Prof. Dr. Gál István László*

Titkos dokumentumok kiszivárogtatása az orosz–ukrán háborúban: a minősített adatok védelméhez és a közvélemény tájékoztatásához fűződő érdek konfliktusa

1. Bevezető gondolatok

A 2022. február 24-én kirobbant orosz–ukrán háború a legnagyobb hagyományos katonai konfliktus Európában a második világháború óta. Az orosz katonai agresszió, amit Oroszországban jelenleg is tilos háborúnak[1] nevezni, eddig óvatos becslések szerint is több százezer ember életét követelte vagy testi épségét, egészségét sértette ukrán és orosz oldalon egyaránt. A katonai konfliktusban rendszeresen szivárognak ki minősített adatok, sokszor a legmagasabb minősítési szintű, szigorúan titkos anyagok is. Ezek nyilvánosságra kerülése emberéleteket is veszélyeztethet, ugyanakkor felmerül a kérdés, hogy a közvélemény tájékoztatásához fűződő érdek nem írja-e felül az államok és a nemzetközi szervezetek azon érdekét, hogy ezeket az információkat megóvják.

A konfliktus kezdete óta folyamatosan kerülnek nyilvánosságra minősített adatok orosz és nyugati oldalon is, de a mostani háborút közvetlenül megelőzően is történtek nagyobb botrányok. Edward Snowden 2013-ban az Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) megfigyelési programjával kapcsolatban minősített adatokat hozott nyilvánosságra a Guardian és a Washington Post közreműködésével.[2] 2013-ban – egy kiszivárogtatott dokumentum szerint – az amerikai NSA egy hónap alatt több mint hárommilliárd telefonhívás és e-mail adatait gyűjtötte össze, amelyek az Amerikai Egyesült Államok telekommunikációs rendszerein keresztül futottak át. A „mindent összegyűjteni" filozófiája határozza meg napjainkban is az NSA törekvéseit, egy 2012-es jelentés szerint az NSA „jóval nagyobb mennyiségű adatot gyűjt össze, mint amennyi az elemzők számára általában hasznos vagy használható".[3] A DNI[4] 2020-ban már vélhetően legalább egy nagyságrenddel több adatot dolgoz fel, feltételezhetően sokkal hatékonyabban, mint 2013-ban. Nagy tömegű adatmennyiségre „vadászik" napjainkban az orosz elhárítás is. Az FSZB[5] tevékenységében a belföldi kémelhárítás egyik módszere már egy évtized óta a viszonylag magasan fejlett, és jelentős erőket foglalkoztató totális internetfigyelés.[6]

2022-ben kezdetben csak orosz katonai titkok kerültek ki az internetre, majd 2023 áprilisában az USA-t is érintette egy rendkívül súlyos kiszivárogtatási botrány. A bűncselekmény gyanúsítottja jelenleg letartóztatásban van. „Az alapvetően számítógépes játékosok által kedvelt Discord chatszobáiban szivárogtatott titkosított hírszerzési értesüléseket Jack Teixeira, a massachussettsi Nemzeti Gárda légierejének katonája, írja a The New York Times. A lap értesülései szerint Teixeira 2022 februárjában, nem sokkal Ukrajna lerohanása után kezdett titkos dokumentumok szivárogtatásába többek között az orosz csapatok mozgásáról egy 600 fős chatszobában. Teixeirát április 13-án tartóztatták le, miután információkat tett közzé egy másik, titkos 50 fős Discord-csoportban, a Thug Shaker Centralban. A The New York Times egy másik csoporttagra hivatkozva írja, hogy ezen a fórumon 2022 októberétől osztott meg információkat. A nagyobb chatcsoporton közzétett, újonnan felfedezett információk az orosz és ukrán áldozatokról, a moszkvai kémügynökségek tevékenységéről és az Ukrajnának nyújtott segélyekről szóló híreket tartalmaztak. A felhasználó azt állította, hogy az NSA, a CIA és más hírszerző ügynökségek információit osztotta meg. A Thug Shaker Centraltól eltérően ez a nagyobb csatorna nyilvánosan elérhető volt a YouTube-on is, bárki pillanatok alatt rátalálhatott."[7]

Tanulmányomban először bemutatom a minősített adat fogalmát, majd áttekintem a konfliktusban közvetlenül vagy

* Tanszékvezető egyetemi tanár (PTE ÁJK Büntetőjogi Tanszék), egyetemi tanár (NKE HHK Katonai Nemzetbiztonsági Tanszék).

[1] A hivatalos elnevezése különleges katonai művelet Ukrajnában: специальная военная операция на Украине.

[2] Michael Geist (ed): *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Törvény, adatvédelem és megfigyelés Kanadában a Snowden utáni korszakban) University of Ottawa Press 2015. 127. o.

[3] Greenwald, Glenn: A Snowden-ügy. Korunk legnagyobb nemzetbiztonsági botránya. HVG Könyvek, Budapest, 2014. 124. és 132. o.

[4] Digital Network Intelligence (digitális hálózati hírszerzés).

[5] Federalnaja Szluzsba Bezopasznosztyi (Szövetségi Biztonsági Szolgálat), Oroszországi Föderáció.

[6] Lantos Mihály: *A bűnügyi hírszerzés története* NKE Budapest, 2012. 81. o.

[7] https://hvg.hu/vilag/20230422_Joval_nagyobb_korhoz_juthattak_el_a_Pentagonbol_kiszivargo_iratok_mint_eddig_gondoltak (2023. április 23.).

közvetve részt vevő állomok és nemzetközi szervezetek közül azoknak a minősített adatok védelmével kapcsolatos szabályozását, amelyik oldalt érintették az eddigi kiszivárogtatások. Az Oroszországi Föderáció titokvédelmi rendszerének a legfontosabb szabályait mutatom be először, majd a NATO és az Amerikai Egyesült Államok titokvédelmi rendszerét ismertetem. A tanulmány záró részében azt vizsgálom, hogy van-e létjogosultsága az ilyen kiszivárogtatásoknak, a közvélemény tájékoztatásához fűződő jog tükrében.

2. Titok, államtitok, minősített adat

Nem minden titok „államtitok", vagyis minősített adat. A titok a legtágabb értelemben az emberi természetben rejlő, az emberré válás folyamatának egy adott minőségi fokán megjelenő kategória. Titok mindaz, amelyről kizárólag egy meghatározott számú ember tud, és amelynek meghatározott ideig történő titokban maradása – értéktartalmától függetlenül – egy vagy több ember vagy a társadalom érdekében áll, és a titokban tartás érdekében a titok birtokosa a megfelelő intézkedéseket megtette. Ha a jog által is védett titokkal kapcsolatos titoktartást egyfajta speciális jogviszonyként vizsgáljuk, akkor ezzel kapcsolatban a következő megállapításokat tehetjük:

- mindig emberek között fennálló,
- abszolút szerkezetű jogviszony (mindenki köteles tűrni, hogy a titokgazda csak azzal ossza meg a titkot, akivel szeretné),
- mindig meghatározott időkereten belül létezik,
- a tárgya valamilyen értéket magában rejtő információ, amely jogi védelmet is igényel és egyben érdemel, valamint
- ennek az információnak az elvesztése, megsemmisülése, nyilvánosságra hozatala vagy illetéktelen személy számára történő hozzáférhetővé tétele különböző jogágak által szabályozott jogkövetkezményeket von maga után.

Az államtitok a Magyar Értelmező Kéziszótár szerint „az állam életét szorosan érintő és illetéktelenekkel szemben gondosan őrzött, nagy fontosságú adat, tény".[8] A többi titokfajta, mint például a gazdasági titok elképzelhető személyes titokként is, az államtitok egyik megkülönböztető ismérve ezzel szemben az, hogy társadalmi jellegű, közvetve vagy közvetlenül az állam biztonságára van kihatással, emiatt kizárólag személyes titokként elképzelhetetlen. „Titok az, amit az érdekelt titokban akar tartani s amit a titoktartásra köteles vagy arra kész egyének zárt körén kívül még senki sem tud. Államtitok az állam fontos érdekeit érintő titok. Nem minden hivatali titok egyúttal államtitok. A titok tárgya lehet múlt-, jelen- vagy jövőbeli tény. Az elárult és nagyobb számú illetéktelen előtt már ismertté vált tény többé nem titok."[9]

Napjainkban a magyar jogi szabályozás és a fejlett nyugati jogrendszerek is az államtitok fogalma helyett már a „minősített adat" kategóriát használják. Minősített adat a legáltalánosabb megfogalmazás szerint minden olyan információ, amely egy adott állam vagy államoknak egy csoportja valamilyen szempontból érzékenynek tekint, és amelyhez emiatt titoktartási kötelezettség kapcsolódik a nemzeti, regionális vagy akár a nemzetközi biztonsági igények alapján is. A minősített adathoz történő hozzáférést törvény vagy más jogszabály korlátozza, az ezzel való visszaélés pedig gyakran büntetőjogi szankciót is maga után vonhat. A minősített adatok kezeléséhez, illetve a minősített adatokhoz való hozzáféréshez általában személyi biztonsági tanúsítvány szükséges, ez az adott személy nemzetbiztonsági ellenőrzése után állítható ki. A minősített adatoknak jellemzően több hierarchikus szintje van minden jogrendszerben, ezek megismeréséhez legtöbbször eltérő szintű biztonsági követelmények szükségesek. Az adatok minősítési szintjének a meghatározása a minősítési eljárás keretében történik.[10] Ezek a jellemzők általában valamennyi ország szabályozásában fellelhetők, de a konkrét gyakorlat és a terminológia természetesen országonként eltérő. Ahhoz, hogy napjainkban egy titokfajta minősített adatnak legyen minősíthető, kell:

- létezik legalább egy minősítéssel védhető közérdek, és az eljárás során a minősítő megbizonyosodott arról, hogy az adott adattal való visszaélés a minősítéssel védhető közérdeket közvetlenül sérti vagy veszélyezteti,
- minősítésre jogosult személy által lefolytatott,
- formai követelményeknek mindenben megfelelő minősítési eljárás,
- amely meghatározott időtartamra minősíti az adatot.[11]

A minősített adatok megjelenési formái is különbözőek lehetnek a gyakorlatban:

- adathordozón rögzített, illetve továbbított minősített adat;
- írásos formában megjelenő információ, minősített adat;
- minősített adatot hordozó objektum, tárgy vagy technikai eszköz;
- nem tárgyiasult formában megjelenített minősített adat, eljárási mód vagy ismeretanyag;
- végül létezik szóban közölt minősített adat is.[12]

Elit Nikolov szerint a titok birtoklója és a titokkutató két ellentétes pozíció. A titokkutató, vagyis a titok megismerésére törekvő személy vagy szervezet pozíciója a megismerő pozíció. Őt a határozatlanság két foka jellemzi: az első az, hogy létezik-e egyáltalán a titok (először ezt a feltételezést igyekszik igazolni vagy megcáfolni), a második pedig a titok tartamára vonatkozik. Ha a titokkutató túl van a határozatlanság első fokán, akkor az erőfeszítései azonnal a titoknak nevezett jelenség lehetőleg minél több ismérvének minél rövidebb időn belüli megismerésére irányulnak. Ha a titokkutató túl van a határozatlanság első fokán, vagyis tudomást szerez egy meghatározott titok létezéséről, akkor a titok birtoklója és a titokkutató közti játszma során mindkét fél a szó szoros értelmében ellenfélként lép fel egymással szemben. Innentől ők ugyanazon

[8] https://www.arcanum.hu/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/a-a-1BFAF/allamtitok-1D1DD/ (2020. 07. 15.).

[9] Angyal Pál – Isaák Gyula: *A Kihágási Büntető Törvénykönyv,* Budapest, 1941. 627. oldal.

[10] https://www.definitions.net/definition/classified+information (2020.04.21.).

[11] Szőke Gergely László: Gondolatok a hazai titokvédelmi szabályozás rendszeréről. *JURA* 2018/2. 253. o.

[12] Kuris Zoltán – Pándi Erik: Komplex információbiztonság megvalósítási lehetőségeinek megközelítése, *Hadmérnök* 2009. 2. szám 312. o.

játszma szereplői, és a játszmához való képességüktől fog alakulni annak kimenetele.[13]

3. Titokvédelem az Oroszországi Föderációban

Oroszország a Szovjetunió felbomlását követően igyekezett az új geopolitikai, geostratégiai helyzethez alkalmazkodni. A hatalmi viszonyokban ekkorra viszont már nagymértékű eltolódás következett be. A hidegháborút valójában gazdasági területen elveszítő Szovjetunió lemaradását öröklő Oroszországi Föderáció nem volt képes kompenzálni ezt a hátrányt.[14]

Az államhatalmi gépezet működésének több szegmense, például a minősített adatokra vonatkozó jogi szabályozás Oroszországban nem sokat változott a Szovjetunió összeomlása után. A szovjet korszakban „Különösen fontos! Szigorúan titkos!" minősítési jelöléssel államtitkokat tartalmazó minősített adatokat látnak el. A „Titkos" minősítési szint olyan esetekben volt alkalmazandó, amikor a minősített adat nem tartalmaz ugyan államtitkot, de a minősítő döntése alapján bizalmas információkat rejt. A „belső használatra" minősítési jelölést akkor alkalmazták, ha az adott dokumentumok, publikációk, rendeletek vagy utasítások stb. nyilvánosságra kerülése államvédelmi érdekeket sértene, ezért sajtóban, rádióban stb. publikálásuk vagy egyéb módon történő nyilvánosságra hozataluk tilos.[15]

A jelenlegi orosz minősítési szintek[16] a következők:

1. ОВ (Совершенно секретно / особой важности, vagy röviden Особой важности) – „Szigorúan titkos / Különösen Fontos", egyenértékű a Szigorúan Titkos minősítéssel,
2. СС (Совершенно секретно) „Szigorúan titkos", ez a Titkos minősítési szintnek felel meg a mi fogalmaink szerint,
3. С (Секретно) „Titkos", ez a mi Bizalmas minősítési szintünknek felel meg,
4. ДСП (Для служебного пользования) „Csak hivatalos használatra" ez elvileg a Korlátozott terjesztésű minősítési szintnek felelne meg, de az orosz szabályozás szerint ez már nem minősített adat.[17]

Vagyis az orosz szabályozás ténylegesen csak három minősítési szintet használ a gyakorlatban, ugyanúgy, mint a szovjet elődje vagy a jelenlegi brit minősítési rendszer. Oroszországban a minősített adatokkal kapcsolatos jogi szabályozás az államtitokról szóló, 1993. évi 5485-1. számú törvényben található, amelyet 2018. július 29-én módosítottak. A törvény viszonylag rövid, a részletszabályokat alacsonyabb szintű jogszabályok és belső utasítások tartalmazzák. A minősített adat (vagyis az orosz terminológia szerint az államtitok) fogalmát a törvény a következőképpen definiálja a 2. §-ban: államtitok az állam által védett minden olyan adat, amely az állam katonai, külpolitikai, gazdasági, kutatási, felderítési vagy elhárítási tevékenységével kapcsolatos, és a nyilvánosságra hozatala káros lehet az Oroszországi Föderáció biztonságára.

A törvény 20. §-a tartalmazza azon szervek felsorolását, amelyeknek a feladata az államtitok védelme. Ez gyakorlatilag az államtitkok védelmével foglalkozó tárcaközi bizottság mellett az összes bűnüldöző és nemzetbiztonsági szervet magában foglalja.

A minősítési jogkörrel rendelkezők száma az elmúlt évtizedben csökkent Oroszországban. Ennek oka nagy valószínűséggel az lehet, hogy a keletkezett minősített adatok számát is csökkenteni szeretnék, bár erre vonatkozóan sincs információnk sem az orosz minősített adatok abszolút számával kapcsolatban, sem a változás dinamikájáról nem rendelkezünk adatokkal. Ezeket az adatokat is szenzitívként kezeli tehát az orosz minősített adatvédelem. Oroszország az elmúlt években nagy figyelmet fordított a minősített adatok elektronikus biztonságára. Ebben nagy valószínűség szerint szerepet játszhatnak a Snowden által nyilvánosságra hozott amerikai minősített adatok az NSA tevékenységével kapcsolatban. 2016 végén Oroszország rendszerbe állított és élesített egy olyan katonai informatikai hálózatot, amely az internettől már teljesen függetlenül, biztonságosan működik, és az összes hozzá csatlakoztatott számítógép védett minden, biztonsági tanúsítással nem rendelkező flash meghajtótól és külső merevlemeztől. Ez a hálózat tartalmaz egy e-mail-szolgáltatást is, amely lehetővé teszi a minősített adatok továbbítását.[18]

A minősített adatok büntetőjogi védelme az Oroszországi Föderáció Büntető törvénykönyvében egyszerű, rövid, ennek ellenére hatékony szabályozási modellnek tekinthető. Négy tényállás található az államhatalom elleni bűncselekményekről szóló X. részben, a 29. fejezetben, amely „Az alkotmányos rendszer alapjai és az állambiztonság elleni bűncselekmények" címet kapta. Ezek közül az első kettő a súlyosabb tényállás, ezek a kémkedéssel kapcsolatos magatartásokat tartalmazzák, két másik bűncselekmény pedig az államtitok általános védelméről szóló rendelkezéseket foglalja magában. A kémkedéssel összefüggő bűncselekmények közül az elsőt orosz állampolgár, a másodikat külföldi vagy hontalan követheti el. Az orosz állampolgárokat szigorúbban bünteti a törvény, ha az Oroszországi Föderáció ellen kémkednek:

275. § Hazaárulás

Az az orosz állampolgár, aki hazaárulást követ el, így kü-

[13] Elit Nikolov: *A titok,* Kommunikációs Kutatóközpont Budapest, 1973. 20–25. o.

[14] Resperger István – Kaiser Ferenc – Háber Péter: Ugyanaz másképpen – az orosz geopolitika változásai a hidegháború végétől napjainkig, *Felderítő Szemle* 2015/1. 25. o.

[15] Vaszilij Mitrohin: *KGB lexikon. A szovjet titkosszolgálat kézikönyve,* Alexandra Kiadó Pécs, 2000. 198. o.

[16] https://fas.org/irp/world/russia/class.htm (2020. 08. 12.)

[17] Megjegyezzük, hogy a hatályos magyar–orosz titokvédelmi megállapodás 3. cikke a következő minősítési szinteket felelteti meg egymásnak: „A Felek, államuk törvényeinek és egyéb jogszabályainak rendelkezései alapján megállapítják, hogy a minősítés szintjei és az azoknak megfelelő jelölések megfelelnek a következőknek:

Magyarországon:	Az Oroszországi Föderációban:
„Szigorúan titkos!"	Совершенно секретно
„Titkos!"	Секретно
„Bizalmas!"	Секретно
„Korlátozott terjesztésű!"	Секретно

(2) Az orosz Fél által átadott Секретно jelölésű minősített adathordozókat a magyar Fél „Titkos!" minősítési szintűként jelöli." (2016. évi CLXXXIX. törvény a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről).

[18] https://www.oneindia.com/international/russia-completes-military-network-classified-data-exchange-2238328.html (2020. 08. 11.).

lönösen kémkedést, államtitkok nyilvánosságra hozatalát, vagy bármilyen más módon segítséget nyújt egy idegen államnak vagy külföldi szervezetnek, illetőleg azok ellenséges képviselőinek, az Oroszországi Föderáció külső biztonságát veszélyeztetve, bármilyen magatartással, 12-től 20 évig terjedő szabadságvesztéssel, és 500 ezer rubelig terjedő vagy legfeljebb háromévi jövedelemének megfelelő pénzbüntetéssel, büntetendő.

Megjegyzés: Mentesül a büntetőjogi felelősség alól az e cikkben vagy a 276. cikkben illetve a 278. cikkben meghatározott bűncselekmények elkövetője, aki az Oroszországi Föderáció érdekei további károsodását megakadályozza azáltal, hogy bűncselekményét a hatóságnak önként és kellő időben feltárja, és ezzel összefüggésben más bűncselekményt nem követett el.

276. cikk. Kémkedés

Az a külföldi vagy hontalan személy, aki átad, gyűjt, eltulajdonít, vagy idegen szervezetnek történő átadás céljából birtokol államtitoknak minősülő adatot, valamint külföldi nemzetbiztonsági szolgálat utasítására másnak átad vagy gyűjt olyan egyéb adatot, amely által kárt okoz az Oroszországi Föderációnak, tíztől húsz évig terjedő szabadságvesztéssel büntetendő.

A törvény tartalmaz egy büntethetőséget megszüntető okot mindkét esetben, aminek az a lényege, hogy nem büntethető, aki önként feltárja a bűncselekményét, mielőtt abból súlyosabb következmények származtak volna, és mindenben együttműködik az orosz bűnüldöző szervekkel és nemzetbiztonsági szolgálatokkal. Erre azonban csak akkor van lehetőség, ha a hazaárulást vagy kémkedést elkövető személy ezekkel halmazatban más bűncselekményt nem követett el.

Az államtitok megsértésével kapcsolatos két tényállás az orosz Btk. ugyanezen fejezetén belül később található meg, a 283. és 284. §-okban.

283. cikk. Államtitok nyilvánosságra hozatala

1. Az az államtitokhoz hozzáféréssel rendelkező személy, aki az árulás esetein kívül államtitkot tartalmazó információkat illetéktelen személynek átad, négytől hat hónapig terjedő elzárással vagy négy évig terjedő szabadságvesztéssel és három évig terjedő foglalkozástól eltiltással büntetendő.

2. Ha az elkövető a bűncselekményt akár szándékosan, akár gondatlanságból követi el, és az súlyos következményekkel jár, háromtól hét évig terjedő szabadságvesztéssel és három évig terjedő foglalkozástól eltiltással büntetendő.

284. cikk. Államtitkot tartalmazó dokumentumok elvesztése

Az az államtitokhoz hozzáféréssel rendelkező személy, aki gondatlanságból megsérti az államtitok kezelésének a szabályait, és államtitkot gondatlanul elveszít, ezzel súlyos következményeket okozva, három évig terjedő elzárással vagy három évig terjedő szabadságvesztéssel, valamint három évig terjedő foglalkozástól eltiltással büntetendő.

4. Titokvédelem a NATO-ban

A titokvédelemre vonatkozó külföldi szabályozási megoldások közül kiemelkedik két nemzetközi szabályrendszer, az Északatlanti Szerződés Szervezete (a továbbiakban: NATO) és az Európai Unió (a továbbiakban: EU) titokvédelmi rendszere.

A NATO csúcsszerve biztonsági kérdésekben a Biztonsági Bizottság, amelynek végrehajtó és koordináló szerve a Biztonsági Hivatal. Ez a hivatal dolgozza ki a legfontosabb biztonsági irányelveket a NATO számára, valamint a tevékenységi körébe tartozik a minősített adatok védelme, az ehhez szükséges egyes intézkedések kidolgozása, végrehajtásának koordinációja és a felügyelete is. Felügyeli mindezek mellett a személyi biztonsági ellenőrzéseket is. A NATO Európai Erőinek Főparancsnoksága (SHAPE) fenntart egy hírszerző csoportot, amelynek az egyik feladata az információk biztonságának a védelme, idetartozik a minősített adatok illetéktelen felhasználók általi megszerzésének a megakadályozása is.[19]

A titokvédelem a NATO szervezetében, annak biztonságpolitikai alapelveit is figyelembe véve (bár ez a nemzetközi szervezet nem titokvédelemként fogalmazza meg ezeket a feladatokat, hanem inkább biztonsági kérdésként) egységes irányítás alatt, sokkal szélesebb területet ölel fel, mint például a nemzeti szabályozások többsége. Többek között a NATO Biztonsági Hivatala hatáskörébe tartozik a biztonsági védelem, ezen belül többek között a látogatók fogadása, beléptetése, az adott objektum őrzésének és technikai biztonságának a feladatai, vagy például a személyi biztonsággal kapcsolatos feladatok is. A NATO Biztonsági Hivatalának a tevékenységét a NATO Biztonsági Bizottság felügyeli, illetve irányítja. Napjainkban a fizikai, az objektum-, a személy- és a dokumentumbiztonság mellett kiemelt szerepet kap az információbiztonság is. Ez további két fő területet ölel fel, a NATO-elveknek megfelelően, az első a számítógépek biztonsága, a második a kommunikációbiztonság.[20]

NATO-információnak minősül a belső szabályozás szerint minden olyan információ, amelyet a NATO készített, vagy amely a NATO számára készült, vagy valamely tagországban keletkezett olyan nemzeti információ, amelyet átadtak a NATO biztonsági rendszere számára. Ezen információk védelmét a NATO biztonsági előírásai szabályozzák, így például a Biztonság a NATO-ban [C-M(2002)49] című dokumentum, amely a legfontosabb biztonsági alapelveket, köztük a minősített adatok védelmével kapcsolatos biztonsági programokat is tartalmazza.[21]

A NATO-n belüli a minősített adatokhoz a hozzáférést az arra jogosult határozza meg, kivéve, ha az átadó a NATO részére történő átadáskor korlátozásokat írt elő ezzel kapcsolatban. A NATO négyfokozatú minősítési rendszert használ, ezek a Cosmic Top Secret (CTS – kiemelten szigorúan titkos), a NATO Secret (NS – NATO titkos), a NATO Confidential (NC – NATO Bizalmas) és a NATO Restricted (NR – NATO korlátozott terjesztésű). Létezik még ezek mellett a NATO Unclassified (NU – NATO Nem Minősített) kategória is, de az ilyen iratok átadására is kizárólag akkor kerülhet sor, ha az nem ellentétes a NATO érdekeivel. Létezik még egy speciális minősítési jelölés is, az ATOMAL. Ezt a CTS, az NS és az NC minősítési szintek után írt „A" betű jelöli. Az ATOMAL az 1954. évi Atomenergia törvény alapján az USA-ban minő-

[19] Karsai László (szerk.): Biztonság és titokvédelem a NATO szabályai szerint, Honvéd Kiadó, Budapest, 1999. 7–9. o.

[20] Mráz István: A katonai titokvédelem kérdéseiről, *Honvédségi Szemle* 1999. 1. szám 13. o.

[21] Csanádi Győző: Information Management in NATO (Part One). (Információmenedzsment a NATO-ban, első rész), *Defence Review Special Issue* 2018/1. 141. o.

sített, vagy az Egyesült Királyságban minősített azon „ATOMIC” adatoknak a minősítési jelölése, amelyeket a NATO-nak adtak át. A különböző minősítési szintekhez eltérő fokú fizikai biztonsági elemek és személyi biztonsági szint meglétének a követelménye tartozik, a differenciált védelem a záloga a magasan minősített információk tényleges védelmének a gyakorlatban.[22]

Fontos szabály, hogy a NATO minősített adatok esetében tilos a minősítés megszüntetése vagy a minősítési szint csökkentése a NATO előzetes hozzájárulása nélkül. Formai követelmény valamennyi NATO minősített adatot tartalmazó irat vagy adathordozó esetében, hogy kívül szerepelnie kell rajtuk a „THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION” (Ez a dokumentum NATO minősített adatot tartalmaz) figyelmeztető feliratnak.

A NATO tagállamai közötti hatékony és sikeres együttműködés egyik garanciája az információbiztonság. Természetes, hogy az együttműködés során érzékeny információk, minősített adatok is felhasználásra vagy megosztásra kerülnek. A katonai erő információkezeléssel kapcsolatos tevékenységét NATO- és EU-szinten is számos dokumentum szabályozza, szab szigorú feltételeket és követelményeket. A saját és a szövetséges csapatok biztonsága érdekében kiemelt fontossága van az információáramlás szabályozásának. Ezt nemcsak az együttműködő megbízhatóságáról és hitelességéről alkotott kép befolyásolja, hanem annak a módja is, ahogy az információt kezeli és továbbítja a saját rendszerében. NATO és EU minősített adat csak minősített adathordozón tárolható, illetve továbbítható, valamint kizárólag ilyen adattovábbító rendszeren kezelhető. Ha az együttműködő nem ilyen rendszeren kezeli a minősített adatot, és az esetleg kiszivárog, akkor ez káros hatással lehet a csapatok életére, a fegyelemre, a műveletek sikerére és a katonák biztonságára is.[23]

A minősített adatok biztonsága tekintetében két tényezőnek, a fizikai és a személyi biztonságnak van kiemelt jelentősége[24]:

1. A fizikai biztonság kapcsán a területi elv érvényesül a NATO szabályozásában. Eszerint minden helyiséget, területet, épületet, szobát vagy irodát, ahol minősített adatokat tárolnak vagy kezelnek, megfelelő biztonsági eszközökkel és módszerekkel védeni kell. Figyelembe kell venni ennek során a minősítés szintjét, az információ mennyiségét és formáját, a személyzet biztonsági átvilágítását, valamint a felderítő szolgálattól származó adatokat az esetlegesen feltárt veszélyekről. Az I. és II. osztályú biztonsági területeken, ahol minősített adatokat tárolnak, a ki- és beléptetést folyamatosan ellenőrizni kell, és reagáló erőt is kell alkalmazni. A minősített információk tárolására A–C kategóriájú biztonsági tárolóeszközöket kell használni, az ezeken lévő zárak is három biztonsági kategóriába sorolt eszközök lehetnek csak. Külön előírások vannak a zárakra és a számkombinációkra vonatkozóan is. Behatolásjelző készülékeket és lehallgatás elleni védelmet is alkalmazni kell. Az irodákban használt berendezéseknek át kell esniük legalább egy biztonsági bevizsgáláson.

2. A személyi biztonság tekintetében alapelv, hogy minden tagállam felel azért a személyért, akinek kiállítja a személyi biztonsági tanúsítványt (Cerificate of Security Clearence). A személyi biztonsági tanúsítvány csak érvényes, kockázati tényezőt nem tartalmazó nemzetbiztonsági ellenőrzéssel rendelkező személynek állítható ki. Minden olyan rendezvényen, ahol minősített adatok is elhangzanak, előzetesen meg kell küldeni a résztvevők igazolásait, hogy rendelkeznek megfelelő szintű betekintési jogosultsággal. Mindezek mellett a NATO rengeteg, az éberségre felhívó plakátot, videóösszeállítást, és egyéb szemléltető eszközt használ, ezek között még képernyővédők és matricák is vannak.

A NATO minősített adatokhoz történő hozzáférés, illetve azok megismerése nem az adott személy beosztásán vagy rangján múlik, nem is a személyi biztonsági tanúsítványa szintjén. A Need-to-Know (szükséges ismeret elve) a főszabály, vagyis mindenki csak azokat a minősített adatokat ismerheti meg, amelyekhez megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkezik, van rá felhasználói engedélye, és a munkavégzéséhez a minősített adat megismerése feltétlenül szükséges.

Összefoglalásképpen megalapítható, hogy a NATO minősített adatok védelmével foglalkozó rendszere a következő alapelemeket foglalja magában: fizikai biztonság, személyi biztonság, dokumentumbiztonság, eljárásbiztonság, elektronikusinformáció-biztonság (INFOSEC). Ez utóbbin belül a speciális fizikai, személyi dokumentum és eljárási követelmények, az összeköttetés biztonsága (rejtjelzés, adatátvitel, kisugárzás elleni védelem) és végül informatikai biztonság (hardver, szoftver, hálózat) a három legfontosabb részelem.[25]

Megjegyezzük, hogy a NATO nem rendelkezik saját büntetőjoggal, így a minősített adataikat támadó, adott esetben akár bűncselekménynek is minősülő magatartások elkövetőinek a felelősségre vonása az egyes tagállamok saját nemzeti büntetőjoga alapján, tagállami szinten történik. Természetesen, ha a minősített adattal visszaélés több tagállamot is érint, vagy azt nem az adott tagállam állampolgára követte el, a hatályos, nemzetközi büntetőjogi együttműködésről szóló egyezmények alapján az elkövető kiadatásának is helye lehet, ha ezt egy másik tagállam kezdeményezi. Mindezek mellett a NATO minősített adatokat a vonatkozó NATO-dokumentumok alapján generálisan az Amerikai Egyesült Államok szövetségi büntetőjoga is védi, ugyanúgy, mint az Amerikai Egyesült Államok minősített adatait. Emiatt is célszerű áttekinteni az Amerikai Egyesült Államok minősített adatokkal kapcsolatos szabályozásának egyes sarokpontjait.

5. A minősített adatok védelme az Amerikai Egyesült Államokban

Az Amerikai Egyesült Államokban számos jogszabály és végrehajtási rendelet szabályozza a minősítési eljárást. Az 1980-as években Reagan elnök kezdeményezésére egy átfogó szabá-

[22] Karsai László (szerk.): *Biztonság és titokvédelem a NATO szabályai szerint,* Honvéd Kiadó, Budapest, 1999. 7–9. o.

[23] Dobák Imre (szerk.): A nemzetbiztonság általános elmélete, NKE Nemzetbiztonsági Intézet, Budapest, 2014. 294. o.

[24] A fizikai és személyi biztonság kérdésköreit Karsai László (szerk.): *Biztonság és titokvédelem a NATO szabályai szerint,* Honvéd Kiadó, Budapest, 1999. 29–41. o. alapján foglaltam össze.

[25] Kassai Károly: *Az információvédelem rendszerszintű feladatai* (http://193.224.76.2/downloads/konyvtar/digitgy/20014/tartalom.html – 2020. 04. 30.).

lyozást alkottak meg a nemzetbiztonsági szempontból fontos információk minősítéséről és védelméről.[26] A rendelet a nemzetbiztonság fogalmát úgy határozza meg, hogy az az Amerikai Egyesült Államok nemzeti és külpolitikai érdekeinek a védelme. Három minősítési szintet határozott meg, kár alapú minősítési rendszer szerint: szigorúan titkos, titkos és bizalmas szint.[27]

George W. Bush elnök 2001. szeptember 11. előtt is hajlott az intenzív mértékű titkosításra, az utána következő években azonban ez a tendencia felerősödött. Így többek között Bush elnök felállított egy titkos katonai bíróságot szeptember 11. után, a zárt bírósági tárgyalások körét bővítette, a végrehajtó hatalom különleges jogköreit tovább szélesítette, kiszélesítette a minősített adatok védelmét a bírósági eljárásokban, megtiltotta a hozzáférést a volt elnökök irataihoz, a kongresszusi megkeresések alapján kért dokumentumok kiadását megtagadta, titokban tartotta az NSA amerikai állampolgárokkal kapcsolatos megfigyelési programját, és sok esetben újból minősített korábban már a minősítés alól feloldott iratokat. A minősített adatok száma az Amerikai Egyesült Államokban azokban az években emelkedő tendenciát mutatott: 2001-ben 8,6 millió, 2002-ben 11,3 millió, 2003-ban 14,2 millió, 2004-ben 15,6 millió minősített adat keletkezett az Amerikai Egyesült Államokban.[28] Ezt az amerikai szakértők már soknak ítélik, pedig lakosságszám-arányosan összehasonlítva a magyar adatokkal, hazánkban több mint kétszer ennyi minősített adat keletkezik évente napjainkban, 1000 lakosra vetített intenzitási viszonyszámmal számolva. Az amerikai törvényhozás viszont a saját minősített adatainak a számát is eltúlzottan soknak tartja, ezért 2010-ben törvényt adtak ki a túlzott mértékű minősítés csökkentése[29] érdekében. E törvény 2. § (3) bekezdése kimondja: „Az eltúlzott mértékű minősítés jelentős zavart okoz abban a tekintetben, hogy milyen információkat kivel lehet megosztani, emellett negatív hatást gyakorol a szövetségi kormányon belüli, valamint az egyes tagállamok és helyi szervek, továbbá a magánszektor között folyó információáramlásra is."

A minősített adat fogalmát jelenleg az Amerikai Egyesült Államokban a 2009. december 29-én hatályba lépett, Obama elnök által aláírt, és jelenleg is hatályos 13526 számú végrehajtási utasítás tartalmazza. Ez a minősített adatot olyan információként határozza meg, amelyet a nemzetbiztonsági érdekből meg kell őrizni „polgáraink, demokratikus intézményeink, hazánk biztonságának és idegen nemzetekkel való kapcsolatunk védelme érdekében".[30] Egy tankönyvi definíció szerint a minősített adat „az a hír, amely annyira érzékeny, hogy terjesztése csak azon személyek körére korlátozódhat, akik megfelelnek bizonyos speciális biztonsági követelményeknek, és akiknek a feladatuk ellátásához okvetlenül szükségük van az adott információra. Minden szervezet kialakítja a saját minősítési rendszerét, de az Egyesült Államokban a szövetségi hírszerző közösség összes ügynökségének a végrehajtási utasításokban megadott szabályokhoz kell tartania magát, amelyeket legutóbb Obama elnök hagyott jóvá."[31]

Obama elnök 2011 októberében kiadta a 13587 számú végrehajtási rendeletet, amely a „Minősített hálózatok biztonságának és a minősített információk felelősségteljes megosztásának és védelmének javítását célzó strukturális reformok"-ról szól. Ez az egész államra kiterjedő programot tartalmaz (bennfentes kockázat program), célja a belső kockázatok elhárítása, felderítése és csökkentése, ideértve a minősített adatok védelmét a jogosulatlan nyilvánosságra hozataltól, figyelembe véve a kockázati szinteket és az egyedi igényeket, az egyes ügynökségek igényeit.[32]

A minősített adatok szabályozása az Amerikai Egyesült Államokban a szövetségi kormány kizárólagos hatáskörébe tartozik. Ugyan magánszemélyeknek vagy szervezeteknek is hozzáférést lehet adni bizonyos esetekben minősített információkhoz, ezen információk viszont mindig a szövetségi kormány tulajdonát képezik a hatályos amerikai jogi szabályozás szerint. A minősítési szint a nemzetbiztonsági kockázat mértékét tükrözi: minél jelentősebb a kockázat, annál magasabb a minősítési szint.[33] A minősítési szintet az adott dokumentumon oldalanként jelölik alul és felül, de pusztán a minősítési szint szerepel a dokumentumon, a minősítő neve, beosztása és a védelmi idő nem. Lehet egy dokumentumot kisebb részekben, különböző szinteken is minősíteni, akár bekezdésenként is meg lehet jelölni az adott bekezdés vagy ábra minősítési szintjét.[34]

A minősített adatokhoz történő hozzáférés a szükséges ismeret[35] elvén alapul, vagyis egy olyan személy, akinek „Szigorúan titkos" szintű személyi biztonsági tanúsítványa van, csak olyan szigorúan titkos minősítésű adatokat ismerhet meg, amelyek a saját munkája vonatkozásában relevánsak. Ezek a korlátozások egyebek mellet azt a célt szolgálják, hogy védjék a forrásokat és a módszereket.[36]

A XXI. század első két évtizedében az Amerikai Egyesült Államokban széles körű viták tárgya az állam titkainak problémaköre. A vita egyik központi kérdése az, hogy mit kellene tenni a minősített adatokat a sajtónak kiszivárogtató állami alkalmazottakkal, akik a nyilvánosságot legtöbbször a kormányzati intézkedések kapcsán szeretnék informálni. Cselekményük jogellenes-e, alkotmányellenes-e vagy pedig adott

[26] Exec. Order No. 12,356, 3 C.F.R. 166 (1983)

[27] Bruce E. Fein: Access to Classified Information: Constitutional and Statutory Dimensions (Minősített adatokhoz való hozzáférés: Alkotmányos és törvényi dimenziók), *William and Mary Law Review* 1985 5. szám 807. o.

[28] Silver, Derigan A.: National Security and the Press: The Governments ability to Prosecute Journalists for the Possession or Publication of National Security Information (Nemzetbiztonság és sajtó: A kormányzatok újságírókkal szemben történő eljárás indítási képessége a nemzetbiztonsági információk birtoklása vagy közzététele miatt), *Communication Law and Policy* 13(4) 450. o.

[29] Reducing Over-Classification Act (A túlminősítés csökkentéséről szóló törvény) https://www.congress.gov/111/plaws/publ258/PLAW-111publ258.pdf (2020. 08. 30.).

[30] Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009); *ld. még: The President Executive Order 13526,*

[31] Jensen, Carl J. – McElreath, David H. – Graves, Melissa: *Bevezetés a hírszerzésbe,* Antall József Tudásközpont, Budapest, 2017. 205. o.

[32] Elsea, Jennifer K.: The Protection of Classified Information: The Legal Framework (A minősített adatok védelme: a jogi keretrendszer) *Congressional Research Service* 2017. május 18. 19. o.

[33] MacKay, Bruce M.: The use of classified information in terrorism trials (Minősített adatok felhasználása a terrorizmussal kapcsolatos büntetőtárgyalásokon), *Southern Illinois University Law Journal* Vol. 42, 2017. 67–68. o.)

[34] Marking Classified National Security Information as Required by Executive Order (A minősített adatok minősítési jelöléséről szóló végrehajtási utasítás), 13526, 4. January 2018.

[35] Exec. Order No. 13526 § 4.1(a), 75 Fed. Reg. 707 § 4.1(a).

[36] Rossmiller, Alex: Adjudicating Classified Information (Minősített adatok megítélése), *St. John's Law Review*, vol. 85, no. 4, 2011. 1301. o.

esetben akár lehet indokolt is, a nyilvánosság ellenőrző szerepének érvényre juttatása érdekében.[37]

A sajtószabadság azonban egy nagyon fontos korlátja a minősített adatokkal kapcsolatos szabályozás gyakorlati érvényesülésének az országban. 1971-ben az Amerikai Egyesült Államok Legfelsőbb Bírósága a híres New York Times és Társai v. Amerikai Egyesült Államok ügyben kimondta, hogy a sajtó bizonyos esetekben közzétehet minősített adatokat tartalmazó információkat is büntetlenül: ez volt a híres Pentagon Ügyiratok jogeset. A Legfelsőbb Bíróság 6:3 szavazattal elutasította a kormány álláspontját, amely szerint a vietnámi háborúval kapcsolatos 7000 minősített dokumentumot nem lett volna szabad nyilvánosságra hozni. A bíróság érvelése szerint csak a szabad sajtó képes arra, hogy a kormányzat visszaéléseit feltárja, és megakadályozza a kormányt abban, hogy félrevezesse az embereket. A tét mindenesetre nagy volt, a hatályos törvények szerint több évtized szabadságvesztés is kiszabható lett volna. Napjainkban sok olyan jogszabály és bírói döntés is született már, amelyek alapján büntetőeljárás indulhat egy újságíró ellen, aki az Amerikai Egyesült Államoknak történő károkozás szándékával publikál minősített adatokat. A legnagyobb, mértékadó újságoknak dolgozó újságírók ellen azonban – bár többször előfordult, hogy minősített adatokat tartalmazó iratokat publikáltak az elmúlt évtizedekben – eddig még nem indult egyszer sem büntetőeljárás egy 2008-ban megjelent tanulmány szerint.[38]

Egy 2019-es tanulmány megerősíti ezt a tíz évvel korábbi megállapítást: a média munkatársai ellen nem indulnak büntetőeljárások az Amerikai Egyesült Államokban, még napjainkban sem, kizárólag a minősített adatot kiszivárogtató kormányzati tisztviselők ellen. Snowden akár 30 év szabadságvesztést is kaphat majd, míg a „The Guardian" nevű újság ellen semmilyen vádat nem emeltek, pedig ők is törvényt sértettek. Ennek egyik oka a szerző szerint az lehet, hogy a sajtó speciális jogosultságokkal rendelkezik a sajtószabadság elve alapján vagy szerepe miatt, hiszen sokan ma már a negyedik hatalmi ágnak is tekintik a médiát. A második érv szerint a szivárogtatók nagyobb kárt okoznak, mint a sajtó. A szerző megállapítja, hogy a jelenlegi amerikai büntetőjogi gyakorlat következetlen: az ügyészeknek mindkettő ellen büntetőeljárást kellene indítani, vagy egyik ellen sem.[39]

Obama elnök alatt öt büntetőeljárás indult hivatalban lévő és volt kormánytisztviselők ellen nemzetbiztonsági szempontból érzékeny információk sajtóban történő nyilvánosságra hozatalával kapcsolatos törvénysértések miatt, a kémkedési törvény alapján. Az egyik ilyen ügyben nyomás alá helyeztek egy újságírót, hogy tegyen vallomást, és fedje fel az általa közzétett információk forrását. Azzal az indokkal próbálták vallomásra bírni az újságírót, hogy ő az egyetlen tanúja a bűncselekménynek, amelynek során szóban kapott minősített adatokat a forrásától, vagyis a kormányhivatalnoktól. Ez az új gyakorlat jelentősen eltér a korábbitól, és egyes szerzők álláspontja szerint veszélyezteti az amerikai polgárok azon jogát, hogy tudjanak róla, mit csinál a kormányuk.[40]

Nagyon érdekes továbbá az Amerikai Egyesült Államok vonatkozó jogi szabályozásában az a rendelkezés, amely alapján egy már nyílttá tett, a minősítés alól feloldott adat ismételt minősítésére is van lehetőség. Ezt „retroaktív minősítés"-nek vagy „visszaminősítés"-nek nevezi az amerikai szabályozás. A rendelkezés létjogosultsága korábban is aggályokat vetett fel, de az internet korában már teljesen megkérdőjelezhető, ahogy erre egy néhány évvel ezelőtt megjelent tanulmány is utal. Ha egyszer valami felkerült az internetre nyilvános anyagként, azt már szinte lehetetlen onnan eltávolítani. A rendelkezés egyetlen következménye az, hogy lehetetlenné válik az ilyen, újból minősített adatokkal kapcsolatos bármilyen nyilvános diskurzus.[41]

Az Amerikai Egyesült Államokban komoly kultúrája és szakirodalma van a titokvédelemnek, emellett nagy figyelmet fordítanak arra is, hogy tréningek során is képezzék a minősített adatokat kezelő szervezetek munkatársait. Erre jó példa az energiaügyi minisztérium egyik oktatási anyaga, melyben hangsúlyozzák, hogy a nyilvános megbeszélések során, beleértve a sajtótájékoztatókat, az előadásokat és az egyéb eseményeket, előre fel kell készülni a válaszadás módjával kapcsolatban. A „No comment" angol kifejezés az egész világban elterjedt, népszerű válasz, de a használata kerülendő, mert ezzel a válaszadó mintegy megerősíti, hogy minősített információ lehet a kérdés hátterében, sőt eldöntendő kérdés esetén egy ilyen válasszal a minősített információ tartalmára is lehet következtetni. Emiatt a következő válaszok közül egyiket sem célszerű választani:

Vannak nukleáris fegyverek az x országban? „Nem."

Van nukleáris fegyver az y országban? „Nem."

Vannak nukleáris fegyverek az x országban? „No comment."

A „No comment" helyes használata ezzel szemben a következő:

Vannak nukleáris fegyverek az x országban? „Elismerjük, hogy nukleáris fegyverek számos országban vannak vagy voltak. Nem tudok részletesebb információval szolgálni a nukleáris fegyverek helyével kapcsolatban. "

Ha pedig a minősített adat birtokában lévő személy a barátaival beszélget, akkor az oktatási anyag szerint legyen humoros, fogalmazzon homályosan, és amint lehet, váltson témát. [42]

[37] Clark, Robert: *Classified Information in the Public Sphere: An Examination of Legal Issues Surrounding the NSA Leaks* (Minősített adatok a nyilvános szférában: az NSA kiszivárogtatásokkal kapcsolatos jogi kérdések vizsgálata) (2013) 41:4 DttP: Documents to the People 7. o.

[38] Silver, Derigan A.: National Security and the Press: The Governments ability to Prosecute Journalists for the Possession or Publication of National Security Information (Nemzetbiztonság és sajtó: A kormányzatok újságírókkal szemben történő eljárásindítási képessége a nemzetbiztonsági információk birtoklása vagy közzététele miatt), *Communication Law and Policy* 13(4):447–483.)

[39] Mokrosinska, Dorota: Why Snowden and not Greenwald? On the Accountability of the Press for Unauthorized Disclosures of Classified Information (Miért Snowden és nem Greenwald? A sajtó elszámoltathatóságáról a minősített adatok jogosulatlan közzététele kapcsán, *Law and Philosophy* (2020) 39: 203–238. o.

[40] Halperin, Morton H.: *Criminal Penalties for Disclosing Classified Information to the Press in the United States* (A minősített adatok sajtóban történő nyilvánosságra hozataláért kiszabható szankciók az Amerikai Egyesült Államokban). (https://www.right2info.org/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf 2020.08 22.)

[41] Abel, Jonathan: Do you have to keep the government's secrets? Retroactively classified documents, the first amendment and the power to make secrets out of the public report (Meg kell őriznünk a kormány titkait? Visszamenőlegesen minősített adatok, az első alkotmánymódosítás és titkosítás hatalma), *University of Pennsylvania Law Review* 163, no. 4 2015 március 1038–1039. o.

[42] https://fas.org/sgp/othergov/doe/gen-16-rev2.pdf (2020. 08 15.).

A minősített adattal kapcsolatos jogsértéseket összefoglaló néven „jogosulatlan közzététel"-nek nevezi az amerikai szakirodalom. Ennek négy tipikus fajtáját különböztetik meg:

1. a minősített adat szándékos kiszivárogtatása (főleg kormányzati tisztviselők által, elsősorban a média részére),

2. a minősített adat kiáramlása (általában elektronikus adatátviteli rendszereken keresztül, szándékosan vagy gondatlanul, például egy e-mailben a nyílt adatok között minősített adatokat is elküldenek),

3. kémkedés,

4. nem megfelelő biztonsági intézkedések (ebben az esetkörben a minősített adat biztonságának a megsértése tipikusan gondatlanul történik, például valaki egy fénymásolóban felejt egy minősített adatot tartalmazó lapot).[43]

Az Amerikai Egyesült Államokban a szövetségi büntetőjog tartalmazza a legsúlyosabb, szövetségi bűncselekményeket, de a kisebb súlyú bűncselekményekre minden tagállam megalkotta a saját büntető törvénykönyvét. Mindehhez járul a katonai büntetőjog és az indián rezervátumok saját büntetőjoga is, vagyis több mint 500 büntetőjogi vonatkozású szabályrendszer van hatályban az országban, ezek áttekintése és megértése egy büntetőjoggal foglalkozó egyetemi professzor számára is szinte megoldhatatlan feladat.

A minősített adatokkal visszaélés szabályozása azonban könnyen áttekinthető, hiszen ez szövetségi bűncselekmény. Egy év szabadságvesztéssel és 1000 dollárig terjedő pénzbüntetéssel büntetendő azon szövetségi alkalmazott vagy tisztviselő, aki erre vonatkozó engedély nélkül minősített adatokat szándékosan hozzáférhetetlenné tesz. A büntetés 10 évig terjedő szabadságvesztés és legfeljebb 10 000 dollár pénzbüntetés, ha ezen alkalmazott vagy tisztviselő olyan személynek ad át szándékosan minősített adatot, aki tudomása szerint külföldi kormánynak dolgozik. Ugyanez a büntetés, ha a szövetségi alkalmazott vagy tisztviselő, vagy bárki más minősített adatot nyilvánosságra hoz, illetéktelen személy számára hozzáférhetővé tesz, illetve az Egyesült Államok által használt kódokra, rejtjelezésre és hírszerzési kommunikációra vonatkozó minősített adatokat használ fel, az Amerikai Egyesült Államoknak kárt okozva. Végül pedig 15 évig terjedő szabadságvesztéssel büntetendő a minősített adat felhasználására jogosult személy, ha szándékosan követi el a bűncselekményt, és annak eredményeként egy vagy több fedett ügynök személye is nyilvánosságra kerül. A bűncselekmény egyéb minősített esetei mind a fedett ügynökökre vonatkozó minősített adatok nyilvánosságra hozatalával kapcsolatosak, a lehetséges maximális büntetési tétel 15 év szabadságvesztés.[44]

A legutóbbi évek egyik legnagyobb botránya minősített adatokkal visszaéléssel kapcsolatban a 2016-os amerikai elnökválasztás kampányában robbant ki Amerikában. Donald Trump és Hillary Clinton egy alkalommal heves szócsatába keveredett a kampány során, amelynek tárgya azon minősített információkkal kapcsolatos állítólagos visszaélés volt, amelyeket Hillary Clinton követett el a 2016-os elnökválasztási kampány során. Hillary Clinton a CNN-nek ezt mondta a minősített adatok szabálytalan továbbításával kapcsolatban: „hiba volt, hogy a személyes e-mailemet használtam. Sajnálom." Majd később ismét reagált a témára a 2016. október 9-i elnöki vitán: „borzasztóan jó, hogy nem egy Donald Trump vérmérsékletű ember irányítja hazánkat". Donald Trump erre így válaszolt: „mert akkor már börtönben lennél".[45] Az ügyben egyébként a mai napig nem indult büntetőeljárás, ennek a körülménynek az értékelése azonban már politikai állásfoglalás is lenne.

6. Bűncselekmény vagy a közvélemény tájékoztatása?

A „kiszivárogtatás", vagyis minősített adatoknak a védelmi időn belüli nyilvánosságra hozatala a sajtóban vagy az interneten nem egyértelműen negatív vagy pozitív jelenség a szakirodalomban, sokkal inkább Janus-arcú jelenség, utalunk ezzel Földesi Tamás titokkal kapcsolatos monográfiájának a címére is.

Egyes politikai pártok, de néha kormányok is élnek a „kiszivárogtatás" eszközével, ahogy erre a szakirodalom is utal. Ilyenkor a minősített adat részleges nyilvánosságra hozatala történik, valamiféle politikai vagy személyi érdekből. A kiszivárogtató úgy hoz nyilvánosságra minősített adatot, hogy eközben ő maga rendszerint titokban marad, vagyis ilyenkor egyszerre jelentkezik a titok elárulása mellett – más vonatkozásban – a titokban maradás is.[46]

Amikor a nemzetbiztonsági érdek[47] ütközik a szólásszabadsággal, vagyis amikor a médiában minősített adatok jelennek meg, jó példa erre a Janus-arcúságra. Nem minden kiszivárogtatás káros a természeténél fogva, olyan példák is akadnak, amelyek a demokratikus eszmék előmozdítását szolgálják.[48] A „Nemzetbiztonságról, a véleménynyilvánítás szabadságáról, valamint az információhoz való hozzáférésről szóló Johannes-

[43] https://www.cdse.edu/documents/student-guides/IF130-guide.pdf (2020. 08. 12.)

[44] Elsea, Jennifer K.: The Protection of Classified Information: The Legal Framework (A minősített adatok védelme: a jogi keretrendszer), *Congressional Research Service* 2017. május 18. 14–15. o.

[45] Perkins, Larry W.: Accountability for Access to Classified Information: The United States Cannot Afford to Ignore Breaches of Confidence (A minősített adatokhoz való hozzáférés elszámoltathatósága: az Amerikai Egyesült Államok nem engedheti meg magának, hogy figyelmen kívül hagyja a bizalmasság megsértését), *Lincoln Memorial University Law Review,* vol. 5, no. 1, Fall 2017. 109–110. o.

[46] Földesi Tamás: *A Janus arcú titok. A titok titka.* Gondolat Kiadó, Budapest, 2005. 88. o.

[47] A WikiLeaks által kiszivárogtatott anyagok között találhatók komoly, titkos minősítésű katonai jelentések is, amelyeknek a nyilvánosságra kerülése komoly műveleti és információbiztonsági fenyegetést jelent az Amerikai Egyesült Államok számára. Az Amerikai Egyesült Államok hadserege kémelhárítással kapcsolatban nyomozást kezdeményezett az ügyben, mivel tartani lehetett attól, hogy a szivárogtató a védelmi minisztérium egyik munkatársa. In: Cummins, Guylyn: Classified Information Necessary to Protect National Security? Says Who? (A nemzetbiztonság védelméhez szükségesek a minősített adatok? Ki mondja?), *Communications Lawyer*, 2010. 1. szám 2. o.

[48] Xanders, Edward L.: A Handyman's Guide to Fixing National Security Leaks: An Analytical Framework for Evaluating Proposals to Curb Unauthorized Publication of Classified Information (Ezermester útmutatója a nemzetbiztonsági kiszivárogtatások kezeléséhez: elemzési keretrendszer a minősített adatok jogosulatlan közzétételének megfékezésére irányuló javaslatok értékeléséhez), *Journal of Law & Politics* 5, no. 4. 1989: 760. o.

burgi Alapelvek"[49] című ENSZ-dokumentum ezzel kapcsolatban a következőt tartalmazza, a 15. alapelvben:

„A titkos információk nyilvánosságra hozatalának általános szabálya

Senki sem büntethető nemzetbiztonsági okokból információk nyilvánosságra hozataláért, ha

(1) a nyilvánosságra hozatal nagy valószínűséggel nem sért ténylegesen semmilyen jogos nemzetbiztonsági érdekeket, vagy

(2) az információk megismeréséhez fűződő közérdek erősebb, mint a közzététellel okozott kár."

Saját álláspontom szerint ez csak nagyon szűk, nagyon kivételes körben lehet elfogadható. Általában sokkal nagyobb veszélyekkel jár(hat) a minősített adatok jogosulatlan nyilvánosságra hozatala a védelmi időn belül, mint amekkora előny származhat a közérdek tekintetében a nyilvánosságra hozatal által egy nyitott, demokratikus társadalomban. Ettől függetlenül el kell ismernünk, hogy ilyen eset előfordulhat. Erre leginkább nagy társadalmi változások, például egy politikai és gazdasági rendszerváltozás esetén lehet példákat találni. Ezzel egybevág Kassai Károly álláspontja is, szerinte az olyan vélekedések teljesen nélkülözik a szakmaiságot, amelyek szerint a jogszabályok nem gátolhatják az oknyomozó, tényfeltáró újságírók munkáját, és az újságírókat ne lenne szabad büntetőjogi felelősségre vonni, ha minősített adatot hoznak nyilvánosságra.[50]

[49] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (A nemzetbiztonság, a véleménynyilvánítás szabadsága és az információkhoz való hozzáférés Johannesburgi alapelvei) U.N. Doc. E/CN.4/1996/39 (1996).

[50] Kassai Károly: *A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere* Doktori (PhD) értekezés Budapest, 2007. 7. o.