DOI: 10.38146/BSZ-AJIA.2024.v72.i12.pp2219-2240

A szürke OSINT gyanús?

The gray OSINT is suspect?

Solti István
Dr. PhD, egyetemi oktató
Nemzeti Közszolgálati Egyetem,
Rendészettudományi Kar
solti.istvan@uni-nke.hu

Absztrakt

Cél: A tanulmány célja az OSINT, vagyis a nyílt forrású hírszerzés egyes vitatottabb információgyűjtő eljárásainak vizsgálata büntetőjogi megközelítésből.
Módszertan: A tanulmány több kutatási módszer párhuzamos alkalmazásán alapszik. Több tudományág eredményeinek feldolgozásával elsősorban az elméleti-logikai kutatás eszközrendszere került alkalmazásra, e mellett különböző megközelítések elemzésére és összehasonlítására, valamint a gyakorlatban megszerzett tapasztalatokkal való összevetésre került sor.
Megállapítások: A szerző arra a következtetésre jut, hogy az OSINT egyes információszerző eljárásai törvényi felhatalmazás nélkül átléphetik azt a határt, amikor a magatartások már a bűntetőjog számára is értékelhetővé válnak. E magatartások egy része vitatott eljárási elem az OSINT-tal foglalkozó közösség életében, de a szerző olyan magatartásokat is elemez, amelyek a személyes adatok gyűjtésekor szintén büntetőjogi relevanciával bírhatnak.
Érték: A magyar büntetőjog egyes tényállási elemeinek tanulmányozásával mutat ki olyan elkövetési módokat, amik az információgyűjtés bűntetőjogi minősítését alapozhatják meg.

Kulcsszavak: OSINT, nyílt forrású hírszerzés, megfigyelés, adatgyűjtés

Abstract

Aim: The purpose of this study is to examine some of the more controversial information gathering procedures of OSINT (open source intelligence) from a criminal law perspective.

A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás: 2023. 11. 29. Átdolgozás: 2023. 12. 12. Elfogadás: 2023. 12. 14.

Methodology: The study is based on the parallel application of several research methods. Primarily, the tool system of theoretical-logical research was applied, by processing the results of several disciplines, in addition to analysing and comparing different approaches, as well as comparing them with experiences gained in practice.
Findings: The author comes to the conclusion that some information-gathering procedures of OSINT can cross the line without legal authorization, when the behaviour becomes appreciable even for criminal law. Some of these behaviours are a controversial procedural element in the life of the OSINT community, but the author also analyses behaviours that may also have criminal law relevance when collecting personal data.
Value: By studying some factual elements of the Hungarian criminal law, it shows ways of committing crimes that can be the basis for the criminal classification of information gathering.

Keywords: OSINT, Open Source Intelligence, surveillance, data collection

Bevezetés

A tanulmány címét olvasva első gondolatként jogosan merülhet fel, hogy nonszensz az abban szereplő állítás. Fogalmilag kizárt, hogy a nyílt forrású információszerző tevékenység (open source intelligence; továbbiakban: OSINT) a bűntetőjog szerint értékelhető magatartást jelentsen. Természeténél fogva nincs és nem is lehet. Az OSINT-nak pont az a meghatározott kiinduló pontja, hogy bárki által megszerezhető és szabadon kezelhető nyilvános adat megszerzésére irányul, mégpedig bárki által alkalmazható információgyűjtő eljárások keretében. Legalitását az adja, hogyha egy adat nyilvános, akkor azt bárki kezelheti külön felhatalmazás nélkül. Ha tehát valaki nyilvános adatokat gyűjt egy csokorba, akkor adatkezelési oldalról nem lehet jogszerűtlen, legyen szó személyes adatokról, különleges adatokról, vagy valamely tevékenységekre, esetleg szervezetekre vonatkozó adatokról, titkokról. Az OSINT ugyanis legalitását a nyilvános adat szabad kezelésének elvére alapozza, míg személyes adatok esetében azon jogelvre, hogy egy adott személy által történő nyilvánosságra hozatalt a személyes adatainak kezeléséhez való általános hozzájárulásának lehet tekinteni (Foulds, 2022).

A vonatkozó szakirodalom eltérő és nem teljesen koherens álláspontjait megvizsgálva azonban azt mondhatjuk, hogy nem ennyire fekete-fehér a helyzet. Az OSINT ugyanis számtalan információgyűjtési módot tekint sajátjának, kezdve

az egyszerű könyvtárlátogatástól egészen a kibertérben alkalmazott speciális keresőeljárások alkalmazásáig. Ezzel párhuzamosan számtalan adattároló platformot tekint forrásának, kezdve a nyomtatott újságtól egészen a felhőben tárolt közösségimédia-adatokig.

Mindezek következtében az OSINT sem forrás, sem eszköz oldalról nem tekinthető egységesen megítélhető tevékenységnek, ezért szükségszerű azok önálló vizsgálata. Ennek láthatjuk megjelenését például akkor, amikor a nyílt forrású információszerzést hivatásszerűen végző egyes csoportok és szervezetek között folyik egy folyamatos vita és gondolkodás az OSINT keretében végezhető információgyűjtő eljárások elfogadhatóságáról. Már számos szereplő felismerte, hogy a nyílt forrásból megszerzett adatok kezelése hasonló személyiségi jogi dilemmákat jelenthet (Mehandru & Koenig, 2019), mint akár a humán hírszerzés vagy a technikai hírszerzés során megszerzett adatok kezelése, különösen azon államok esetében, ahol ezen alapjogok védelme magas szinten áll. E mellett vitatható az is, hogy az információgyűjtés egyes eszközeinél magától értendő-e, hogy az valóban mindenki által jogszerűen alkalmazható eszköznek tekinthető.

Éppen ezért megítélésem szerint a kérdést két oldalról szükséges megközelíteni, mégpedig forrás oldalról és eszköz oldalról egyaránt. Forrás oldal esetében azt érdemes megvizsgálni, hogy melyek azok az adatkörök, amik már kikerülhetnek a „ha könnyen elérhető, akkor megszerezhető és kezelhető" nagy halmazból. Hiszen személyes adat esetében mindez csak addig lehet egyértelmű, amíg meg nem dől az adott személyes adat esetében a vélelem, miszerint egy platformon valaki által elérhetővé tett személyes adat kivétel nélkül csakis nyilvános és az érintett által nyilvánossá tett adat lehet, valamint addig, amíg a bárki által elérhető kitételen azon eljárásokat is értjük, amihez már különleges ismeretek, képességek és felhatalmazások is szükségesek.

Különösen igaz az állítás az online térre. A laikus szemlélőben az a kép alakulhat ki az adatbőség időszakában az OSINT tevékenységet hivatásszerűen végzők egyes nyilvános kijelentései alapján, hogy minden OSINT tevékenységnek tekinthető, ami az online tér bármely szegletében fellelhető adat megszerzésére irányul.

Feltételezésem szerint az általános felvetés alapján, ha az OSINT tevékenységet akár hivatásszerűen, akár csak alkalmanként folytató személyek, csoportok vagy szervezetek a legalitás előbb említett alapvető követelményeit kiterjesztik, akkor az OSINT szürke zónájába tévednek. A szürke zóna kifehérítéséhez hozzájárulhatunk például azzal, ha a büntetőjog szemüvegén keresztül vizsgáljuk meg, hogy mely tevékenységek lehetnek azok, amelyek már e zónán is kívül eshetnek, vagyis olyan információgyűjtő tevékenységek, amelyek a büntetőjog

által igazoltan nem tekinthetők legálisnak. Olyan magatartások, amik büntetőjogi relevanciával bírhatnak, amelyek esetében olyan bűncselekmények kerülhetnek látókörbe, mint például a személyes adattal visszaélés, a tiltott adatszerzés, vagy az információs rendszer vagy adat megsértése.

Hipotézisem megvizsgálásához mindenekelőtt tisztázni szükséges, hogy mit jelent az OSINT, vagyis a nyílt forrású hírszerzés, és miért beszélhetünk az OSINT szürke zónáiról. Ami az első dilemmát jelenti, hogy nem rendelkezünk pontos, valamennyi alkalmazói szféra és tevékenységi funkció számára megfelelő meghatározással. Így máshova helyezi a hangsúlyt az állami szféra, azon belül is a rendészet vagy a nemzetbiztonság, valamint megint máshova a gazdasági és magánbiztonsági terület. Ennek mentén a jelenlegi tanulmánynak nem célja az OSINT határainak kijelölése, vagy az OSINT szürke zónáinak kifehérítése, csupán arra vállalkozik, hogy az OSINT felől közelítve kutasson fel a büntetőjog szerint értékelhető magatartásokat.

Az OSINT és annak szürke zónái

Az OSINT igen széles körű szakirodalommal rendelkezik, melynek köszönhetően ezen hírszerzési mód fogalma, eszközkészlete és tevékenységének tartalma meglehetősen vitatott. A legkülönbözőbb megközelítésekkel találkozhatunk. Michel Bazzell például az OSINT eszközök rendkívül kiterjedt és gyakorlati alkalmazást bemutató könyvében egyszerű megfogalmazással él, mikor azt írja, hogy *„A nyílt forráskódú hírszerzés, amelyet gyakran OSINT néven emlegetnek, sok ember számára sok mindent jelenthet. Hivatalos definíció szerint minden olyan, nyilvánosan elérhető információból előállított hírszerzési adat, amelyet egy adott hírszerzési követelmény teljesítése céljából összegyűjtenek, felhasználnak és a megfelelő közönség számára megfelelő időben terjesztenek."* (Bazzell, 2021).

Ezzel a kérdés elméleti megalapozottságát le is zárja, majd számos ingyenes, de az általános felhasználói ismereteket jóval meghaladó informatikai szakismeretet igénylő online adatgyűjtési módszert mutat be, amiket nyíltnak minősíteni forrás oldalról talán kérdéses is lehet. Számos olyan információgyűjtő eszközt találunk a leírások között, amelyben nem egy érintett által nyilvánosságra hozott adat megszerzése, hanem mögöttes rendszer-, meta- vagy másodlagos adatok kinyerése a cél. Ilyen például egy Facebook-felhasználó rendszerben tárolt másodlagos profiladatainak a megszerzése, amely során a Facebook által egy adott felhasználó saját közösségi oldalának használatáról gyűjtött adatok kinyerése a cél. Ezek kinyeréséhez a célpont felhasználói számának ismerete szükséges,

ami egyedi azonosító és nem nyilvános adat, s már a Facebook is igyekszik elrejteni az illetéktelenek elől. Ennek begyűjtése szintén megoldható – ami már önmagában nem feltétlenül tekinthető legális tevékenységnek –, ha pedig sikerült kinyerni, akkor ennek felhasználásával alapvető rendszerismereteket igénylő eljárás útján lehet a végső sikert elérni (Bazzell, 2021).

Mind a nyilvános adat, mind pedig a legalitás kérdése több bemutatott adatszerző eszköznél visszaköszön, így például bármely másik közösségimédia-platformon folytatott adatszerzésnél, vagy a felhasználói név kinyerésénél, de említhető akár az eBay oldaláról a felhasználónév ismeretében az egyes megrendelésekhez tartozó helyadatok kinyerése is (Bazzell, 2021).

Az OSINT-ról találhatunk olyan értelmezést is, ami azt hangsúlyozza, hogy *„a tevékenység nem pusztán adott információk nyílt elérését jelenti, hanem annál sokkal szélesebb körben (például adatok célirányos gyűjtése, elemzése, felhasználása) értelmezendő. Az OSINT során egyfajta alaptételként jelenik meg, hogy – a HUMINT területtel szemben – csak nyílt forrásokból elérhető információk szerezhetők meg. A források közé sorolhatók például a közösségi oldalakon nyíltan megosztott, az egyes felhasználókhoz és a velük kapcsolatba hozható személyekhez kötött információk is, felvetve azonban számos etikai és jogi kérdéskört is.*" (Dobák & Tóth, 2021). Mint látható a hasonló szemléletet követő szerzők azt hangsúlyozzák, hogy el kell különíteni a SOCMINT (Social Media Intelligence – közösségi médiából történő információgyűjtés) tevékenységet az OSINT-tól. A SOCMINT nem hagyományos, hanem digitalizált adatokra támaszkodik, amelyek magukban foglalják a közösségi médiát, a kommunikációs metaadatokat és földrajzi hely adatokat is. A digitális adatok új formáinak gyűjtése révén, amelyek mélyen érintik a magánélet védelmét, a SOCMINT túlmutat az információszerzés egyéb formáin, új típusú tudásnak tekinthető (Donohue, 2015). A közösségimédia-tartalmak kinyerését célzó eljárásokat nem lehet az OSINT részének tekinteni, mivel a célba vett adatok nem tekinthetők nyilvánosnak és bárki által jogszerűen megszerezhetőnek (Dobák & Tóth, 2021).

Hasonló következtetéseket találhatunk az OSINT nyomozásokban betöltött szerepének alapjogok szemszögéből történő vizsgálata során. A szerzők ezesetben is általában elismerik, hogy az OSINT egy hasznos hírszerzési mód, amely nyilvánosan elérhető adatokon alapul, és nyilvános jellege miatt minden lényeges adatvédelmi aggálytól mentes információra vonatkozik. Ugyanakkor azt is hangsúlyozzák, hogy ezzel párhuzamosan a magánélethez való jogot aláásó vizsgálati módszernek is tekinthető, amely ugyan a magánéleti vonatkozásoktól mentesnek mutatja magát, mégis az eljárás keretében felhasznált információk egy része nem feltétlenül olyan információ, amelyet az emberek annyira vagy

egyáltalán nyilvánossá akarnának tenni (Hulsen, 2020). Sőt, olyan szintű megállapításra is jutottak már a kontextuális integritás elmélete alapján, miszerint az információ minden aspektusához kapcsolódik a magánélet bizonyos fogalma, ezért valódi „nyílt" források vagy „nyilvános" információk nem léteznek (Hulsen, 2020). A kontextuális integritás elmélete szerint az adatvédelmi normák öt paraméter – küldő, címzett, alany, információtípus és átviteli elv – alapján írják le az információáramlást. Mivel a magánélet megismerése egyes részadatokon keresztül történik (például egészségügy, oktatás, civil élet stb.), e paraméterek értékei a teljes környezet lételemein – az információtípusokon (vagy témák) és a szereplőkön (alanyok, feladók és címzettek) – keresztül terjednek (Nissenbaum, 2019).

Mint az előző megállapításokból is látható, a téma vizsgálatakor külön szempontként kezelendő a nyílt forrású információ (open source information; továbbiakban: OSINF) kérdésköre. Fogalmi jelentősége van, hogy az OSINF az OSINT alapját képezi, amelyet nyilvánosan elérhető, nem minősített forrásokból gyűjtenek össze. Ezek például olyan források, mint az írott médiumok, a kormányzati jelentések, a nyilvános adatok, a térképek, a tudományos oldalak, blogok, közösségi oldalak, alkalmazások és webalapú közösségek.

Újabb szempontként emelhető ki, hogy a kibertér fejlődésével rengeteg információ vált elérhetővé egyetlen egérkattintással. Ezzel párhuzamosan az online felhalmozott adatok között nagy mennyiségű személyes információt találhatunk. Az egyének rendszeresen megosztanak személyes adatokat internetes felületeken, amelyek tárolása azt követően digitális adatként történik online adatbázisokban vagy felhőben.

Márpedig, ahogy Eijkman és Weggemans megállapította, az új adattároló platformok új megközelítést igényelnek a tekintetben, hogy miként lehet ezeket a személyes adatokat biztonsági és védelmi célokra felhasználni. Sok területen az OSINF használata – például a különböző közösségi oldalak, blogok vagy alkalmazások figyelése – jelentősen növekszik. Számos állami és magán kutatóközpontot és agytrösztöt hoztak létre kizárólag azzal a céllal, hogy tanulmányozzák, koordinálják vagy új megközelítéseket dolgozzanak ki az OSINT alkalmazása területén (Eijkman & Weggemans, 2013).

Az OSINT-tal hivatásszerűen foglalkozó szervezetek körében a legalitás igazolására általánosan elfogadott értelmezés, hogy ezen hírszerzési mód „*csak azokat az információkat használja fel, amelyeket az emberek és a vállalkozások nyilvánosan közzétettek az interneten. Bár az OSINT segítségével nyomon követheti az emberek online viselkedését, ez nem megfigyelés, mert a tartalmat közzé tévő beleegyezett, hogy az információ nyilvános legyen. Ezért a nyomozók nem gyűjtenek személyes adatokat a tudtuk nélkül*." (URL1). Ezen érvelésnek

azonban van egy gyenge pontja. Egy adatot nem az minősít nyilvánosnak, hogy az az „interneten közzétett", hanem az, hogy azt az érdekelt saját maga tette közzé, ráadásul a közzététel köre és oka sem közömbös.

A fentieken túl van olyan álláspont, amely megállapítja ugyan, hogy az OSINT nem tekinthető potenciálisan káros adatgyűjtési módszernek, mivel vitathatatlanul nem sérti az emberi jogokat, viszont e mellett azt is megállapítja, hogy vannak hírszerző szolgálatok, vállalatok, szervezetek, csoportok és egyének, amik néha olyan módon használják az OSINT-t, aminek törvényessége nem teljesen egyértelmű. Ezen eljárások legalitását pedig az OSINT szürke zónájában találja meg. Ezen elmélet szerint e dilemma úgy oldható fel, ha az OSINT esetében eltekintünk a klasszikus logika alkalmazásától, és a pontos érvelés helyett a közelítő érvelés kerül előtérbe. E szerint az OSINT-nál a bináris megoldási szisztéma helyett széles átmenetre van szükség, nem lehet valamiről egyértelműen kimondani, hogy teljesen legális vagy teljesen illegális. Mivel a klasszikus logikával nem lehet meghatározni az OSINT arányait, határait és jellemzőit, a fuzzy logikát olyan részhatárok meghatározására használják, amelyeket a klasszikus logika nem képes elfogadhatóan leírni. Az OSINT használatánál éppen ezért azt kell kiemelni, hogy fontos annak felismerése, hogy ugyan az OSINT nyilvános adatok feldolgozására épül, viszont az emberi jogokat nem szabad megsérteni. A kémkedés és az OSINT közötti határ nagyon vékony lehet, ezért az OSINT tevékenységet óvatosságnak kell jellemeznie és kétszeres ellenőrzésnek megelőznie (Hribar, Podbregar & Ivanusa, 2014).

Mint már fentebb megállapítottam, az OSINT megítélésekor az OSINF mellett önálló szempontként kezelendő az adatgyűjtéshez alkalmazott legális eszközök problematikája. Valóban minden offline és online információgyűjtő módszer legális, vagy legalábbis nem teljesen illegális, amit az általános ismertetőkben megadnak? Valóban lehet a kibertérben szabadon adathalász, megtévesztő és félrevezető technikákat alkalmazni? Valóban lehet személyiséget fedve vagy fedő szervezetet létrehozva és annak révén információt gyűjteni OSINT-ra hivatkozva?

Vannak olyan nézetek, amelyek szerint igen, azonban az online és a hagyományos módszerek esetében van egy jellemző különbség. A kibertérben teljes egészében elfedhető az adatgyűjtő személye, ellenben a hagyományos adatgyűjtéssel, ahol egy élő személynek fizikai valójában, arccal, viselkedéssel, külső ismertető jegyekkel mégiscsak meg kell jelennie az információ forrásánál. Az elfedéshez pedig az internet esetében találunk számos olyan útmutató- és eszközgyűjteményt (URL2; URL3; URL4; URL5), amik az OSINT-ra hivatkozva leírásokat és kellékeket adnak például ahhoz, hogy a kereső hogyan maradhat láthatatlan és visszakövethetetlen az online térben, hogyan és milyen szempontok mellet

hozhat létre online álszemélyiséget az információ gyűjtéséhez, vagy akár ahhoz, hogyan kell hamis SMS, Facebook-, X- stb. üzeneteket létrehozni. Sőt, még az offline világban történő OSINT folytatásához is számos olyan eljárásra láthatunk leírást ezek között, amelyek az információt adó személy megtévesztésével és félrevezetésével, vagy harmadik személy közbeiktatásával valósul meg. Egy nyílt forrású hírszerzésben érdekelt szervezet a honlapján például azt emeli ki, hogy *„Ezek az OSINT eszközök több információhoz férnek hozzá, mint amennyi az átlagos keresőmotor-felhasználó számára elérhető. Az olyan keresőmotorok, mint a Google vagy a Bing, csak a Surface Webhez vagy az internet körülbelül 4%-ához férhetnek hozzá, amelyet a keresőmotorok képesek indexelni. Egyes OSINT-eszközök hozzáférhetnek a Deep Web olyan részeihez, amelyek bejelentkezés vagy fizetős szolgáltatások során érhető el. Például a Skopenow hozzáférhet a szövetségi bírósági nyilvántartásokhoz és más közösségi API-khoz, amelyekhez nehéz lehet hozzájutni. Ezenkívül számos OSINT eszköz lehetővé teszi a nyomozók számára, hogy névtelenek maradjanak keresés közben."* (URL1).

Az OSINT szürke zónáinak kitisztítására és nemzetközi szinten elfogadott jó gyakorlat kialakítására ugyan még nem került sor, viszont különböző tudományterületek és az OSINT-ot kizárólagos információgyűjtő módszerként alkalmazó egyes szervezetek (elsősorban azok, amelyek alapfeladatként az alapvető jogok védelme érdekében dolgoznak) folyamatosan foglalkoznak a problematikával, aminek eredményeképpen tudományos alapokon nyugvó válaszok is születtek már. Egyik legismertebb példája a *Berkeley Protokoll*, ami már meghatározásában is árnyaltabban fogalmaz, mikor kijelenti, hogy *„a nyílt forráskódú vizsgálatok olyan vizsgálatok, amelyek részben vagy egészben nyilvánosan elérhető információkra támaszkodnak […] a Berkeley Protokoll nem az egyes technológiákra, platformokra, szoftverekre vagy eszközökre összpontosít, hanem a mögöttes elvekre és módszertanokra. Következetesen alkalmazható, még akkor is, ha maga a technológia változik. Ezek az elvek felvázolják a hatékony nyílt forráskódú vizsgálatok lefolytatásának minimális jogi és etikai normáit."* A *Berkeley Protokoll* értelmezésében a legalitás nem magától értetődően az elérhető információból ered, hanem megítéléséhez az online térből információt gyűjtő nyomozóknak ismerniük kell azokat a jogi kereteket, amelyek között működnek. Ez magában foglalja az eljárásukra vonatkozó alkalmazandó jogrendszerek és azon joghatóságok jogi kereteinek ismeretét, amelyekben nyomozási tevékenységet folytatnak. Maga a jegyzőkönyv a nemzetközi közjog három kategóriáját külön is vizsgálja, úgymint a nemzetközi humanitárius jogot, a nemzetközi emberi jogot és a nemzetközi büntetőjogot (OHCHR & Human Rights Center, 2022).

Adatkezeléssel kapcsolatos bűncselekmények a magyar büntetőjogban

A *Berkeley Protokoll* ajánlását figyelembe véve a magyar joghatóság alá tartozó személyek, csoportok és szervezetek számára a hazai jogi környezet keretében a büntetőjog ide vonatkozó részeinek vizsgálatát kell elvégeznünk. A magyar 2012. évi C. törvény a Büntető Törvénykönyvről (továbbiakban: Btk.) számos személyes adat kezelésével és információgyűjtéssel kapcsolatos törvényi tényállást tartalmaz. Így a Btk. az emberi méltóság és egyes alapvető jogok elleni bűncselekmények között nevesíti a személyes adattal visszaélés (219. §), a magántitok megsértése (223. §), a levéltitok megsértése (224. §) bűncselekményeket. Az állam elleni bűncselekmények között az ellenség támogatását (260. §), a kémkedést (261. §), kémkedést az Európai Unió intézményei ellen (261/A §) és a szövetséges fegyveres erő ellen elkövetett kémkedést nyilvánítja büntetendőnek. A gazdálkodás rendjét sértő bűncselekmények között pedig a gazdasági titok megsértése (413. §), míg a fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények között az üzleti titok megsértése (418. §) bűncselekményeket találjuk. A tiltott adatszerzés (422. §), az információs rendszer vagy adat megsértése (423. §) és az információs rendszer védelmét biztosító technikai intézkedés kijátszása (424. §) a tiltott adatszerzés és az információs rendszer elleni bűncselekmények közé került.

Mint látható legalább 11 olyan bűncselekmény van a hatályos magyar jogrendszerben, amely összefüggésbe hozható adatkezelő tevékenységgel, legyen az valamilyen adat begyűjtése, rögzítése, tárolása, megismerése, feldolgozása vagy átadása. A megjelölt bűncselekmények közül a Btk. XXIV. fejezetben lévők esetében már megtörtént a büntetőjog szerint releváns lehetséges magatartások körének leszűkítése. Gál István László még csak nem is az OSINT szürke területeivel kapcsolatban, hanem már az általános OSINT tevékenység esetében arra az eredményre jutott, hogy elképzelhető a kémkedés bűntettének megállapítása, ha az elkövető rendszeres kapcsolatban állt egy idegen szervezettel, valamint folyamatosan küldött általa megszűrt és elemzett információkat (Gál, 2014).

A személyes adattal visszaélés vs. OSINT

A magyar jogrendszerben a személyes adatok védelméhez való jogot az Alaptörvény VI. cikk (2) bekezdése biztosítja. E jog érvényesülését az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII.

törvény (továbbiakban: Infotv.), valamint 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) szóló, az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete (továbbiakban: GDPR) biztosítja. Az általános büntetőjogi védelmet a Btk. 219. §-ában található személyes adattal visszaélés tényállás hivatott ellátni.

A törvényi tényállás keretdiszpozíció, hiszen visszautal az Infotv. és a GDPR rendelkezéseire, ezért a lehetséges elkövetési magatartások bemutatásához ezek vizsgálatát kell elvégezni.

A bűncselekmény jogi tárgya természetes személyeknek a személyes adat megismeréséhez és biztonságos kezeléséhez, őrzéséhez fűződő joga, míg elkövetési tárgya a személyes adat (Karsai, 2021). Személyes adat az „*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*."[1] Ennél az Infotv. még általánosabban fogalmaz, hiszen azt mondja, hogy személyes adat *„az érintettre vonatkozó bármely információ"*.[2] Ezen túlmenően az Infotv. meghatároz még fokozottabb védelmet igénylő[3] két kategóriát is: a különleges adatot[4] és a bűnügyi személyes adatot.[5]

A bűncselekmény elkövetője bárki lehet. Vagyis az 1/2012. évi Büntető Jogegységi Határozat megállapítása értelmében, amely jogértelmezés irányadó a GDPR hatályba lépését követően is (Karsai, 2021), bárki, aki OSINT tevékenységet folytat, legyen az akár csoport vagy szervezet tagja, amint egy beazonosítható természetes személyről[6] szerez meg rá vonatkozó adatot, akkor adatkezelőként lép fel (URL6). Az adatkezelői minősége független attól, hogy

1 GDPR 4. cikk 1. pont.
2 Infotv. 3. § 2. pont.
3 Infotv. 5. § (2), (6), (7) bekezdések; 6. § c) pontja.
4 Különleges adat: 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.
5 A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.
6 Infotv. 3. § 1. szerint az érintett.

az adatkezelést milyen jogcímen végzi, így a releváns jogszabályok adatkezelőkre vonatkozó előírásainak betartásával kell eljárnia.

Az adatkezelés meghatározását mind az Infotv., mind a GDPR megteszi. Adatkezelésnek minősül az adaton végzett bármely művelet, így például az adat gyűjtése, rendszerezése, tárolása, továbbítása, összekapcsolása, nyilvánosságra hozása stb.

Visszatérve a Btk. rendelkezéseire, az első tényállási alakzat szerint a bűncselekményt az követheti el, aki jogosulatlanul, vagy a céltól eltérően kezel személyes adatot.[7]

Ennek következtében első lépésként azt szükséges vizsgálni, hogy az OSINT tevékenységet végző adatkezelő rendelkezik-e az adatkezeléshez jogalappal. Jogalap hiányában az adatkezelés jogtalan és így tényállásszerű lesz. Az Infotv. értelmében személyes adat kezelése akkor jogszerű, ha:[8]

a) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli, vagy
b) az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges, és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, vagy
c) az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy
d) a személyes adatot az érintett kifejezetten nyilvánosságra hozta, és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

A különleges adatok kezelésének jogalapjait az Infotv. még tovább szűkíti. Különleges adat, csak az imént említett c) és d) pontban meghatározottak szerint, vagy akkor kezelhető, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében, vagy honvédelmi érdekből törvény elrendeli.

Az OSINT tevékenységet végzők esetében két olyan jogcím látható, aminek alkalmazása jellemzően kizárható. Egyrészt az OSINT tevékenység általában kizárja a b) pont lehetőségét, vagyis az érintettel meglévő jogviszony alapján

7 Btk. 219. § (1) a) pont.
8 Infotv. 5. § (1) bekezdés.

a kifejezett hozzájárulással történő adatkezelést, másrészt a c) pontra hivatkozás sem tekinthető jellemző indoknak. Így viszont az OSINT tevékenységet végzők jól elkülöníthető két kategóriába sorolhatók. Vannak olyan szervezetek – jellemzően állami szervek –, amik törvényi felhatalmazás alapján végezhetik e tevékenységet, ezen kívül viszont mindenki más a d) pontra hivatkozással szerezhet jogosultságot. Azonban a d) pont esetében több szempont további érvényesülésére van szükség a jogszerűség megállapításához, a feltételeknek együttesen kell érvényesülniük. Mégpedig az vizsgálandó, hogy az „*érintett*" a személyes adatát „*kifejezetten*" és személyesen „*nyilvánosságra hozta*". Vagyis a magyar büntetőjog hatálya alá eső személyek esetében téves az a szemlélet személyes adatok – még hangsúlyosabban a különleges adatok – gyűjtésénél, amely szerint elegendő arra hivatkozni, hogy az adatok nyilvános felületen elérhetők. Ugyanis, amennyiben az adatkezelő tisztában lehet azzal a körülmények alapján, hogy például az érintett:

- azt a személyes adatot nem hozta nyilvánosságra (például dark weben elérhető belépési adatok), vagy
- nem kifejezetten hozta nyilvánosságra (például zárt Facebook-csoportban, néhány másik személlyel bizalmasan közölte), vagy
- nem hozta nyilvánosságra, csak szolgáltatónak megadta ügyintézés végett (például lakcímet webáruházban történő vásárláskor), akkor az adatkezelés jogszerűtlen és tényállásszerű lehet.

A Btk. 219. § (1) a) pont második fordulata szerint szintén elkövetési magatartásnak tekintendő, ha valaki az adatkezelést a céltól eltérő módon végzi. A célhoz kötöttség értelmében *„csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető."*[9] A törvényi felhatalmazás alapján történő személyes adat kezelése esetében a jogszabály meghatározza az adatkezelés célját is, viszont az adatkezelés csak abban az esetben jogszerű, ha mind az adatra vonatkozóan, mind a feldolgozó számára a törvény kifejezetten lehetővé teszi (Péterfalvi & Eszteri, 2017). Így olyan személy esetében is elképzelhető az elkövetői minősítés, aki rendelkezik adatkezeléshez jogalappal, viszont a felhatalmazásának kereteit túllépi. Ennek körében elkövetési mód lehet, ha az adatgyűjtő az adatgyűjtés folytatásához rendelkezik jogalappal és az adatgyűjtés elsődlegesen célszerű, viszont más tevékenységet is folytat. Például harmadik személy számára – akár térítés ellenében, akár a nélkül – átadja az összegyűjtött személyes adatokat,

9 Infotv. 4. § (2) bekezdés.

vagy olyan típusú személyes adat gyűjtését is végzi, amelyre jogszabályi felhatalmazása egyébként nem terjed ki.

Az alap tényállás b) pontjában meghatározott mulasztásos magatartás alapértelmezetten az OSINT tevékenységet folytatóknál megítélésem szerint nem jelentkezik,[10] hiszen az OSINT információgyűjtő tevékenységet jelent. Ehhez természetesen kapcsolódnak további adatkezelési, azon belül adattárolási műveletek, viszont ez esetben már nem az OSINT mint meghatározó tevékenység okán jelentkezhet büntetőjogi felelősség.

A fent vázolt elkövetési magatartások tanúsítása önmagában még nem elegendő a bűncselekmény megállapításához, ahhoz célzat (haszonszerzés) vagy eredmény (jelentős érdeksérelem) meglétét is megköveteli a jogalkotó. Célzat esetében a bűncselekmény megvalósulásához elegendő a szándék megléte, eredmény esetében azonban a bűncselekmény csak a jelentős érdeksérelem bekövetkeztével valósul meg.

E bűncselekmény akkor célzatos, ha a magatartás haszonszerzés céljából történik, ami OSINT tevékenységet folytató személyek, csoportok és szervezetek esetében nagy valószínűséggel meg is állapítható. Az OSINT ugyanis rendszerint nem öncélú. Nem arra szolgál, hogy valaki elmondhassa magáról, hogy milyen érdekes adatokat tudott összegyűjteni, mintha bélyeg- vagy képeslapgyűjteményt mutogatna. Az OSINT többnyire valamilyen folyamatnak a kezdeti szakasza, amit követően az adatok feldolgozásra, átadásra, értékelésre és elemzésre stb. kerülnek egy tájékoztató, vagy egy döntési folyamat részeként. Vagyis az adatgyűjtésnek pont az az oka, hogy vagy közvetlenül az adatgyűjtő (például ellenérték fejében történő értékesítéssel), vagy annak megbízója számára biztosítson valamilyen kézzelfogható előnyt, például információs előnyt egy versenytárssal szemben.

Az eredmény bűncselekményi alakzata akkor valósul meg, ha az információgyűjtés jelentős érdeksérelmet okoz, ami szintén következhet az OSINT eljárás lényegéből. A magyar bírói gyakorlat a jelentős érdeksérelem megállapítását az emberi élet bármely területén bekövetkezett hátrány esetében elfogadhatónak tartja. Bekövetkezhet például azáltal, ha az érintett elveszíti munkahelyét vagy jövedelmének egy részét, ha családi állapotában nem kívánt változás áll be, de azzal is, ha környezetében való elismertsége csorbát szenved. Így például, ha egy munkahelyi felvételi eljáráskor lefolytatott OSINT során történik olyan személyes adat begyűjtése, amelyet az adott szervezet nem kezelhetne a törvény erejénél vagy a felvételi eljárás jellegénél fogva, valamint azt az érintett

10 Btk. 219.§ (1) b) az adatok biztonságát szolgáló intézkedést elmulasztja, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

sem hozta kifejezetten nyilvánosságra, és ennek eredményeként a felvételizőt hátrányos jogkövetkezmény éri, akkor a bűncselekmény megállapítható lehet. Arra tekintettel pedig, hogy az eredmény-bűncselekmények esetében a kísérlet is büntetőjogi relevanciával bír, a jelentős érdeksérelmet okozó személyes adattal visszaélés vétségének kísérlete is megállapítható lehet, ha egyébként a haszonszerzési cél hiányzik.

Fontos azonban, hogy ez a bűncselekmény csak szándékosan követhető el. Az elkövető tudatának valamennyi tényállási elemet át kell fognia. Így tudatában kell lennie jogosultsága határaival és a személyes adat jellegével. Életszerű lehet a nyilvánosan elérhető személyes adat esetében a tévedésre való hivatkozás. Vagyis arra, hogy a körülmények alapján az adatgyűjtő joggal feltételezte, hogy a személyes adatot az érintett hozta kifejezetten nyilvánosságra. Természetesen számos olyan eset elképzelhető, amikor az érvelésnek lehet alapja, azonban e tanulmány keretében is említésre került már több olyan OSINT-nak minősített eljárás, amelyek esetében ezen magyarázat indokolhatósága meglehetősen vitatható.

A haszonszerzés céljából elkövetett személyes adattal való visszaélés csak egyenes szándékkal követhető el (Btk. indoklás, 2012), vagyis ha az OSINT tevékenységet végzőnek alapvető szándéka a haszonszerzésre irányul. Viszont a jelentős érdeksérelem okozása egyenes vagy eshetőleges szándékkal is elkövethető. Ehhez nem szükséges, hogy akarata az érdeksérelem okozására is kiterjedjen, elegendő, ha látja előre az érdeksérelem bekövetkeztét, és abba bele is nyugszik.

Az eddigiek alapján azt mondhatjuk, hogy OSINT tevékenység törvényi felhatalmazás nélküli folytatásakor meglehetősen elmosódott a határvonal a jogszerű és a nem jogszerű között, hiszen könnyen előfordulhat, hogy a személyes adat minősítéséhez nem rendelkezünk megfelelő támpontokkal. Ráadásul, ha egy személyes adatot valóban nyilvánosnak tekinthetünk, és ezen alapon az OSINT keretében jogosultan begyűjthető, az nem ad felhatalmazást az adat gyűjtésén túli egyéb adatkezelői (például: adatbázisba rendezés, másodlagos nyilvánossá tétel, forgalmazás stb) magatartások folytatásához. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) számos ilyen esetben élt már a feljelentés jogával. Feljelentést tett például, amikor egyébként nyilvános személyes adatokat tematikus adatbázisba rendeztek és azt nyilvánosságra hozták, vagy amikor nagy mennyiségű összegyűjtött, ömlesztett személyes adatot hoztak forgalomba (Péterfalvi & Eszteri, 2017).

Üzleti titok megsértése vs. OSINT

A személyes adatok mellett az OSINT tevékenység másik lényeges tárgya lehet üzleti adatok gyűjtése és felhasználása, hiszen az ipari kémkedés és az üzleti hírszerzés is alapvető eszközének tekinti a nyílt forrású információszerzést. Ez esetben az OSINT tevékenység végzése elsősorban üzleti információk kezelésével történik. Az egyik üzleti hírszerzéssel is foglalkozó magyar magánnyomozói iroda megfogalmazása szerint, e tevékenység során törvényes forrásokból beszerezhető nyílt és bizalmas jellegű üzleti információk gyűjtése, feldolgozása, értékelése és elemzésé történik (URL7). *„Az információ gyűjtése elsődleges – az adott ágazat szakértői, kutatói, vásárlók, beszállítók, a konkurens vállalatok vezetői – és másodlagos – különböző adatbázisok, publikációk, szakértői és kormányzati elemzések, jelentések, ágazati hírlevelek, a versenytársak éves jelentései, vezetőik által adott interjúk, technikai és szabadalmi hírek – forrásból származó adatok beszerzésre és elemzésére irányul."* (URL8).

Bemutatkozásában maga a nyomozó iroda is megemlíti, hogy a nyílt adatok megszerzése mellett bizalmas információk megszerzésére is törekednek, viszont sem az elsődleges, sem a másodlagos források között nem sorol fel illegális területeket. E ponton azonban hangsúlyos lehet, hogy az üzleti információk köréből az üzleti titok büntetőjogi védelmet kapott. A Btk. 418. §-ában kimondja, hogy *„aki jogtalan előnyszerzés végett, vagy másnak vagyoni hátrányt okozva üzleti titkot jogosulatlanul megszerez, felhasznál, más személy részére hozzáférhetővé tesz vagy nyilvánosságra hoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."*

A törvény az üzleti titok megsértése bűncselekményét a versenytársak védelmét szolgáló tényállások közé illeszti, mivel a tisztességtelen piaci magatartások egyik leggyakoribb előfordulási formája (Btk. indoklás, 2012). Az üzleti titok a gazdasági titok körébe tartozik, fogalmát szintén másik jogszabály, az üzleti titok védelméről szóló 2018. évi LIV. törvény (továbbiakban: Ütv.) határozza meg. A hatályos rendelkezések szerint a know-how is üzleti titokként minősül.[11]

A bűncselekmény elkövetője bárki lehet. Befejezett a bűncselekmény bármely elkövetési magatartás tanúsításával, így az üzleti titok megszerzésével is. Hasonlóan az előző személyes adattal visszaélés bűncselekményéhez, ezen

11 Ütv. *„1. § (1) Üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető –, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.*
(2) Védett ismeret (know-how) az üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása."

bűncselekmény is két alakzattal rendelkezik, célzatos vagy eredmény-bűncselekményről beszélhetünk. Azonban itt az eredménynek nem érdeksérelem formájában, hanem vagyoni hátrányként kell megjelennie, ami beállhat vagyonban okozott kár vagy elmaradt vagyoni előny formájában is. Ez esetben tehát nem elegendő csupán valamilyen megítélésbéli vagy egyéb nem vagyoni hátrány bekövetkezése, viszont a szándékosság tekintetében azonos megítélés alá esik a két bűncselekmény.

Az OSINT tevékenységek szempontjából azt mondhatjuk, hogy az üzleti titok megsértése bűntettének egyes tényállási elemeit tekintve párhuzamba állítható a személyes adattal visszaélés egyes tényállási elemeivel, egyet kivéve, ami a bűncselekmény tárgya. Egyrészt az üzleti adatok szűk köre minősül üzleti titoknak, másrészt általában az üzleti adatok kezelésének és így gyűjtésének sincsenek a személyes adatokhoz mérhető jogi korlátai. A személyes adatok kezelése egészében jogalaphoz kötött és a jogosultság megállapítása több tényező egyidejű fennállása esetében lehetséges, ezért az üzleti titoknál a jogosultság kérdése is kézenfekvőbb. Üzleti információk megóvására kiadott EU irányelv szerint az üzleti titok esetében a jogosultság forrása kizárólag a titokgazda lehet, a jogosult beleegyezése vagy felhatalmazása nélkül csak jogosulatlan megszerzésről beszélhetünk.[12] Éppen ezért döntő momentum, hogy mit tekinthetünk üzleti titoknak, és meddig lesz titok a titok. A témát Sántha Ferenc egy 2019-ben született tanulmányában már részleteiben feltárta, viszont nem jutott olyan megállapításra, ami a kérdést egyértelműen megválaszolhatta volna. Ugyanis végső következtetése szerint ugyan az üzleti titok lényeges fogalmi elemei eléggé leszűkítik a lehetséges kört, viszont az üzleti titok meghatározása nem szakkérdés, hanem a bíróság feladata megállapítani, hogy a megszerzett üzleti adat az üzleti titok fogalmi kritériumainak megfelel-e vagy sem (Sántha, 2019).

Tekintettel arra, hogy az OSINT eszközrendszerének egyik meghatározó eleme az interjúkészítés, a magyar munkajogban arra is látunk példát, hogy ez mikor válhat illegális eszközé. A 2012. évi I. törvény a munka törvénykönyvéről (továbbiakban: Mt.) értelmében egy munkáltató versenytilalmi megállapodást köthet előre meghatározott munkakörökben foglalkoztatott munkavállalójával, amiben a munkavállaló – legfeljebb a munkaviszony megszűnését követő két évig – vállalja, hogy nem tanúsít olyan magatartást, amellyel munkáltatója jogos gazdasági érdekét sértené vagy veszélyeztetné.[13] A munkavállaló a megállapodás lejárta után sem nyilatkozhat szabadon, hiszen egyébként minden munkavállaló köteles a munkája során tudomására jutott üzleti titkot

12 Irányelv 4. cikk (2) bekezdés.
13 Mt. 228. § (1) bekezdés.

megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járhat.[14] Vagyis ha információszerzés érdekében valaki egy volt munkavállalót arra bír rá, hogy számára üzleti titkot kiadjon, akkor esetében a felbujtói minősítés jelenhet meg, ha pedig ezt megtévesztéssel teszi, akkor maga tanúsít tényállásszerű magatartást. Amennyiben azonban a nyilatkozó az óvatlan, és ennek köszönhetően kotyog ki üzleti titkot, és a kérdező jóhiszemű, akkor részéről nem valósul meg bűncselekmény.

Az OSINT tevékenység szempontjából feltétlenül fontos lehet az üzleti titok fogalmának utolsó fordulata, vagyis, hogy a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja. Ha ezt megteszi, akkor az OSINT – a fejezet elején említett – forrásai között az üzleti titok nem fog megjelenni, azok megszerzéséhez más, jogszerűnek nem tekinthető eszköz bevetése szükséges. Például olyan eszközök alkalmazása, amelyek büntetőjogi minősítését a tiltott adatszerzés bűntettének törvényi tényállásában találjuk meg.

Tiltott adatszerzés vs. OSINT

A tiltott adatszerzés bűntettének jogi tárgya az Alaptörvény VI. cikkében mindenki számára biztosított zavartalan magánélet védelméhez való jog, valamint a tisztességes gazdasági verseny biztosításához fűződő társadalmi érdek (Btk. indoklás, 2012). A Btk. a személyes adat és üzleti titok mellett elkövetési tárgyként a magántitkot és gazdasági titkot is felsorolja, jelen tanulmány szempontjából azonban a lehetséges elkövetési magatartásoknak, pontosabban az első bekezdés utolsó pontjában meghatározott elkövetésnek lehet relevanciája. Az a)-d) pontokban a törvény olyan tevékenységeket határoz meg,[15] amelyek kizárhatók OSINT keretében. A titkos kutatás, a helyiségmegfigyelés, a levéllenőrzés és a kommunikáció-lehallgatás mind olyan információgyűjtő módszer, amiket csak egyes állami szervek folytathatnak törvényi felhatalmazás

14 Mt. 8. § (4) bekezdés.

15 Btk. 422. § *„(1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából*
a) más lakását, ahhoz tartozó egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
b) más lakásában, ahhoz tartozó egyéb helyiségében vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával titokban megfigyeli vagy rögzíti,
c) más postai küldeményét vagy egyéb zárt küldeményét titokban felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
d) elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban kifürkészi, és az észlelteket technikai eszközzel rögzíti.”

alapján az egyes intézkedésekre feljogosító külön igazságügy miniszteri vagy bírói engedély birtokában. Ennek következtében ezen magatartások az OSINT tevékenységet hivatásszerűen folytatók körében is elismerten jogszerűtlenek (Hulsen, 2020). Alapvetően a fenti megállapítás lehetne igaz a Btk. 422. § (1) bekezdés e) pontjára is, az információs rendszereken kezelt adatok megismerésére, viszont számos példát és leírást találunk olyan OSINT eljárásokra, amik ennek ellentmondhatnak (Hribar, Podbregar & Ivanusa, 2014).

A Btk. 422. § (1) bekezdés e) pontja szerint, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából információs rendszerben kezelt adatokat titokban kifürkész, és az észlelteket technikai eszközzel rögzíti, az bűntettet követ el.

A Btk. az információs rendszer büntetőjogi fogalmát meghatározza. E szerint *„információs rendszer: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.”*[16] Más szóval minden digitális adathordozó függetlenül attól, hogy hálózatba kapcsolt vagy sem, online vagy offline, felhőtárhely szolgáltatásban vagy saját háttértáron tárolás történik-e stb. Információs rendszernek tekinthető manapság gyakorlatilag minden elektromos kütyü, ami a napi életünket körül veszi. Példálózó jelleggel néhány: bármely online nagyméretű háztartási gép (például hűtő), bármely online kisméretű háztartási gép (például robotporszívó), bármely szórakoztató elektronikai eszköz (például set-top-box), de ilyen a digitális fényképezőgép, e-book, laptop, asztali számítógép, tablet, mobil készülék, épület biztonsági berendezések, okos otthon rendszerek, adattárolók, felhőtárhelyek stb.

Mivel az információ források teljes spektrumát számba sem tudjuk venni, valamint modern világunkban az emberek jelentős része a mindennapjait a digitális térben tölti, ezért természetesnek vesszük a digitális platformokon elérhető adatok felhasználását. Sokkal magasabban van az ingerküszöb online tevékenység esetében. Ennek oka igen sokrétű lehet. Egyrészt bizonyos tevékenységeknél fel sem merül, hogy jogellenesen cselekednének, másrészt kevesebb energiaráfordítást igényel az adatok megszerzése, harmadrészt kicsi az esélye, hogy az érintett valaha is észleli, negyedrészt a magas látencia miatt rendkívül alacsony a lelepleződés és a büntetés valószínűsége.

Az információs rendszerben elkövetett tiltott adatszerzés bűncselekménye OSINT szempontú vizsgálatánál az előzőek okán két lényeges tényállási elemet tartok szükségesnek kiemelni, amelyek elkülönítik például a személyes adattal való visszaélés bűncselekményétől. Az egyik az elkövetési magatartás (kifürkészés),

16 Btk. 459. § (1) bekezdés 15. pont.

a másik pedig az elkövetés módja (titokban), míg a technikai eszközzel történő rögzítés elemzésére nem szükséges külön kitérni, mert OSINT esetében az alaptevékenységhez tartozik, hogy a megszerzett adatok rögzítésre is kerülnek.

A kifürkészés az adatgyűjtés speciális magatartása. Olyan aktív, tevőleges, tervszerű, akaratlagos és tudatos, kutató-kereső adatgyűjtő tevékenységet jelent (Btk. indoklás, 2012), ami szándékolt, előre jól körülhatárolható ismeret vagy adat megszerzése érdekében folyik. Ilyen lehet például az OSINT szürke zónái bemutatásakor említett álprofillal (álszemélyiséggel) folytatott megismerő tevékenység, ahol az adatokhoz való hozzáférésnek még csak nem is kell jogosulatlan belépéssel vagy speciális informatikai eljárás (például malware) alkalmazásával megtörténnie. Elegendő, ha az elkövető az adatok megszerzésére törekedve, a céljának elérésére alkalmas módon jár el.[17] Vagyis a kifürkészés nem egyszerű adatgyűjtő tevékenység, hanem előre meghatározott adatok megismerése érdekében folytatott tudatos adatszerzés.

A másik tényállási kitétel, hogy a magatartását titokban tegye, vagyis az érintett és környezete elől szándékoltan rejtett módon vigye véghez. Arra hozzon intézkedéseket és a tevékenységét úgy szervezze meg, hogy ő maga és adatszerzése minden illetéktelen számára észrevétlen maradjon. Az informatikai rendszerek mint az információgyűjtés platformja ennek alkalmas terepe, hiszen megfelelő informatikai ismeretek alkalmazásával valószínűbb az adatszerző személyét és tevékenységét titokban tartani, mint egyébként erre lehetőség lenne fizikai kontaktussal történő információgyűjtés esetében. A kibertérben nincs a felek között fizikai kontaktus, az adatgyűjtő nem jelenik meg fizikai valójában az érintett környezetében, ezért a személyéről sem lehet leírást adni, hanem csupán digitális lábnyomait lehet észlelni. Vagyis azt mondhatjuk, hogy akkor beszélhetünk titokban történő kifürkészésről, ha az adatszerző mind a személyét megpróbálja elrejteni (például álprofil használatával), mind pedig digitális tevékenységét igyekszik visszakövethetetlenné tenni (például virtuális gépek és hálózatok alkalmazásával).

Konklúzió

Az eddig bemutatottak alapján azt mondhatjuk, hogy az OSINT, vagyis a nyílt forrású hírszerzés egyes információszerző eljárásai bizonyos esetekben átléphetnek egy bizonyos határt, amikor a magatartások büntetőjogi értékelése már valósággá válhat. Ezen tevékenységek egy része eddig is vitatott eljárási elem

17 Lehetséges forgatókönyvek leírása (Hribar, Podbregar & Ivanusa, 2014).

volt az OSINT-tal foglalkozó közösség életében, viszont ezek mellett személyes adatok gyűjtése közepette előfordulhat olyan adat forrás alkalmazása is, ami szintén büntetőjogi relevanciával bírhat. Ezek szerint viszont nemcsak a szürke OSINT az, ahol az adatgyűjtőnek folyton résen kell lennie, hanem az általánosan elfogadott eljárások között személyes adatok gyűjtése alkalmával is érzékeny területekre lehet tévedni.

Mindez azt jelentheti, hogy ameddig valaki a számára meghatározott legális cél érdekében nyílt forrású információszerzéséhez valóban csak a nyilvánosan elérhető adatbázisokat és platformokat használja fel, illetve eszköz oldalon sem vesz igénybe megtévesztő vagy fürkésző kellékeket, addig vitathatatlanul a legalitás talaján áll.

Viszont egy személyiségprofil felállításánál már figyelemmel kell lenni arra, hogy az általa is tudottan csak látszólag nyilvános személyes adat kezelését érdemes elkerülni, hiszen ez esetben a jogosulatlan személyes adatkezelésének vétsége akár meg is állhat. Ami, ha az elkövetés tárgya különleges vagy bűnügyi személyes adat, akkor akár két évig terjedő szabadságvesztéssel is sújtható lehet.

Súlyosabb megítélés alá eshet, ha az információgyűjtő tevékenységét titkoltan, előre meghatározott valamilyen személyes adat, magántitok körébe eső adat, gazdasági vagy üzleti titoknak minősülő adat felkutatása érdekében fejti ki az elkövető, és a kutatása során már nyilvánosnak nem tekinthető adatbázis területeket is felkutat és áttekint, vagy az információ megszerzése érdekében az adatot szolgáltató felé megtévesztő magatartást tanúsít. Vagyis, ha nem a „mindent begyűjtünk, amit csak a témában találunk", hanem a „nekem az az infó kell, mindegy honnan" mentalitás működik, akkor a legálistól való eltérésnek is nagyobb az esélye.

Felhasznált irodalom

Bazzell, M. (2021). *Open Source Intelligence Techniques: Resources for searching and analyzing online information, Eighth Edition*.

Dobák I. & Tóth T. (2020). Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle, 69*(2), 195–212. https://doi.org/10.38146/BSZ.2021.2.2

Donohue, L. (2015). The Dawn of Social Intelligence (SOCINT), *Drake Law Review, 63*(1061).

Eijkman, Q. & Weggemans, D. (2013). Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights, 23*(4), 285–296. https://doi.org/10.1163/18750230-99900033

Foulds, R. (2022). *Open Source Investigations: Legal Accountability and Ethical Labyrinths in the Dawn of a New Era of International Justice*. Berkeley Political Review.

Gál I. L. (2014). Az OSINT (Open Source Intelligence) mint a kémkedés lehetséges elkövetési magatartása, *JURA, 20*(1), 57–62.

Hribar, G., Podbregar, I. & Ivanuša, T. (2014). OSINT: A "Grey Zone"? *International Journal of Intelligence and CounterIntelligence, 27*(3), 529–549. https://doi.org/10.1080/08850607.2014.900295

Hulsen, L. (2020). Open sourcing evidence from the internet- the protection of privacy in civilian criminal investigations using OSINT (Open-Source Intelligence). *Amsterdam Law Forum, 12*(2) 3–48. https://doi.org/10.37974/ALF.353

Karsai K. (Szerk.) (2021). *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*. Wolters Kluwer.

Mehandru, N. & Koenig, A. (2019). *Open source evidence and the international criminal court*. Harvard Human Rights Journal.

Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law, 20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

Péterfalvi A. & Eszteri D. (2017). A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és információszabadság Hatóság kapcsolódó gyakorlat. In Görög M., Menyhárd A. & Koltay A. (Szerk.). *A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül* (pp. 405–420). ELTE Állam- és Jogtudományi Kar.

Sántha F. (2019). Az üzleti titok büntetőjogi védelme a nemzetközi jogfejlődés tükrében. *Miskolci Jogi Szemle, (14)*1, 42–64.

UN Office of the High Commissioner for Human Rights & Human Rights Center, University of California, Berkeley (2022). *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source and Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*.

A cikkben található online hivatkozások

URL1: *8 Open Source Intelligence (OSINT) Myths.* https://www.skopenow.com/news/8-open-source-intelligence-osint-myths

URL2: *Open Source Intelligence / OSINT / I3 / III*. https://www.uk-osint.net/index.html

URL3: *Your Randomly Generated Identity*. https://www.fakenamegenerator.com/

URL4: *10 Best VPN Services 2023: Security, Features + Speed*. https://www.safetydetectives.com/best-vpns/

URL5: *OSINT Framework*. https://osintframework.com/

URL6: Kúria *1/2012. számú BJE határozat*. https://kuria-birosag.hu/hu/joghat/12012-szamu-bje-hatarozat

URL7: *Üzleti hírszerzés*. https://www.barathandpartners.hu/uzleti-hirszerzes/

URL8: *Versenypiaci hírszerzés*. https://www.barathandpartners.hu/uzleti-hirszerzes/versenypiaci-hirszerzes/

Alkalmazott jogszabály

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
2012. évi C. törvény a Büntető Törvénykönyvről
2012. évi I. törvény a munka törvénykönyvéről
2018. évi LIV. törvény az üzleti titok védelméről
Az Európai Parlament és a Tanács (EU) 2016/943 irányelve (2016. június 8.) a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, hasznosításával és felfedésével szembeni védelemről
GDPR: 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) szóló, az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete
Magyarország Alaptörvénye (2011. április 25.)

A cikk APA szabály szerinti hivatkozása

Solti I. (2024). A szürke OSINT gyanús? *Belügyi Szemle*, *72*(12), 2219–2240. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i12.pp2219-2240

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Levelező szerző

A cikk levelező szerzője Solti István, aki a solti.istvan@uni-nke.hu e-mail címen érhető el.