Válaszok az aktuális kihívások tükrében

Csányi Csaba

Magyarország számára biztonsági kockázatot jelentő kihívások más országok számára is kockázati elemként jelentek meg, így a világ más államai által ezekre adott – jogi vagy nem jogi – válaszok iránymutatásul szolgálhatnak hazánk számára is. A fenti biztonsági kockázatot vagy fenyegetést jelentő elemek közül néhányat önkényesen kiemelve, mint például a kiberbiztonság, valamint hozzá kapcsolódóan a mesterséges intelligencia, a migrációs fenyegetettség, valamint az általam biztonsági kockázatként értékelt elemeket mint hiátust – úgymint adatkezelés versus adatvédelem, innováció, K+F kérdéskör mint nemzetbiztonsági kérdés – beemelve és megvizsgálva kívánom bemutatni az azokra adott lehetséges válaszokat.

Kiberbiztonság

A kiberbiztonság a nemzetbiztonsági stratégia egyre központibb elemévé válik. Az Európai Unió szigorította a kiberbiztonsági szabályait, hogy kezelni tudja a kibertámadások jelentette egyre nagyobb fenyegetést, valamint hogy kihasználja az új digitális kor által kínált lehetőségeket. A Tanács 2019. április 9-én rendeletként elfogadta az úgynevezett kiberbiztonsági jogszabályt, amely bevezeti az egész EU-ra kiterjedő tanúsítási rendszerek keretét, valamint létrehozta az Európai Uniós Kiberbiztonsági Ügynökséget, amely bővített hatáskörrel átveszi a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepét.

E kiberbiztonsági reform részeként az uniós intézmények olyan jogszabályon is dolgoznak, amely létrehozza majd a Kiberbiztonsági Ipari, Technológiai és Kutatási Központot, amelynek tevékenységét a nemzeti koordinációs központok hálózata fogja támogatni. A Kiberbiztonsági Ipari, Technológiai és Kutatási Központ révén javulni fog a kiberbiztonsági kutatás és innováció koordinálása. Ez a központ emellett az EU fő eszköze lesz ahhoz, hogy összevonja a kiberbiztonsági kutatás, technológia és ipari fejlesztés területére irányuló beruházásokat.

A Kiberbiztonsági Kompetenciahálózatot a tagállamok által kijelölt nemzeti koordinációs központok alkotják majd. A nemzeti központok rendelkeznek majd kiberbiztonság-technológiai szakértelemmel, illetve ehhez hozzáférésük lesz,

https://doi.org/10.36250/00904_12

például az olyan területeken, mint a kriptográfia, az IKT hálózatvédelem vagy a biztonság emberi tényezői.

A Kiberbiztonsági Ipari, Technológiai és Kutatási Központ a kompetenciahálózattal együttműködve végrehajtási mechanizmusként szolgál majd az Európai horizont és a Digitális Európa program keretében megvalósuló, kiberbiztonsági célú pénzügyi támogatáshoz. Együttesen hozzájárulnak majd az uniós kiberbiztonsági ipar versenyképességének növeléséhez, és a kiberbiztonságot versenyelőnnyé teszik a többi uniós iparág számára. E központok finanszírozását elsősorban a Digitális Európa és az Európai horizont program fogja biztosítani, de egyúttal lehetőség lesz önkéntes tagállami hozzájárulások biztosítására is.

A javaslat harmadik struktúraként létrehoz egy kiberbiztonsági kompetenciaközösséget is, amely összefogja a fő érdekelt feleket azért, hogy az EU egészében javuljon, és elérhetővé váljon a kiberbiztonsági szakértelem. A közösség tagjai közé fognak tartozni többek között az ágazati és a felsőoktatási szervezetek, a nonprofit kutatóhelyek, a működési és technikai kérdésekkel foglalkozó állami szervezetek, valamint – adott esetben – kiberbiztonsági kihívásokkal szembesülő egyéb ágazatok szereplői. A központ a 2021. január 1. és 2029. december 31. közötti időszakra jön létre. Ezt követően felszámolják, kivéve, ha a vonatkozó rendelet felülvizsgálata során más döntés születik.

Ezzel párhuzamosan az EU olyan horizontális intézkedéseket dolgoz ki, amelyek egyszerre több területen veszik fel a küzdelmet a kiberfenyegetésekkel. Idetartozik például a szervezett bűnözés elleni küzdelem, ahol a kiberbűnözés a 2018–2021-es időszak tíz legfontosabb prioritásai között szerepel a közös kül- és biztonságpolitika, ahol a kibertámadásoktól való elrettentés alapvetően fontos az Európai Unió közös kül- és biztonságpolitikája (KKBP) céljainak elérése szempontjából, vagy a kibervédelem, amelynek kereteit az EU a változó biztonsági kihívásokra figyelemmel aktualizálta.

Az egyre növekvő kiberbiztonsági kihívások fényében az EU-nak jobban fel kell hívnia a figyelmet a tagállamokkal vagy uniós intézményekkel szembeni kibertámadásokra, és javítania kell az azokra adandó válaszlépéseket. Ezek a nemzeti és uniós határokon átnyúló kihívások nemcsak a biztonságot és a stabilitást, hanem a jólétünket és a demokratikus rendet is veszélyeztetik. Mára valósággá vált a „dolgok internete", és az EU-ban 2020-ra várhatóan több tízmilliárd összekapcsolt digitális eszköz lesz.

Az uniós polgároknak támogatásra van szükségük, hogy bizalom alakuljon ki bennük e technológiák iránt, kezdve a testen hordható eszközöktől a hálózatba kapcsolt autókig. Lehetővé kell tenni egyúttal, hogy az uniós vállalkozások

igénybe vehessék e technológiákat a határokon átnyúló üzleti tevékenységükhöz, legyen szó akár ipari automatizálásról, akár intelligens energiahálózatokról. A mai IKT-rendszerek ugyanakkor komoly károkat szenvedhetnek biztonsági események, például üzemzavarok vagy vírusok miatt. Ezek az események, amelyeket gyakran hálózat- és információbiztonsági (NIS) eseményeknek neveznek, egyre sűrűbben fordulnak elő, és egyre nehezebb őket kezelni, továbbá a vállalkozásokat és a közszolgáltatásokat egyaránt érinthetik, ami pedig aláásható a fogyasztók bizalmát.

Kiberbiztonsági tanúsítási rendszerek

Az Európai Bizottság a 2017 szeptemberében elindított reformcsomagban javaslatot tett az IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási rendszerek bevezetésére. A kezdeményezés célja az uniós kiberbiztonsági piac növekedésének elősegítése.

E tanúsítási rendszerek szabályok, műszaki követelmények és eljárások formájában valósulnának meg. Csökkentenék a piac széttagoltságát, és felszámolnák a szabályozási akadályokat, továbbá segítenék a bizalomépítést is. Emellett valamennyi tagállamban alkalmaznák őket, ami megkönnyítené a vállalkozások számára a határokon átnyúló kereskedelmet.

Európai Uniós Kiberbiztonsági Ügynökség

A Bizottság javasolta továbbá azt is, hogy a meglévő Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) struktúráját felhasználva jöjjön létre egy uniós kiberbiztonsági ügynökség. Az új ügynökség állandó jogállással rendelkezne, és nagyobb szerepet töltene be az európai kiberbiztonság területén. E továbbfejlesztésnek köszönhetően az Európai Uniós Kiberbiztonsági Ügynökség támogatná a tagállamokat, az uniós intézményeket és a többi érdekelt felet a kibertámadások kezelésében.

Az Egyesült Államok is hasonló úton jár. 2018. november 16-án az Egyesült Államokban Trump elnök aláírta a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökség törvényt. Ez az irányadó jogszabály a DHS-en[1] belüli korábbi

[1] *Department of Homeland Security.*

Nemzeti Védelmi és Program Igazgatóság (NPPD) küldetését emelte ki, és létrehozta a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökséget (CISA). A CISA összehangolja a biztonsággal és az ellenálló képességgel kapcsolatos erőfeszítéseket megbízható partnerségek felhasználásával a magán- és az állami szektorban, valamint technikai segítséget és értékeléseket nyújt a szövetségi érdekelt felek, valamint az infrastruktúra tulajdonosai és üzemeltetői számára országszerte. Magyarországon a Nemzetbiztonsági Szakszolgálat (NBSZ) szervezetén belül 2015. október 1-jén szintén létrehozták a Nemzeti Kibervédelmi Intézetet.

Innováció és nemzetbiztonság a 21. században

Azok az országok, amelyek képesek kihasználni a jelenlegi innovációs hullámot, kihasználni annak átalakító erejét, azok enyhíteni tudják a jövőbeni lehetséges problémákat, ebből kifolyólag gazdasági és katonai előnyben lesznek a potenciális riválisokkal szemben. Álláspontom szerint a nemzetbiztonság szempontjából eddig egy nagyon fontos fel nem használt terület a K+F+I.

Az amerikai Külkapcsolatok Tanácsa[2] az amerikai technológiai innováció jelenlegi helyzetének felmérésére egy munkacsoportot hozott létre. A munkacsoport megjegyezte, hogy az innováció, a kutatás és a technológia megfelelő módon – egységesen – történő kezelése és finanszírozása a II. világháború után az Egyesült Államokat a világ legbiztonságosabb és gazdaságilag legfejlettebb országává tette. „Ma ez a vezetői pozíció veszélyben van" – figyelmeztetett a munkacsoport. A K+F szövetségi támogatása és finanszírozása az elmúlt két évtizedben stagnált. „Washington nem tudta fenntartani az alapvető tudományok megfelelő szintű állami támogatását és finanszírozását. A K+F-be fektetett szövetségi beruházások GDP-hez viszonyított aránya 1964-ben 1,86%-ot ért el, de az 1990-es kicsit több mint 1%-ról 2016-ban 0,66%-ra csökkent."[3]

Az innovációt három tényező: a sebesség, a szétszakadás és a méretarány jellemzi manapság. Érdemes megfigyelnünk ezt az alábbi példákon keresztül: 50 év telt el a telefon feltalálásától addig, amíg az összes amerikai ház felébe

[2] A Council on Foreign Relations, CFR 1921-ben alapított magánintézet azzal a céllal, hogy külpolitikai problémák kutatásával foglalkozzon. Hivatalosan független, pártatlan szervezet.

[3] Irving Wladawsky-Berger: Innovation and National Security in the 21st Century. *The Wall Street Journal,* 2020. január 17.

eljutott egy, de az amerikaiak felének a mobil feltalálása után már öt évvel volt okostelefonja. Az emberi genomot először 2003-ban szekvenálták, a költségei hihetetlenül sokba kerültek. Ma 50 órára vállalnak genomszekvenálást, és a kezdeti százmillió dollárról már 1000 dollár alá csökkentek a költségek. A gazdasági teljesítmények egyre inkább távolodnak egymástól, a szétszakadás üteme és mértéke mindinkább növekszik. Az átlagos idő, amelyet a vállalatok a Standard & Poor's 500-on[4] töltöttek, az 1958-as 61 évről 2011-re 17 évre csökkent. Szakemberek az elkövetkező tíz év alatt azt várják, hogy a jelenleg az S & P-on működő vállalatoknak csak 25%-a marad benne.

Három fő tényező veszélyezteti a gazdasági fejlődést és a nemzetbiztonságot világszinten. Az első, hogy a globális innováció felgyorsult, ezáltal zavart okozva a különböző iparágaknak, a gazdaságoknak és a társadalmaknak. A második veszély, hogy a magánszektor globális ellátási láncai és piacai most fejlesztenek több nemzetbiztonsági technológiát és forgalmaznak is, amelyek a különböző államok mindegyike számára elérhető, és a harmadik, hogy Kína – amely mind az USA gazdasági partnere, mind pedig stratégiai versenytársa lett – jelentősen növeli a kormány által irányított kutatás-fejlesztési beruházásokat, így kíván versenyelőnyt teremteni a maga számára mind az Egyesült Államok, mind az EU ellenében.

Az új technológiák és eljárások, mint például a Mesterséges Intelligencia (MI) és az automatizálás jelentős változásokhoz vezet a munkaerőpiacon. A McKinsey Global Institute 2017. évben egy publikációt jelentetett meg ezzel kapcsolatban. A McKinsey-tanulmány arra a következtetésre jutott, hogy míg 2030-ig a foglalkozások kevesebb mint 10%-a lesz teljesen automatizált, addig a munkahelyek 60%-a átalakul az alkotóelemeik jelentős részének automatizálása révén. A tanulmány megjegyezte, hogy „bár a legtöbb forgatókönyv szerint elegendő munka áll fenn a teljes foglalkoztatás 2030-ig tartásáig, az átmenetek nagy kihívást jelentenek".[5]

A CFR-tanulmány megállapításai szerint az évtizedes amerikai vezetés az innováció és a K+F területén most veszélyben van. Ennek okai a K+F szövetségi finanszírozásának csökkentése; az otthoni oktatási kezdeményezések hiánya; bevándorlási akadályok, amelyek megnehezítik a tehetséges külföldi

[4] A Standard & Poor's 500 index rövidített elnevezése, amely a NYSE és a NASDAQ által jegyzett, érték alapján legnagyobb amerikai vállalatok indexe.

[5] James Manyika et al.: *Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages.* McKinsey Global Institute, 2017. november 28.

hallgatók és munkavállalók vonzását és megtartását; és olyan kereskedelempolitika, amely elidegeníti a korábbi gazdasági partnereket, szövetségeseket és együttműködőket. Kína gyorsan behozza technológiai hátrányát az Amerikai Egyesült Államokkal szemben. Kína jelentős forrásokat fektet be új technológiák fejlesztésébe, és 2030 után valószínűleg a világ legnagyobb kutatási és fejlesztési büdzséje lesz. Noha valószínűleg nem fogja teljes egészében utolérni az Egyesült Államok képességeit, várhatóan vezető szerepet fog játszani a kulcsfontosságú technológiákban, beleértve az MI-t, a robotikát, az energiatárolást és az 5G-s mobilhálózatokat. Tehát Kína más típusú kihívást jelent az USA számára, mint a régi Szovjetunió. Kína gazdasági partner és stratégiai versenytárs is jelenleg a világpiacon. Az Egyesült Államok és Kína egyaránt részesültek a kétoldalú beruházásokból és a kétoldalú kereskedelemből származó előnyökből. Ugyanakkor Kína arra irányuló erőfeszítései, hogy tudományos és technológiai hatalommá váljanak, hozzájárulhat a globális jólét előmozdításához, de a szellemi tulajdon másolása/lopása és annak piaccal manipuláló iparpolitikája veszélyezteti az Egyesült Államok gazdasági versenyképességét és a nemzetbiztonságot.[6]

A CFR-munkacsoport szerint az Egyesült Államoknak – ha továbbra is sikeres akar lenni a világban, valamint nemzetbiztonsági érdekeit is megfelelően kívánja védeni és érvényesíteni – új innovációs stratégiát kell kidolgoznia, amely négy kulcsfontosságú pillérre kell hogy épüljön:

A K+F szövetségi támogatását vissza kell állítani a múltbeli átlagra, a GDP jelenlegi 0,7%-át kitevő összegről (146 milliárd dollár) minimum a GDP 1,1%-ára (230 milliárd dollár) növelve. A kormányzatnak támogatnia kell a *moonshot* kezdeményezéseket[7] olyan kulcsfontosságú területeken, mint az MI, 5G, a genomika és a szintetikus biológia. Ugyanakkor a szövetségi és az állami kormányoknak évente dollármilliárdokkal kell növelniük az egyetemekbe történő beruházásokat, hogy támogassák a gazdasági és nemzetbiztonsági területeken folytatott kutatásokat.

Tudományos és technológiai munkaerő vonzása és oktatása. A kormányzatnak és az egyetemeknek ki kell dolgoznia egy kutatási, kutatói, hallgatói programot azzal a céllal, hogy versenyképes egyetemi ösztöndíjat és diplomás ösztöndíjjal támogatva kibővítse a tehetségek körét, különös figyelmet fordítva a kisebbségek és a nők alulreprezentáltságának kezelésére a területen. Hasonló kezdeményezés kezdetei, alapjai vannak lefektetve Magyarországon

[6] Manyika et al. (2017): i. m. 9.

[7] Értsd: első pillanatban hihetetlen, őrült ötletek.

az Innovációs és Technológiai Minisztérium, a Nemzeti Kutatási, Innovációs és Fejlesztési Hivatal, valamint a felsőoktatási intézmények által a különböző tudományterületeken az úgynevezett „Nemzeti Laboratórium" projekt által, amelynek a nemzetbiztonsági kutatások témakörében a Nemzeti Közszolgálati Egyetem lenne a felelőse.

Támogatni kell a kormányzatnak a K+F eredmények, technológiák bevezetését, alkalmazását a védelmi ágazatban. „A szövetségi ügynökségeknek és a katonai szolgálatoknak költségvetésük 0,5–1%-át kell a technológia gyors integrálására fordítaniuk."[8]

Technológiai szövetségek és ökoszisztémák létrehozása. Ez magában foglalja a technológiai szövetségek létrehozását a kritikus feltörekvő technológiák felhasználására és irányítására, együttműködés a kereskedelmi partnerekkel a biztonságos és szabad adatáramlás kapcsán, valamint a közös technológiai szabványok kidolgozásának előmozdítása érdekében. Ösztönözni kell az amerikai vállalatokat, hogy fektessenek be, exportáljanak és hozzanak létre kutatási és fejlesztési partnerségeket a cégekkel szerte a világon. Nemzetközi együttműködésre kell törekedni, tudományos és technológiai partnerségek hálózatát fejleszteni az élvonalbeli technológiák alkalmazására olyan globális kihívásokra, mint például az éghajlatváltozás.

Magyarországon a már korábban említett „Nemzeti Laboratórium" projekt keretében az egyetemeken a nemzetközi tudományos láthatóság megerősítése érdekében nemzetbiztonsági témakörben kutatócsoportok bekapcsolásával interdiszciplináris tudományos és technológiai kihívásokat célzó kutatási tevékenységek támogatására nyílna lehetőség a kormány által, továbbá nemzetközi szinten is elismert kutatóközpontot alakíthatnak ki.

Adatkezelés vs. adatvédelem

Az adatkezelés globális architektúrájának értékelése

A digitális gazdaság fellendülése példátlan növekedést és innovációt hajtott végre az elmúlt évtizedekben, de új politikai kihívásokat is támaszt a globális vezetők számára. A következőkben a Digital Rights Ireland-ítélet és a Schrems-ítélet kapcsán vázolom az adatvédelem és a biztonság, a digitális kereskedelem

[8] Manyika et al. (2017): i. m. 12.

és a technológia kapcsolatát az adat-ökoszisztéma megértése érdekében, valamint azt, hogy ezen ítéletek kapcsán milyen jogszabályi módosítások képzelhetők el. A cél az adatvédelmi törvények legfontosabb kihívásainak feltárása mind a nemzetek, mind az EU szintjén, amelyeket a tömeges megfigyelés során le kell küzdeni, hogy az állampolgárok/magánélet és az államok/nemzetbiztonság között megfelelő egyensúlyt lehessen fenntartani.

Snowden[9] 2013-ban hozott nyilvánosságra olyan szigorúan titkos NSA-dokumentumokat, amelyekből kiderült, hogy az amerikai titkosszolgálatok széles körben megfigyelik az emberek mobiltelefon-hívásait és internetes tevékenységét, ezzel a magánélet és a biztonság kérdését a nyilvános reflektorfénybe állítva. Ezek kihangsúlyozták az erős adatvédelmi keret szükségességét. Ugyanakkor a biztonsági aggályok és a terrortámadások elleni küzdelemre való hivatkozás gyengítheti a magánélet és az adatvédelem szigorát.

Az Európai Unió Bírósága (EUB) két kiemelkedő ítélete, nevezetesen a Digital Rights Ireland-ítélet, amely hatálytalanítja az adatvédelmi irányelvet, és a Schrems-ítélet, amely érvényteleníti a Safe Harbour-határozatot,[10] amely a transzatlanti adattovábbítás jogalapját képezi, lettek azok a döntések, amelyeknek messzemenő hatása volt az EU és a nemzeti adatvédelmi mechanizmusokra, valamint a határokon átnyúló adattovábbítási keretre is. A határozatok jelentősége abban állt, hogy meghatározták a magánélethez és az adatvédelemhez való jogot a digitális tömegmegfigyelés keretében, az USA részére átadott személyes adatok kapcsán az európai állampolgárok esetében.

Az EUB számos mérföldkőnek számító ítéletet fogadott el annak értékelésére, hogy az adatkezelés és a személyes adatok összegyűjtése összhangban álljon a 2004-ben meghatározott magánélethez való joggal és az adatvédelemmel. Az EUB 2014 áprilisában a Digital Rights Ireland-ítéletben[11] megsemmisítette az adatmegőrzési irányelvet.

A Digital Rights Ireland-ügyben 2014. április 8-án az EUB megvizsgálta a 2006/24/EK irányelv (adatmegőrzési irányelv) összeegyeztethetőségét a Charta 7. és 8. cikkével. Az irányelv kötelezte az elektronikus hírközlési szolgáltatókat,

[9] Edward Joseph Snowden (Elizabeth City, Észak-Karolina, USA, 1983. június 21.) amerikai számítógépes szakember, volt CIA-alkalmazott.

[10] Az Egyesült Államokba menő adatforgalom biztonságáról szóló Safe Harbour- (biztonságos kikötő) megállapodás.

[11] Európai Unió Bírósága, C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek.

hogy a forgalommal és a helymeghatározással kapcsolatos adatokat legalább hat és legfeljebb 24 hónapig megőrizzék, és hogy az illetékes nemzeti hatóságok számára hozzáférést biztosítsanak ezen adatokhoz súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében. Az irányelv nem engedélyezte az elektronikus kommunikáció tartalmának megőrzését. Az EUB megjegyezte, hogy az irányelv alapján a szolgáltatók által megőrzendő adatok tartalmazzák a közlés forrásának és címzettjének megtalálásához és azonosításához, továbbá valamely közlés napjának, időpontjának, időtartamának meghatározásához szükséges adatokat, a hívó telefonszámát és a hívott számot, valamint az IP-címet. Ezek az adatok

> „együttesen véve, igen pontos következtetések levonását tehetik lehetővé azon személyek magánélete vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében”.[12]

Ezért a személyes adatok irányelv szerinti megőrzése a magánélet és a személyes adatok védelméhez való jogba történő különösen súlyos beavatkozásnak minősült. Az EUB azonban úgy vélte, hogy a beavatkozás nem befolyásolta hátrányosan e jogok lényegét. A magánélethez való jogot illetően nem sérült a jog lényeges tartalma, mivel az irányelv nem tette lehetővé magának az elektronikus közlések tartalmának a megismerését. Hasonlóképpen, a személyes adatok védelméhez való jog lényege sem sérült, mivel az irányelv előírta az elektronikus hírközlési szolgáltatók számára bizonyos adatvédelmi és adatbiztonsági elvek betartását, illetve e célból megfelelő technikai és szervezési intézkedések megvalósítását. A Bíróság döntött a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről szóló 2006/24/EK európai parlamenti és tanácsi irányelv érvénytelenségéről. Az EU Bírósága ebben az ítéletben utalt arra, hogy az arányosság elve megköveteli, hogy az uniós intézmények aktusai alkalmasak legyenek a szóban forgó szabályozás által kitűzött jogszerű célok elérésére, és ne haladják meg az e célok eléréséhez szükséges mértéket. E feltételek tiszteletben tartásának bírósági felülvizsgálatát tekintve elmondható, hogy ha alapvető jogokba való beavatkozásról van szó, az uniós jogalkotó mérlegelési jogkörének terjedelme korlátozott lehet bizonyos körülményektől

[12] C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek, 21.

függően, amelyek között szerepel többek között az érintett terület, a szóban forgó, Charta által biztosított jog jellege, a beavatkozás jellege és súlyossága, valamint annak célja. A szóban forgó Digital Rights Ireland-ügyben a Bíróság kimondta, hogy – figyelembe véve egyrészről azt a fontos szerepet, amelyet a személyes adatok védelme tölt be a magánélet tiszteletben tartásához való alapvető jog tekintetében, másrészről pedig az e jogot érintő, a 2006/24/EK irányelv által megvalósított beavatkozás mértékét és súlyosságát – az uniós jogalkotó mérlegelési jogköre korlátozott, és ezért azt szigorú felülvizsgálatnak kell alávetni.[13]

A Bíróság 2015. október 6-án hozott ítéletet a Schrems-ügyben.[14] Az ítélet az egyének védelmével foglalkozott személyes adataik harmadik országba – az adott esetben az Egyesült Államokba – továbbítását illetően. Schrems, egy osztrák állampolgár, aki éveken keresztül Facebook-felhasználó volt, panaszt nyújtott be az ír adatvédelmi felügyeleti hatóságnál, amelyben kifogásolta személyes adatainak továbbítását a Facebook ír leányvállalatától a Facebook Inc. vállalat részére, és az USA-ban lévő szerverekre, ahol azokat kezelték. Azzal érvelt, hogy figyelemmel Edward Snowdenre, a megfigyelési visszaélést bejelentő amerikai személy által 2013-ban az Egyesült Államok hírszerző szolgálatainak a tevékenységeire vonatkozóan kiszivárogtatott információkra, az Egyesült Államok joga és gyakorlata nem biztosít elégséges védelmet az amerikai területre továbbított személyes adatok tekintetében. Snowden feltárta, hogy a National Security Agency (Nemzetbiztonsági Ügynökség) közvetlenül rákapcsolódik cégek, például a Facebook szervereire, és elolvashatja a csevegések és privát üzenetek tartalmát.

Az adatok USA-ba történő továbbítása egy 2000-ben elfogadott bizottsági megfelelőségi határozaton alapult, amely lehetővé teszi az adattovábbítást azon amerikai vállalatok számára, amelyek nyilatkoztak arról, hogy az EU-ból továbbított személyes adatokat védik, és megfelelnek az úgynevezett „biztonságos kikötő" adatvédelmi elveknek. Amikor az ügyet az EUB elé vitték, a Bíróság a Charta alapján vizsgálta meg a bizottsági határozatot. Emlékeztetett arra, hogy az EU-ban az alapjogok védelmével szemben támasztott követelmény, hogy az érintett jogokra vonatkozó eltérések és korlátozások a feltétlen szükségesre korlátozódjanak. Az EUB az olyan szabályozást, amely lehetővé teszi a közjogi hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, úgy tekintette, hogy az „a magánélet tiszteletben

[13] C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek, 17.
[14] EUB, Maximillian Schrems kontra Data Protection Commissioner, C-362/14. sz. ügy.

tartásához való, a Charta 7. cikkében biztosított alapvető jog lényegét sérti". A jogot a lényegétől fosztaná meg, ha az amerikai hatóságok válogatás nélkül hozzáférhetnének az elektronikus kommunikációhoz anélkül, hogy szükség lenne az érintett egyénekkel konkrét kapcsolatban nemzetbiztonsági vagy bűnmegelőzési megfontolásokra alapított objektív igazolásra, és anélkül hogy e megfigyelési gyakorlatokhoz megfelelő visszaélésekkel szembeni garanciák társulnának.

Ráadásul az EUB megállapította, hogy „az olyan szabályozás, amely nem biztosítja a jogalany számára a jogorvoslat lehetőségét abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse",[15] összeegyeztethetetlen a hatékony bírói jogvédelemhez való alapjoggal (Charta 47. cikk). Ezért a biztonságos kikötőről szóló határozat lényegét tekintve nem biztosította az alapjogoknak a Charta fényében értelmezett irányelv alapján az EU-ban garantált védelmi szinttel egyenértékű védelmét. Az EUB következésképp érvénytelenítette a határozatot.

Az EUB-ítéletek kapcsán néhány kérdéskört kívánok vizsgálni a magánélettel és a nemzetbiztonsággal kapcsolatos alapvető kérdések és kihívások témakörében. A terrorizmus elleni küzdelem szükségessége, különösen a szeptember 11-i támadások után, vezetett a tömeges megfigyelési gyakorlatok bevezetéséhez mind az EU-ban, mind az Egyesült Államokban. Fontos megjegyezni, hogy az EU adatvédelmi szabályai nemcsak a gazdasági fejlődés fontos eszközévé váltak, hanem a nemzetbiztonsági célok megvalósítójává is, ily módon befolyásolva a magánélethez való jogot. Ennek kapcsán szükséges feltárni az adatvédelmi törvény és a nemzeti, valamint az uniós szintű politikai kihívásokat, amelyeket a tömeges digitális megfigyelésre adott válaszként le kell küzdeni annak érdekében, hogy fenntartható legyen a megfelelő egyensúly a magánélet és a nemzetbiztonság között.

A biztonság mint az EU adatvédelmi szabályainak célja

Az információs és kommunikációs technológiák ágazatának gyors fejlődése új lehetőségeket, de új kihívásokat is felszínre hozott. A határok nélküli információkhoz való hozzáférés képessége döntő jelentőségű a társadalmi és gazdasági kölcsönhatások és a technológiai fejlődés szempontjából. Az adatfeldolgozás

[15] C-362/14. sz. ügy 24.

növekvő gazdasági jelentősége azonban aggodalmakat vet fel az alapvető jogok hatékony védelme miatt az információs társadalomban.

Az új uniós adatvédelmi szabályok végleges elfogadása jelentős lépést tett az uniós polgárok alapvető jogainak a digitális korban történő megerősítése érdekében. Az adatvédelmi csomag magában foglalja az általános adatvédelmi rendeletet,[16] amely 2016. május 24-én lépett hatályba, és 2018. május 25-től alkalmazandó. Ez magában foglalja a rendőrség és a büntető igazságügyi hatóságok adatvédelmi irányelvét,[17] amely 2016. május 5-én lépett hatályba és amelyeket az EU-tagállamoknak 2018. május 6-ig kellett átültetniük a nemzeti jogukba. Ezeknek a célja az adatvédelem megfelelően magas szintjének biztosítása volt.

Hasonlóképpen, a terrorizmus elleni küzdelem szükségessége korábban olyan adatmegőrzési rendszerek bevezetéséhez vezetett, amelyek lehetővé tették a kommunikáció állami megfigyelését biztonsági célokból. Az adatmegőrzési irányelvet a madridi (2004) és a londoni (2005) terroristatámadásokra adott válaszként hozott sürgős terrorizmusellenes intézkedésként vezették be. Az alapvető jogok tiszteletben tartásával kapcsolatos aggodalmak ellenére hatalmas politikai nyomás alatt gyorsan elfogadták, és 2006-ban lépett hatályba. Az adatmegőrzési irányelv a tagállamokat arra kötelezte, hogy a távközlési és internetszolgáltatókat kötelezzék a forgalmi és helymeghatározási adatok tárolására a vezetékes és a mobiltelefon, valamint az internetes e-mail-kommunikáció vonatkozásában legalább hat hónapig, de legfeljebb két évig, és ezekhez biztosítsanak hozzáférést kérésre a bűnüldöző hatóságok számára a súlyos bűncselekmények és a terrorizmus kivizsgálása, felderítése és üldözése céljából. A Digital Rights Ireland-ügyben az EUB azonban érvénytelennek nyilvánította az adatmegőrzési irányelvet azon az alapon, hogy az indokolatlanul sérti az alapvető jogokat.

[16] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyek védelméről a személyes adatok feldolgozása során és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről. EK (általános adatvédelmi rendelet) [2016]. HL L 119.

[17] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a természetes személyek védelméről a személyes adatoknak az illetékes hatóságok általi feldolgozása során az ilyen személyek megelőzése, kivizsgálása, felderítése vagy üldözése céljából, bűncselekmények vagy büntetőjogi szankciók végrehajtása, valamint az ilyen adatok szabad mozgásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről miközben javítja az egész Európában a terrorizmus és más súlyos bűncselekmények elleni küzdelem terén folytatott együttműködést. A személyes adatok védelmére vonatkozó új uniós szabályok tehát a digitális egységes piaci stratégia, valamint az EU biztonsági menetrendje alapvető elősegítői.

A kommunikációs adatok megőrzését a terrorizmus elleni küzdelem eszközeként széles körben alkalmazták az Atlanti-óceánon túl is. A szeptember 11-i terrorista támadások után az Egyesült Államok egyoldalúan elkezdte kiaknázni a digitális kommunikációs technológiák sebezhetőségét az elektronikus megfigyelés és a kommunikáció lehallgatása érdekében mind az Egyesült Államokban, mind a világ más országaiban. Az USA Nemzeti Biztonsági Ügynöksége (NSA) volt alkalmazottjának, Edward Snowdennek a 2013. évi leleplezése során felfedték a korábban elképzelhetetlen léptékű globális megfigyelését az Egyesült Államok állampolgárainak és más, külföldi személyek telekommunikációjának és adatáramlásának, az úgynevezett „Öt Szem"[18] hírszerzési információhálózat segítségével. Az „Öt Szem" magában foglalja az Egyesült Királyságot, az Egyesült Államokat, Ausztráliát, Kanadát és Új-Zélandot, az NSA irányításával, valamint kiterjedt együttműködés jött létre az EU különböző tagállamainak hírszerző hatóságai között, különösen az Egyesült Királyságban, Németországban és az Egyesült Államokban.

Ezek a felfedések globális aggodalomra adtak okot az emberi jogokra gyakorolt negatív hatásaik miatt. A nemzetközi közösség, különösen az Egyesült Nemzetek Szervezete (ENSZ) szervei komoly aggodalommal figyelték a kommunikáció megfigyelésének és lehallgatásának, valamint a személyes adatok gyűjtésének kialakult gyakorlatát. A digitális kommunikációs technológiák jogellenes vagy önkényes megfigyelésének és elfogásának kockázata visszatarthatja az innovációt és alááshatja a digitális gazdaság nyújtotta lehetőségeket, mivel a magánélet védelmét kritikusnak tekintik a bizalom szempontjából, amely különösen fontos eszköz a globális online környezetben.

Az extraterritoriális digitális tömegmegfigyelés feltárása szintén befolyásolta a transzatlanti kapcsolatokat, és kérdéseket vetett fel az Egyesült Államok és az EU közötti hosszú távú adattovábbítási megállapodások jogszerűségéről. A személyes adatok harmadik országokba történő továbbításának fő szabályait az EU adatvédelmi irányelvének 25. és 26. cikke tartalmazza, amely meghatározza azt az alapelvet, miszerint a személyes adatok átadására csak akkor kerülhet sor, ha a harmadik ország megfelelő szintű védelmet biztosít (Schrems-ügy). Nevezetesen ebben az esetben az alapvető kérdés az volt, hogy az Egyesült Államok biztosítja-e az adatvédelem megfelelő szintjét az uniós polgárok személyes adataival való visszaélésének megakadályozása érdekében, mivel a „biztonságos kikötő" szabályait a nemzetbiztonsági követelmények felülbírálhatják.

[18] UKUSA-egyezmény, Five Eyes, FVEY.

A magánélet védelméhez és az adatvédelemhez fűződő beavatkozások indokolása a nemzetbiztonság érdekében

Az EUB mindkét ítéletében elismerte, hogy a magánélethez és az adatvédelemhez való jog beavatkozása a Charta 52. cikkének (1) bekezdése alapján szigorú szükségesség és arányosság vizsgálatát követeli meg. E cikk értelmében korlátozásokat lehet előírni az alapvető jogok és szabadságok gyakorlására, mindaddig, amíg ezeket a korlátozásokat törvény írja elő, vizsgálva azt, hogy tiszteletben tartják e jogok és szabadságok lényegét, és az arányosság elvére figyelemmel szükségesek-e, és valóban megfelelnek az EU által elismert általános érdekű céloknak, vagy mások jogai és szabadságai védelmének szükségességéhez. A Schrems-ügyben kijelentette, hogy az Egyesült Államok jogszabályai, a hatóságok általános hozzáférési lehetősége a kommunikációs adatok tartalmához veszélyeztetik a magánélethez való jog lényegét.

Az EUB felhívta a figyelmet a magánélet és az adatvédelem fogalmai közötti különbségekre annak az elméletnek megfelelően, hogy a magánélethez való jog „optikai eszköz", amely tiltja a behatolást a magánszférába, míg az adatvédelemhez való jog „átláthatósági eszköz", amely a személyes adatok kezelésére vonatkozik, és felhatalmazza az egyént az adatok és a felhasználásuk bizonyos szintű ellenőrzésére.

Az ítéletek következményei

Az adatvédelem következményei a tagállamokban

Az EUB ítéletei jelentősen befolyásolják a tagállami adatvédelmi törvényeket, valamint a tagállamok adattovábbítási gyakorlatait is. A Digital Rights Ireland-ítélet eltérő igazságügyi és jogalkotási reakciókat váltott ki a tagállamok között a nemzeti adatvédelmi törvények tekintetében. A Schrems-ítélet emellett felhívta a figyelmet arra, hogy politikai megállapodásra kell jutni a tagállamok között az állami felügyeleti kérdésekben. Az EUB jelentősen megerősítette az adatvédelmi hatóságok szerepét azáltal, hogy felhatalmazta őket arra, hogy megvizsgálják a harmadik országok adatvédelmének szintjét az alapvető jogok megsértésére alapított egyedi igények kezelése érdekében. A hatóságok korlátozhatják az adattovábbítást, amennyiben az alapvető jogok megsértését találják.

Az adatvédelem következményei az EU-ban

Az EUB ítéleteiben körvonalazott alapelveket figyelembe kellett venni az adatkezelő rendszerek vonatkozásában. A személyes adatok továbbítását lehetővé tevő, harmadik országokkal kötött megállapodásokat szintén felül kellett vizsgálni a Schrems- és a Digital Rights Ireland-ítéletek fényében, például az Egyesült Államokkal, Kanadával és Ausztráliával kötött PNR-megállapodásokkal és az EU–USA TFTP[19] megállapodással kapcsolatban. A Schrems-ítélet jelentősen felgyorsította a személyes adatok transzatlanti cseréjére vonatkozó új adatvédelmi rendszerről folytatott tárgyalásokat. Az Európai Bizottság 2016. július 12-én elfogadta az EU – Egyesült Államok adatvédelmi pajzsot, amely felváltotta a korábbi, az EUB által érvénytelenített Safe Harbour-határozatot.

A fent említett kihívásokat, amelyekkel az EU szembesül, a jelenlegi nemzetközi kontextusban kell vizsgálni, ahol az adatok tömeges megjelenése és a növekvő biztonsági igények új megoldásokat igényelnek. A megfigyelésre és a nemzetközi adatvédelmi normákra vonatkozó új nemzetközi normák kidolgozására irányuló globális kezdeményezések lehetnek a nemzetbiztonság és a magánélet közötti közösen elfogadott egyensúly megteremtésének új eszközei.

Következtetések

Az EU adatvédelmi szabályai nemcsak fontos gazdasági fejlesztési eszközökké váltak, hanem a nemzetbiztonság elősegítőjévé is. A növekvő biztonsági fenyegetések az EU-polgárok személyes adatainak belföldi és extraterritoriális digitális megfigyelését eredményezte, amely komoly aggodalmakat vet fel az alapvető jogok hatékony védelme miatt. Ezek az aggodalmak az EUB-nál jelentkeztek elsőnek, amely két mérföldkőnek mondott – korábban is említett – ítéletet fogadott el, nevezetesen a Digital Rights Ireland-ítéletet és a Schrems-ítéletet, amelyeknek nagy jelentősége van a Charta 7. és 8. cikkében rögzített, magánélethez és az adatvédelemhez való jog megerősítése szempontjából.

Az EUB mindkét esetben szigorú szükségesség és arányosság követelménye vizsgálatát követeli meg az alapvető jogokba való beavatkozás értékelésekor

[19] A terrorizmus finanszírozásának felderítését célzó program (*Terrorist Finance Tracking Programme,* TFTP) keretében pénzügyi adatok átadása ellenőrzött keretek között.

a nemzetbiztonság érdekében, és ösztönzi az erős eljárási biztosítékok, például a független felügyeleti mechanizmusok és a hatékony jogorvoslatok alkalmazását tömeges adatgyűjtés és a személyes adatok cseréje során. E garanciák ellenére azonban az egyének nemzetbiztonsági célú nagyszámú és válogatás nélküli felügyelete nem tekinthető indokoltnak. Az EUB szerint további tisztázást igényel annak kérdése, hogy a tömegmegfigyelési intézkedések milyen mértékben tartják tiszteletben a magánélethez és az adatvédelemhez való jog lényegét, és összhangban állnak-e ezekkel a jogokkal.[20]

Az EUB ítéletei politikai megállapodásra szólítanak fel az EU tagállamai között a tömeges megfigyelés kérdésében. A Digital Rights Ireland-ítélet eltérő igazságügyi és jogalkotási reakciókat váltott ki az EU-tagállamokban; ugyanakkor lassan felülvizsgálják a tagállamok a nemzeti adatmegőrzési törvényeket a meghatározott alapjogi normák fényében. Hasonlóképpen, a Schrems-ítélet, amely felhatalmazza a nemzeti adatvédelmi hatóságokat arra, hogy adatküldés esetén megvizsgálják a harmadik országok adatvédelmének szintjét, eltérő személyes adatvédelmi előírások alkalmazását eredményezheti. Az EUB ítéleteit figyelembe kell venni minden olyan létező vagy tervezett uniós jogszabály vonatkozásában, amely a személyes adatok nagyszabású gyűjtését és feldolgozását vonja maga után. Látni kell, hogy az EU-n belüli adatmegőrzési mechanizmusok, különösen az EU PNR-irányelv, valamint a harmadik országokkal kötött PNR-megállapodások[21] megfelelnek-e a Digital Rights Ireland-ítéletben megállapított követelményeknek. Figyelembe véve a Schrems-ítéletnek a transzatlanti adattovábbítási keretre gyakorolt hatását, az EU–USA adatvédelmi pajzs,[22] bár új eljárási biztosítékokat vezet be, nem lesz képes hatékony védelmet nyújtani a nemzetbiztonsági célokból történő megfigyelés ellen. Ezek a kihívások új megközelítéseket igényelnek mind az EU-n belül, mind azon kívül, hogy meghatározzák a megfelelő korlátokat a tömeges digitális megfigyelés számára, és megtalálják a nemzetbiztonság és a magánélet közötti közösen elfogadott egyensúlyt.

[20] Irena Nesterova: *Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards.* European Society of International Law, (ESIL) 2016 Annual Conference (Riga). 2017.

[21] Utasnyilvántartási adatállomány.

[22] Az adatvédelmi pajzs akkor engedi meg a személyes adatok továbbítását az EU-ból egy amerikai vállalathoz, ha az amerikai vállalat a személyes adatok kezelése (például felhasználása, tárolása és továbbadása) során szigorú adatvédelmi szabályok és biztosítékok szerint jár el.

Felhasznált irodalom

Arkin, William M. – Alexa O'Brien: *The Most Militarized Universities in America: A VICE News,* 2015. november 6. Online: www.vice.com/en_us/article/j59g5b/the-most-militarized-universities-in-america-a-vice-news-investigation

Balogh László Levente: Állam és erőszak. *Politikatudományi Szemle,* 20. (2011), 1. 119–132. Online: www.poltudszemle.hu/szamok/2011_1szam/balogh.pdf

Bailey, Ronald: Is Russia's Surveillance State Being Modelled on the West? New Russian Anti-encryption and Data Retention Laws Look Sadly Familiar. *Reason,* 2016. július 22. Online: https://reason.com/archives/2016/07/22/is-russias-surveillance-state-being-mode/print

Bán Ernő: *Kémek – hazaárulók.* Budapest, Zrínyi, 1966.

Barker, Anne: Captagon: Evidence Paris Attackers Used 'Jihadist's Drug' Favoured by Islamic State Fighters. *ABC News,* 2015. november 25. Online: www.abc.net.au/news/2015-11-24/captagon-the-drug-that-kept-the-paris-attackers-calm/6970464?nw=0&r=Gallery

Besenyei Lajos: A generációváltás forradalma. *Opus et Educatio,* 3. (2016), 4. 371–378. Online: https://doi.org/10.3311/ope.19

Beke József: Az Európai Unió hírszerző képességének technikai támogatása. *Nemzetbiztonsági Szemle,* 6. (2018), 2. 56–68. Online: https://epa.oszk.hu/02500/02538/00023/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_02_056-068.pdf

Béres János: A hírszerzés feladatrendszere. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 117–128. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8567/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y

Béres János (szerk.): *Külföldi nemzetbiztonsági szolgálatok.* Budapest, Zrínyi, 2018.

Bischoff, Paul: The word's most-surveilled cities. *Comparitech,* 2019. Online: www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Boda József – Regényi Kund (szerk.): *A hírszerzés története az ókortól napjainkig.* Budapest, Dialóg Campus, 2019. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12692/web_PDF_Hirszerzes_tortenete_okortol_napjainkig.pdf;jsessionid=0572E51ED460A99D94B07ADDAE7657EA?sequence=1

Bond, David: Britain Preparing to Launch New Cyber Warfare Unit. *Financial Times,* 2018. szeptember 21. Online: www.ft.com/content/eef717f2-bb6e-11e8-8274-55b72926558f

Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására). *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/2066

Buda András: Generációk, társadalmi csoportok a 21. században. *Magyar Tudomány,* 180. (2019), 1. 120–129. Online: https://doi.org/10.1556/2065.180.2019.1.12

Bulgakov, Mihail A.: *A Mester és Margarita.* (ford. Szőllősy Klára) Budapest, Európa, 2019.

Burds, Jeffrey: *The Second Oldest Profession. A World History of Espionage.* Boston, Recorded Books, 2011.

Bures, Oldrich – Helena Carrapico: Private Security beyond Private Military and Security Companies: Exploring Diversity within Private-Public Collaborations and its Consequences for Security Governance. *Crime, Law and Social Change,* 67, (2017), 3. 229–243. Online: https://doi.org/10.1007/s10611-016-9651-5

Brown, Dalvin: The U.S. Navy banned TikTok from Government-issued Smartphones over Cybersecurity Concerns. *USA Today,* 2019. december 23. Online: https://eu.usatoday.com/story/tech/2019/12/23/us-navy-bans-personnel-using-tiktok-government-issued-phones/2732203001/

Chikán Attila: *Vállalatgazdaságtan.* Budapest, Aula, 2008.

Cornely, David Dwaine: *Leadership and Security: Factors that Support or Prevent Successful Integration into Research and Development Organizations.* Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Management in Organizational Leadership. University of Phoenix, 2003.

Contentgroup: Social Media on the Campaign Trail: Barack Obama and Donald Trump. (2017). Online: https://contentgroup.com.au/2017/09/social-media-campaign-trail-obama-trump/

Csepeli György: *Szociálpszichológia.* Budapest, Osiris, 2001.

Csiki Tamás – Tálas Péter: A védelmi beszerzés és kutatás-fejlesztés kapcsolata a védelmi tervezés rendszerében – nemzetközi tapasztalatok. *Nemzet és Biztonság,* (2013), 3–4. 107–142. Online: www.nemzetesbiztonsag.hu/cikkek/nb_2013_3-4_09_csiki_tamas-talas_peter_-_a_vedelmi_beszerzes_es_kutatas-fejlesztes_kapcsolata_a_vedelmi_tervezes_rendszereben_-_nemzetkozi_tapasztalatok.pdf

Dahl, Erik J.: *Warning of Terror: Explaning the Failure of Intelligence against Terrorism.* Master of Arts in Law and Diplomacy Thesis, The Fletcher School, 2004. Online: https://dl.tufts.edu/pdfviewer/nc580z70h/ks65hq04h

Dalha, Tenzin: Beijing's Export of Surveillance Technology. *Modern Diplomacy,* 2020. január 7. Online: https://moderndiplomacy.eu/2020/01/07/beijings-export-of-surveillance-technology/

Dhami, Mandeep K.: Behavioural Science Support for JTRIG'S (Joint Threat Research and Intelligence Groups) Effects and Online HUMINT Operations. 2011. *The Intercept,* 2015. június 22. Online: https://theintercept.com/document/2015/06/22/behavioural-science-support-jtrig/

Deák András György: Kevés egyezmény, kívánt eredmény? – Trump kínai „vámháborújának" mérlege. *NKE Stratégiai Védelmi Kutatóintézet Elemzések,* (2020), 8. 1–12. Online: https://tinyurl.com/3w5c9je7

Deák Veronika: Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle,* 12. (2019), 3. 95–111. Online: https://doi.org/10.32563/hsz.2019.3.6

Dobák Imre: Technológiai fejlődés – titkosszolgálatok. In Fekete Károly (szerk.): *Kommunikáció.* Budapest, Nemzeti Közszolgálati Egyetem, 2013. 61–71.

Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8567/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y

Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12. (2017), 2. 235–249. Online: http://hadmernok.hu/172_19_dobak.pdf

Dobák Imre: OSINT – Gondolatok a kérdéskörhöz. *Nemzetbiztonsági szemle,* 7. (2019), 2. 83–93. Online: https://doi.org/10.32561/nsz.2019.2.7

Dobák Imre – Regényi Kund (szerk.): *Szakmatörténeti szemelvények.* Budapest, Nemzetbiztonsági Szakszolgálat, 2014.

Dodsworth, Francis: Police and the Prevention of Crime: Commerce, Temptation and the Corruption of the Body Politic, from Fielding to Colquhoun. *British Journal of Criminology,* 47. (2007), 3. 439–454. Online: https://doi.org/10.1093/bjc/azl054

Domokos Erika: Oroszország letilt egy üzenetküldő szolgáltatást. *Napi.hu,* 2018. április 13. Online: www.napi.hu/tech/oroszorszag_letilt_egy_uzenetkuldo_szolgaltatast.660552.html

Drobinina, Ekaterina: Russian Search-Engine Yandex Passed Information to FSB. *BBC News,* 2011. május 3. Online: www.bbc.com/news/business-13274443

Drusza Tamás: A szervezeti kultúra jelentősége a generációs kihívás és a nemzetbiztonsági szolgálatok fejlesztése szempontjából. *Nemzetbiztonsági Szemle,* 6. (2018), 2. 69–89. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1591

Drusza Tamás: Jövőbeni kihívások a (polgári) nemzetbiztonsági elhárítás területén. In Drusza Tamás (szerk.): *A magyar elhárítás fejlődése.* Budapest, Dialóg Campus, 2019. 211–238.

Eftimiades, Nicolas: Uncovering Chinese Espionage in the US. *The Diplomat,* 2018. november 28. Online: https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/

Erdész Viktor: A SOCMINT helye, szerepe az összadatforrású hírszerzésben. *Felderítő Szemle,* (2018), 4. 27–40.

Európai Unió Alapjogi Ügynöksége – Európa Tanács: *Európai adatvédelmi jogi kézikönyv* 2018. évi kiadás, Luxembourg, Az Európai Unió Kiadóhivatala, 2019. Online: www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf

Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései. *Infokommunikáció és Jog,* 12. (2015), 62–63. 45–57.

Finszter Géza: Állambiztonság – nemzetbiztonság. *Nemzetbiztonsági Szemle,* 7. (2019), 3. 98–117. Online: https://doi.org/10.32561/nsz.2019.3.8

Firsing, Scott: The Growing Link between Intelligence Communities and Academia. *The Conversation,* 2015. szeptember 30. Online: http://theconversation.com/the-growing-link-between-intelligence-communities-and-academia-47184

Foulkes, Imogen: Swiss Crypto AG Spying Scandal Shakes Reputation for Neutrality. *BBC News,* 2020. február 16. Online: www.bbc.com/news/world-europe-51487856

Fukuyama, Francis: *A történelem vége és az utolsó ember.* Budapest, Európa, 2014.

Galántai Zoltán: Big data, tudomány, kauzalitás. *Információs Társadalom,* 16. (2016), 2. 32–43. Online: https://doi.org/10.22503/inftars.XVI.2016.2.2

Gearon, Liam: The Counter-Terrorist Campus: Securitisation Theory and University Securitisation – Three Models. *Transformation in Higher Education,* 2. (2017), a13. 2519–5638. Online: https://doi.org/10.4102/the.v2i0.13

Green, J. J.: The Fog of Espionage. Part 3: 'A Bewildering Variety of Poisonous Snakes'. *Wtop News,* 2019. szeptember 27. Online: https://wtop.com/j-j-green-national/2019/09/the-fog-of-espionage-part-3-a-bewildering-variety-of-poisonous-snakes/

Greenwald, Glenn: *A Snowden-ügy: korunk legnagyobb nemzetbiztonsági botránya*. Budapest, HVG, 2014.

Gutheil, Mirja – Quentin Liger – Aurélie Heetman – James Eager – Max Crawford: *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Study for the LIBE Committee, European Union, 2017. Online: www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

Haig Zsolt – Kovács László – Ványa László – Vass Sándor: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10964/webview.pdf?sequence=1&isAllowed=y

Harris, Matthew: The Limit of Intelligence Gathering: Gianni Vattimo and the Need to Monitor 'Violent' Thinkers. In Jai Galliott – Warren Reed (szerk.): *Ethics and the future of spying, Technology, National Security and Intelligence Collection*. Routledge, 2016. 27–38.

Héjja István: Nemzetbiztonsági szervezeti modellek. In Dobák Imre: *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 57–72.

Huntington, Samuel P.: *A civilizációk összecsapása és a világrend átalakulása.* Budapest, Európa, 2019.

Jávor Endre: A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban. *Nemzetbiztonsági Szemle,* 5. (2017), 3. 36–60. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1679

Jasenszky Nándor (szerk.): *Mindennapi biztonság.* Budapest, Terrorelhárítási Központ, 2019.

Johnson, Loch K.: *National Security Intelligence, Secret Operations in Defense of the Democracies.* Second edition, Malden, John Wiley & Sons, Polity Press, 2017.

Joint Economic Committee: *Soviet Economy in the 1980's: Problems and Prospects Part 1.* Washington, Joint Committee Print, 1983. Online: www.jec.senate.gov/reports/97th%20Congress/Soviet%20Economy%20in%20the%201980s%20-%20Problems%20and%20Prospects%20Part%20I%20%281185%29.pdf

Kadomtsev, Andrej: 5G: A New Stage in Civilization Development amid Global Competition. *Modern Diplomacy,* 2019. december 26. Online: https://moderndiplomacy.eu/2019/12/26/5g-a-new-stage-in-civilization-development-amid-global-competition/

Kadtke, James – John Wharton: Technology and National Security: The United States at a Critical Crossroads. *Defense Horizons,* 2018. március 1. Online: https://inss.ndu.edu/Portals/68/Documents/defensehorizon/DH-84.pdf

Kampe, Christopher – Gwendolynne Reid – Paul Jones – S. Colleen – S. Sean – Kathleen M. Vogel: Bringing the National Security Agency into the Classroom: Ethical Reflections on Academia-Intelligence Agency Partnerships. *Science and Engineering Ethics,* (2019), 25. 869–898. Online: https://doi.org/10.1007/s11948-017-9938-7

Kasznár Attila: A terrorelhárítás feladatrendszere a turizmusban. In Kiglics Norbert (szerk.): *II. Turizmus és Biztonság Nemzetközi Tudományos Konferencia Konferenciakötet.* Nagykanizsa, Pannon Egyetem, 2017. 48–55. Online: https://uni-pen.hu/files/konferencia/2017/Teljes_konf_tanulmanykotet.pdf

Kenedli Tamás: A nyílt forrású információszerzés (OSINT). In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Kenyeres Ágnes (szerk.): *Magyar Életrajzi Lexikon.* Budapest, Akadémiai Kiadó, 1994.

Kis-Benedek József: A nemzetbiztonsági szolgálatok nemzetközi együttműködése *Hadtudomány,* 23. (2013), 1–2. 100–114. Online: www.mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf

Kovács Zoltán: Az alkalmazásszolgáltatók törvényes ellenőrzésének jövője – a technológiák konvergenciájának tükrében. *Nemzetbiztonsági Szemle,* 4. (2016), 1. 79–99. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1815/1105

Külgazdasági és Külügyminisztérium Magyarország Nagykövetsége, Peking, Vezetői összefoglaló, 2017–18 TET éves beszámoló.

Kris, Davis S.: Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond. *Hoover Institution Essay, Aegis Paper Series,* (2016), 1601. Online: www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf

Laufer Balázs – Takács Gergely: A HUMINT vége? *Arc és Álarc,* 2. (2018), 1–2. 175–185. Online: www.hamvasintezet.hu/wp-content/uploads/2018/10/HAMVAS_2018_TAVASZ_NYAR_net.pdf

Lenyűgöző közösségi média statisztikák I. rész. *Szubjektív,* (2018. szeptember 12.). Online: https://szubjektiv.com/lenyugozo-kozossegi-media-statisztikak-1/

Loringhoven, Arndt Freytag von: Adapting NATO intelligence in support of "One NATO". *NATO Review,* 2017. szeptember 8. Online: www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html

Loringhoven, Arndt Freytag von: A New Era for NATO Intelligence. *NATO Review,* 2019. október 29. Online: www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html

Lowenthal, Mark M.: *A titkoktól a politikai döntésig.* Budapest, Antall József Tudásközpont, 2017.

Mackinnon, Amy: How Russia is Strong-Arming Apple. *Foreign Policy,* 2019. január 31. Online: https://foreignpolicy.com/2019/01/31/how-russia-is-strong-arming-apple-data-security-icloud/

Major Milán: Az orosz védelmi ipari komplexum a Szovjetunió szétesésétől napjainkig. *NKE Stratégiai Védelmi Kutatóintézet Nézőpontok,* (2020), 2. 1–10. Online: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKK_N%C3%A9z%C5%91pontok_2020_2_Az%20orosz%20vedelmi%20ipari%20komplexum%20a%20Szovjetunio%20szetesesetol%20napja%20inkig_(Major%20M.).pdf

Manyika, James – Susan Lund – Michael Chui – Jacques Bughin – Jonathan Woetzel – Parul Batra – Ryan Ko – Saurabh Sanghvi*: Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages.* McKinsey Global Institute, 2017. november 28. Online: www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

McPherson, Peter – Mary Sue Coleman: We Must Have Both. *Inside Higher Ed,* 2019. augusztus 5. Online: www.insidehighered.com/views/2019/08/05/research-universities-must-bolster-both-security-and-openness-opinion

M. Császár Zsuzsa – Bányai Bence – Gyura Gábor – Farkas Marcell: A nemzetközi hallgatói migráció biztonságpolitikai kockázatainak egyes aspektusai. *Nemzetbiztonsági Szemle,* 6. (2018), 3. 49–64. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1498/820

Meretei Barbara: Generációs különbségek a munkahelyeken. *Vezetéstudomány,* 48. (2017), 10. 10–18. Online: https://doi.org/10.14267/VEZTUD.2017.10.02

Mitnick, Kevin D. – William L. Simon: *Art Of Deception: Controlling the Human Element of Security.* Hoboken, John Wiley & Sons, 2003.

Moody, Glyn: Revised Snooper's Charter Ignores Key Criticisms, Widens Police Powers Further. *Ars Technica,* 2016. március 2. Online: http://arstechnica.co.uk/tech-policy/2016/03/revised-snoopers-charter-ignores-key-criticisms-widens-police-powers-further/

Moraes, Claude*: Working Document 1 on the US and EU Surveillance Programmes and their Impact on EU Citizens Fundamental Rights.* Committee on Civil Liberties, Justice and Home Affairs, 2013. Online: www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf

M. Tóth Balázs – Pap András László: *A hatékonyság mítosza. Az etnikai profilalkotás alkotmányos és rendészeti kérdőjelei.* Budapest, L'Harmattan, 2012.

Nesterova, Irena: *Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards.* European Society of International Law, (ESIL) 2016 Annual Conference (Riga), 2017. Online: https://doi.org/10.2139/ssrn.2911999

Nishimura, Hiroshi – Kanoshima, Emiko – Kono, Kazuhiro: Advancement in Science and Technology and Human Societies. In Seiji Abe – Mamoru Ozawa – Yoshiaki Kawata (szerk.): *Science of Societal Safety Living at Times of Risks and Disasters.* Springer, 2019. 15–26. Online: https://doi.org/10.1007/978-981-13-2775-9_2

O'Connell, Kevin M.: The Role of Science and Technology in Transforming American Intelligence. In Peter Berkowitz (szerk.): *The Future of American Intelligence.* Hoover Press, 2005.

Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012.

Pál Eszter – Törőcsik Mária: *Irodalmi áttekintés a Z generációról.* Pécs, Pécsi Tudományegyetem, 2013. Online: https://ktk.pte.hu/sites/ktk.pte.hu/files/images/szervezet/intezetek/mti/pal_torocsik_irodalmi_attekintes_a_z_generaciorol_2013.pdf

Perry, Tom: Factbox: Hezbollah and Allies Gain Sway in Lebanon Parliament. *Reuters,* 2018. május 22. Online: www.reuters.com/article/lebanon-election-parliament-factbox-idINKCN1IN1OB

Pigeon, Luc – Clark J. Beamish – Michel Zybala*: HUMINT Communication Information Systems for Complex Warfare.* Defence Research and Development Canada Valcartier (QUEBEC), 2002.

Pilch Jenő: *A hírszerzés és kémkedés története* I–III. Budapest, Franklin Társulat, 1936.

Privacy and Civil Liberties Oversight Board: *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA* (2014. július 2.). Online: https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

Pink, Daniel H.: *Motiváció 3.0.* Budapest, HVG Könyvek, 2016.

Ladetto, Quentin: *Defence Future Technologies, Emerging Technology Trends 2015.* (DEFTECH) Federal Department of Defence, Civil Protection and Sport DDPS armasuisse Science and Technology, 2016. Online: https://deftech.ch/wp-content/uploads/2018/07/DefenceFutureTechnologies_EmergingTechnologyTrends2015.compressed.pdf

Ramsay, Anna – Augusta Whittall: *Sir Robert Peel.* New York, Books for Library Press, 1969.

Regényi Kund Miklós: OSINT a második generációs internetet megelőző korokban. *Nemzetbiztonsági Szemle,* 7. (2019), 2. 32–37. Online: https://doi.org/10.32561/nsz.2019.2.3

Regényi Kund (szerk.): *Információszerzés kapcsolati forrásai.* Budapest, Nemzeti Közszolgálati Egyetem, 2019. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14284/Informacioszerzes_kapcsolati_forrasai_2019.pdf?sequence=1

Redden, Elizabeth: Science vs. Security. *Inside Higher Ed,* 2019. április 16. Online: www.insidehighered.com/news/2019/04/16/federal-granting-agencies-and-lawmakers-step-scrutiny-foreign-research

Regli, William: Universities in service to National Security, DARPA's call to academia. In *DARPA Defense Advanced Research Projects Agency 1958–2018 (60 years).* Faircount Media Group, 2018. 134–136. Online: www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf

Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Comittee on Intelligence (2002). Online: www.intelligence.senate.gov/sites/default/files/documents/CRPT-107srpt351-5.pdf

Révész Béla: Állambiztonság és pszichológia. Beszélő, 10. (2005), 5. 48–62. Online: http://beszelo.c3.hu/cikkek/allambiztonsag-es-pszichologia

Rolington, Alfred: *A hírszerzés a 21. században – a mozaikmódszer.* Budapest, Antall József Tudásközpont, 2015.

Somerville, Heather – Jane Lanhee Lee: U.S. Universities Unplug from China's Huawei under Pressure From Trump. *Reuters,* 2019. január 24. Online: www.reuters.com/article/us-usa-china-security-universities-insig/u-s-universities-unplug-from-chinas-huawei-under-pressure-from-trump-idUSKCN1PI0GV

Spracher, William C.: *National Security Intelligence Professional Education: A Map of U.S. Civilian University Programs and Competencies*. The Faculty of The Graduate School of Education and Human Development of The George Washington University in partial fulfillment of the requirements for the degree of Doctor of Education, Dissertation, 2009. Online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.604.7161&rep=rep1&type=pdf

Steinhart, Amit: *The Future is Behind us? The Human Factor in Cyber Intelligence: Correlations between Cyber-HUMINT and Hackers' Social Engineering* (é. n.). Online: www.academia.edu/8457596/The_future_is_behind_us_The_human_factor_in_cyber_intelligence_Correlations_between_Cyber-HUMINT_and_Hackers_Social_Engineering

Stout, Mark: The Pond: Running Agents for State, War, and the CIA. The Hazards of Private Spy Operations. *Studies in Intelligence,* 48. (2004), 3. 69–82. Online: https://ia903106.us.archive.org/16/items/DTIC_ADA523244/DTIC_ADA523244.pdf

Swire, Peter – Kenesa Ahmad: Encryption and Globalization. *The Columbia Science & Technology Law Review,* 13. (2012), Spring. Online: https://doi.org/10.2139/ssrn.1960602

Szabó Károly: Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről. *Nemzetbiztonsági Szemle,* 7. (2019), 2. 68–82. Online: https://doi.org/10.32561/nsz.2019.2.6

Szalai Flóra: *A terrorizmus és a terrorelhárítás törzsfejlődése.* A TEK előadása az ÁJK-n. 2017. március 13. Online: https://juratus.elte.hu/a-terrorizmus-es-a-terrorelharitas-torzsfejlodese-a-tek-eloadasa-az-ajk-n/

Tóth Balázs: Hatszorosára gyorsult a jégtakarók olvadása. *Index,* 2020. március 12. Online: https://index.hu/techtud/2020/03/12/hatszorosara_gyorsult_a_jegtakarok_olvadasa/

Tóth Tamás: Egyes Social Engineering módszerek elhatárolása és rendszerezése. *Szakmai Szemle,* 18. (2020), 1. Online: www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf

Tyler, Richard: GCHQ Recruits Eight Universities to Counter Cyber Attacks. *The Telegraph,* 2012. április 1. Online: www.telegraph.co.uk/finance/newsbysector/industry/defence/9179442/GCHQ-recruits-eight-universities-to-counter-cyber-attacks.html

Törőcsik Mária – Szűcs Krisztián – Kehl Dániel: Generációs gondolkodás – A Z és az Y generáció életstílus csoportjai. *Marketing & Management,* (2014), 2. ksz. 3–15. Online: https://journals.lib.pte.hu/index.php/mm/article/view/861/732

Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle,* 8. (2020), 1. 5–32. Online: https://doi.org/10.32561/nsz.2020.1.1

Urban, Rudolf – Martin Macko: *Place and Role of the Defense Science in the Czech Research and Development System.* Brno, University of Defence, 2011.

Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69. Online: www.nemzetesbiztonsag.hu/cikkek/varga_krisztian-katonai_biztonsagi_maganvallalatok_amerikai_alkalmazasa_irakban.pdf

Vellela, Tony: *New Voices: Student Political Activism in the '80s and '90s.* Boston, South End Press, 1988.

Vida Csaba: A hírszerző elemző-értékelő munka alapjai. *Felderítő Szemle,* 12. (2013), 3. 90–99.

Wagner, Kurt: Facebook Says Cambridge Analytica may have had Data from as Many as 87 Million People. *Vox,* 2018. április 4. Online: www.vox.com/2018/4/4/17199272/facebook-cambridge-analytica-87-million-users-data-collection

Weir, Fred: Russian Internet Giant Yandex Takes Rare Stand Against State Snooping. *The Christian Science Monitor,* 2019. június 14. Online: www.csmonitor.com/World/Europe/2019/0614/Russian-internet-giant-Yandex-takes-rare-stand-against-state-snooping

Weinbaum, Cortney – Richard Girven – Jenny Oberholtzer: *The Millenial Generation – Implications for the Intelligence and Policy Communities.* Santa Monica, Rand Corporation, 2016. Online: www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1306/RAND_RR1306.pdf

Westerlund, Fredrik: *Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?* Stockholm, Defence Analysis FOI Memo 3126, 2010.

Wladawsky-Berger, Irving: Innovation and National Security in the 21st Century. *The Wall Street Journal,* 2020. január 17. Online: https://blogs.wsj.com/cio/2020/01/17/innovation-and-national-security-in-the-21st-century/

Zalai-Göbölös Noémi*:* A Z és az alfa generációk jövője a nemzetbiztonsági szolgálatoknál. *Belügyi Szemle,* 66. (2018), 2. 46–59. Online: https://doi.org/10.38146/BSZ.2018.2.3

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

Európai Unió Bírósága, C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek. Online: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=hu&mode=lst&dir=&occ=first&part=1&cid=3050767

Európai Unió Bírósága, Maximillian Schrems kontra Data Protection Commissioner [nagytanács], C-362/14. sz. ügy

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyek védelméről a személyes adatok feldolgozása során és az ilyen adatok szabad áramlásáról, valamint a 95/46 / irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a természetes személyek védelméről a személyes adatoknak az illetékes hatóságok általi feldolgozása során az ilyen személyek megelőzése, kivizsgálása, felderítése vagy üldözése céljából, bűncselekmények vagy büntetőjogi szankciók végrehajtása, valamint az ilyen adatok szabad mozgásáról, valamint a 2008/977 / IB tanácsi kerethatározat hatályon kívül helyezéséről

Internetes források

2015 Charlie Hebdo Attacks Fast Facts. *CNN,* (2020. december 18.). Online: www.cnn.com/2015/01/21/europe/2015-paris-terror-attacks-fast-facts/index.html

A 9/11 Bizottság jelentése (The 9/11 comission report) (é. n.). Online: https://govinfo.library.unt.edu/911/report/911Report.pdf

Access to innovation: NSA's Technology Transfer Program. *The Next Wave,* 19. (2012), 3. Online: www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-19-3.pdf

Alkotmányvédelmi Hivatal: *Awareness Program* (é. n.). Online: https://ah.gov.hu/awareness-program/

The Alan Turing Institute: *Current Partnerships and Collaborations* (é. n.). Online: www.turing.ac.uk/collaborate-turing/current-partnerships-and-collaborations

The Apple-F.B.I. Case. *The New York Times,* (2016). Online: www.nytimes.com/news-event/apple-fbi-case

The Art of Deception. *Edwardsnowden.com,* (é. n.) Online: https://edwardsnowden.com/docs/doc/the-art-of-deception-training-for-a-new.pdf

Diákmunka: Az FBI diákokkal figyelteti a kínaiakat. *Librarius,* (2019. június 30.). Online: https://librarius.hu/2019/06/30/diakmunka-az-fbi-diakokkal-figyelteti-a-kinaiakat

Establishment of the DNI Open Source Center. *ODNI News Release,* (2005. november 8.). Online: www.dni.gov/files/documents/Newsroom/Press%20Releases/2005%20Press%20Releases/20051108_release_content.htm

FBI: *9/11 Investigation* (é. n.). Online: www.fbi.gov/history/famous-cases/911-investigation

FBI: *East African Embassy Bombings* (é. n.). Online: www.fbi.gov/history/famous-cases/east-african-embassy-bombings

FBI: *Operation Ghost Stories* (2011. október 31.). Online: www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case

FBI: *USS Cole Bombing* (é. n.). Online: www.fbi.gov/history/famous-cases/uss-cole-bombing.GCHQ: *Bletchley Park & WWII.* (é. n.). Online: www.gchq.gov.uk/section/history/bletchley-park-and-wwii

GCHQ: *Education & Outreach* (é. n.). Online: www.gchq.gov.uk/section/culture/education-and-outreach

Gemeinsames Terrorismusabwehrzentrum: Verfassungsschutz.de. Online: www.verfassungsschutz.de/EN/protection-of-the-constitution/mission-and-working-methods/national-and-international-co-operation/national-and-international-co-operation_node.html

Government of the United Kingdom: *New ACT app launched* (2020. március 5.). Online: www.gov.uk/government/news/new-act-app-launched

Institute for Human Rights and Business: *Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model* (2016. január 15.). Online: www.ihrb.org/focus-areas/information-communication-technology/report-lawful-interception-and-government-access-to-user-data

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA): *Justice Information Sharing* (2004). Online: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282

MTI: Hadat üzent a Gmail-nek a francia kormány. *Napi.hu,* (2013. szeptember 13.). Online: www.napi.hu/nemzetkozi_gazdasag/hadat_uzent_a_gmail-nek_a_francia_kormany.564438.html?p=2

National Commission on Terrorist Attacks Upon the United States (2004). Online: www.9-11commission.gov/

NATO: *Civilian Intelligence Committee (CIC)* (2011. november 16.). Online: www.nato.int/cps/en/natohq/topics_69278.htm

Number of College and University Students from China in the United States from Academic Year 2009/10 to 2019/20. *Statista*. Online: www.statista.com/statistics/372900/number-of-chinese-students-that-study-in-the-us/

Number of Monthly Active Facebook Users Worldwide as of 1st quarter 2020. *Statista,* (2021). Online: www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Number of Students from China Going Abroad for Study from 2008 to 2018. *Statista,* (2020). Online: www.statista.com/statistics/227240/number-of-chinese-students-that-study-abroad/#statisticContainer

Secure Trend 2015. Online: www.secure-trend.hu/2015/blog/posts/207

Security Service MI5: *Joint Terrorism Analysis Centre* (é. n.). Online: www.mi5.gov.uk/joint-terrorism-analysis-centre

Sandy Hook Promise: Gun Violence Warning Signs. *Youtube,* (2016.december 6.). Online: www.youtube.com/watch?v=9qyD7vjVfLI

NPCC: *More Than Seven Million People Watch Counter Terrorism Safety Video as UK Policing Increases its Global CT Presence* (2018. július 6.). Online: https://news.npcc.police.uk/releases/more-than-seven-million-people-watch-counter-terrorism-safety-video-as-uk-policing-increases-its-global-ct-presence

Office of the Director of National Intelligence: *About the ISE* (é. n.). Online: www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise

OSCE: *Countering the use of the Internet for Terrorist Purposes* (é. n.). Online: www.osce.org/secretariat/107810

Terrorist drives truck through a Bastille Day celebration. *History,* (2016. július 14.). Online: www.history.com/this-day-in-history/2016-nice-terrorist-attacks

U.S. Embassy in Luxembourg: *Secretary Pompeo and Secretary Esper Speak at Munich Security Conference 2020* (2020. február 19.). Online: https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/

U.S. Department of Homeland Security: If You See Something, Say Something. (é. n.). Online: www.dhs.gov/see-something-say-something/about-campaign/seesay-day

Vault 7: CIA Hacking Tools Revealed. *WikiLeaks,* (é. n.). Online: https://wikileaks.org/ciav7p1/