Takács Gergely[1]

Big Data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában

I. rész

Abstract

Today data is, in many aspects, the basis of production, and, therefore, has serious economic and social value. Besides handling and processing historical data, Big Data methods and technologies help to process enormous amounts of information almost real-time in the business sphere, as well as at institutions of public and national security. Big Data methods constitute an additional tool of extracting the meaning of assorted and processed data piles and drawing the attention of the decision makers to certain aspects, trends, or even patterns. In the first part of my study, I wish to describe the legal framework of extracting knowledge that pertains to the U.S. law enforcement agencies and national security services in the country where this method is used in the broadest spectrum of such work.

[1] PhD aspiráns, PTE BTK Interdiszciplináris Doktori Iskola

Afterwards, in the second part, I shall review certain methods along with fields of possible usage.

Bevezetés

Manapság annak lehetünk a tanúi, hogy a valós világ adatai korlátlan növekedésnek indultak, és ebből adódóan egyre nagyobb igény jelenik meg arra vonatkozóan az üzleti élet, a kormányzatok és a rendvédelmi szervek részéről is, hogy valós időben lehessen lekérdezéseket végrehajtani és információt, tudást kinyerni a meglévő adatbázisokból. Napjainkra ugyanis sok tekintetben az adat lett az alapanyag a termeléshez, ezáltal komoly gazdasági és társadalmi értékkel is bír.[2]

A Big Data jelenséget úgy lehet a legjobban leírni, hogy hirtelen olyan exponenciális mértékben megnőtt a rendelkezésre álló és a nagy sebességgel, rendkívül sokféle formátumokban folyamatosan keletkező adatok mennyisége, hogy azokat a hagyományos eszközökkel (pl. Microsoft Excel) és módszerekkel menedzselni, tárolni és feldolgozni már nem lehetséges.

Az adatok mennyiségének drasztikus növekedéséért részben azok az eszközök a felelősek, amelyek az internetre kapcsolódnak (Internet of Thing, a dolgok internete, továbbiakban

[2] WORLD ECONOMIC FORUM (2012): Big Data, Big Impact: New Possibilities for International Development. World Ecnomic Forum. Forrás: http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf (Letöltés időpontja: 2017. 03. 05.)

IoT), és napjainkra teljesen hétköznapivá, megszokottá váltak. A számítógépeken, laptopokon, táblagépeken és mobiltelefonokon kívül ide sorolhatók a fényképezők és videókamerák, amelyek WiFi használatával köthetők a hálózathoz, valamint az olyan eszközök is, mint a lakásokba, házakba telepíthető okosmérők, amelyeknek a segítségével optimalizálni lehet az energiafogyasztásunkat, és jelentős költségeket takaríthatunk meg.

A rendelkezésre álló informatikai tárolókapacitások tizennégy havonta megduplázódtak az elmúlt három évtizedben, és ezzel párhuzamosan az adatok tárolásának költsége is drasztikus zuhanáson ment keresztül.[3] Ennek tudható be, hogy a vállalatok gondolkodásában fordulat következett be, és az adatok törlése, vagy figyelmen kívül hagyása helyett egyre inkább a megőrzés és a feldolgozás, hasznosítás mellett döntöttek és kötelezték el magukat stratégiai megfontolásokból. A Big Data módszerek és technológiák abban segítenek, hogy a historikus adatok kezelésével és feldolgozásával párhuzamosan a rendkívül nagy mennyiségű információk közel valós idejű processzálására is lehetőség legyen akár az üzleti szféra, akár a közfeladatokat ellátó intézmények számára.

[3] HILBERT, Martin – LÓPEZ, Priscila (2011): The World's Technological Capacity to Store, Communicate, and Compute Information. http://science.sciencemag.org/content/332/6025/60 (Letöltés időpontja: 2017. 03. 04.)

BIG DATA

A világ információinak mennyisége éves szinten 59%-kal nő, ami jelentős kihívást jelent a tárolás kérdésének megoldására nézve is. Azonban ahhoz, hogy az ebből fakadó lehetőséget is ki lehessen használni, nem szabad kizárólag erre az aspektusra koncentrálni. Legalább ekkora figyelmet kell fordítani az adatok sokféleségére és a keletkezésük sebességére is. Manapság olyan társadalomban élünk, amelyben lényegében minden tevékenységünk adatokat generáló tényezőnek számít, aminek az eredményeként a különböző vállalatok számára fullasztóan nagy tömegben és szinte feldolgozhatatlan sebességgel keletkeznek adatok rólunk.[4] Ebből a szempontból kiemelten fontos kérdés az adatok letárolásának a módja.

A Big Data módszer lényege és egyik legfontosabb eleme, hogy az adatokat egy olyan hierarchizált és kereszthivatkozásokat lehetővé tevő struktúrába (adattárház) kell feltölteni és tárolni, amely lehetővé teszi, hogy az adatból információ, az információból tudás, a tudásból pedig „bölcsesség" alakulhasson ki.[5] Ez a fajta bölcsesség természetesen mást jelent a pénzügyi és az energiaszektorban, illetve a nemzetbiztonsági szférában is.

[4] GARTNER.COM: Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data. http://www.gartner.com/newsroom/id/1731916 (Letöltés időpontja: 2017. 03. 02.)

[5] Ez az úgynevezett „Data – Information – Knowledge – Wisdom hierarchy", ami az adattárházak létrehozásánál az egyik elvi alapkövetelmény.

Forrás: i-SCOOP.EU: The DIKW model for knowledge management and data value extraction. https://www.i-scoop.eu/big-data-action-value-context/dikw-model/ (Letöltés időpontja: 2017. 03. 05.)

Az adatok ilyen módon való tárolásának a jelentősége abban van, hogy ez teszi lehetővé az információk valós vagy megközelítőleg valós idejű feldolgozását.[6] A Big Data módszer lényege ugyanis az, hogy olyan algoritmusok segítségével dolgozik, amelyek képesek logikailag összekötött gépek hálózatán működni időbeli és térbeli korlátozások nélkül.[7] A feldolgozásra pedig szükség van, hiszen ez adja meg az adatok üzleti vagy éppen társadalmi értékét. Annak eldöntésében is segítséget nyújthatnak ezek az analitikai (korrelációs) módszerek, hogy egy adott szervezet eldöntse, melyik információ számít fontosnak, és melyikkel nem szükséges a továbbiakban foglalkozni. A korábban alulértékelt adatokról a Big Data módszer révén kiderülhet, hogy olyan rejtett tartalommal bírnak, amelyeket adatbányászati módszerek segítségével a kormányzat vagy egy szervezet előnyére lehet felhasználni annak érdekében, hogy például csalásokat vagy más bűncselekményeket akadályozzanak meg a segítségével.

A terrorizmussal, a különböző bűncselekményekkel, valamint az egyéb fenyegetésekkel szemben kizárólag abban az esetben lehet hatékonyan és megfelelő eszközökkel fellépni, ha adott

[6] Az adattárházak technológiai megvalósítására természetesen számos vállalat nyújt megoldási lehetőségeket, ilyen például a Hadoop és a MapReduce is.

[7] GUALTIERI, Mike (2013): The Forrester Wave: Big Data Predictive Analytics Solutions Q1 2013.
http://webcache.googleusercontent.com/search?q=cache:NQGhw9x85U0J:www.sas.com/resources/asset/Forrester85601-LR8KBD.pdf+&cd=2&hl=hu&ct=clnk&gl=hu (Letöltés időpontja: 2017. 04. 03).

időben és megbízható tartalommal állnak rendelkezésre a hírszerzési információk. A korábbi időszakokban az volt a jellemző, hogy a nemzetbiztonsági szolgálatok kizárólag a saját munkájuk során keletkezett információkkal dolgoztak. Ebből adódóan a keletkező adatmennyiség kezelhető méretű volt a számukra. Napjainkra ez a helyzet teljesen megváltozott, mert az ember szinte minden tevékenysége adatokat generál.

Ráadásul viszonylag új jelenség az is, hogy a belső adattárakkal párhuzamosan egyre nagyobb számban vannak, jönnek létre „házon kívül" is olyan adatbázisok (pl. automata rendszámtábla-felismerő rendszerek, közösségi média, pénzügyi, telekommunikációs szolgáltatók adatai), amelyek szintén értékesek lehetnek a szolgálatok számára ahhoz, hogy holisztikus módon tudjanak bizonyos problémákat megközelíteni.

Az elemzőknek pedig az a feladata, hogy valamennyi információ birtokában készítsenek értékeléseket, előrejelzéseket. A külsős adatbázisok számának megtöbbszöröződésével párhuzamosan új kihívást jelent az is, hogy az ezekben tárolt információk jelentős része strukturálatlan. Egyes becslések szerint a napi szinten keletkező adatoknak megközelítőleg 80%-a tartozik ebbe a kevésbé felhasználóbarát kategóriába.[8] Jellemzően a közösségi, a videó- és fotómegosztó oldalak, valamint a

[8] Forrás: SCHNEIDER, Christie (2016): The biggest data challenges that you might not even know you have. https://www.ibm.com/blogs/watson/2016/05/biggest-data-challenges-might-not-even-know/ (Letöltés időpontja: 2017. 03. 03.)

telekommunikációs eszközök által generált adatok, valamint a rendvédelmi szférán belül keletkező rendőrségi vallomások sorolhatók ide. Ezáltal nemcsak az adatbázisok és adatforrások megnövekedett száma jelent kihívást az üzleti és a nemzetbiztonsági szféra számára egyaránt, hanem az is, hogy azokban rendezetlen struktúrában és formátumban találhatók meg az értékes információk, amelyeket a feldolgozásukat követően lehet kinyerni belőlük. A hasznosíthatóság szempontjából nagyon fontos az is, hogy ezek az adatbázisok egymással összeköttetésben legyenek.

A Big Data Analitikai módszerek között előkelő helyen szerepel a prediktív analitika, az előrejelző elemzés, ami segíthet a bűnmegelőzésben és akár a terrorelhárításban is. A módszer aggályos részét az jelenti, ha eközben olyan szenzitív információkkal kell dolgozni, mint például az egészségi állapotra, fajra, szexuális beállítottságra, vallási nézetre vonatkozó személyes adatok. Ebből adódóan a legnagyobb kihívást az jelenti, hogy biztosítva legyenek a magánélethez és a személyes adatok védelméhez való jogok és garanciák úgy, hogy közben a nemzetbiztonsági és rendvédelmi érdekek, szempontok se szenvedjenek hátrányt.

Az internet nemcsak az információk megosztására és a különböző közösségi oldalak intenzív használatára alkalmas, hanem kiváló terepül szolgál a pénzügyi csalásokban és kiberbűnözésben érintett csoportok, valamint a terrorista szervezetek számára is. Az utóbbiak esetében az internet egyszerre szolgál toborzó és propaganda felületként, ami komoly kihívások elé állítja az igazságszolgáltatási és nemzetbiztonsági

szerveket is. A Big Data elemzési módszerek a nyílt (OSINT – Open Source Intelligence) és a műveleti információk kombinációjával segíthetnek megtalálni és azonosítani a terrorista hálózatokat és a velük együttműködőket. Emellett a közösségi felületeken folytatott kommunikáció tartalmának elemzése alapján felmérhetők az aktuális témák, a várható trendek, az egyes csoportokon belüli hangulat, és a tagok viselkedése is. A megosztott képek automatizált – elsődleges – elemzésére szintén van már lehetőség, ezáltal az elemzőknek már csak azokkal a fotókkal kell foglalkozniuk, amelyeken valamilyen szempontból releváns információ található.

A Big Data módszerek tehát egy plusz eszközt jelentenek ahhoz, hogy a kiválasztott és feldolgozott adathalmazok értelmét kinyerjük, és ráirányítsuk a döntéshozók figyelmét bizonyos aspektusokra, trendekre vagy éppen mintákra. De ahogy a fotókkal kapcsolatban is utalást tettem rá, ezek csak előkészítői lehetnek a humán erővel végrehajtott szakértői elemzésnek. A Big Data Analitikai (BDA) módszerek alkalmazhatóságának alapfeltétele a nagy mennyiségben és folyamatosan rendelkezésre álló adathalmazok megléte. A nemzetbiztonsági és a rendvédelmi szférában az adatok többsége jellemzően valamilyen műveleti munka eredményeként keletkezik, amelynek a hatályos jogszabályok keretet (korlátot) szabnak. Ebből következően a két részesre tervezett tanulmány első fejezetében az amerikai adatgyűjtési és kezelési szabályokat kívánom bemutatni. A Terror & Elhárítás következő számában kerül sor – a teljesség igénye nélkül – azoknak a BDA-módszereknek bemutatására, amelyeket széleskörűen alkalmaznak jelenleg is az amerikai (és feltételezhetően a brit, francia és német)

nemzetbiztonsági és rendvédelmi szférában is. Végül – a konklúzió részeként – arra kívánok kitérni, hogy Magyarország vonatkozásában milyen adaptálási módokra nyílna lehetőség megfelelő kormányzati (törvényi és jogi) támogatás esetén.

I. Az adatgyűjtési és kezelési szabályok az Egyesült Államokban

A Big Data vagy más néven adatvezérelt elemzési módszerek alkalmazhatóságának alapfeltétele, hogy nagy mennyiségben álljanak rendelkezésre aktuális és lehetőség szerint historikus adatok is elektronikus, feldolgozható formában. A nemzetbiztonsági szolgálatok esetében adatok nagy mennyiségben kétféleképpen keletkezhetnek: műveleti úton, technikai eszközök alkalmazása nélkül, humán források különböző típusainak felhasználásával, illetve a rádióelektronikai jelfelderítés (Signals Intelligence–SIGINT) kategóriájába tartozó valamennyi, a kommunikáció irányának, tartalmának és egyéb tulajdonságainak megismerésére irányuló tevékenység révén.

Míg az előbbi esetében hosszú évek folyamatos és tervszerű munkájának eredményeként keletkezhet már Big Dataként kezelhető mennyiségű adat, addig az utóbbinál – az eszközök jellegétől és a tevékenység kiterjedtségétől függően – akár pár perc alatt is. Erre a sajátosságra való tekintettel a tanulmány témája szempontjából jelentőséggel a technikai úton összegyűjtött nagy mennyiségű adatok bírnak, ezért a műveleti információk közül a továbbiakban kizárólag a SIGINT-tel kívánok foglalkozni.

BIG DATA

A 19. század végétől, a 20. század elejétől a telefonkészüléket használók számának drasztikus növekedése kihatással volt a biztonsági szolgálatokra, szükségességé vált a lehallgatási képesség kialakítása és fokozatos fejlesztése. Számos országban külön technikai szolgálatok jöttek létre, amelyeknek elsődleges feladata az információ megszerzése volt. A 20. század első évtizedeinek fegyveres konfliktusai során felismerték az üzenetek elektronikus továbbításának jelentőségét, az ellenséges közlemények megszerzésének, valamint a saját kommunikáció rejtjelezésének szükségességét. Ennek következtében a 19-20. század fordulójára tehető a rádiófelderítés megjelenése – ekkor még kizárólag – a katonai szférán belül.

A fényképezés, valamint a mozgóképek, később videók készítése, illetve ennek a területnek a gyors fejlődése kihatással volt a légi- és az űrfelderítésre is. A közlekedésben megjelenő új távlatok ebben az esetben is együtt jártak a kommunikációs eszközök fejlődésével, hasonlóan a 19. század fordulóján látott vasút-telefon (kezdetben távíró) párosításhoz.

A huszadik század utolsó évtizedeiben tapasztalt információfelderítési képességek rohamos fejlődése forradalmasította a felderítés egészét. Ezzel párhuzamosan a régebbi technikai eszköznek számító rádió, illetve rádiófelderítés szerepe és súlya a biztonsági szférán belül átértékelődött. Helyét fokozatosan a mobilkommunikációs eszközökön és a világhálón folytatott tevékenység megismerése vette át.

A hidegháborús korszakban és azóta is rendkívüli jelentősége van ezeknek a képességeknek. A technikai felderítési eszközök fejlesztésével – a műholdak megjelenésével – egyre nagyobb igény mutatkozott a technikai-hírszerzési kapcsolat-, és együttműködési rendszerek (BRUSA, majd KUSA-egyezmény, később Five Eye) [9] kialakítására annak érdekében, hogy a hidegháborús időszak szembenálló felei a lehető legteljesebb mértékben ellenőrizni tudják a másik tevékenységét, kommunikációját.

Ennek megfelelően a hidegháborús időszakban kialakításra került az amerikai és a brit szolgálatoknál – feltételezhetően korlátozottabb földrajzi kiterjedtséggel a szovjet szövetségi rendszeren belül is – az a képesség, amely lehetővé tette számukra a tömeges lehallgatást. Az Amerikai Egyesült Államok esetében – ahogy erre a későbbiekben részletesen is kitérek – hosszú évtizedeken keresztül kizárólag az Alkotmány negyedik

[9] Több mint hatvan évnyi titkosítást követően 2010-ben publikált dokumentumok tanúsága szerint az Amerikai Egyesült Államok már 1946-ban egyezményt írt Nagy-Britanniával annak érdekében, hogy globális megfigyelési/lehallgatási képességet alakítsanak ki. Később UKUSA, majd pedig a résztvevői kör kiszélesítését követően – Kanadával, Új-Zélanddal és Ausztráliával – a Five Eyes nevet kapta a megállapodás. Az angolszász országokon kívül harmadik félként 1952-ben Norvégia, 1954-ben Dánia, 1955-ben pedig Németország is csatlakozott. Később Olaszország, Írország, Törökország és Fülöp-szigetek is az együttműködés tagjaivá váltak.
Forrás: NORTON-TAYLOR, Richard (2010): Not so secret: deal at the heart of UK-US intelligence https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released (Letöltés időpontja: 2017. 02. 05.)

kiegészítése[10] jelentett korlátot és védelmet, azonban csak az amerikai állampolgárok számára. Ennek kiterjesztésére az EU állampolgárokra vonatkozóan egészen 2016-ig kellett várni, miközben a globális lehallgatási programok már a hatvanas-hetvenes években működtek.

Az adatvédelmi törvények, valamint a lehallgatási tevékenységre vonatkozó jogszabályok csak a hetvenes években kerültek elfogadásra az amerikai törvényhozásban, a Kongresszusban, amelyeket az évek során aztán több alkalommal is módosítottak, kiegészítettek. Jellemzően csak akkor, amikor a lehallgatási tevékenység egyes – törvénytelenül, vagy megfelelő felhatalmazás hiányában folytatott – részei nyilvánosságot kaptak. A továbbiakban az amerikai tömeges adatgyűjtést lehetővé tevő jogszabályi hátteret kívánom bemutatni.

1.1 Adatgyűjtés és lehallgatás az Amerikai Egyesült Államokban

1.1.1. A Foreign Intelligence Surveillance Act of 1978

Az 1978-ban elfogadott, külföldi hírszerzési célú lehallgatásról szóló törvény, a Foreign Intelligence Surveillance Act of 1978 (továbbiakban FISA-1978) szabályozza azokat a folyamatokat és

[10] Az amerikai alaptörvény negyedik kiegészítése tiltja azt, hogy a hatóságok a polgárokat házkutatással, irataik vagy más személyes tulajdonuk átvizsgálásával vagy lefoglalásával indokolatlanul zaklassák. Házkutatási parancsot csak bűncselekmény alapos gyanúja esetén lehet kiadni. A negyedik kiegészítés olyan helyzetekben védi az állampolgárokat a hatóságok zaklatása ellen, amikor észszerűen elvárható a személyük és tulajdonuk háborítatlansága.

eljárásokat, amelyek révén lehetőség nyílik technikai úton történő hírszerzési tevékenységre azokkal szemben, akiket kémkedéssel vagy terrorizmus gyanújával vonnak ellenőrzés alá. A törvény elfogadása óta a kormányügynökségeknek bírói engedélyre van szüksége – a bűnügyi nyomozásokhoz hasonlóan – ahhoz, hogy a szövetségi ügynökségek elektronikus megfigyelés alá vonják az adott személyeket nemzetbiztonsági okból.[11]

A jogszabály megszületését a Nixon elnök ideje alatt elkövetett, az ellenzéki politikusokat és újságírókat érintő, illegális lehallgatások indokolták, és a célja az volt, hogy bírósági és kongresszusi felügyeletet biztosítsanak a külföldi entitások és egyének USA területén való ellenőrzéséhez úgy, hogy közben a nemzetbiztonsági érdekek ne sérüljenek, és ennek megfelelően a titkosság is biztosított legyen.

A törvény egyúttal létrehozta a Foreign Intelligence Surveillance Court (Külföldi Hírszerzési célú Lehallgatást Engedélyező Bíróság – továbbiakban FISC) nevű testületet is, ami jóváhagyja a lehallgatási kérvényeket, amelyeket szövetségi bűnüldöző és hírszerző szolgálatok nyújthatnak be hozzá.

A bíróság tizenegy tagját a Legfelsőbb Bíróság vezető bírája jelöli ki, és legfeljebb hét évig szolgálhatnak ebben a testületben. A tizenegyből háromnak a bíróság washingtoni székhelyétől számított húsz mérföldes körön belül kell laknia, hogy bármikor

[11] Ezt megelőzően ügyészi engedély is elég volt a technikai ellenőrzés elrendelésére.

elérhetők legyenek, amennyiben sürgősségi engedélyezésre lenne szükség.

A Washington Post 2013. júniusi cikkében[12] megtalálható adatok szerint az 1979-es megalapítása óta benyújtott több mint 34.000 előterjesztésnek 99.97%-át eddig jóváhagyta a testület, mindösszesen tizenegy esetben utasította el a kérvényt. (A 2001 előtti időszakban kizárólag egy elutasítás volt.) A 2001. szeptember 11-ei terrortámadást követően az évi, átlag 600 előterjesztés majdnem a háromszorosára növekedett. Ezt követően évente átlagosan 1700 darab kérvény benyújtására került sor még Barack Obama első elnöki terminusa (2008-2012) idején is.

A FISA-1978 jogszabály progresszív, előremutató jellege ellenére továbbra is lehetővé tette, hogy bírói engedély nélkül, az aktuálisan hivatalban lévő elnök felhatalmazása alapján Legfőbb Ügyészi (továbbiakban LÜ) meghatalmazással akár egy évig folytassanak elektronikus hírszerzést kizárólag olyan személyekkel vagy entitásokkal szemben, amelyek külföldi hatalom/állam szolgálatában állnak, és semmi nem utal arra, hogy amerikai állampolgár lenne érintett az ügyben. A törvény egyben meghatározta azt is, hogy mi számít külföldi hírszerzési

[12] Forrás: LINDEMAN, Todd (2013): The Foreign Intelligence Surveillance Court https://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graphic.html?utm_term=.5c87edf26def (Letöltés időpontja: 2017. 02. 05.)

információnak: az USA ellen irányuló aktuális vagy jövőbeni súlyos támadásról, szabotázsról vagy nemzetközi terrorista cselekményről szóló ismeret, adat.[13] A törvényben rögzítésre került az is, hogy mi számít külföldi hatalomnak: külföldi kormány, vagy egy másik külföldi ország egy része, amelyet alapvetően nem amerikai állampolgárok alkotnak, és amely entitásnak a tevékenységét külföldi kormány irányítja. A definíció magában foglalja a nemzetközi terrorizmusban és külföldi politikai szervezetekben részt vevő csoportokat is.[14]

Ezek közül a FISA kizárólag a nemzetközi terrorista tevékenységben részt vevő csoportok esetében nem tette lehetővé a bírói engedély nélküli lehallgatást (később ez a korlátozás kikerült). A LÜ-nek természetesen jeleznie kell ezen kondíciók meglétét a FISC-nek, és rendszeresen jelentést kell készítenie a Képviselőháznak, valamint a Szenátus hírszerzési ügyekben illetékes bizottságainak.

Amennyiben amerikai személy merülne fel, akkor bírósági engedélyt kell kérni annak érdekében, hogy a kommunikációja 72 óránál hosszabb ideig megőrizhető legyen. Ha bűncselekmény gyanúja merülne fel egy amerikai státusszal (állampolgársággal,

[13] CORNELL LAW SCHOOL: 50 U.S. Code § 1802 – Electronic surveillance authorization without court order; certification by Attorney General. Forrás: https://www.law.cornell.edu/uscode/text/50/1802. (Letöltés időpontja: 2017. 02. 05.)

[14] CORNELL LAW SCHOOL: 50 U.S. Code § 1801 – Definitions; Forrás: https://www.law.cornell.edu/uscode/text/50/1801. (Letöltés időpontja: 2017. 02. 05.)

letelepedési engedéllyel) rendelkező személy kapcsán, akkor bírói engedély nélkül is meg lehetett őrizni 72 órát túlhaladóan a kommunikációját.

A törvény[15] természetesen meghatározza azokat az esetek is, amikor a FISC engedélyére van szükség: külföldi hatalommal, vagy annak külföldi ügynökével szemben olyan helyen, amelyet feltételezhetően a külföldi hatalom vagy annak az ügynöke használ. Bírósági engedéllyel 90, 120 és 360 napra lehet elrendelni a technikai ellenőrzését olyan személyeknek, akik idegen hatalomnak dolgoznak.

A törvény értelmében minimalizálni kell az olyan információk keletkeztetését, felhasználását, illetve továbbítását a megrendelő szolgálatok/ügynökségek számára, amelyek alapján amerikai státusszal rendelkező, az ügyhöz nem kapcsolódó személyek beazonosíthatóvá válnak. A bírói engedélyeket a titkosszolgálati információgyűjtésre dedikáltan létrehozott testület, a FISC adja ki. Az ügyeket az igazságügyi miniszter terjeszti a bíróság elé. Az elutasítással szemben van lehetőség fellebbezni, amit egy háromtagú bírói testület vizsgál meg és hoz döntést.

Az 1978-as jogszabályt 2001-ben, a Patriot Act (Hazafias törvény) elfogadását követően kiegészítették. Ezután a bírói engedély nélküli megfigyelés lehetőségét az olyan terrorista

[15] CORNELL LAW SCHOOL: 50 U.S. Code § 1805 – Issuance of order: https://www.law.cornell.edu/uscode/text/50/1805. (Letöltés időpontja: 2017. 02. 05.)

csoportokkal szemben is lehetővé tették, amelyek nem voltak közvetlenül külföldi kormányhoz köthetők.

Pár évvel később, 2004-ben a törvényt ismételten kiegészítették a „magányos farkas/elkövető" terminológiával, aki egy olyan nem amerikai személy, aki részt vesz benne, vagy készül nemzetközi terrorcselekmény elkövetésére. Emellett bekerült még az idegen hatalom megfogalmazás azokra az esetekre is, amikor nem mutatható ki egyértelműen, hogy egy konkrét külföldi kormány vagy terrorista csoport állna az egyén mögött. Ezt viszont egyértelműen alá kellett támasztania a lehallgatási kérvényt benyújtónak.

2007-ben Bush elnök kezdeményezésére módosították a törvényt ismételten úgy, hogy az olyan kommunikációt, amelynek vagy a kezdete vagy a vége külföldi országra mutat, az amerikai kormányzat lehallgathatja a FISC jóváhagyása nélkül, és ebből adódóan az igazságügyi tárca oldaláról sincs szükség kérelem/előterjesztés benyújtására.[16]

A 2007-es kiegészítés következtében a Nemzeti Hírszerzési Igazgatóság vezetője (Director of National Intelligence – továbbiakban DNI) vagy a LÜ is engedélyezheti maximum egy évre a lehallgatást, amennyiben a következő öt feltétel

[16] Forrás: Protect America Act of 2007. https://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm. (Letöltés időpontja: 2017. 02. 06.)

együttesen megáll. Jogosan feltételezhető, hogy a célszemély az USA területén kívül van. Nem csak belföldi lehallgatásra szorítkozik az előterjesztés. A kommunikációs adatokat a telekommunikációs szolgáltató cégektől és/vagy segítségével kell megszerezni (nem saját eszközök alkalmazásával). Elsődlegesen hírszerzési célúnak kell lennie az adatgyűjtésnek. A személyiségi jogok sérülésének és a felesleges adatok gyűjtésének minimalizálását előíró irányelveket kell alkalmazni.

Fontos kitétele a törvénynek, hogy a szolgáltatók immunitást élveznek az átadott információk, illetve a támogató tevékenységük kapcsán bármilyen szintű bírói szerv előtt.[17] Ez feltételezhetően arra vezethető vissza, hogy a törvényi szabályozás következtében a titkosszolgálatok bírói engedély nélkül kérhetnek le információkat a telekommunikációs és internetszolgáltató cégektől, amelyek együttműködésre vannak kötelezve. Ezáltal a tevékenységükkel kapcsolatos felelősség megállapítása is kétséges lenne.

1.1.2. Az 1978-as FISA törvény 2008-as módosítása (FISA-2008)[18]

[17] A Patriot Act 2007-es módosítását követően az NSA folyamatosan vonta be a cégeket az adatszolgáltatásba. Elsőként a Microsoft lépett be 2007-ben, majd 2008-ban következett a Yahoo, egy évvel később pedig a Google és a Facebook is. A YouTube 2010-ben, a Skype 2011-ben, míg az Apple 2012-ben tett eleget az NSA kérésének.

[18] Forrás: FISA Amendments Act of 2008. https://www.congress.gov/bill/110th-congress/house-bill/6304/text. (Letöltés időpontja: 2017. 02. 06.)

BIG DATA

Az 1978-as törvény drasztikus átdolgozására 2008-ban került sor, aminek az eredményeként hosszabb ideig lehetett bírói engedély nélkül lehallgatni a kommunikációt (48 óráról hét napra nőtt), és ez vonatkozott külföldön tartózkodó amerikai állampolgárokra is; egyértelműen rögzítésre került a szolgáltatók immunitása, és további lehetőségeket biztosított a lehallgatások sürgősségi engedélyezésére. [19] A 2008-as módosítás legtöbb kritikát és ellenkezést kiváltó 702. paragrafusa lehetővé teszi, hogy a LÜ és a DNI közösen – bírói hozzájárulás szükségessége nélkül – engedélyezze az ellenőrzés elrendelését a feltételezhetően az USA területén kívül tartózkodó, nem kizárólag amerikai személyekkel szemben, amely akár egy évig is tarthat.

A 702. paragrafust azért érte még sok kritika, mert folytonosságot biztosított azon – elnöki hatáskörben elrendelt, bírói felhatalmazás nélküli – titkos, tömeges mennyiségű információ gyűjtésére irányuló programoknak, amelyeket a szeptember 11-ei terrortámadást követően Bush elnök rendelt el. A FISA-2008 ráadásul szélesebb körű felhatalmazást adott, mint a 2001-es Terror Surveillance Program. Ez utóbbival kapcsolatban először 2006-ban az USA Today[20] írt arról, hogy az NSA tömeges

[19] BARNES, Robert (2013): Secrecy of Surveillance Programs Blunt Challenges about Legality. https://www.washingtonpost.com/politics/secrecy-of-surveillance-programs-blunt-challenges-about-legality/2013/06/07/81da327a-cf9d-11e2-8f6b-67f40e176f03_story.html?utm_term=.9e6ef6707ae7 (Letöltés időpontja: 2017. 02. 05.)

[20] CAULEY, Leslie (2006): NSA has Massive Database of Americans' Phone Calls. http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm (Letöltés időpontja: 2017. 03. 10.)

mennyiségben gyűjt adatokat amerikaiakról is az AT&T, a Verizon, a BellSouth szolgáltatóktól származó metaadatokból.

Természetesen 2008-ban is kerültek bele korlátozások: szándékosan nem lehet lehallgatni olyan személyt, aki annak megkezdése idején tudottan az USA-ban tartózkodott. Nem lehet azt a kommunikációt megszerezni, amelyiknek a küldőjéről/kezdeményezőjéről és minden címzettjéről tudva levő, hogy az USA területén tartózkodnak.

Nem lehet célszemély olyan amerikai, akiről erősen feltételezhető, hogy nem az USA-n kívül tartózkodik. Nem lehet célszeméllyé nyilvánítani egy olyan személyt, akiről erősen feltételezhető, hogy az USA területén kívül tartózkodik.

Amennyiben a hétnapos szabály alkalmazásával kezdtek megfigyelést és azt utólag a FISA nem hagyja jóvá, akkor a keletkezett információ nem használható fel bizonyítékként. Ha a LÜ megítélése szerint az információ testi sértés vagy halál bekövetkeztét vetíti előre, akkor megpróbálhatják egy jövőbeli feldolgozásnál felhasználni bizonyítékként.

Szükség van a FISC engedélyére, hogy a tengerentúlon tartózkodó amerikaiakat hallgassanak le. Amennyiben az amerikai állampolgár, mint célszemély az USA területére lép, akkor csak bírói engedéllyel folytatható az információgyűjtés. Bírói engedélyhez kötik azt is, ha külföldi személy lehallgatását egy amerikai hívása vagy e-mailje alapján kezdenék meg.

1.1.3. A USA FREEDOM Act[21]

A Freedom Act törvényt 2015. június 2-án fogadta el az amerikai kongresszus, ami az egy nappal korábban érvényét veszített Patriot Act-et[22] váltotta fel. A törvényt eredetileg 2013. október 29-én nyújtották be Snowden szivárogtatását követően pár hónappal, de abban az ülésszakban nem került megtárgyalásra a Kongresszusban. Az új szabály korlátokat szab a telekommunikációs és internetes metaadatok gyűjtésének, emellett helyreállította azt a korábbi helyzetet, amely lehetővé tette a követő lehallgatást[23] és a magányos elkövetők figyelését.

---

[21] **U**niting and **S**trengthening **A**merica by **F**ulfilling **R**ights and **E**nding **E**avesdropping, **D**ragnet-collection and **O**nline **M**onitoring **A**ct.

[22] A Patriot Act sokat vitatott 215. cikkelye értelmében az FBI-nak lehetősége volt arra, hogy minden lehetséges eszközt igénybe vegyen, hogy külföldi hírszerzési információhoz jusson. A nyomozóhatóság a Freedom Act 2015. november 29-ei hatályba lépését követően már csak a FISC határozatának birtokában kérheti ezt. Fontos megjegyezni, hogy a szövetségi fellebbviteli bíróság 2015. május elején meghozott döntésében mondta ki, hogy a Patriot Act soha nem tette lehetővé az NSA számára azt a fajta tömeges adatgyűjtést az amerikai állampolgárok vonatkozásában, mint amit az elmúlt években az ügynökség folytatott a 215. cikkelyre hivatkozva. A bíróság azonban nem volt annyira bátor, hogy az alkotmány negyedik kiegészítésére hivatkozva – ami kimondja a felhatalmazás nélküli megfigyelés és házkutatás tilalmát – utasítsa el a 215. cikkely keretében folytatott metaadat-gyűjtést.
Forrás: GREENBERG, Andy (2015): Court Rules NSA Bulk Data Collection Was Never Authorized By Congress. https://www.wired.com/2015/05/breaking-news-federal-court-rules-nsa-bulk-data-collection-illegal/ (Letöltés időpontja: 2017. 04. 06.)

[23] Követő lehallgatás: Amennyiben a célszemély telefonszámot, telefonkészüléket cserél, akkor nem kell új engedélyt kérni a lehallgatásra, hanem automatikusan érvényes maradt az előző is. Ezt az eszközt, amúgy is ritkán használták. 2013-as adatok szerint ilyenre 11 esetben adott csak engedélyt a bíróság.

BIG DATA

A Freedom Act által bevezetett korlátozások valamennyi aspektusának megértése érdekében a FISA-n kívül indokolt röviden kitérni több más, információgyűjtést szintén lehetővé tevő jogszabályra is.

Ahogy arra Snowden szivárogtatása is rávilágított, az amerikai igazságszolgáltatási és nemzetbiztonsági szerveknek széleskörű jogaik voltak és vannak jelenleg is a legális adatgyűjtésre, amelyek egyértelműen az adatvédelmi garanciák ellen hatnak. A 2015-ben elfogadott Freedom Act további korlátozásokat vezetett be, amelyek értelmében kizárólag konkrétan meghatározott személyekre, entitásokra, telefonszámokra és számlaszámokra, felhasználói fiókokra vonatkozóan fordulhatnak a szolgáltatókhoz információigénnyel.[24] Hasonló jogszabályi módosításra került sor a pénzügyi és fogyasztói adatokhoz való hozzáférés tekintetében is. Mindezen szigorítások sokkal inkább a tömeges adatgyűjtés limitálását, mintsem megakadályozását szolgálták. Korlátozást jelent továbbá az is, hogy az illegálisan megszerzett információk nem használhatók fel bizonyítékként. A szigorítás komoly hiányossága, hogy nem vonatkozik az összegyűjtött adatok további felhasználásáról.

Forrás: HARRIS, Shane (2015): Zombie Patriot Act Will Keep U.S. Spying—Even if the Original Dies (2015.01.06.) http://www.thedailybeast.com/articles/2015/05/31/zombie-patriot-act-will-keep-u-s-spying-even-if-the-original-dies.html (Letöltés: 2017. 04. 04).

[24] Bolcsó Dániel (2015): Csatát vesztett az NSA, de a totális megfigyelésnek nincs vége. (Letöltés időpontja: 2017.04.03. http://index.hu/tech/2015/12/11/nsa_freedom_act_megfigyeles_snowden/

A törvény továbbra is lehetőséget ad arra, hogy sürgős esetekben bírói engedély nélkül a LÜ jóváhagyásával induljon meg az információgyűjtés, illetve az adatok beszerzése a telekommunikációs és internetszolgáltató társaságoktól. Az FBI azonban kizárólag abban az esetben használhatja fel az információkat, ha a LÜ által engedélyezett technikai ellenőrzést utólag, hét napon belül a bíró is jóváhagyja. Fontos azonban megjegyezni, hogy ez a korlátozás kizárólag az amerikai állampolgárokra vonatkozik.[25]

A Freedom Act-ben bevezetésre kerültek olyan időbeli korlátok, amelyek szintén a személyek védelmét szolgálják. Ezek közül az egyik, hogy a hívásforgalmi adatok gyűjtése nem haladhatja meg a 180 napot. Természetesen bizonyos körülmények és feltételek megléte esetén van lehetőség a hosszabbításra, de ennek a passzusnak a törvénybe foglalása egyértelműen azt mutatja, hogy csökkenteni kívánják a készletező jellegű információgyűjtést. Újszerű és egyben korlátozó elemként jelenik meg, hogy a bíróság kötelezheti az adott kormányzati ügynökséget az adatok megsemmisítésére, amennyiben az nem tartalmaz külföldi hírszerzésre alkalmas információkat.

[25] BOEHM, Franziska (2015): A Comparison Between US And Data Protection Legislation for Law Enforcement. Study for the LIBE (Civil Liberties, Justice and Home Affairs) Committee, Directorate General for Internal Policies, Policy Department C: Citizens' rights and constitutional Affairs. Brussels, 59-65. o. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf (Letöltés időpontja: 2017. 04. 04.)

Ez a kitétel azonban szintén csak az amerikai állampolgárokra vonatkozik, tekintettel arra, hogy az ő hívásforgalmi adataikra alapesetben nem lehet hírszerzési információként tekinteni.

Ezen túlmenően a bíróság felhatalmazást kapott arra is, hogy további, az egyének jogkorlátozásával járó adatgyűjtések minimalizálására kötelezze a szolgálatokat. Határozatában a bíró ugyanis előírhatja, hogy az információkat belátható/indokolható időn belül meg kell semmisíteni, kötelező érvényű kitételek szerepelhetnek még a tárolásra és a más szervekkel való megosztás lehetőségére vonatkozóan is. De ezek a korlátozások is csak amerikai állampolgárokra vonatkoznak. A FISC-en keresztül történő bírói kontroll gyakorlásának új eszközeként jelent meg annak a lehetősége, hogy harmadik felet, azaz külső szakértőket vonjanak be, akik jártasak a polgári jogok és a hírszerzés területén is. A döntés ettől függetlenül a bíró diszkrecionális joga marad, viszont eggyel több vélemény becsatolására és megjelenítésére nyílik mód.[26]

A Freedom Act a korábban meghozott FISC és legfőbb ügyészi döntések felülvizsgálatára és ellenőrzésére is több módosítást, illetve kiegészítést hozott. A felülvizsgálati eljárásoknak magukban kell foglalniuk a 2012 és 2014 közötti években engedélyezett információgyűjtéseket, és azt kell megvizsgálni, hogy azok megfelelnek-e a minimalizálási előírásoknak, emellett értékelni kell azt is, hogy az a mód, ahogy gyűjtötték, tárolták,

[26] BOEHM, Franziska (2015): i. m.

elemezték és megosztották az adatokat a nemzetbiztonsági szférán belül, az alkotmányban lefektetetteknek megfelelően történt-e.

Az átláthatóságot kívánják szolgálni azok a paragrafusok, amelyek részletesebb jelentési kötelezettséget írnak elő az adatgyűjtésekről a Kongresszus irányába, emellett a telekommunikációs és internetszolgáltató cégek is félévente közölhetik a megkeresések számát.

A Snowden-ügy kapcsán nemzetközi szintéren és Amerikán belül is kialakult széleskörű társadalmi és politikai diskurzus középpontjában a FISA-2008 jogszabály 702. cikkelye állt, ami törvényileg lehetővé tette a tömeges mértékű adatgyűjtést az NSA számára a nem-amerikai kommunikációs csatornák vonatkozásában. A Freedom Act ebben nem hozott érdemi változást, kizárólag az amerikai állampolgárok kapcsán illegálisan megszerzett adatok bizonyítási eljárásból való kizárásának lehetősége jelent eltérést a korábbi gyakorlattól.

Abban a tekintetben sincs eltérés, hogy a nem-amerikai célpontok/célszemélyek esetében továbbra sem szükséges azonosítást teljes mértékben elősegítő adatok biztosítása, ami egyértelműen szembe megy az Európai Unió adatvédelmi szabályaival. Sok kritikát váltott ki korábban az is, hogy a külföldön gyűjtött információkra úgy tekintenek, mint nem amerikaiakkal összefüggésben keletkezett adatokra. A törvénymódosítás értelmében amennyiben mégis amerikaiakhoz kapcsolódó információ is keletkezik, akkor arra, mint „véletlenül

összegyűjtött" adatra tekintenek, amit tárolhatnak későbbi felhasználás érdekében, amibe bele kell érteni a szolgálatok közötti megosztását is, amennyiben felmerül a gyanúja a szövetségi, állami, helyi vagy éppen külföldi törvénysértésnek.

A törvénymódosítások alapján látható, hogy azok leginkább belpolitikai célokat szolgáltak, ugyanis szinte kizárólag az amerikai állampolgárokkal kapcsolatos, tömeges adatgyűjtési gyakorlat korlátozására irányulnak. Visszalépést jelent, hogy a Freedom Act-be nem applikálták be az amerikai elnök 2014. januári 28. számú politikai direktíváját, ami egyfajta adatvédelmi garanciát jelentett (a benne lévő arányossági kritériumok és a magánszféra védelmét szolgáló korlátozások révén)[27] a nem

[27] A Presidential Policy Directive (PPD) egyfajta végrehajtási rendelet, amit az elnök ad ki a Nemzetbiztonsági Tanács elemzését és tanácsát figyelembe véve. A rendeletek az elnök, mint végrehajtó hatalom nemzetbiztonsági politikájának artikulálására szolgálnak, és ugyanolyan kötelező erővel bírnak, mint egy törvény. A PPD-28-at 2014. január 17-én írta alá Obama elnök, és több olyan kritikára próbált meg reagálni, amelyeket az NSA által folytatott adatgyűjtési módszerekkel kapcsolatban a korábbi években megfogalmaztak. Ennek megfelelően szerepel benne, hogy a technikai hírszerzés során is tekintettel kell lenni arra az alapelvre, hogy nem teszünk különbséget az emberek között a nemzetiségük alapján (1. cikk. b. pont). A 2. cikkelyben felsorolásra kerülnek azok a célok, amelyek érdekében jogosnak tekinthető a PRISM-hez hasonló tömeges adatgyűjtés: kémelhárítás, terrorveszély, proliferáció, tömegpusztító fegyverek terjedése, kiberbiztonság, az amerikai és a szövetséges katonai erők tagjaira nézve megjelenő kockázatok, nemzetközi szervezett bűnözés, nemzetközi szankciók megkerülésére irányuló törekvések. Korlátozásként van megjelölve, hogy a nem amerikai állampolgárokkal kapcsolatos adatok megosztására is ugyanazokat az elveket kell alkalmazni, mint az amerikaiak esetében. A kormányzati ügynökségek közötti információmegosztás spektruma azonban rendkívül széles, ebből adódóan ez nem jelent való garanciát például az uniós állampolgárok számára. Az adatok

amerikai állampolgárok számára is a tömeges adatgyűjtéssel szemben. Visszalépést jelent a FISA engedélyek kapcsán az is, hogy a külföldi hatalom ügynökének már nem feltétlenül kell az ország határán kívül lennie a megfigyeléshez.
A Freedom Act jelentőségét tovább csökkenti, hogy annak passzusai egyáltalán nem térnek ki a FISA-2008. törvény 702. paragrafusaival párhuzamosan legalább annyi kritikát kapó 12333. számú elnöki végrehajtási rendelet által elrendelhető külföldi irányú technikai hírszerzésre sem.

1.1.4. A 12333. számú elnöki végrehajtási rendelet

Az 1981-ben aláírt végrehajtási rendelet lehetővé teszi nemcsak a metaadatok gyűjtését, hanem a kommunikáció tartalmának megismerését is. Az egyes személyeket viszont nem lehet bírósági engedély nélkül megfigyelni a végrehajtási rendelet értelmében. Azonban, ha egy amerikai állampolgár

tárolására vonatkozóan is szerepel a PPD-28-ban egy kitétel (4. cikkely), amely szerint ugyanolyan hosszú ideig lehet tárolni a nem amerikaiak kapcsán keletkezett adatokat, mint a 12333. elnöki rendeletben az amerikai állampolgárok esetében meghatároztak. Tekintettel arra, hogy a 12333-ban ilyen nem szerepel, az általános, ötéves megőrzési időt alkalmazzák, kivéve, ha a DNI hosszabbat tart indokoltnak. Mindezek alapján a PPD-28 inkább szolgál politikai „marketing" célokat, mintsem a sokat kritizált adatgyűjtési gyakorlat tényleges megváltoztatását. Forrás: The White House Office of the Press Secretary (2014): Presidential Policy Directive - Signals Intelligence Activities https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (Letöltés időpontja: 2017. 04. 04.)

kommunikációjának tartalma véletlenül[28] vált ismertté egy törvényesen folytatott tengerentúli külföldi hírszerzési tevékenység során, akkor a végrehajtási rendelet 2.3 (c) bekezdése alapján lehetőség van annak megőrzésére, tárolására. Nem szükséges hozzá, hogy az amerikai állampolgár bármilyen törvénytelen tevékenységgel gyanúsított legyen, és nem szab korlátot a kommunikáció volumenét illetően sem.

Manapság, főleg az e-mailezés kapcsán elég gyakran előfordul, hogy az olyan cégek, mint a Google és a Yahoo esetében az elküldött levél nem marad az USA területén, hanem a vállalat brazíliai, japán, vagy brit szerverein keresztül megy, mielőtt például New Yorkból a New Jersey-ben található címzetthez megérkezne. Az 12333-as végrehajtási rendelet nem akadályozza meg az NSA-t abban, hogy az ilyen típusú leveleket (tartalmukat és a kapcsolódó metaadatokat egyaránt) gyűjtse törvényes külföldi információszerzési tevékenységre hivatkozva.[29] Ehhez ráadásul nincs szükség bírói engedélyre és nincs beszámolási kötelezettség a Kongresszus irányába sem.

[28] Nem lehet tudni, hogy a véletlenül megszerzett üzenetek mekkora arányt tesznek ki, ugyanis az NSA ezt sohasem vizsgálta – állítólag. Feltételezhető, hogy jelentős mennyiségről lehet szó, ugyanis a külföldi optikai kábeleken és szateliteken keresztül folytatott információszerzés jellemzően tömeges és nem célzott.

[29] Korábban azért nem szabályozták le ezt a kört, mert amikor a végrehajtási rendeletet elfogadták 1981-ben, akkor még nem volt jellemző, hogy az amerikaiak kommunikációja „külföldre ment volna”. Az internet világában azonban ez már nincs így.

BIG DATA

A Snowden által 2013 májusában kiszivárogtatott anyagok alapján látható volt, hogy az Obama-kormányzat 2010 novemberében titokban megváltoztatta a szabályokat, ami lehetővé tette az NSA számára, hogy amerikaiak olyan metaadatait[30] elemezzék, amelyeket a 12333 végrehajtási rendelet keretében gyűjtöttek össze. Az ügynökség mindezt külső engedélyezés nélkül, külföldi hírszerzési és terrorelhárítási célból egyaránt felhasználhatja.

Ez egyben azt is jelenti, hogy az amerikaiakkal összefüggésben, külföldön tömegesen gyűjtött adatok esetében kevesebb korlátozás van, mint amelyeket belföldön szereztek. A Freedom Act és a 12333. sz. végrehajtási rendelet közötti különbségek és hasonlóságok könnyebb áttekinthetőségét szolgálja az alábbi táblázat.

A FISA ÉS A 12333 JOGAINAK ÖSSZEHASONLÍTÁSA		
	FISA	**12333. végrehajtási rendelet**
Mire vonatkozik?	belföldi hálózatokra	külföldi hálózatokra
Ki határozza meg a szabályokat?	Kongresszus és a FISC	az elnök
Van bírósági felügyelet?	igen	nem

[30] A metaadat leírja más adat(ok) jellemzőit, tulajdonságait, információval szolgál az adott elem tartalmáról. Egy fotó esetében a metaadatok mutatják meg, hogy mekkora méretű, milyen felbontású fényképről van szó, illetve mikor készítették.

Adatgyűjtési technikák		
az NSA gyűjthet és tárolhat adatokat tömeges mennyiségben amerikaiakról, ami alapján látható, hogy kivel állnak kapcsolatban?	2015. november 29-ig	igen
Bírósági engedély nélkül elfoghatnak és tárolhatnak véletlenül megszerzett üzeneteket?	Kizárólag akkor, ha az amerikai külföldiről vagy külföldi célponttal beszél.	Kizárólag akkor, ha az amerikai külföldiről vagy külföldi célponttal beszél, illetve ha tömeges adatgyűjtés eredményeként fogták el.
Metaadatok		
Mikor lehet használni egy amerikai e-mail címét, mint kiindulási pontot egy szociális háló elemzése érdekében a metaadatok alapján?	Kizárólag akkor, ha a bíróság kimondja, hogy megalapozott a gyanú arra, hogy amerikai terrorizmushoz köthető.	Bármilyen külföldi hírszerzési célra, külön bírói engedély nélkül.
Hányadik szintig mehetnek el az elemzők a metaadatok alapján.	kettő	nincs korlát
Tárolt tartalom		

Az NSA megoszthatja a kiértékeletlen információkat pl. az FBI-jal, vagy CIA-val?	igen	Még nem, de a végrehajtó hatalom dolgozik egy iránymutatáson.
Milyen szintű engedélyre van szükség, hogy az adatbázisokban folytassunk lekérdezéseket egy amerikai üzenete kapcsán, amelyet engedély nélkül gyűjtöttek le?	Nem szükséges magas szintű engedély hozzá	A főügyésznek ki kell mondania, hogy az amerikai külföldi hatalmat szolgál
Milyen célból folytathatnak lekérdezéseket adatbázisokban neveket és kulcsszavakat felhasználva, amelyek esetlegesen amerikai tartalmat hoz felszínre?	Külföldi hírszerzés, valamint az FBI bűnügyi nyomozásai kapcsán	Külföldi hírszerzési célból.
Mit kell tennie egy elemzőnek, ha egy amerikai	Meg kell semmisíteni, kivéve, ha hírszerzési szempontból, bűnügyi vagy testi sértési esetekben relevanciával bír.	

kommunikációjával találja szembe magát?	Az igazságügyi minisztériumnak kell átadni őket.[31]	
Bűncselekményre utaló információk		
Az ügyészek figyelmeztetik a bűnügyi vádlottakat, ha a bizonyítékot bírósági engedély nélküli lehallgatások során szerezték?	Igen, az utóbbi időszakban történt változtatások eredményeként	Nem

1. sz. táblázat a Freedom Act és a 12333. sz. elnöki rendelet összehasonlításáról[32]

Az 1. táblázat alapján látható, hogy az elnöki végrehajtási rendelet rendkívül széles külföldi információgyűjtési lehetőséget biztosít az NSA számára. A Nemzetbiztonsági Ügynökségnek ezt a jogát, illetve a végrehajtási rendeletet egyáltalán nem érintik a Barack Obama által a 2015 júniusában beterjesztett Freedom Act keretében bevezetni szándékozott reformok, amelyek 180 napos türelmi/felkészülési időt követően 2015. december 1-től léptek hatályba.

[31] A gyakorlatban ritkán kerül sor olyanra, hogy az ötéves határidő előtt törölnének bármilyen adatot.

[32] SAVAGE, Charlie – PARLAPIANO, Alicia (2014): Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil. https://www.nytimes.com/interactive/2014/08/13/us/two-sets-of-rules-for-surveillance.html (Letöltés időpontja: 2017. 04. 07.)

Az Európai Unió által talán leginkább kifogásolt adatvédelmi hiátust igyekezett pótolni az amerikai Kongresszus azzal, hogy 2016 februárjában elfogadták a Judicial Redress Act-et, amely kiterjesztette a Privacy Act (adatvédelmi törvény) személyi hatályát az uniós állampolgárokra is. A törvény lehetővé teszi az EU-tagországok polgárai számára, hogy jogorvoslattal éljenek, amennyiben egy amerikai kormányzati szerv nem hajlandó végrehajtani azokat az adatpontosításokat, amelyeket az adott személy jogosnak vél, vagy amennyiben visszautasítja a hozzáférési kérelmet, illetve amennyiben az amerikai kormányzati ügynökség szándékosan és tevőlegesen a Privacy Act-tel ellentétesen tárolja az EU állampolgárok személyes adatait. A Privacy Act hatálya alá bevonható országok köréről az amerikai LÜ hoz döntést.[33]

Ezzel párhuzamosan született megállapodás az USA és az EU között Privacy Shield34 néven, amely az EU Bírósága által korábban érvénytelenített Safe Harbor egyezményt volt hivatott pótolni. Az új megállapodás három hónappal később, 2016 májusában lépett hatályba. Ennek részét képezi egy ombudsmani pozíció létrehozása is az amerikai külügyminisztériumon belül, aki egyfajta kapcsolattartói szerepet

[33] GELLER, Eric (2016) Everything You Need to Know about the Big New Data-Privacy Bill In Congress. Forrás: https://www.dailydot.com/layer8/what-is-the-judicial-redress-act-europe-data-privacy-bill/ (Letöltés időpontja: 2017. 04. 05.)

[34] GELLER, Eric (2016): U.S. and E.U. Reach New Data-sharing Deal after Rift Over Mass Surveillance. Forrás: https://www.dailydot.com/layer8/us-eu-data-sharing-privacy-shield-deal-reached-safe-harbor/ (Letöltés időpontja: 2017. 04. 05.)

is ellát az uniós állampolgárokkal, akik jelezni kívánják aggodalmaikat a személyes adataik kezelését illetően.

Az EU állampolgárok számára három lehetőség fog rendelkezésre állni: a kifogásaikat megküldhetik közvetlenül az amerikai cégeknek, amelyeknek válaszadási kötelezettségük van. Jelezhetik aggodalmaikat az Európai Bizottságnak és a Szövetségi Kereskedelmi Bizottságnak (Federal Trade Committee, továbbiakban FTC) is, amely szerveknek közösen kell vizsgálatot indítaniuk és kidolgozniuk a választ. A viták rendezése érdekében létrehoznak egy arbitrázs/választott bírósághoz hasonló mechanizmust is. Az amerikai FTC-nek[35] lehetősége lesz arra, hogy a jogsértések megszüntetését kikényszerítse.

Befejezés

A bemutatottak alapján látható, hogy az USA-ban a rendvédelmi és nemzetbiztonsági érdekek felülírják az alapvető állampolgári jogokat, és széleskörű hozzáférést biztosítanak a személyes adatokhoz. Az adatvédelmi garanciák mértéke – az európai sztenderdekhez képest – még kisebb lesz, ha nem amerikai

[35] Az FTC feladata egyúttal az is, hogy az amerikai vállalatok számára tanúsítványt állítson ki arról, hogy az európai ügyfelek, állampolgárok adatait az EU adatvédelmi előírásaival összhangban tárolják és kezelik. Tekintettel arra, hogy a tanúsítvány kiállításához csak egy kérvényt kellett kitölteni, és az előírások betartásának ellenőrzésére lényegében soha nem került sor, ez az intézkedés semmilyen garanciát nem jelentett.

állampolgárok adatainak a védelméről van szó az USA területén, ugyanis ezt a kérdést a szövetségi szintű törvények nem érintik.
Az amerikai jogrendszer – összehasonlítva az európaival, beleértve a magyart is – kevésbé átfogó jellegű és szektoronként rendkívül eltérő védelmet biztosít. Az uniós adatvédelmi standardok nagy része nem létezik az amerikai joganyagban. Például a kormányzati ügynökségek, nemzetbiztonsági szolgálatok közötti információcserére, megosztásra harmadik féllel nincs reguláció.

A legegyszerűbb és napi szintű kérdés, a szolgálatok közötti információcsere az EU területén csak esetről esetre, specifikusan történhet meg, az USA-n belül viszont az igazságszolgáltatási szervek és a titkosszolgálatok főszabályként megosztják az adatokat, és az a ritkább, ha erre nem kerül sor. Ezen a helyzeten nem változtatott az USA Freedom Act sem, amely leginkább az amerikai állampolgárok adatainak a védelmét erősítette csak. Némi korlátozást jelent a törvénymódosítás eredményeként, hogy a szolgálatoknak – a korábbiaknál konkrétabban – meg kell indokolniuk az adatgyűjtést.

Sajnálatos módon ez a korlátozás nem érinti a FISA-2008 702-es cikkelyét és a 12333. sz. elnöki végrehajtási rendeletet sem, amelyek keretében ezt követően is széleskörű, masszív adatgyűjtési tevékenységet folytathatnak az amerikai ügynökségek. Mindezek alapján elmondható, hogy ha minden, az USA állampolgárok számára rendelkezésre álló adatvédelmi lehetőséget kiterjesztenének az uniós polgárokra is, akkor sem nyújtanának elégséges garanciákat az

igazságszolgáltatási/rendvédelmi és nemzetbiztonsági szektoron belül.

Ezzel szemben az uniós irányelvek, kerethatározatok és rendeletek sem a versenyszféra, sem a nemzetbiztonsági szolgálatok számára nem teszik lehetővé azt a fajta készletező adatgyűjtést, amely az Egyesült Államokban a napi rutin részének tekinthető.

Magyarország esetében – uniós tagállamként – a készletező/tömeges méretű adatgyűjtésnek és adatkezelésnek a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról azon rendelkezései szabnak korlátot, amelyek a célhoz kötöttségről, valamint az érintett beleegyezéséről szólnak az adatkezeléshez. Kivéve, ha ezek hiányában más, arra jogosító törvényi felhatalmazás áll rendelkezésre.

Jogi lényegét tekintve tehát, a készletező adatgyűjtés a konkrét adathoz tartozó, közvetlen célhoz kötöttség hiányát jelenti. Erre a jelenlegi magyar szabályozás és a törvényi garanciák megléte – és feltételezhetően a technikai/technológiai adottságok hiánya – miatt nincs ténylegesen lehetőség.

Korlátot jelent továbbá – az amerikai helyzethez képest – az is, hogy a telekommunikációs és internetszolgáltató vállalatok is csak konkrét személyekre vagy személyes adatnak minősülő azonosítókat tartalmazó megkeresésekre válaszolhatnak és adhatnak információkat. Ebből adódóan a világon folyamatosan növekvő adatmennyiségben rejlő lehetőségeket a magyar

nemzetbiztonsági és rendvédelmi szférán belül csak korlátozottan – értve ez alatt a célhoz kötöttség elve mentén összegyűjtött és tárolt információk mennyiségét – nyílik mód kihasználni.

Irodalomjegyzék

- BARNES, Robert (2013): Secrecy of Surveillance Programs Blunt Challenges about Legality. https://www.washingtonpost.com/politics/secrecy-of-surveillance-programs-blunt-challenges-about-legality/2013/06/07/81da327a-cf9d-11e2-8f6b-67f40e176f03_story.html?utm_term=.9e6ef6707ae7 (Letöltés időpontja: 2017. 02. 05.)
- BOEHM, Franziska (2015): A Comparison Between US And Data Protection Legislation for Law Enforcement. Study for the LIBE (Civil Liberties, Justice and Home Affairs) Committee, Directorate General for Internal Policies, Policy Department C: Citizens' rights and constitutional Affairs. Brussels, 59-65. o. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf (Letöltés időpontja: 2017. 04. 04.)
- Bolcsó Dániel (2015): Csatát vesztett az NSA, de a totális megfigyelésnek nincs vége. (Letöltés időpontja: 2017.04.03. http://index.hu/tech/2015/12/11/nsa_freedom_act_megfigyeles_snowden/
- CAULEY, Leslie (2006): NSA has Massive Database of Americans' Phone Calls.

http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm (Letöltés időpontja: 2017. 03. 10.)
- CORNELL LAW SCHOOL: 50 U.S. Code § 1801 – Definitions; Forrás: https://www.law.cornell.edu/uscode/text/50/1801. (Letöltés időpontja: 2017. 02. 05.)
- CORNELL LAW SCHOOL: 50 U.S. Code § 1802 – Electronic surveillance authorization without court order; certification by Attorney General. Forrás: https://www.law.cornell.edu/uscode/text/50/1802. (Letöltés időpontja: 2017. 02. 05.)
- CORNELL LAW SCHOOL: 50 U.S. Code § 1805 – Issuance of order: https://www.law.cornell.edu/uscode/text/50/1805. (Letöltés időpontja: 2017. 02. 05.)
- FISA Amendments Act of 2008: https://www.congress.gov/bill/110th-congress/house-bill/6304/text. (Letöltés időpontja: 2017. 02. 06.)
- GARTNER.COM: Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data. http://www.gartner.com/newsroom/id/1731916 (Letöltés időpontja: 2017. 03. 02.)
- GELLER, Eric (2016) Everything You Need to Know about the Big New Data-Privacy Bill In Congress. Forrás: https://www.dailydot.com/layer8/what-is-the-judicial-redress-act-europe-data-privacy-bill/ (Letöltés időpontja: 2017. 04. 05.)
- GELLER, Eric (2016): U.S. and E.U. Reach New Data-sharing Deal after Rift Over Mass Surveillance. Forrás: https://www.dailydot.com/layer8/us-eu-data-sharing-privacy-shield-deal-reached-safe-harbor/ (Letöltés időpontja: 2017. 04. 05.)
- GREENBERG, Andy (2015): Court Rules NSA Bulk Data Collection Was Never Authorized By Congress.

https://www.wired.com/2015/05/breaking-news-federal-court-rules-nsa-bulk-data-collection-illegal/ (Letöltés időpontja: 2017. 04. 06.)

- GUALTIERI, Mike (2013): The Forrester Wave: Big Data Predictive Analytics Solutions Q1 2013. http://webcache.googleusercontent.com/search?q=cache:NQGhw9x85U0J:www.sas.com/resources/asset/Forrester85601-LR8KBD.pdf+&cd=2&hl=hu&ct=clnk&gl=hu (Letöltés időpontja: 2017. 04. 03).
- HARRIS, Shane (2015): Zombie Patriot Act Will Keep U.S. Spying—Even if the Original Dies (2015.01.06.) http://www.thedailybeast.com/articles/2015/05/31/zombie-patriot-act-will-keep-u-s-spying-even-if-the-original-dies.html (Letöltés: 2017. 04. 04).
- HILBERT, Martin – LÓPEZ, Priscila (2011): The World's Technological Capacity to Store, Communicate, and Compute Information. http://science.sciencemag.org/content/332/6025/60 (Letöltés időpontja: 2017. 03. 04.)
- i-SCOOP.EU: The DIKW model for knowledge management and data value extraction. https://www.i-scoop.eu/big-data-action-value-context/dikw-model/ (Letöltés időpontja: 2017. 03. 05.)
- LINDEMAN, Todd (2013): The Foreign Intelligence Surveillance Court https://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graphic.html?utm_term=.5c87edf26def (Letöltés időpontja: 2017. 02. 05.)
- NORTON-TAYLOR, Richard (2010): Not so secret: deal at the heart of UK-US intelligence https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released (Letöltés időpontja: 2017. 02. 05.)

- Protect America Act of 2007. https://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm. (Letöltés időpontja: 2017. 02. 06.)
- SAVAGE, Charlie – PARLAPIANO, Alicia (2014): Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil. https://www.nytimes.com/interactive/2014/08/13/us/two-sets-of-rules-for-surveillance.html (Letöltés időpontja: 2017. 04. 07.)
- SCHNEIDER, Christie (2016): The biggest data challenges that you might not even know you have. https://www.ibm.com/blogs/watson/2016/05/biggest-data-challenges-might-not-even-know/ (Letöltés időpontja: 2017. 03. 03.)
- The White House Office of the Press Secretary (2014): Presidential Policy Directive - Signals Intelligence Activities https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (Letöltés időpontja: 2017. 04. 04.)
- WORLD ECONOMIC FORUM (2012): Big Data, Big Impact: New Possibilities for International Development. World Ecnomic Forum. Forrás: http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf (Letöltés időpontja: 2017. 03. 05.)