the UK Surveillance State Impacted OSINT Investigations? *Journal of Cyber Policy,* 5(3), 429–448. Online: https://doi.org/10.1080/23738871.2020.1832129

Solti István (2019): Az OSINT információgyűjtő eszközeiről. *Nemzetbiztonsági Szemle,* 7(2), 3–18.

Stieglitz, Stefan – Mirbabaie, Milad – Ross, Björn – Neuberger, Christoph (2018): Social Media Analytics – Challenges in Topic Discovery, Data Collection, and Data Preparation. *International Journal of Information Management,* 39, 156–168. Online: https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Vopham, Trang – Hart, Jaime E. – Laden, Francine – Chiang, Yao-Yi (2018): Emerging Trends in Geospatial Artificial Intelligence (GeoAI): Potential Applications for Environmental Epidemiology. *Environmental Health,* 17(1). Online: https://doi.org/10.1186/s12940-018-0386-x

Wong, B. L. William (2016): Fluidity and Rigour: Addressing the Design Considerations for OSINT Tools and Processes. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser (szerk.): *Open Source Intelligence Investigation. From Strategy to Implementation.* Cham: Springer, 167–185. Online: https://doi.org/10.1007/978-3-319-47671-1_11

Zago, Mattia – Nespoli, Pantaleone – Papamartzivanos, Dimitrios – Pérez, Manuel Gil – Mármol, Félix Gómez – Kambourakis, Georgios – Pérez, Gregorio Martínez (2019): Screening Out Social Bots Interference: Are There Any Silver Bullets? *IEEE Communications Magazine,* 57(8), 98–104. Online: https://doi.org/10.1109/MCOM.2019.1800520

Jogszabályok

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

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Magyarország Alaptörvénye

Ajánlott irodalom

Bielska, Aleksandra – Kurz, Noa Rebecca – Baumgartner, Yves – Benetis, Vytenis (2020): *Open Source Intelligence Tools and Resources Handbook.* [H. n.]: I-intelligence. Online: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

Burns, Matt (2020): Open Source Intelligence: What Social Media Can Tell Us. *CameraForensics,* 2020. február 14. Online: www.cameraforensics.com/blog/2020/02/14/open-source-intelligence-what-social-media-can-tell-us/

Echosec Systems Ltd. (2019): 5 Reasons Why Every Organization Needs an OSINT Team. *Flashpoint,* 2019. május 31. Online: www.echosec.net/blog/-5-reasons-why-every-organization-needs-an-osint-team

g0tmi1k (2021): *What is Kali Linux?* Online: www.kali.org/docs/introduction/what-is-kali-linux

Mckay, Dave (2020): How to Use OSINT to Protect Your Organization. *How-To Geek,* 2020. november 27. Online: www.cloudsavvyit.com/8214/how-to-use-osint-to-protect-your-organization/

Social Media and Cybersecurity – Navigating the risks. *Sophos Home,* 2020. november 5. Online: https://home.sophos.com/en-us/security-news/2020/social-media-and-cybersecurity.aspx

What is a Digital Footprint? *Netsafe,* 2021. április 22. Online: www.netsafe.org.nz/digital-footprint/

Williams, Heather J. – Blum, Ilana (2018): *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* Santa Monica: RAND Corporation.

Vákát

Melléklet

A vizsgálat során feltett interjúkérdések

Az alábbiakban ismertetjük azokat a kérdéseket, amelyek alapján a Nemzeti Közszolgálati Egyetem hallgatói elkészítették az interjúkat, továbbá meghatározták a tudatossági és készségi eredményeket a megkérdezett vállalaton belül. A kérdések négy fő témakör köré összpontosultak, ezek az általános ismeretek, a kapacitás felmérése, az OSINT-tevékenységek típusai és a javaslatok.

Az interjúkérdések a következők voltak:

1. *Hogyan definiálja az OSINT-ot?*

2. *Véleménye szerint az OSINT a szervezetére nézve inkább lehetőség vagy kockázat?*

3. *Milyen, az OSINT-tal kapcsolatos normatív szabályzókat ismer?*

4. *Végeznek-e nyílt forrású információgyűjtést?*

5. *Ha nem végeznek, akkor szeretnének-e kialakítani ilyen képességet?*

6. *Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:*
   a) *szükséges technológiai erőforrás beszerzése;*
   b) *szükséges humán erőforrás biztosítása;*
   c) *szükséges szaktudás biztosítása?*

7. *Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?*

8. *Ha végeznek nyílt forrású információgyűjtést, annak lépései mennyire dokumentáltak?*

9. *Milyen felületeken, platformokon végeznek nyílt forrású információgyűjtést?*

10. *Külön rendszeren végzik a nyílt forrású információgyűjtést, vagy ugyanazt a rendszert használják, mint amelyet a napi munkavégzésre is?*

11. *Virtualizációt használnak?*

12. *Automatizáltan vagy manuálisan folytatnak információgyűjtést?*

13. *Amennyiben manuálisan folytatják a nyílt forrású információgyűjtést, milyen gyakorisággal teszik? Mennyi humánerőforrás-időt igényel naponta/hetente?*

14. *Milyen keresőmotort használnak jellemzően?*

15. *Használnak-e rejtett kommunikációt?*

16. *Milyen elérhető források között keresnek?*

17. *Mire keresnek jellemzően?*

18. *Melyek azok a kulcsszavak, információk, amelyek az OSINT szempontjából lényegesek a vállalata számára?*

19. *Igénybe veszik-e külső, harmadik felek (beszállítók, alvállalkozók, tanácsadók) segítségét az OSINT bármelyik állomása során?*

20. *Hogyan dolgozzák fel a találatokat? Használnak-e szabadszavas keresőt?*

21. *Hogyan és meddig tárolják az információgyűjtés során szerzett nyers adatokat?*

22. *A mobilalkalmazások adatait felhasználják-e nyílt információszerzéshez?*

23. A nyílt információgyűjtésbe bevonják-e az alkalmazottak közösségimédia-profiljait is, és ha igen, milyen mélységben?

24. Végeznek-e profilalkotást a kinyert információk alapján? Ha igen, ezt hogyan és meddig tárolják?

25. Történt-e a szervezetükben olyan információbiztonsági incidens, amelynek hátterében OSINT-tevékenység állhatott?

26. Ha igen, ezt hogyan követték vissza?

27. Az egyes incidenseket besorolják-e veszélyességi szintek szerint?

28. Milyen jogi lépéseket tettek az incidenskezelést követően?

29. Lehetséges-e Ön szerint az OSINT-ot alkalmazni a reputációs veszteségek csökkentésére?

30. Milyen megelőző intézkedéseket tesznek, hogy a vállalat működése során a dolgozókról gyűjtött adatok ne legyenek nyíltan elérhetőek?

31. Ha nem tesznek ilyen megelőző intézkedéseket, akkor szeretnének-e a jövőben ilyen képességet kialakítani?

32. Ezen képesség kialakításában mely tényezők jelentik a legfőbb kihívást az alábbiak közül:
   a) *szükséges technológiai erőforrás beszerzése;*
   b) *szükséges humán erőforrás biztosítása;*
   c) *szükséges szaktudás biztosítása?*

33. Lát-e egyéb tényezőt, amely kihívást jelenthet ezen képesség kialakításában?

34. Szerveznek-e rendszeres sérülékenységvizsgálatot? Ennek a fingerprinting/reconnaissance, vagyis a teszteket megelőző információgyűjtési fázisának

része-e a vállalatukról online hozzáférhető információk vizsgálata? Ha igen, hogyan kezelik az esetleges találatokat?

35. *Ön szerint OSINT-támadások elleni védelem esetén meddig tud eljutni egy támadó, azaz van-e olyan pont (és azt lehetséges-e meghatározni) a szervezetben, amelyen semmilyen esetben sem hatolhatnak át?*

36. *A szervezetre irányuló, felderítő célú OSINT-tevékenységek naplózási adatait elemzik-e?*

37. *Védekezés és támadás tekintetében használnak AI-alapú módszert, vagy van-e tervben ilyesmi alkalmazása a jövőben?*

38. *Foglalkoznak-e nyílt információgyűjtésre alkalmas szoftver fejlesztésével? Ha igen, mikor kezdték meg ezt, illetve milyen hatékonysággal működik?*

39. *Rendelkezik-e a terület valamilyen szabályozással? Van-e eljárásrend releváns találat esetén esemény eszkalálására?*

40. *Milyen jogi akadályokba ütköznek, amelyek a hatékony és szükséges információgyűjtést gátolják?*

41. *Ön szerint milyen hazai és/vagy nemzetközi jogi szabályozásra vagy változtatásra lenne szükség?*

42. *Hogyan értékeli szervezete OSINT-képességét (1–10-es skálán, ahol az 1-es a leggyengébb, a 10-es a legjobb)?*

43. *Önnek milyen javaslatai lennének szervezete OSINT-fejlesztésére?*