Magyar Rendészet 2016/1. 141–146.

Adatvédelem vagy biztonság?

SCHUBAUER Petra

Az Európai Unió Bírósága 2015. október 6. napján a C-362/14. számú ügyben érvénytelenné nyilvánította az ún. Safe Harbor programot, amely lehetőséget teremtett az Egyesült Államokba való adattovábbításra. A döntés alapját az amerikai nemzetbiztonsági szolgálatok általi tömeges és válogatás nélküli megfigyelés adta, amelyet az Európai Unió Bírósága jogellenesnek ítélt meg, és amellyel kapcsolatban megállapította, hogy az USA adatvédelmi gyakorlata nem biztosítja a megfelelő szintű védelmet az uniós polgárok személyes adatai számára. Az általános jellegű megfigyelés közel sem jelenti a nemzetbiztonsági veszélyekkel, így különösen a terrorizmussal szembeni hatékony fellépés eszközét.

A Schrems kontra Data Protection Commissioner ügy

2015. október 6. napján az Európai Unió Bírósága kimondta az ún. *Safe Harbor* ('biztonságos kikötő') határozat érvénytelenségét, amely alapjaiban bolygatta meg az európai adattovábbítási gyakorlatot. Az Egyesült Államok Kereskedelmi Minisztériuma 2000. július 21. napján adta ki a Safe Harbor adatvédelmi elveket, amelyek alapján az EU-ból az USA-ba történő adattovábbítás biztonságosnak tekintendő, amennyiben az USA-ban letelepedett vállalkozások az elveknek megfelelő tevékenységet fejtenek ki. A Safe Harbor önszabályozáson alapul, az elveket magukra nézve kötelezőnek elismerő vállalkozásokról bejelentés után a Kereskedelmi Minisztérium bárki számára elérhető nyilvántartást[1] vezet. A Safe Harbor gyakorlati jelentőségét mutatta, hogy a legnagyobb amerikai adatkezelők – így a Facebook, a Yahoo, az eBay, az Amazon és a Google is – a Safe Harbor adatvédelmi elveknek való megfelelőséggel teremtettek jogalapot adatkezeléseikhez.[2] 2000 júliusától 2015 októberéig biztonságosnak tekintették az adattovábbítást a Safe Harbor elvek alapján, azonban ezt a közel 15 éves gyakorlatot megszüntette az Európai Unió Bíróságának a C-362/14. számú ügyben hozott határozata.

A döntés alapját a Maximillian Schrems kontra Data Protection Commissioner ügy adta, amelyben Schrems a Facebook Ireland Ltd. (a továbbiakban: Facebook Ireland) ellen 2013. június 25. napján panaszt nyújtott be a Data Protection Commissionerhez ('adatvédelmi biztoshoz', a továbbiakban: Commissioner). A panasz alapját az képezte, hogy a Facebook US az USA-ban található szervereken tárolta felhasználói személyes adatait (a magánszemélyekről készült, különböző online felületeken – így a közösségi

1 https://safeharbor.export.gov/list.aspx (2015. 11. 08.)
2 Liber (2011) 181.

oldalakon is – megosztott fényképek, illetve az általuk folytatott beszélgetések, az általuk létrehozott profilok és más virtuális tartalmak személyes adatnak minősülnek, mivel azok az érintett személlyel kapcsolatba hozhatók, és azokból következtetés vonható le rájuk nézve[3]). Schrems azzal érvelt, hogy az Egyesült Államok joga és gyakorlata nem biztosít az uniós állampolgárok adatai számára megfelelő védelmet az állami felügyelettel szemben, amely állítását a Snowden-ügy során kiderült információkkal támasztotta alá.

2013 júniusában Edward Snowden felfedte, hogy az amerikai Nemzetbiztonsági Ügynökség (*National Security Agency,* a továbbiakban: NSA) és további amerikai nemzetbiztonsági szolgálatok a *Prism* nevű program[4] alkalmazásával tömeges és szabad hozzáférést kaptak az Egyesült Államok szerverein tárolt adatokhoz. Ezeket a szervereket számos, az internet és technológia területén tevékenykedő, a Facebook US-hez hasonló vállalkozás birtokolta vagy felügyelte,[5] így a szervereken többek között az uniós Facebook-felhasználók személyes adatai is megtalálhatók voltak. Bár a Safe Harbor határozat I. mellékletének 4. bekezdése alapján lehetőség van eltérni az elvektől nemzetbiztonsági megfontolások alapján, a Snowden-ügy kapcsán Schrems érvei szerint a Prism hírszerző program megkérdőjelezi a Bizottság döntésének érvényességét, miszerint az USA-ban a Safe Harbor-programban részt vevő vállalkozások esetében biztosított a megfelelő adatvédelem.[6] A személyes adatok USA-ba való továbbítását követően az NSA és más szövetségi ügynökségek hozzáférhetnek az adatokhoz azok tömeges és válogatás nélküli megfigyelése és lehallgatása útján, amely jelentős túlkapást jelent, és így túlterjeszkedik az I. számú melléklet 4. bekezdése által megengedett határokon. (A nemzetbiztonsági megfontolások alapján történő eltérést a legtöbb adattovábbításra vonatkozó szabályozás tartalmazza, nemcsak a Safe Harbor határozat, hanem az Európai Bizottság által kiadott ún. *model clause* is, azaz az általános szerződési feltételek.)

A Commissioner úgy ítélte meg, hogy a panaszt nem köteles kivizsgálni, mivel véleménye szerint nem volt bizonyíték arra, hogy az NSA hozzáférhetett Schrems adataihoz. Schrems a panaszt elutasító határozat ellen keresetet nyújtott be a High Court of Irelandhez, amely arra a megállapításra jutott, hogy Schrems panasza nem a Facebook Ireland magatartására, hanem magára a Safe Harbor-rendszerre és az USA adatvédelmi jogára és gyakorlatára irányult. Ezek alapján a panasz az uniós jogot közvetlenül érinti, így a High Court of Ireland előzetes döntéshozatali eljárásban fordult az Európai Unió Bíróságához.

Az előzetes döntéshozatali eljárás során Yves Bot főtanácsnok (a továbbiakban: főtanácsnok) kifogásolta, hogy az uniós Facebook-felhasználókat nem tájékoztatják a regisztráció során arról, hogy a személyes adataikat egy olyan harmadik országba továbbítják, amelyben az adatok az ottani szabályozásnak megfelelően elérhetőek lesznek a nemzetbiztonsági ügynökségek számára. Az USA joga és gyakorlata széles körben lehetővé teszi az uniós polgárok személyes adatainak gyűjtését és általános jellegű lehall-

3 A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az online adatok halál utáni sorsáról.
4 www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
5 Bot (2015)
6 Pfeifle (2015)

gatását anélkül, hogy az érintettek hatékony jogi védelmet élveznének, vagyis a Prism nevezetű program aránytalan és szükségtelen mértékben fér hozzá az uniós polgárok adataihoz: nemcsak azokéhoz, akik a nemzetbiztonságra nézve veszélyt jelentenek, hanem mindenkiéhez, aki a Facebook elektronikus hírközlési szolgáltatását igénybe veszi. Megállapításra került, hogy az uniós polgároknak nincs tényleges meghallgatási joguk, nincs lehetőségük betekinteni az adatokba, azok helyesbítését, törlését kérni vagy jogorvoslattal élni, valamint nincs megfelelő független felügyeleti szerv, hatóság, amely az adatkezelés jogellenességét vizsgálhatná.

A fent említett indokok alapján, a főtanácsnok indítványával összhangban az Európai Unió Bírósága arra az álláspontra jutott, hogy a Safe Harbor határozat nem tartalmaz elég biztosítékot,[7] és így érvénytelennek kell nyilvánítani, mivel az alapvető jogoknak a fentiekben leírt megsértése miatt nem fogadható el, hogy az e határozat által létrehozott biztonságos kikötő rendszere megfelelő védelmi szintet biztosít az EU-ból az USA-ba továbbított személyes adatok számára.[8]

Tömeges lehallgatások vagy terrorizmus elleni küzdelem?

Az Európai Unió Bírósága ítéletében gyakorlatilag abban a kérdésben is állást foglalt, hogy milyen szintig engedhető meg a nemzetbiztonsági szolgálatok megfigyelő tevékenysége, és mikor lépik át a jogszabályok által kijelölt határokat. A 2015. november 13-ai terrorcselekmények kapcsán ismét fellángolt a vita arról, hogy milyen mértékben szükséges megfigyelni a személyek kommunikációját azzal a céllal, hogy a terrorizmus nyomon követhető és megfékezhető legyen. Minden jóérzésű emberben talán felmerül az igény arra, hogy a nemzetbiztonsági szolgálatok inkább figyeljék meg személyes kommunikációit, amennyiben ezzel elháríthatóvá válnak a terrorcselekmények. Fontos ugyanakkor megjegyezni, hogy jelenleg az informatika világában számtalan lehetőség akad arra, hogy a kommunikáció elérhetetlen vagy feltörhetetlen legyen a nemzetbiztonsági szolgálatok számára, valamint a tömeges lehallgatás nagyobb veszélyeket rejthet, mint amelyek megfékezésére képes.

Az internet, az internetes kommunikáció – ugyanúgy, mint minden más technikai megoldás – a hétköznapi, rendeltetésszerű céloktól egészen eltérően is felhasználható: a terrorizmus is előszeretettel használja a legújabb megoldásokat, trendeket, eszközöket propagandája terjesztéséhez, terrorcselekményei megszervezéséhez. Az Iszlám Államhoz hasonló terrorszervezetek egyre jobban ügyelnek kommunikációjuk műveleti biztonságára[9] (ún. *opsec*), s olyan módszereket és eszközöket használnak, amelyek lehallgatása gyakorlatilag lehetetlen (ahogy novemberben több hírportálon is olvasható volt, a Telegram- vagy a Playstation-konzolokon keresztül történő kommunikáció teszi ki a szervezet információcseréjének nagy részét).

7 Bot (2015)
8 Az Európai Unió Bíróságának döntése a C-362/14. számú ügyben.
9 Zetter (2015)

A 2015. novemberi támadások után sok amerikai tisztviselő nyilatkozta, hogy az Edward Snowden-ügy kapcsán megindult általános titkosítás terjedése az oka, hogy a nemzetbiztonsági szolgálatok nem tudták megakadályozni a terrorcselekményeket. (Azt azonban leszögezhetjük, hogy a problémát a Snowden-ügy kapcsán nem az adta, hogy a nemzetbiztonsági szolgálatok lehallgatják a terroristagyanús személyeket, hanem hogy lehallgatnak mindenki mást is,[10] minden egyes személyt, aki valamilyen elektronikus hírközlési szolgáltatást vett igénybe.) Az igazság az, hogy a terrorszervezetek sokkal régebb óta igyekeznek titkos csatornákat használni, valamint titkosítás nélkül is megtalálják a módját, hogy rejtve kommunikáljanak.

Gondoljuk csak arra, hogy a világon a legegyszerűbb módon történő kódolás elvileg mindenki számára megfejthetetlen: nem kell hozzá más, csak egy véletlenszerű számokból álló számsor és a titkosítani kívánt üzenet. Az üzenet minden betűjét az ábécében a véletlenszerű számmal el kell tolni, így kijön egy értelmetlen betűhalmaz, amely visszafejtése a random számokból álló számsor ismeretének hiányában elvileg lehetetlen, éppen véletlenszerűsége miatt. Ha a titkos üzenet mondjuk az *ADATVEDELEM* szó, a véletlenszerű számsor pedig a 27691348597, akkor a kapott eredmény *CKGCWHIMQNT*. (Az *A* 2 helyi értékkel eltolva *C* lesz, a *D* 7 helyi értékkel eltolva *K*, és így tovább.) Az üzenet fogadójának csak a megfelelő dekódoló számsort kell ismernie ahhoz, hogy a kommunikáció megvalósuljon, és minden külső személy számára érthetetlen legyen.

Láthatjuk, hogy akár a kommunikáció teljes megfigyelése esetén is van mód a rejtett információcserére, ráadásul különösebb anyagi ráfordítást sem igényel: elegendő, ha például az üzenet küldője és fogadója megvesz egy ugyanolyan DVD-filmet, amelynek képkockái gyakorlatilag véletlenszerű számokból állnak, és amely számok alkalmasak az üzenetek kódolására és dekódolására.

Az ún. *end-to-end* titkosított kommunikáció azt jelenti, hogy az üzenet tartalmát kizárólag a feladó és a fogadó ismeri. A különböző kormányzatok általában megkövetelik, hogy a kódolást végző biztonsági szoftverekben *backdoor*okat ('hátsó ajtó'), azaz lyukakat hagyjanak, amelyeken keresztül a nemzetbiztonsági szolgálatok megfigyelhetik a kommunikációt (ilyeneket használt fel az ún. Prism program is). Az Information Technology Industry Council igazgatója, Dean Garfield szerint a biztonság gyengítésének a biztonság fokozása érdekében egyszerűen nincs értelme.[11] Egy ilyen backdoor mindenki számára backdoor, azaz fennáll a veszélye, hogy a kiberbűnözők is felhasználják a biztonsági szoftverekbe telepített réseket.[12] A nagy cégek – így a Facebook, a Google, a Microsoft stb. – lehallgatásával valójában csak azt lehet elérni, hogy a saját adatai védelmével kevésbé foglalkozó átlagfelhasználót is nagyobb kockázatoknak teszik ki.[13]

10 Greenwald (2015)
11 Gibbs (2015)
12 Uo.
13 Bolcsó (2015)

Összegzés

Láthatjuk, hogy a kommunikáció – akár egészen primitív módon történő – titkosítása nem jelent különösebb problémát a terrorszervezetek számára, s ez a lehallgatást feleslegessé teszi. Az általános jellegű lehallgatás és a biztonsági szoftverek gyengítése pedig nem a terrorizmus elleni harcot könnyíti meg, hanem az átlagos felhasználók adatbiztonságát veszélyezteti, így a tömeges megfigyelés egyenesen kontraproduktívvá válik. A hatóságok számára az egyetlen lehetőség az igazán hatékony fellépésre a metaadatokhoz való hozzáférés – hogy ki, kivel és mikor kommunikált –, vagyis a már ismert terroristák kapcsolatelemzése.[14]

A terror okozta általános félelem miatt az Európai Unió polgárai maguk követelhetik a különlegesen széles európai szabadságok korlátozását: azt, hogy a rendőrség és a titkosszolgálatok több jogosítványt kapjanak, vagy hogy az európai belső határokat újra ellenőrizzék. Miközben teljesen természetes reakció a védekezés szándéka fenyegetés esetén, egyáltalán nem egyértelmű, hogy az európai szabadságjogok – így a személyes adatok védelméhez fűződő jog – leépítése a hatékony és megfelelő válasz.[15] Nagy kihívást jelent ez Európának: úgy legyőzni a terrort, hogy közben nem adja fel saját értékrendjét, amely a szabadságon alapul.

FORRÁSJEGYZÉK

A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az online adatok halál utáni sorsáról. (2015) Forrás: www.naih.hu/files/Ajanlas_online-adatok-halal-utani-sorsarol.pdf (2016. 01. 29.)

Az Európai Unió Bíróságának döntése a C-362/14. számú ügyben. (2015) Forrás: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en (2015. 10. 28.)

Bolcsó Dániel (2015): *Mit művel az interneten az Iszlám Állam?* Forrás: http://index.hu/tech/2015/11/25/mit_muvel_az_interneten_az_iszlam_allam/ (2015. 11. 27.)

Bot, Yves főtanácsnok indítványa. (2015) Forrás: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddf7ae5498dabc4aa1a38bcb7cc7136a13.e34KaxiLc3qMb40Rch0SaxuSb350?text=&docid=168421&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=806780 (2015. 10. 10.)

Gibbs, Samuel (2015): *Apple, Google and Microsoft: Weakening Encryption Lets the Bad Guys In.* Forrás: www.theguardian.com/technology/2015/nov/23/apple-google-microsoft-weakening-encryption-back-doors (2015. 12. 02.)

Greenwald, Glenn (2015): *Exploiting Emotions About Paris to Blame Snowden, Distract from Actual Culpits Who Empowered ISIS.* Forrás: https://theintercept.com/2015/11/15/exploiting-emotions-about-paris-to-blame-snowden-distract-from-actual-culprits-who-empowered-isis/ (2015. 11. 29.)

https://safeharbor.export.gov/list.aspx (2015. 11. 08.)

Liber Ádám (2011): Személyes adatok nemzetközi továbbítása. Az új adatvédelmi törvény margójára. In: *Infokommunikáció és Jog,* 8. évf. 46. sz. 179–187.

14 Uo.

15 Magyari (2015)

Magyari Péter (2015): *Győzni nem tudnak, de ettől még veszthetünk.* Forrás: http://444.hu/2015/11/15/gyozni-nem-tudnak-de-ettol-meg-veszthetunk?google_editors_picks=true (2015. 11. 15.)
Pfeifle, Sam (2015): *ECJ: Safe Harbor "Invalid".* Forrás: https://iapp.org/news/a/first-reactions-to-the-ecj-decision (2015. 10. 31.)
www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data(2015. 10. 28.)
Zetter, Kim (2015): *Security Manual Reveals The Opsec Advice ISIS Gives Recruits.* Forrás: www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/(2016. 01. 31.)

SUMMARY

Data Protection or Security?

SCHUBAUER Petra

On the 6th of October, 2015 the Court of Justice of the European Union decided in the case no. C-362/14. that Safe Harbour is invalid. Safe Harbour created a legal base for transferring personal data to the United States from the European Union. The most important reason for the decision was the massive surveillance of the National Security Agency, which is illegal. The law and practice of the USA do not ensure the adequate level of data protection for the personal data of the citizens of the European Union. The general and massive surveillance is not effective against terrorism and against other dangers to national security.