Gál István László:

A TITOKVÉDELEM ESZKÖZEI ÉS KORLÁTAI AZ OROSZ–UKRÁN KATONAI KONFLIKTUS IDEJÉN

DOI: 10.35926/HSZ.2025.2.4

ÖSSZEFOGLALÓ: *Az orosz–ukrán háborúról, amely a kubai rakétaválság óta a legsúlyosabb érdekkonfliktus, rendszeresen kerülnek fel az internetre minősített adatok, néhány esetben szigorúan titkos minősítésűek is. Az adminisztratív, az elektronikus és a fizikai biztonság a jogi szabályozás tekintetében kielégítő, a büntetőjogi szabályok mindkét országban kellő elrettentő erővel bírnak. A rendszer gyenge pontja az emberi tényező. A közvélemény kíváncsiságát lehetetlen kielégíteni, és egyes esetekben politikai érdekek is állhatnak a kiszivárogtatás mögött. A tanulmány a minősített adatok védelmének hatékonyságát és annak korlátait vizsgálja a vonatkozó jogi szabályozás elemzésén keresztül.*

KULCSSZAVAK: *titok, titokvédelem, államtitok, minősített adat, kémkedés, johannesburgi alapelvek*

A SZERZŐRŐL:
Dr. Gál István László (PhD), a Pécsi Tudományegyetem tanszékvezető egyetemi tanára (Büntetőjogi Tanszék), a Nemzeti Közszolgálati Egyetem egyetemi tanára (Katonai Nemzetbiztonsági Tanszék) (MTMT: 10000151; ORCID: 0000-0002-0258-8587; Scopus ID: 57217106143)

BEVEZETŐ GONDOLATOK

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, amely a kubai rakétaválság óta a legsúlyosabb érdekkonfliktus a két atomhatalom között, 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 érdeke nem írja-e felül az államoknak és a nemzetközi szervezeteknek azt az érdekét, hogy ezeket az információkat megóvják. A háború első időszakában komoly orosz és amerikai minősített adatok szivárogtak ki. A katonai konfliktusban az Ukrajnát támogató országok közül az Egyesült Királyság és Németország titokvédelmi szabályozása hordoz még olyan egyedi sajátosságokat, amiket érdemes megvizsgálni.

A titok általános fogalmát sokan sokféleképpen definiálták már, hiszen ez a témakör a biztonságpolitika és a nemzetbiztonság tudományának egyik alapfogalma. Resperger István kiválóan foglalja össze a titok kialakulását. Álláspontja szerint a titkok jelenléte az emberi

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

társadalomban az emberiség megjelenésével egyidős, a történelem során az emberré válás és az emberi társadalom kialakulása óta folyamatosan jelen van a titok is. Már az első emberek is igyekeztek a titkokat elrejteni a külső és a belső ellenségeik elől. A polgári fejlődés során az állami titkok a hatalom legfelsőbb szintű gyakorlói (kormányfők, miniszterek stb.) kezébe kerültek, és ekkor már különböző szabályok is kialakultak az olyan dokumentumok különleges kezelésére, amelyek titkokat tartalmaztak.

Mindezek négy csoportba oszthatók:

– a titkokat tartalmazó iratok megkülönböztetett jelölése;
– annak a személyi körnek a kijelölése, amely ezeket az iratokat létrehozhatta;
– az iratok megismerhetőségére vonatkozó előírások (betekintők);
– az iratok különleges kezelésére vonatkozó előírások.

Resperger István rámutat arra is, hogy a polgári és a katonai titokvédelem csak a 18. századtól kezdődően különült el egymástól. Ennek oka, hogy a katonai titokvédelemben nagy mennyiségű minősített adat keletkezett, de azok kezelése szigorúan szabályozott, zárt körben történt. Ezzel szemben a polgári titokvédelem főleg a diplomácia, a pénzügyek, a bűnüldözés, illetve a legfelsőbb szintű végrehajtó hatalom döntéseinek titkosítását jelentette, emiatt sokkal tágabb minősítői és betekintői kört jelentett. Ezek a szabályok alapjaiban a modern titokvédelemben is megtalálhatók.[2]

Napjainkban a magyar jogi szabályozás és a fejlett nyugati jogrendszerek is az államtitok fogalma helyett a „minősített adat" kategóriát használják. Minősített adat a legáltalánosabb megfogalmazás szerint minden olyan információ, amelyet egy adott állam vagy államoknak egy csoportja valamilyen szempontból érzékenynek tekint, és amelyhez emiatt titoktartási kötelezettség kapcsolódik nemzeti, regionális vagy akár nemzetközi biztonsági igények alapján is.

2025. február 24. a harmadik évfordulója az orosz–ukrán háború kirobbanásának, amely a legnagyobb hagyományos katonai konfliktus Európában a második világháború óta.

A VÉDELEM KORLÁTAI ÉS HIÁNYOSSÁGAI: A MINŐSÍTETT ADATOK „KISZIVÁRGÁSA"

A minősített adatok nyilvánosságra kerülése a védelmi idő lejárta előtt legalább négyféle veszélyt rejt magában egy, az Amerikai Egyesült Államokban megjelent tanulmány szerint. Először is, a fedett műveletek, programok, kapcsolati rendszerek stb. nyilvánosságra kerülése műveleti változtatásokat, igazodást és bizonyosfajta alkalmazkodást is indukál az ellenséges csoportok, például terrorszervezetek működésében. Velük szemben a további információgyűjtés tehát nehezebbé és drágábbá válik. Másodszor, a közzététel negatívan befolyásolja az adott ország külkapcsolatait, gyengül a bizalom az adott ország vonatkozásában. Harmadszor, egy ilyen lépés rombolja a bizalmat az állami szektor és a magánszektor közötti együttműködésben is. Negyedszer, a minősített adatok kontrollálatlan nyilvánosságra kerülése a közbizalmat is rombolja.[3]

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

[2] Resperger 2018, 355–356.
[3] Young 2014, 369–371.

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 tartalmára 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 játszma szereplői, és a játszmához való képességük szerint fog alakulni annak kimenetele.[4]

Az információvédelem alkalmazási szintjének feladatai szerint a minősített adatok védelmi rendszere a következő elemeket foglalja magában: fizikai védelem, hardver és szoftver, valamint emellett idesorolható a rejtjelezés, az átviteli utak informatikai védelme, a kompromittáló kisugárzás elleni védelem, a dokumentumvédelem, a személyi védelem és az eljárásvédelem is.[5] A minősített adatok védendő tulajdonságai pedig a legtágabb értelemben a következők lehetnek:

– bizalmasság (az információhoz kizárólag a jogosultsággal rendelkező személy férhet hozzá);
– hitelesség (az információ azon jellemzője, amely az eredetiséget reprezentálja);
– rendelkezésre állás (az arra jogosultak a megfelelő szabályzatokban foglalt rendelkezések szerint férnek hozzá az információhoz);
– sértetlenség (a megfelelő módon működő információs rendszer az adatokat megfelelő formában reprezentálja).[6]

A minősített adatok bármelyik védendő tulajdonsága sérülhet, ezt összefoglaló általános elnevezéssel titoksértésnek nevezzük. A titoksértés fogalma kapcsán a klasszikus magyar büntetőjogász, Angyal Pál megkülönböztet befelé és kifelé ható erőket. Kívül vannak a titok körén kívül álló személyek, ezek próbálnak az idegen titokkörbe benyomulni, majd utána az idegen titokról vagy titkokról tudomást szerezni. A másik ponton belülről kifelé folyik a harc. Ilyenkor a kívül álló harmadik személy az általa beépített kémek segítségével szerzi meg a titok tárgyát képező ismeretet, vagy árulókkal áll összeköttetésben.[7] A titoksértésnek különböző módjai ismeretesek az elhárítás szemszögéből nézve is. Az Alkotmányvédelmi Hivatal jogelődje által összeállított anyag[8] alapján ezek a következők:

1. A „sötét hírszerzés”. Ennek lényege, hogy az ellenérdekelt felek megtévesztéssel jutnak információhoz. E cél érdekében fedőintézményeket, -pozíciókat hoznak létre, gyakran diplomáciai fedésű munkatársakat is alkalmaznak a műveletek végrehajtásához.
2. A befolyásolás, tudatos megnyerés. Ez történhet hivatalos kapcsolatfelvétel útján, amelyet kisebb ajándékozások követnek, de elmehet egészen a megvesztegetésig is. A leghatékonyabb azonban – a gyakorlatban ritkább – az, amikor a titokbirtokost az ellenérdekelt fél ügynökként beszervezi.
3. A munkahelyi és a lakókörnyezet felhasználása információszerzésre. Idetartoznak a titokbirtokos lakása, nyaralója, de tágabb értelemben a társasági kapcsolatai is.

[4] Nikolov 1973, 20–25.
[5] Kassai 2001.
[6] Kuris–Pándi 2009, 312.
[7] Angyal 1908, 19.
[8] A titokvédelem… 2001, 15–25.

4. A papíralapú dokumentumok, illetve tartalmuk megszerzése. Ez a másolásra, sokszorosításra vonatkozó szabályok kijátszásával történhet. Ha például a minősített adatot tartalmazó iratok megsemmisítése nem szabályszerűen történik, akkor még eredeti iratok is kerülhetnek ellenérdekelt felekhez.
5. Az elektronikus információk megszerzése. Nagyon fontos az informatikai eszközök kompromittáló kisugárzásának minimálisra csökkentése, és a minősített adatokat tároló számítástechnikai eszközök függetlenítése a külső, internetre csatlakozó eszközöktől. Napjainkban az elektronikusan tárolt minősített adatok védelme az egyik legfontosabb kihívás az állam titkainak védelme szempontjából.
6. A lehallgatás. Korszerű technikai eszközökkel bizonyos fokig lehet védekezni ellene, de ennek megszervezése és technikai végrehajtása elsődlegesen az elhárítás feladata.
7. A külföldi tartózkodás felhasználása információszerzésre. Akár hivatalos, akár magáncélú külföldi utazás során is előfordulhat, hogy a titokbirtokos mozgását, telefon- és egyéb beszélgetéseit az ellenérdekelt szolgálatok ellenőrzik, szállodai szobáját átkutatják.
8. A nyílt információk összegyűjtése, elemzése és értékelése. Ma már egyes szolgálatok az információk 60–90%-át szerzik be nyílt forrású hírszerzés során. Nyilvános szerepléseken, tárgyalásokon, előadások és sajtótájékoztatók alkalmával erre különösen figyelnie kell a minősített adatokat felhasználó, minősített adatok birtokában lévő személyeknek.

Itt kell megjegyeznünk, hogy 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[9]. Amikor a nemzetbiztonsági érdek[10] 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.[11] A „Nemzetbiztonságról, a véleménynyilvánítás szabadságáról, valamint az információhoz való hozzáférésről szóló johannesburgi alapelvek"[12] című ENSZ-dokumentum ezzel kapcsolatban a 15. alapelvben a következőket tartalmazza:

„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."

[9] Földesi 2005.

[10] 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, melynek hadserege a kémelhárítással kapcsolatban nyomozást kezdeményezett az ügyben, mivel tartani lehetett attól, hogy a szivárogtató a Védelmi Minisztérium egyik munkatársa. Cummins 2010, 2.

[11] Xanders 1989, 760.

[12] The Johannesburg Principles… 1996.

AZ ÁLLAMTITOK VÉDELMÉNEK ESZKÖZEI 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.[13]

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 láttak 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.[14]

A jelenlegi orosz minősítési szintek[15] 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.[16]

Vagyis az orosz szabályozás ténylegesen csak három minősítési szintet használ a gyakorlatban, ugyanúgy, mint a szovjet elődje vagy például 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, felde-

[13] Resperger István et al. 2015, 25.

[14] Mitrohin 2000, 198.

[15] Classification Levels… 1997.

[16] Megjegyezzük, hogy a hatályos magyar–orosz titokvédelmi megállapodás 3. cikke a következő minősítési szinteket felelteti meg egymásnak: „(1) 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.

rítési 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 Oroszország, amely az elmúlt években nagy figyelmet fordított a minősített adatok elektronikus biztonságára. Ebben nagy valószínűséggel szerepet játszhatnak a Snowden által nyilvánosságra hozott amerikai minősített adatok a Nemzetbiztonsági Ügynökség (NSA[17]) 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 különösen 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, 12–20 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 azzal 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

[17] National Security Agency.
[18] Russia completes… 2016.

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. cikkekben.

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.

A MINŐSÍTETT ADATOK VÉDELMÉNEK ESZKÖZEI 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 szabályozást alkottak meg a nemzetbiztonsági szempontból fontos információk minősítéséről és védelméről.[19] 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, káralapú minősítési rendszer szerint: szigorúan titkos, titkos és bizalmas szint.[20]

George W. Bush elnök 2001. szeptember 11., az országot ért terrortámadás előtt is hajlott az intenzív mértékű titkosításra, az utána következő években azonban ez a tendencia felerősödött. Így többek között szeptember 11. után Bush elnök felállított egy titkos katonai bíróságot, bővítette a zárt bírósági tárgyalások körét, tovább szélesítette a végrehajtó hatalom különleges jogköreit, kiszélesítette a minősített adatok védelmét a bírósági eljárásokban, megtiltotta a hozzáférést a volt elnökök irataihoz, megtagadta a kongresszusi megkeresések alapján kért dokumentumok kiadását, titokban tartotta az NSA amerikai állampolgárokkal kapcsolatos megfigyelési programját, valamint sok esetben újból minősített a minősítés alól korábban már feloldott iratokat.

[19] Exec. Order… 1983.

[20] Fein 1985, 807.

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 darab minősített adat keletkezett az Amerikai Egyesült Államokban.[21] Ezt az amerikai szakértők már soknak ítélik, pedig hazánkban napjainkban – a lakosságszám arányait összehasonlítva a magyar adatokkal – több mint kétszer ennyi minősített adat keletkezik évente, 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 minősítések csökkentése[22] 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 nemzetbiztonsági érdekből meg kell őrizni *„polgáraink, demokratikus intézményeink, hazánk biztonságának és idegen nemzetekkel való kapcsolatunk védelme érdekében"*.[23] 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"*.[24]

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.[25]

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, ezek az 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.[26] 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

[21] Silver 2008, 450.
[22] Reducing Over-Classification Act 2010.
[23] Exec. Order No. 13526 § 4.1(a), 75 Fed. Reg. 707 § 4.1(a). 2009; lásd még: The President Executive Order 13526.
[24] Jensen et al. 2017, 205.
[25] Elsea 2017, 19.
[26] MacKay 2017, 67–68.

kisebb részekben, különböző szinteken is minősíteni, akár bekezdésenként is meg lehet jelölni az adott bekezdés vagy ábra minősítési szintjét.[27]

A minősített adatokhoz történő hozzáférés a szükséges ismeret[28] 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 mellett azt a célt szolgálják, hogy védjék a forrásokat és a módszereket.[29]

A 21. század eleje óta 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 esetben akár lehet indokolt is, a nyilvánosság ellenőrző szerepének érvényre juttatása érdekében.[30]

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 kontra 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 szavazati aránnyal 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 –, egy 2008-ban megjelent tanulmány szerint addig még nem indult egyszer sem büntetőeljárás.[31]

Egy 2019-es tanulmány megerősíti ezt a tíz évvel korábbi megállapítást: a média munkatársai ellen addig sem indultak büntetőeljárások az Amerikai Egyesült Államokban, és még napjainkban sem, csak a minősített adatot kiszivárogtató kormányzati tisztviselők ellen. Snowden akár 30 év szabadságvesztést is kaphat majd, míg a *The Guardian* 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 a szerepe miatt, hiszen sokan ma már a negyedik hatalmi ágnak 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 indítaniuk – vagy egyik ellen sem.[32]

[27] Marking Classified National Security…2018.
[28] Exec. Order No. 13526 2009: i. m.
[29] Rossmiller 2011, 1301.
[30] Clark 2013, 7.
[31] Silver 2008: i. m. 447–483.
[32] Mokrosinska 2020, 203–238.

Obama elnök alatt a kémkedési törvény alapján öt büntetőeljárás indult hivatalban lévő és volt kormánytisztviselők ellen nemzetbiztonsági szempontból érzékeny információk sajtóban történő nyilvánosságra hozatalával kapcsolatos törvénysértések miatt. 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.[33]

A minősített adatokkal történő visszaélés szabályozása azonban könnyen áttekinthető, hiszen ez szövetségi bűncselekmény. Egy év szabadságvesztéssel és 1000 dollárig terjedő pénzbüntetéssel büntetendő az a szövetségi alkalmazott vagy tisztviselő, aki erre vonatkozó engedély nélkül minősített adatokat szándékosan hozzáférhetetlenné tesz. A büntetés tíz évig terjedő szabadságvesztés és legfeljebb tízezer dollár pénzbüntetés, ha ez az 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 Amerikai 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.[34] Ez véleményem szerint kellő elrettentő erőt jelent.

AZ EGYESÜLT KIRÁLYSÁG TITOKVÉDELMI SZABÁLYOZÁSÁNAK NÉHÁNY KÉRDÉSKÖRE

Európában az Egyesült Királyság az egyik legfontosabb geopolitikai és katonai tényező. Az Egyesült Királyság minősítési rendszere egyszerű és könnyen áttekinthető, jelenleg csupán három minősítési szintet használ: Official (Hivatalos), Secret (Titkos), Top Secret (Szigorúan titkos).

Az Official minősítési szintet használják általában a közszféra által létrehozott vagy feldolgozott információk többsége esetében. Ilyenek például az olyan gazdasági adatok, amelyek esetében káros következményei lehetnek, ha azok elvesznek, ellopják, vagy a médiában közzéteszik őket.

A Secret minősítési szinten védik azokat a nagyon érzékeny információkat, amelyek esetében indokoltak a fokozott védelmi intézkedések. Például olyan adatok, amelyek nyilvánosságra kerülése súlyosan károsíthatja a katonai védelmi képességeket, a nemzetközi kapcsolatokat, de idetartoznak a szervezett bűnözés elleni küzdelemmel kapcsolatos adatok is.

A Top Secret minősítési szint a legmagasabb. Ezzel védik a kormány legérzékenyebb információit, azokat az adatokat, amelyek a legmagasabb szintű védelmet igénylik a legsúlyosabb

[33] Halperin [é. n.]

[34] Elsea 2017: i. m. 14–15.

fenyegetések ellen. Például olyan adatok tartozhatnak e körbe, ahol a nyilvánosságra kerülés vagy illetéktelen személy általi megszerzés életveszélyt okozhat, vagy veszélyeztetheti az ország vagy a szövetséges nemzetek biztonságát vagy gazdasági jólétét.

A minősített adatokhoz történő hozzáférés a brit rendszer szerint is a szükséges ismeret elvén *(need to know)* alapul. A szabályozás azonban különleges helyzetekben megengedi a *need to share* elvének alkalmazását is, vagyis lehetőséget ad rá, hogy különösen indokolt esetben minősített adatokat osszanak meg a megfelelő személyi biztonsági tanúsítvánnyal nem rendelkező személyekkel, például akkor, ha azonnali intézkedésre van szükség az élet védelme vagy súlyos bűncselekmény elkövetésének megakadályozása érdekében. Ilyen körülmények között egyfajta észszerű megközelítést kell alkalmazni a brit szabályozás szerint: ha az idő engedi, fontolóra kell venni az egyes alternatívákat is, és lépéseket kell tenni az információ forrásának védelme érdekében.[35]

Az Egyesült Királyság egyébként tagja a Five Eyes (Öt Szem) nevű hírszerző közösségnek, amely a SIGINT[36] területén öt állam részvételével működik napjainkban is, magas fokú hatékonysággal. A mai Five Eyes alapjai a második világháború alatt jöttek létre. Az Amerikai Egyesült Államok és Nagy-Britannia szorosan együttműködtek a SIGINT területén is a háború alatt, az ellenség kommunikációjának hatékony lehallgatása érdekében. A britek feltörték Németország szupertitkos Enigma rendszerét, az Amerikai Egyesült Államok pedig feltörte a japán titkosítást. Ezt az együttműködést az Egyesült Királyság és az Amerikai Egyesült Államok megállapodással intézményesítették 1946-ban. A kialakuló hidegháborúban a Szovjetunió ellen folytatott hírszerzésben pedig már szükségesnek ítélték a hírszerzési együttműködés megtartását és megerősítését békeidőben is, a potenciális konfliktusok előrejelzésére. Kanada 1948-ban csatlakozott a szövetséghez, valamint 1956-ban Ausztrália és Új-Zéland, ezzel létrejött egy globális, hírszerzési adatokat megosztó szervezet.[37] A Five Eyes közösség tagjai között napjainkban már olyan szoros a kapcsolat, hogy a részt vevő kormányok az Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége, vagyis az NSA kéréseit saját állampolgáraik magánszférájának védelme elé helyezik.[38]

A TITOKVÉDELEM ESZKÖZEI NÉMETORSZÁGBAN

Németországban a minősített adatok védelme a hatályos szabályozás szerint magában foglal minden olyan intézkedést, amelyek alapján egy állami szerv egyes tényeket, tárgyakat vagy ismereteket meghatározott eljárás keretében minősített adattá nyilváníthat. A német szövetségi és állami szintű jogszabályok számos rendelkezése szabályozza a minősített adatok témakörét.

A szövetségi állam biztonságának alapja jogilag elsősorban a Biztonsági Ellenőrzésről Szóló Törvény (SÜG[39]) és a hozzá kapcsolódó közigazgatási rendeletek. A titokvédelemnek Németországban is vannak személyi és fizikai követelményei – a nemzetközi gyakorlatnak megfelelően.

A német titokvédelmi jogi szabályozás kulcsfogalma a minősített adat (Verschlusssache). Négy minősítési szintet használnak:

---

[35] Government Security Classifications 2024.

[36] Signal Intelligence – jelhírszerzés, vagyis a rádióelektronikai jelfelderítés az elektronikus kommunikációs jelek lehallgatását és feldolgozását jelenti.

[37] Dailey 2017/, 1.

[38] Greenwald 2014, 164.

[39] Sicherheitsüberprüfungsgesetz.

– VS-Nur für den Dienstgebrauchs (VS-NfD) – csak szolgálati használatra (ez a korlátozott terjesztésű minősítési szintnek felel meg);
– VS-Vertraulich (VS-Vertr.) – bizalmas;
– Geheim (Geh.) – titkos;
– Streng Geheim (Str. Geh.) – szigorúan titkos.

A német rendszer is kár alapú minősítési rendszer, szinte teljes egészében a magyar szabályozással egyező módon határozza meg az egyes minősítési szintekhez rendelt potenciális veszélyeket. Csak a feltétlenül szükséges ideig és minősítési szinten szabad minősített adatot létrehozni és kezelni. A német szabályozás is a már körbejárt szükséges ismeret elvét *(need to know – Kenntnis nur, wenn nötig)* hangsúlyozza a minősített adatok megismerése kapcsán.[40]

Összességében megállapítható, hogy talán a legközelebb a német szabályozás áll a magyar minősített adatok védelméről szóló törvényhez (Mavtv.), nagy valószínűséggel egyik mintapéldaként használtuk fel a kodifikáció során.

A német büntetőjog a Btk. (Stgb.) mellett más ágazati törvényekben is tartalmaz büntető rendelkezéseket, de a büntetőjog legfontosabb része (Kernstrafrecht) a német Btk.-ban található meg, a mellékes büntetőjogi rendelkezések (Nebenstrafrecht) pedig egyéb jogszabályokban. A minősített adatok védelme annyira fontos a német jogalkotó álláspontja szerint, hogy:

1. a Stgb. tartalmazza az összes idevonatkozó büntetőjogi rendelkezést;
2. több tényállás is védi a minősített adatokkal kapcsolatos jogi tárgyakat;
3. a résznek viszonylag az elején, a második fejezetben találhatók ezek a rendelkezések, a törvényhozó ezzel is jelzi a fontosságukat.

A minősített adatok védelmével kapcsolatos tényállások a német Btk. második fejezetében, az *Árulás és az állam külső biztonságának veszélyeztetése* cím alatt találhatók. Ezzel a német büntetőjog egyértelműen kimondja, hogy állam elleni, a nemzetbiztonságot veszélyeztető bűncselekményeknek tekinti ezeket a magatartásokat.

ÖSSZEGZÉS

A minősített adatok védelmének eszközei a vizsgált országokban mind megfelelőek. Az adminisztratív, az elektronikus és a fizikai biztonság a jogi szabályozás tekintetében kielégítő, a büntetőjogi szabályok mind a négy országban kellő elrettentő erővel bírnak. A rendszer gyenge pontja a személyi biztonság, vagyis az ember. A közvélemény kíváncsiságát lehetetlen kielégíteni, és egyes esetekben politikai érdekek is állhatnak a kiszivárogtatás mögött, főleg egy komoly jelentőségű katonai és politikai konfliktus kapcsán. Ennek ellenére a már említett johannesburgi alapelveket véleményem szerint csak nagyon szűk, nagyon kivételes körben lehet alkalmazni, hiszen a katonai műveletekkel kapcsolatos minősített adatok kiszivárgása emberéletekbe kerülhet. 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, vagyis az újságírókat nem lenne szabad büntetőjogi felelősségre vonni, ha minősített adatot hoznak nyilvánosságra.[41]

[40] Vogt–Wahlen 2015, 4–9.
[41] Kassai 2007, 7.

FELHASZNÁLT IRODALOM

- 2016. évi CLXXXIX. törvény a Magyarország Kormánya és az Oroszországi Föderáció Kormánya között a minősített adatok kölcsönös védelméről szóló egyezmény kihirdetéséről. https://net.jogtar.hu/jogszabaly?docid=a1600189.tv (Letöltés időpontja: 2024. 11. 23.)
- Angyal Pál: *A titok védelme anyagi és alaki büntetőjogunkban*. Athenaeum Kiadó, Budapest, 1908.
- A titokvédelem nemzetbiztonsági jelentősége. NBH, Budapest, 2001.
- Clark, Robert: *Classified Information in the Public Sphere: An Examination of Legal Issues Surrounding the NSA Leaks*. Documents to the People, Vol. 41, No. 04, 2013, 7–10. https://www.altera-ed.org/images/Publications/LiteracyLibraryServices/Opening%20the%20Windows%20to%20Transparent%20Government.pdf (Letöltés időpontja: 2024. 11. 24.)
- Classification Levels Used by the Russian Federation. FAS Intelligence Resource Program, 1997. 11. 17. https://fas.org/irp/world/russia/class.htm (Letöltés időpontja: 2020. 08. 12.)
- Cummins, Guylyn: *Classified Information Necessary to Protect National Security? Says Who?* Communications Lawyer, 2010/1., 2.
- Dailey, Jane Elizabeth: *The Intelligence Club: A Comparative Look at Five Eyes*. Journal of Political Sciences & Public Affairs, 2017/5. DOI: 10.4172/2332-0761.1000261
- https://www.longdom.org/open-access/the-intelligence-club-a-comparative-look-at-five-eyes-2332-0761-1000261.pdf (Letöltés időpontja: 2024. 11. 24.)
- Elsea, Jennifer K.: *The Protection of Classified Information: The Legal Framework*. Congressional Research Service, 2017. 05. 18. https://sgp.fas.org/crs/secrecy/RS21900.pdf (Letöltés időpontja: 2024. 11. 23.)
- Exec. Order No. 12,356, 3 C.F.R. 166 – National Security Information. Office of the Federal Register (OFR), 1983. https://www.archives.gov/federal-register/codification/executive-order/12356.html (Letöltés időpontja: 2024. 11. 23.)
- Fein, Bruce E.: *Access to Classified Information: Constitutional and Statutory Dimensions*. William and Mary Law Review, 1985/5., 805–844. https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=2181&context=wmlr (Letöltés időpontja: 2024. 11. 23.)
- Government Security Classifications. Cabinet Office, 2024. 08. 05. https://assets.publishing.service.gov.uk/media/66b0d3c9ab418ab0555932d9/2024-08-05_-_2024_GSCP_UPDATE_.docx__1_.pdf (Letöltés időpontja: 2024. 11. 23.)
- Greenwald, Glenn: *A Snowden-ügy. Korunk legnagyobb nemzetbiztonsági botránya*. HVG Könyvek, Budapest, 2014.
- Halperin, Morton H.: *Criminal Penalties for Disclosing Classified Information to the Press in the United States.* https://www.right2info.org/resources/publications/Halperin_CriminalPenaltiesforDisclosingClassifiedInformationtothePressintheUnitedStates.pdf (Letöltés időpontja: 2020. 08. 22.)
- Jensen, Carl J. et al.: *Bevezetés a hírszerzésbe*. Antall József Tudásközpont, Budapest, 2017.
- Kassai Károly: *A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere.* Doktori (PhD) értekezés, Budapest, 2007. https://docplayer.hu/10043015-Kassai-karoly-mk-alezredes-a-magyar-honvedseg-informaciovedelmenek-mint-a-biztonsag-reszenek-feladatrendszere-doktori-phd-ertekezes.html (Letöltés időpontja: 2024. 11. 24.)
- Kassai Károly: *Az információvédelem rendszerszintű feladatai*. Nemzetvédelmi Egyetemi Közlemények, 5. évf. 2001/4., 111–120. http://193.224.76.2/downloads/konyvtar/digitgy/20014/tartalom.html (Letöltés időpontja: 2020. 04. 30.)

- Kuris Zoltán – Pándi Erik: *Komplex információbiztonság megvalósítási lehetőségeinek megközelítése.* Hadmérnök, IV. évf. 2009/2., 311–318. http://hadmernok.hu/2009_2_kuris.pdf (Letöltés időpontja: 2024. 11. 24.)
- MacKay, Bruce M.: *The use of classified information in terrorism trials.* Southern Illinois University Law Journal, Vol. 42, 2017, 63–84. https://law.siu.edu/_common/documents/law-journal/articles-2017/fall-2017/8-mackay-sm.pdf (Letöltés időpontja: 2024. 11. 24.)
- Marking Classified National Security Information as Required by Executive Order. 13526, 2018. 01.
- Mitrohin, Vaszilij: *KGB lexikon. A szovjet titkosszolgálat kézikönyve.* Alexandra Kiadó, Pécs, 2000.
- Mokrosinska, Dorota: *Why Snowden and not Greenwald? On the Accountability of the Press for Unauthorized Disclosures of Classified Information*. Law and Philosophy, 2020/39, 203–238. https://doi.org/10.1007/s10982-019-09367-1 (Letöltés időpontja: 2024. 11. 24.)
- Nikolov, Elit: *A titok*. Tömegkommunikációs Kutatóközpont, Budapest, 1987.
- Reducing Over-Classification Act. https://www.congress.gov/111/plaws/publ258/PLAW-111publ258.pdf (Letöltés időpontja: 2020. 08. 30.)
- Resperger István: *A nemzetbiztonság elmélete a közszolgálatban*. Dialóg Campus Kiadó, Budapest, 2018.
- Resperger István et al.: *Ugyanaz másképpen – az orosz geopolitika változásai a hidegháború végétől napjainkig.* Felderítő Szemle, XIV. évf. 2015/1., 21–36. https://www.knbsz.gov.hu/hu/letoltes/fsz/2015-1.pdf (Letöltés időpontja: 2024. 11. 23.)
- Rossmiller, Alex: *Adjudicating Classified Information*. St. John's Law Review, Vol. 85, No. 4, 2011, 1275–1342. https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=5592&context=lawreview (Letöltés időpontja: 2024. 11. 24.)
- Russia completes military network for classified data exchange. Oneindia, 2016. 10. 19. https://www.oneindia.com/international/russia-completes-military-network-classified-data-exchange-2238328.html (Letöltés időpontja: 2020. 08. 11.)
- Silver, Derigan A.: *National Security and the Press: The Governments ability to Prosecute Journalists for the Possession or Publication of National Security Information*. Communication Law and Policy Vol. 13 2008/4, 447–483. https://doi.org/10.1080/10811680802388881 (Letöltés időpontja: 2024. 11. 11.)
- The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. U.N. Doc. E/CN.4/1996/39, 1996. https://documents.un.org/doc/undoc/gen/g96/118/04/pdf/g9611804.pdf (Letöltés időpontja: 2024. 11. 23.)
- Vogt, Marten – Wahlen, Dierk: *Geheimschutzrecht – Voraussetzungen und Folgen der Einstufung von Informationen als Verschlusssachen.* Deutscher Bundestag, WD 3 – 3010 – 036/15. 2015. https://www.bundestag.de/resource/blob/384456/52c23ac82c63178f15e7610be21ee2ba/geheimschutzrecht-data.pdf (Letöltés időpontja: 2024. 11. 24.)
- 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.* Journal of Law & Politics, Vol. 5, No. 4. 1989, 759–826. https://www.gmsr.com/wp-content/uploads/2016/06/A-Handymans-Guide-to-Fixing-National-Security-Leaks.pdf (Letöltés időpontja: 2024. 11. 24.)
- Young, Mark D.: *National Insecurity: The Impacts of Illegal Disclosures of Classified Information.* A Journal of Law and Policy for the Information Society, Vol. 10, No. 2, 2014, 369–371.