Az alkalmazásszolgáltatók törvényes ellenőrzésének jövője – a technológiák konvergenciájának tükrében

Dr. Kovács Zoltán[1]

Absztrakt:

Az internet-technológiára épülő szolgáltatások gyors ütemű terjedése, fejlődése, ugrásszerűen változása új kihívás elé állítja a törvényes ellenőrzésére feljogosított nemzetbiztonsági és rendvédelmi szerveket. Jelen cikk áttekinti az internet-technológiára épülő szolgáltatások bővülése és fejlődése kapcsán kialakult technológiai konvergencia hatásait az alkalmazásszolgáltatók törvényes ellenőrzésére, publikus forrásokból elérhető információkra alapozva jellemző példát mutat be külföldi nemzetbiztonsági szolgálatok által használt módszerekre, majd elemzi a hazai megvalósítás lehetőségét.

Kulcsszavak: alkalmazásszolgáltató, törvényes ellenőrzés, internet-technológiára épülő szolgáltatások

Abstract:

The national security services and law enforcement agencies, which are authorized for lawful monitoring, are challenged by the fast spreading, developing, and changing of the Internet based services and quick growth of their use. This article reviews the effect of convergence of technologies for the lawful monitoring of the application service providers caused by developing, and changing of the Internet based services, presenting representative lawful monitoring methods used by foreign national security services and law enforcement agencies based on public sources, and then analysis the possibility of national implementation of it.

Keywords: application service provider, lawful monitoring, Internet based services

[1] *zkovacs@nbsz.gov.hu*

Bevezetés

Felgyorsult életritmusunk, a – sokszor napi nyolc órát meghaladó – munka melletti számtalan kötelezettségünk, egyéb teendőink okán egy-egy feladat, ügy elintézésére egyre kevesebb időnk marad. Az internet és az internet-alapú alkalmazások segítenek abban, hogy számtalan teendőnket gyorsabban, kényelemsebben, sorban állás nélkül akár otthonról is elintézhessük. Ezek pedig jelentős mértékben befolyásolják, alakítják mindennapi tevékenységeinket.

A változások legszembetűnőbben talán kommunikációs szokásaink átalakulásában érhetők tetten. A kommunikáció formái, lehetőségei az internet és az azt kihasználó alkalmazások, valamint az ezek elérését biztosító eszközök fejlődésével ugrásszerűen változnak, bővülnek. Mindezek egyfajta összefonódó spirált képezve, egymást is erősítve, egyre nagyobb mértékű felhasználást gerjesztve növelik tovább a fejlődés ütemét. Mindemellett markánsan megjelenik a technológiák konvergenciája, összeolvadása, amit az eszközöknél és az azokkal igénybe vett szolgáltatásoknál egyaránt megfigyelhetünk.[2,3] Az eszközök esetében láthatjuk, hogy ma már egy kisméretű eszköz biztosítja a hang és adatkommunikációt, valamint szinte az összes, korábban dedikált számítógéppel, vagy más eszközzel ellátott funkciót, a szolgáltatások tekintetében pedig elmondható, hogy sokszor egy alkalmazásszolgáltatótól vehetünk igénybe például kommunikációs, tárhely és csoportmunkával kapcsolatos szolgáltatásokat egyaránt.

Kommunikációnk egyre gyorsuló átalakulásában nagy szerepük van tehát az internet-technológiára épülő szolgáltatásoknak, ezeken belül is a nyilvános számítási felhő (Public cloud) telepítési modell szerint működő, elsősorban szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) szolgáltatási modell típusú rendszereknek (továbbiakban: PC/SaaS felhő alapú rendszerek). Ezek azok a mindenki számára elérhető, meglévő eszközökkel (pl. notebook, okostelefon stb.), akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, Gmail, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

Ám az internet-technológiára épülő szolgáltatások nemcsak kommunikációs szokásainkra hatnak, hanem az élet minden más területén is új lehetőségeket biztosítanak. Igénybe vehetünk banki szolgáltatásokat[4], fizethetünk web boltok-

---

[2] *SALLAI Gyula – ABOS Imre: A távközlés, információ- és médiatechnológia konvergenciája. Magyar Tudomány. Infokommunikációs hálózatok. 168. Évfolyam. 2007. július pp. 844-851. ISSN 1588-1245*

[3] *HAIG Zsolt: Információ - társadalom - biztonság. Budapest. NKE Szolgáltató Kft., 2015. ISBN 978-615-5527-08-*

[4] *https://www.otpbank.hu/portal/hu/OTPdirekt/Home. Letöltés ideje: 2013. 10. 27.*

ban[5], játszhatunk[6], szerkeszthetjük dokumentumainkat[7], képeinket[8], tárolhatjuk, megoszthatjuk adatainkat[9], készíthetünk útvonaltervet[10], és még nagyon hosszan lehetne folytatni a felsorolást.

Az internet-technológiára épülő szolgáltatások, azokon belül is a felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, ugyanakkor a törvényes ellenőrzést végző szervek több – jogi és technikai – problémával is szembesülnek.

A témakörrel már több tanulmányomban foglalkoztam. A „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk[11] elemezte azokat a problémákat, amelyekkel a törvényes ellenőrzésre feljogosított szervek az új technológiák megjelenése okán találkoznak, majd több, a megoldást elősegítő, elvégzendő feladatot is megfogalmazott. Az itt leírtak alapján a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II." című cikkek[12,13] bemutatták a törvényes ellenőrzésre jelenleg rendelkezésre álló módszereket, felállítottak egy, az azok elemzéséhez szükséges szempontrendszert, és elvégezték a felsorolt technikai megoldások elemzését, csoportosítva azok előnyeit, hátrányait. Az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből" című cikk[14] pedig felállított egy, a felvetett problémákat kezelni képes, a hírközlési szolgáltatói modellt potenciálisan felváltó új szolgáltatói modellt, fogalmi meghatározásokat is adva az abban szereplőként megjelenített infrastruktúra-, alkalmazás- és tartalomszolgáltatókra. Ez az az új modell ráadásul úgy alkalmas a gyakorlati életben már jelenleg is létező, de a jogszabályokban még le nem követett szolgáltatatói struktúra leírására, hogy ebbe a modellbe nem csak a kommunikációt lehetővé tevő internet-technológiára épülő, hanem minden más, pl. pénzügyi, útvonaltervezést lehetővé tevő stb. szolgáltatás, szolgáltató is beilleszthető, beleérthető.

---

[5] https://www.paypal.com/hu/webapps/mpp/home Letöltés ideje: 2013. 10. 27.

[6] http://eu.battle.net/wow/en/. Letöltés ideje: 2013. 10. 27.

[7] http://office.microsoft.com/hu-hu/business/. Letöltés ideje: 2013. 10. 27.

[8] http://www.adobe.com/hu/products/photoshop.html. Letöltés ideje: 2013. 10. 27.

[9] dropbox.com. https://www.dropbox.com/. Letöltés ideje: 2014. 03. 14.

[10] https://maps.google.hu/maps?hl=hu&tab=wl. Letöltés ideje: 2013. 10. 27.

[11] KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. 2013. március, Hadmérnök, VIII. Évfolyam 1. szám. pp. 233 – 241. ISSN 1788-1919.

[12] KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 184 – 197. ISSN 1788-1919.

[13] KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 198 – 210. ISSN 1788-1919.

[14] KOVÁCS Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-375

A törvényes ellenőrzésre feljogosított szolgálatok az említett cikkekben megfogalmazott és kidolgozott javaslatok és eredmények egy részét már ma is képesek felhasználni, míg más részükhöz a hazai, sőt a nemzetközi jogszabályi háttér átalakítása szükséges. Ez utóbbi azonban, azaz a jogi szabályozás átalakítása – a fenti cikkekben feltárt problémák fényében – mindenképpen elkerülhetetlen. Ezt bizonyítják az említett cikkekben is megjelenő, az Európai Unióban is tetten érhető, sokszor országonként eltérő úton induló különböző kezdeményezések.

Mindezek mellett azonban érdemes azt is megvizsgálni, hogy a technológiák konvergenciája milyen irányba viszi, viheti az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből" című cikkben[15] definiált alkalmazásszolgáltatók törvényes ellenőrzéséhez szükséges technikai eszközrendszer kialakítását. Ennek érdekében jelen tanulmány bemutatja technológiák konvergenciájából adódó törvényes ellenőrzési kihívásokat, valamint elemzi, hogyan lehet – a jelen és a közeljövő várható jogi és technikai keretei között is – biztosítani a törvényes ellenőrzés technikai eszközrendszereinek hatékonyan működtetését.

A technológiai konvergencia hatása az alkalmazásszolgáltatók törvényes ellenőrzésére

Az internet-technológiára épülő szolgáltatások nem csak a felhasználói szokásokat változtatták, változtatják meg alapjaiban, hanem a hírközlés struktúráját is teljesen átformálják. Ennek talán a leglényegesebb eleme az, hogy a tényleges kommunikációs szolgáltatást valamint az ahhoz szükséges infrastruktúrát – ellentétben például a hagyományos telefóniával – nem egyazon szolgáltató biztosítja a felhasználó számára. Sőt, ezek a legtöbb esetben nem is tudnak egymásról, nincsenek semmilyen kapcsolatban egymással. Gondoljunk csak például egy mobilinternet szolgáltatáson használt Skype, vagy Viber alkalmazásra. Ez a gyakorlatban azt jelenti, hogy a különböző funkciókat, így a kommunikációt is biztosító alkalmazásszolgáltatók és az azokhoz szükséges infrastruktúrát kiépítő és üzemeltető, infrastruktúraszolgáltatóvá váló, korábbi hírközlési szolgáltatók általában élesen elkülönülnek egymástól.

A jelenlegi, törvényes ellenőrzéssel kapcsolatos jogszabályokat, sőt az elérhető ellenőrzési technológiák jelentős részét is a régi hírközlési szolgáltatói struktúrának megfelelően alakították ki, amely mára már nem biztosítja a megfelelő eredményeket és hatékonyságot a törvényes ellenőrzés során. Mint ahogy azt a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II." című

[15] *Kovács Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-375*

írások ismertetik[16,17], léteznek ugyan törvényes ellenőrzést biztosító technológiák, ám egyrészt ezek egyike sem nyújt teljes körű megoldást, másrészt jogi elfogadottságuk, megítélésük is jelentősen eltér az egyes országokban, sőt, adott esetekben még legitimitásuk is vitatott.

Mindezek mellett a technológiák konvergenciája is jelentős mértékben befolyásolja azt, hogy hogyan érdemes kiépíteni egy, már a jelen, és a közeljövőben szükségszerűen bekövetkező jogszabályi változások mellett is hatékonyan működő, működtethető ellenőrzési struktúrát.

A technológiák konvergenciájának meghatározó jelentőségét mutatja be „A 21. század hírközlési trendjei" című tanulmány[18], amely a titkosszolgálatok feladatainak ellátása szempontjából tekinti át a hírközlési megatrendeket. Ebben a globalitás, a regionális szövetségek megjelenése, a mobilitás, a szélessávú infrastruktúrák előretörése és a liberalizáció mellett a konvergencia is megjelenik, ráadásul úgy, mint a legmeghatározóbb trend. A technológiák konvergenciája alatt a távközlés, az informatika és a média szinte elválaszthatatlan és megkülönböztethetetlen összefonódását érti a szerző, amely mind a szolgáltatások, mind az azok használatát biztosító végberendezések esetében megfigyelhető.

Ezt a konvergenciát jól szemlélteti az infokommunikáció fogalmának megjelenése is. A '90-es évek közepétől a számítástechnika és a kommunikáció egyre jobban összefonódott, integrálódott, létrejöttek az infokommunikációs (ICT)[19] hálózatok.[20] Az infokommunikáció fogalmát – bár pontos, mindenki által elfogadott meghatározása nincs és jelentéséről a mai napig is sok vita folyik[21] – az információtechnológia (IT)[22] kiterjesztett szinonimájaként is használják, beleértve olyan hardver és szoftver elemeket, tárolókat, middleware-t, audio-vizuális rendszereket stb. is, amelyek az információk előállításához, tárolásához, haszná-

---

[16] KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 184 – 197. ISSN 1788-1919.

[17] KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 198 – 210. ISSN 1788-1919.

[18] BARTOLITS István: A 21. század hírközlési trendjei, A SIGINT a XXI. század kihívásainak tükrében. Felderítő Szemle, VI. évfolyam. 2007. február pp.: 49-61. ISSN 1588-242X.

[19] ICT: Information and Communications Technology (információ- és kommunikációtechnológia vagy infokommunikációs technológia)

[20] HAIG Zsolt – KOVÁCS László – MUNK Sándor – VÁNYA László: Az infokommunikációs technológia hatása a hadtudományokra. Budapest: Nemzeti Közszolgálati Egyetem, 2013. ISBN 978-615-5305-02-3.

[21] MUNK Sándor: A kommunikáció fogalomrendszerének keretei az integrálódó információs technológiák korában. In: Kommunikáció 2009. Budapest. ZMNE, 2009. pp. 51-64. ISBN 978-963-7060-70-0

[22] IT: Infomation technology (információtechnológia vagy informatika)

latához, megosztásához, archiválásához és törléséhez szükségesek.[23] Elfogadva ezt a megközelítést, jelen cikk is így használja az infokommunikáció fogalmát, olyan helyeken is ezt alkalmazva, ahol a különböző, jelen kutatás alapját is képező dokumentumok készítői IT rendszereket írtak. Ennek oka pedig az, hogy az IT az ICT részhalmazát képezi, ugyanakkor ma nagyon nehéz, sokszor képtelenség meghatározni mikor van szó „csupán" IT rendszerről, így az ICT fogalma pontosabban, teljeskörűbben lefedi ezeket a rendszereket.

Amint azt a „Új technológiák hatása a hírszerzésre" című tanulmány[24] is bemutatja, a technológiák konvergenciája nem csak a felhasználásban figyelhető meg, hanem a törvényes ellenőrzés tekintetében is. Az infokommunikációs rendszerek törvényes ellenőrzési feladatrendszerébe – a mai megközelítés szerint – alapvetően az alábbi három tevékenységet soroljuk:

- adatszolgáltatás,
- kommunikáció ellenőrzés,
- forensic tevékenység.

Mindez azonban a korábbi ellenőrző tevékenységekhez képest vegyes képet mutat. Míg az adatszolgáltatásról és a kommunikáció ellenőrzésről elsősorban a klasszikus hírközlési hálózatoknál beszéltünk, addig a forensic tevékenység eddig kifejezetten számítástechnikai rendszerek vizsgálatára volt jellemző. Ma már a fejlett infokommunikációs rendszerek jellege, valamint az azokból kinyerhető, a nemzetbiztonsági és a bűnüldözési feladatokat segítő információk köre miatt mindháromra egyaránt, ráadásul sokszor egyszerre szükség van. Ebből levonható tehát az a következtetés, hogy nem csak a technológiák konvergenciája figyelhető meg napjainkban, hanem ennek kapcsán a törvényes ellenőrzési metódusok konvergenciája is. Márpedig ez olyan technológiai megoldásokat kíván, amelyek korábban egyáltalán nem, vagy legalábbis ebben a formában nem léteztek. Így ezek kialakítása a (közel)jövő fontos feladata.

Ráadásul mind az infokommunikációs rendszerek, mind azok törvényes ellenőrzésénél megfigyelhető konvergencia kapcsán, többek között az alábbi jelentős problémákkal kell a feljogosított szervezeteknek megbirkóznia:

- Növekvő adatmennyiség:

A szélessávú internet elérésének terjedése, az új típusú kommunikációs és egyéb szolgáltatások kialakulása és folyamatos fejlődése, az online tartalmak fogyasztásának emelkedése az adatforgalom drasztikus emelkedését is magával hozza. Ez

[23] *SALLAI Gyula: Defining Infocommunications and Related. Acta Polytechnica Hungarica. 9. Évfolyam 6. szám – 2012. pp. 5-15. ISSN 1785-8860*

[24] *DOBÁK Imre - KOVÁCS Zoltán: Új technológiák hatása a hírszerzésre. In: A nemzetbiztonság általános elmélete. Szerk.: Dobák Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2014. pp. 206-220. ISBN: 978-615-5305-49-8*

pedig azt jelenti, hogy a nemzetbiztonsági szolgálatok a törvényes ellenőrzés során is drasztikusan növekvő mennyiségű – ráadásul eltérő kódolású és más protokoll szerint átvitt – adatot kell, hogy feldolgozzanak. Az ehhez szükséges erőforrások, azaz mind a humán erőforrás, mind a technikai eszközrendszer kialakítása, fenntartása (finanszírozás, elhelyezés, képzés, karbantartás stb.) kihívások elé állítja a szolgálatokat.

- Titkosítások:

A mai infokommunikációs eszközök, hálózatok segítségével gyorsan, egyszerűen és olcsón tudunk kommunikálni, vagy adatainkat felhő alapú rendszerekben tárolni. A „biztonságosan" jelző azonban hiányzik a fenti felsorolásból – nem véletlenül. Ez ugyanis az egyik legnagyobb problémája ezeknek a – sokszor ingyenesen használható – rendszereknek. Egyrészt a szolgáltatók is felismerték ezt és egyre többen tesznek lépéseket a megoldás érdekében, pl. a HTTPS protokoll bevezetésével.[25] Másrészt az interneten számtalan olcsón – vagy adott esetben sokszor ingyenesen – elérhető titkosító alkalmazás áll a felhasználók rendelkezésére (pl. HTTPS Everywhere).[26] Ezek ugyanakkor jelentősen megnehezítik (megnehezíthetik), vagy adott esetben el is lehetetleníthetik a nemzetbiztonsági szolgálatok hozzáférését is a törvényes ellenőrzés kapcsán megszerzendő adatokhoz.

- Anonimitás:

Az Internet, és az azt használó információcserét, adattárolást stb. lehetővé tevő rendszerek, alkalmazások jelentős része lehetővé teszi a teljesen anonim, vagy korlátozott felhasználói adatok megadásával (azok valóságtartalmának vizsgálata nélkül) történő használatot (pl. új email, Skype fiók létrehozása, fórumokon való hozzászólás stb.). Ez pedig, kombinálva a – következő pontban megjelenő – többfajta eszköz és szolgáltatás párhuzamos használatával, jelentősen megnehezíti egy adott célszemély teljes, elektronikus úton folytatott kommunikációjának elfogását, sőt már magának a használónak az azonosítását, vagy adott kommunikációk egy személyhez rendelését.

- Több eszköz, szolgáltatás párhuzamos használata:

Ma már az átlagos felhasználó, így a törvényes ellenőrzés célszemélyei is több fajta infokommunikációs eszközt (pl. asztali és hordozható számítógépek, okostelefonok, táblagépek stb.), sokfajta szolgáltatást (pl. mobiltelefónia, Skype,

---

[25] PEREZ, Juan Carlos: Google tightens HTTPS protections in Gmail in light of government snooping. 2014. 03. 20. http://www.pcworld.com/article/2110480/google-tightens-https-protections-in-gmail-in-light-of-government-snooping.html. Letöltés ideje: 2015. 12. 28.

[26] WAWRO, Alex: A simple guide to Deep Packet Inspection. 2012. 02. 01. http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/. Letöltés ideje: 2013. 06. 28.

Viber stb.) és többfajta internetelérést (pl. mobilnet, vezetékes net, internetkávézó, nyílt WIFI hálózatok stb.) használnak, használhatnak egymással párhuzamosan. Figyelembe véve a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II." című, már hivatkozott cikkekben leírt ellenőrzési technológiák korlátait, ez azt jelenti, hogy az arra feljogosított szolgálatoknak egyszerre több technológiát is alkalmazni kell a teljes körű adatszerzés érdekében, az egyes technológiákkal megszerzett információkat pedig össze kell futtatniuk.

Az összadatforrású felderítés jelentősége az alkalmazásszolgáltatók törvényes ellenőrzésében

A fentiek alapján megállapítható, hogy a technikai fejlődés, a kommunikációs szokások változása, az informatikai és hírközlő rendszerek összeolvadása és az ezekből következő törvényes ellenőrzési metódusok konvergenciája komplex problémákat vetnek fel a törvényes ellenőrzésre feljogosított szervezetek számára.

A rádióelektronikai felderítésből származó információkra jelentős mértékben támaszkodó katonai felderítés/hírszerzés is szembesült a kommunikációs formák változásából adódó problémákkal. A kis valószínűséggel felderíthető rádióadások, az IP-alapú kommunikáció, valamint a titkosítások fejlődése, terjedése a kommunikáció tartalmához való hozzáférést jelentősen megnehezítette, sokszor ellehetetlenítette. Éppen ezért megnőtt az egyéb kísérő-, vagy metaadatok, valamint más forrásokból származó információk megszerzésének és feldolgozásának a jelentősége. Miután a döntésekhez szükséges információkat ma már nem lehet egyetlen forrásból megszerezni, ráadásul különböző forrásokból származó, nagy tömegű adatot kell feldolgozni és más, már meglévő adatokkal korreláltatni, ezért kialakultak az ezt biztosító összadatforrású felderítő rendszerek, amelyek alapját a fúziós adatfeldolgozás adja.[27,28]

Az összadatforrású felderítés fogalmának tisztázásakor Kovács László[29] a következőket írja: *„Az összadatforrású felderítés azt jelenti, hogy úgy végzünk felderítési tevékenységet, hogy abban szerepet kap minden elérhető felderítő szerv és szervezet." „Ez lehetővé teszi, hogy az összes rendelkezésre álló és a lehető legszélesebb körben elérhető adatszerző forrásokat használjuk, illetve szintén*

---

[27] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: Elektronikai hadviselés. Budapest. Nemzeti Közszolgálati Egyetem, 2014. ISBN 978-615-5305-87-0

[28] Balogh Péter: As elektronikai támogatás és a SIGINT helyzete a Magyar Honvédségben. Felderítő Szemle, XII. évfolyam. 1. szám, 2013. szeptember-október, pp.: 58-99. ISSN 1588-242X.

[29] Kovács László: Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben. Doktori (PhD) értekezés. ZMNE, Budapest, 2003.

lehetővé válik, hogy egy célobjektumról ezek alapján a lehető legtöbb forrásból szerezzünk adatot."[30]

A fúziós adatfeldolgozást pedig a következőképpen határozza meg: *„a fúziós adatfeldolgozás a beérkezett adatokat összegyűjti, egymással a valamilyen rendező elv alapján összetartozó adatokat összehasonlítja, azokat korreláltatja, ezek eredményeit összegzi, majd a beérkező adatoknál magasabb szintű – értékesebb – adatot, adatok sorozatát, azaz információt állít elő. A fúziós adatfeldolgozás célja tehát: a különböző forrásokból származó, különböző formátumban rendelkezésre álló adatokból – a döntés előkészítésben meghatározó jelentőségű – megbízható információt állítson elő."* [31]

Jelen cikkben korábban, valamint a „Felhő alapú rendszerek törvényes ellenőrzési problémái"[32] és a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II." című cikkekben leírtak alapján elmondható, hogy ma célszemélyeik kibertérben történő tevékenységének lehető legteljesebb megismerése, és így az alkalmazásszolgáltatók törvényes ellenőrzése kapcsán az arra feljogosított szervezeteknek a hatékony feladatellátás érdekében hasonló, összadatforrású felderítést és fúziós adatfeldolgozást kell alkalmazniuk. Csupán egyetlen adatszerző módszer, eszköz alkalmazása az esetek döntő többségében nem hoz, nem hozhat megfelelő eredmény. Természetesen mind az adatszerző szervek, szenzorok, mind pedig a fúziós adatfeldolgozás tartalmi elemei mások, mint a katonai felderítés esetében, azonban a fő logikai eljárásrend mindkét esetben azonos.

Az alkalmazásszolgáltatók törvényes ellenőrzése kapcsán említett problémák, azaz a növekvő adatmennyiség, a titkosítások, az anonimitás, több eszköz, szolgáltatás párhuzamos használata, valamint a fent említett cikkekben leírt, az alkalmazásszolgáltatók együttműködési kötelezettségét előíró jogszabályok hiányosságai, és emiatt azok együttműködési hajlandóságára való utaltság miatt még több eszköz, módszer egyidejű alkalmazása esetén sem garantálható, hogy az arra feljogosított szolgálatok minden, számukra releváns információhoz hozzá tudnak jutni. Éppen ezért a célszemélyek tevékenységének teljes körű hatékony felderítéséhez – ekkor már beleértve a kibertérben végzett és azon kívülit is – minden más felderítő forrás (pl. helyiségellenőrzés, figyelés, OSINT) alkalmazása és bekapcsolása is szükséges. Ennek elemzése azonban túlmutat jelen cikk keretein és célkitűzésein.

Ugyanakkor, bár teljes siker nem garantálható az alkalmazásszolgáltatók ellenőrzése kapcsán leírt módszerekkel, azok – az esetek többségében ráadásul egyszerre több módszer egyidejű – használata mégis szükséges és megkerülhe-

---

[30] *Uo. p. 85.*

[31] *Uo. p. 78.*

[32] *Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. 2013. március, Hadmérnök, VIII. Évfolyam 1. szám. pp. 233 – 241. ISSN 1788-1919.*

tetlen. Ennek az oka pedig az, hogy az így megszerzett adatokhoz más forrásokból nem, vagy csak irreálisan magas költség-, és kockázati tényezők mellett lehetne hozzájutni. Így tehát megkerülhetetlen a több adatforrásra és a fúziós adatfeldolgozásra támaszkodó felderítés is. A több adatforrást használó felderítés és a fúziós adatfeldolgozás kibertérben történő, technikai hírszerzést folytató titkosszolgálatok általi alkalmazásáról a Snowden-ügy[33] kapcsán megjelent hírekből[34] is lehetett következtetni.

Az NSA[35] Prism programjáról nyilvánosságra került adatok szerint az Egyesült Államokban technikai hírszerzésben központi szerepet játszó ügynökség – szolgáltatónként változó formában és mélységben – hozzáfért a vezető internetes alkalmazásszolgáltatók (Skype, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, YouTube, Apple) rendszerein tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.). (1. ábra)

[33] Edward Joseph SNOWDEN, az NSA volt alkalmazottja rengeteg, közöttük minősített iratokat csempészett ki az Ügynökségtől, amelyeket különböző újságokban nyilvánossá tett. Így derült fény az Egyesült Államok nagyszabású, a kibertér teljes ellenőrzését, az ott folyó kommunikáció totális lehallgatását célzó projektjeire (pl. PRISM), valamint arra, hogy az Egyesült Államok világszerte széles körben, szűrő-kutató és készletező adatgyűjtő jelleggel monitorozta az emberek Internetes tevékenységét és hallgatta le mobiltelefonjait. Forrás: (MACASKILL, Ewen – DANCE, Gabriel: NSA Files: Decoded. 2013. 11. 01. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Letöltés ideje: 2014. 02. 17.)

[34] MACASKILL, Ewen – DANCE, Gabriel: NSA Files: Decoded. 2013. 11. 01. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Letöltés ideje: 2014. 02. 17.

[35] NSA (National Security Agency – Nemzetbiztonsági Ügynökség)

1. ábra. A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok.[36] (fordította: szerző)

Az így megszerzett adatokat megosztotta többek között az FBI-jal[37] és az angol GCHQ-val[38,39], valamint – hasonlóan az ECHELON[40] projekthez – feltételezhetően az ún. „Öt Szem", azaz az Egyesült Államok, Egyesült Királyság, Kanada, Ausztrália, Új-Zéland más ügynökségeivel is. Sőt adott esetben más országok (pl. a német BND) szervezeteivel is.[41] Ezek a szervezetek pedig ezt az egyik – jelen-

---

[36] Forrás: (NSA slides explain the PRISM data-collection program. washingtonpost.com. 2013. 06. 06. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Letöltés ideje: 2013. 06 28.)

[37] FBI (Federal Bureau of Investigation – Szövetségi Nyomozó Iroda)

[38] GCHQ (UK Government Communications Headquarters – Kormányzati Kommunikációs Központ)

[39] POITRAS, Laura – GELLMAN, Barton: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. 2013. 06. 07. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Letöltés ideje: 2013. 06. 28.

[40] ECHELON: Az „Öt Szem" által működtetett, globális rádiófelderítő és lehallgató rendszer, amely segítségével telefon, fax, email, Internet forgalmakat hallgathatnak le.

[41] BAUMGÄRTNER, Maik - BLOME, Nikolaus - GUDE, Hubert - ROSENBACH, Marcel - SCHINDLER, Jörg - SCHMID, Fidelius: Spying Close to Home: German Intelligence Under Fire for NSA Cooperation. 2015. 04. 24. http://www.spiegel.de/international/germany/german-

tős – adatforrásként kezelték, összefuttatva az innen származó eredményeket saját adataikkal.

Ezt mutatja az is, hogy maga az NSA is több adatforrásból dolgozott. Az alkalmazásszolgáltatók bekapcsolása ugyanis azok nagy száma, más országokbeli honossága stb. miatt nem lehet teljes körű. Éppen ezért alkalmazzák az említett országok szolgálatai további információszerzésre az ún. mély csomagelemzés (DPI)[42] módszerét. Ennek lényege, hogy adott helyen átfolyó adatforgalom minden csomagjának a tartalmát vizsgálat alá veszik. Ez a hozzáférés azonban meglehetősen korlátozott, hiszen bár a nyíltan küldött adatok könnyen ellenőrizhetők, feldolgozhatók, a titkosított forgalmak esetében a titkosítást fel kell törni, ami időben hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat.[43] E korlátok ellenére az angol GCHQ ezt a módszert használja „TEMPORA" nevű, a „PRISM"-hez hasonlóan nagyszabású, ám technikailag más alapokon nyugvó ellenőrző programjához. Itt – a kiszivárgott adatok szerint – 200 darab, egyenként 10 Gb/s adatátviteli sebességű optikai kábelen (ezek közül egy időben legalább 46-on) átfolyó összes információt kicsatolják és feldolgozzák a 2007 elején elindított „Mastering the Internet" projekt keretében. A programban öt ország (USA, UK, Kanada, Új Zéland és Ausztrália) titkosszolgálati szervei dolgoznak együtt és osztják meg egymás között az információkat – a kinyert tartalmat és a kísérő un. metaadatokat egyaránt.[44,45] Az NSA hasonló, „Upstream" fedőnevű tevékenységét a 2. ábra szemlélteti, amelyből jól látszik, hogy a Prism csak egy része az NSA, és így az USA lehallgató rendszerének.

intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html. Letöltés ideje: 2016. 01. 02.

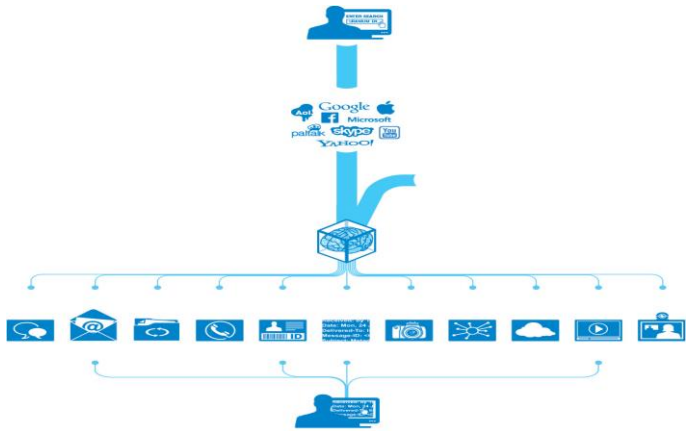
[42] DPI: Deep Packet Inspection mély csomag elemzés

[43] KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 184 – 197. ISSN 1788-1919.

[44] MACASKILL, Ewen – BORGER, Julian – HOPKINS, Nick – DAVIES, Nick – BALL, James: GCHQ taps fibre-optic cables for secret access to world's communications. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Letöltés ideje: 2013. 07. 05.

[45] MACASKILL, Ewen – BORGER, Julian – HOPKINS, Nick – DAVIES, Nick – BALL, James: Mastering the internet: how GCHQ set out to spy on the world wide web. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Letöltés ideje: 2013. 07. 05.

2. ábra. Az Upstream és a Prism program viszonya, felhasználhatósága.[46] *(fordította: szerző)*



3. ábra A PRISM program működése[47]

[46] *Forrás: NSA slides explain the PRISM data-collection program. washingtonpost.com. 2013. 06. 06. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Letöltés ideje: 2013. 06 28.*

[47] *Forrás: (GELLMAN, Barton - LINDEMAN, Todd: Inner workings of a top-secret spy program. 2013. 06. 29. https://www.washingtonpost.com/apps/g/page/national/inner-workings-of-a-top-secret-spy-program/282/. Letöltés ideje: 2013. 09. 15.)*

A több adatforrásra támaszkodást mutatja be a 3. ábra is, ahol a korábban jelzett alkalmazásszolgáltatók mellett egy másik vastag kék vonal jelzi az egyéb forrásokból származó információk becsatolását. Ugyanakkor ezen ábrán a kockába foglalt agy szimbolizálja a fúziós adatfeldolgozást, amelynek eredményeképpen megjelennek az egy célszemélyhez, célobjektumhoz tartozó különböző típusú tartalmak, információk, adatok.

A hazai megvalósítás lehetősége

A fenti leírásból és ábrákból is jól látszik a több adatforrásra támaszkodó felderítés és az adatok összefuttatásának jelentősége. Ugyanakkor azt is érdemes kiemelni, hogy még az olyan, a titkosszolgálatok tevékenységére óriási erőforrásokat biztosító országok, mint az Egyesült Államok[48] és az Egyesült Királyság[49] is alapvetően koncentráltan hozta létre az ellenőrzéshez szükséges kapacitásokat. Az előbbi esetében ez az NSA-nál, az utóbbi esetében pedig a GCHQ-nál jött létre.

A koncentrált kapacitások kialakításának több oka is van. Az egyik alapvetően költségvetési. Egy ellenőrző rendszer kiépítése, fenntartása, a megfelelő szakemberek fizetése, továbbképzése stb. óriási összegeket emészt fel. A „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II." című cikkekben leírt aktív ellenőrző eszközök, vagy közismertebb nevükön kémprogramok – az ott leírt korlátokkal – is alkalmasak célszemélyek kibertérben végzett tevékenységének, így az általa igénybe vett és az alkalmazásszolgáltatók által biztosított szolgáltatások kapcsán keletkező információk, adatok, kommunikáció stb. ellenőrzésére. Az ellenőrző rendszerek árát jól szemlélteteti a WikiLeaks által közzétett, nem nemzetbiztonsági szolgálatnak, hanem a New York County District Attorney Office[50]-nak szóló árajánlat, amely az olasz Hacking Team által gyártott, kifejezetten kormányzati szereplőknek értékesített kémprogram 10 célszemély egyidejű ellenőrzését lehetővé tevő rendszerre szól. Ennek a végösszege 1 142 000 USD, amelyből 760 000 USD maga az eszközrendszer, a többi pedig

[48] Egyes források szerint az NSA éves költségvetése 10 milliárd USD körül alakul 2011 és 2017 között. (Budget of the U.S. National Security Agency in line with the U.S. National Intelligence Program for fiscal years 2011 to 2017 (in billion U.S. dollars). http://www.statista.com/statistics/283545/budget-of-the-us-national-security-agency/. Letöltés ideje: 2016. 01. 02.)

[49] Az Egyesült Királyság titkosszolgálatainak (MI5, MI6, GCHQ éves költségvetése 1,9 milliárd Font körül alakult 2012-ben. (Winnett, Robert: Spy agencies win millions more to fight terror threat. 2013. 06. 25. http://www.telegraph.co.uk/news/politics/spending-review/10142443/Spy-agencies-win-millions-more-to-fight-terror-threat.html. Letöltés ideje: 2016. 01. 02.)

[50] New York County District Attorney Office, azaz New York Megyei Ügyészi Hivatal.

egyéb szolgáltatások (pl képzés, éves támogatás stb.).[51] És ez csupán 10 célszemély egyidejű ellenőrzését biztosítja!

A másik szempont technikai jellegű. Jelenleg ugyanis az alkalmazásszolgáltatók által nyújtott szolgáltatások és az általuk használt technológiák is rendkívül heterogének és nincsenek kiforrott, a törvényes ellenőrzést biztosító eszközrendszerek. Amíg a hagyományos hírközlés ellenőrzésénél a jól ismert törvényi és technikai háttér okán teljes értékű technikai megoldásokat kínálnak az erre szakosodott gyártók, addig az alkalmazásszolgáltatók által nyújtott, internettechnológiára épülő szolgáltatások ellenőrzésére elsősorban egyedi problémákat megoldó eszközöket tudnak csak szállítani. Ez pedig drágává, bonyolulttá és esetivé teszi az ellenőrzéseket.

A harmadik ok, a törvényes ellenőrzésben az alkalmazásszolgáltatók kötelezettségeihez kapcsolódik, ezen belül is elsősorban az együttműködést előíró jogszabályok hiányához. Jelenleg nincs ugyanis olyan szabályozás, amely európai szinten irányadó lenne a kérdésben és amely rövid időn belül, nagyobb szolgáltatói ellenállás nélkül átemelhető lenne a magyar törvényekbe. Ez pedig két gondot okoz. Az első, hogy az alkalmazásszolgáltatók hajlandóságán múlik, hogy engedi-e ellenőrző eszköz telepítését, esetleg saját eszközeivel biztosítja a törvényes ellenőrzést a szolgálatok számára, vagy teljesen elutasítja az együttműködést. Ez utóbbira – sajnos negatív – példa a Google esete, aki az európai, és így hazánk törvényben felhatalmazott rendvédelmi és nemzetbiztonsági szolgálataival nem, hogy nem működik együtt, de átláthatósági jelentéseiben még közzé is teszi, hogy melyik országból hány adatszolgáltatási kérést kapott és abból menynyit, milyen minőségben teljesített. A cég Magyarországnak annak ellenére sem szolgáltatott információkat, hogy az azokra vonatkozó kérések teljes mértékben kielégítették a hazánkban jelenleg hatályos törvényi feltételeket.[52]

A fent leírtak alapján az alkalmazásszolgáltatók törvényes ellenőrzését hazánkban koncentráltan célszerű kialakítani. Ennek több feltétele is adott.

Az első – és talán legfontosabb – a feladatot ellátó megfelelő szervezet megtalálása. Ma Magyarországon a Nemzetbiztonsági Szakszolgálat (NBSZ) az, amely a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. (továbbiakban: Nbtv.) alapján

---

[51] *Hacking Team - Remote Control System - Budgetary Proposal. 2015. 04. 14. https://www.documentcloud.org/documents/2157711-dany-galilelo-budgetary-proposal-150414.html. Letöltés ideje: 2016. 01. 02.*

[52] *DAJKÓ Pál: A Google továbbra sem ad ki adatokat a magyar kormánynak 2013. 01. 24. http://itcafe.hu/hir/google_atlathatosag_transparency.html. Letöltés ideje: 2013. 02. 09. 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. http://www.complex.hu /jr/gen/hjegy_doc.cgi?docid=99500125.TV. Letöltés ideje: 2013. 07. 01.*

*„**8. §** (1) A Nemzetbiztonsági Szakszolgálat*
a) a jogszabályok keretei között a titkos információgyűjtés, illetve a titkos adatszerzés eszközeivel és módszereivel - írásbeli megkeresésre - szolgáltatást végez a titkos információgyűjtésre, illetve a titkos adatszerzésre feljogosított szervek titkos információgyűjtő, valamint titkos adatszerző tevékenységéhez,”.

Az NBSZ tehát már ma is ilyen módon nyújt szolgáltatást a többi szolgálat számára, így tehát Magyarországon mind a szervezeti, mind a szervezet ilyen irányú működésének jogi feltételei megvannak egy, a cikkben leírt koncentrált ellenőrző rendszer kialakítására.

A második, hogy az elektronikus hírközlési hálózatokon folytatott kommunikáció tartalmának megismerése kapcsán már most is kizárólagosság áll fenn, hiszen az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről szóló 180/2004. (V. 26.) Korm. rendelet alapján
*„**6. §** (1) Amennyiben az elektronikus hírközlő hálózaton folytatott kommunikáció tartalma és a kísérőadatok megismeréséhez az igazságügyért felelős miniszter vagy bíró engedélye szükséges, a titkos információgyűjtésre felhatalmazott szervezetek igényeinek kielégítését - külön törvényben meghatározott feltételek mellett - az NBSZ látja el.”*

Ez a koncentráltság tehát amellett, hogy – elektronikus hírközlő rendszerek esetében – már ma is létezik, egyrészt hatékonyan működik, másrészt a nemzetbiztonsági szolgálatok, a rendvédelmi szervek, de az ügyészségi és bírósági oldalról is megvan a teljes elfogadottsága.

A harmadikként pedig az NBSZ-nél meglévő feltételek emelendők ki. Ilyen a tapasztalatok a kapcsolattartásban, valamint az ennek nyomán a szolgáltatók részéről kialakult bizalom, amelyek elengedhetetlenek a hatékony feladatellátáshoz, de ide sorolható, hogy a szolgálatnál a megfelelő technikai ismeret és háttér, valamint szakembergárda is rendelkezésre áll az ellenőrzéshez szükséges komplex feladatok teljes spektrumának elvégzéséhez.

Az előzőekben felsorolt, meglévő feltételek mellett, az alkalmazásszolgáltatók törvényes ellenőrzésének koncentrált kialakítása több lehetőséget, előnyt is biztosíthat Magyarország számára.

Az első, hogy egy ilyen, egykapus rendszer, a szolgáltatók számára is egyszerűbb, átláthatóbb, ráadásul olcsóbb módját biztosítja a tőlük elvárt, és remélhetőleg a későbbiekben törvényben is szabályozottan megjelenő ellenőrzési kötelezettségek ellátásának. Ráadásul a szolgáltató és az ellenőrzést végzők között is ebben az esetben könnyebb a bizalmat kiépíteni és megtartani, mintha minden érintett szolgálat külön-külön fordulna a szolgáltatókhoz.

A második előny, hogy a koncentrált kapacitásokat igénybevevő szolgálatoknak is egyszerűbb a feladat végrehajtása, hiszen nem kell a szolgáltatókkal mű-

szaki egyeztetéseket folytatniuk, az ellenőrzéshez szükséges technikai rendszert kiépíteniük, a megfelelő szakembergárdát felvenniük és fenntartaniuk, ráadásul a technikai fejlődés követése, az ellenőrző rendszerek továbbfejlesztése is egyszerűbb, olcsóbb ily módon a számukra. Mindezek mellett még az ellenőrzési igényeik is fedettebben jelennek meg, hiszen Magyarország esetében a Nemzetbiztonsági Szakszolgálat a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára egyaránt végez törvényes ellenőrzési tevékenységet, így adott esetben a szolgáltató számára nem derül ki, hogy az adott célszemélyt melyik szervezet ellenőrzi. Ennek azért is van nagy jelentősége, mert az alkalmazásszolgáltatók szinte mindegyike külföldi székhelyű, és az érzékeny, sőt adott esetben minősített adatok kezelését, az azokhoz hozzáférő személyeket jelenleg nem, vagy csak adminisztratív úton, egyedi szerződésekkel lehet kontrollálni.

Harmadik előnyként említhető, hogy koncentrált ellenőrző kapacitások esetében, egyazon célszemély, egy időben, több szolgálat általi ellenőrzése során nem kell többször ugyanazt az adatot megszerezni, ahhoz az érintett szolgálatok egyformán hozzájutnak. Ennek a hírközlési szolgáltatók kizárólagos ellenőrzése kapcsán a Nemzetbiztonsági Szakszolgálatnál már kialakult, mindenki által elfogadott, jól működő és kellően szabályozott módszere létezik.

Negyedik, de talán legjelentősebb előnynek az mondható, hogy koncentrált kiépítés esetén a teljes rendszer kialakítása, fenntartása és hosszabb távon a külső infokommunikációs környezetre reagáló folyamatos fejlesztése olcsóbb Magyarországnak, mintha azokat az egyes szolgálatok külön-külön hoznák létre. Ráadásul egyes többletfunkció kiépítésének költséghatékonysága is jobb, mint egyedi ellenőrző rendszerek esetében, arról nem is beszélve, hogy így azon szervezetek is hozzájuthatnak minden információhoz, és funkcióhoz, akiknek az anyagi lehetőségeik önállóan ezt nem tették volna lehetővé.

Ötödik előnyként nevezhető meg, hogy koncentrált ellenőrző rendszer kiépítése kapcsán több ellenőrző módszer egyidejű alkalmazása is egyszerűbben, olcsóbban lehetséges, így az azokból, azaz több adatforrásból befutó adatok feldolgozása, összefuttatása, fúziós feldolgozása is megoldható. Márpedig ezekre, a technológiai és a törvényes ellenőrzés konvergenciája kapcsán a cikkben feltárt okok miatt, a hatékony ellenőrzés érdekében szükség van.

Összefoglalás és következtetések

A cikk bemutatta az internet és az azt kihasználó alkalmazások fejlődésével változó és ugrásszerűen bővülő internet-technológiára épülő szolgáltatások, ezen belül is kiemelten a kommunikációs formák, lehetőségek, valamint az ezek kapcsán kialakult technológiai konvergencia hatásait az alkalmazásszolgáltatók törvényes ellenőrzésére. Következtetésként megállapítható, hogy

1. Az információs és kommunikációs technológiák konvergenciája mellett a törvényes ellenőrzési metódusok konvergenciája is megfigyelhető.

2. Ez a két folyamat, valamint az alkalmazásszolgáltatók törvényes ellenőrzésének hiányos jogszabályi háttere új kihívások elé állítja az ellenőrzésre jogosult szolgálatokat.
3. A napjainkban rendelkezésre álló eszközök és módszerek, valamint a jelenleg hatályos jogszabályi háttér mellett, a hatékonyabb ellenőrzés kialakításához, új, több adatforrást alkalmazó felderítés és az így keletkező adatok fúziós feldolgozása szükséges.
4. Ezt – figyelembe véve a külföldi példákat is – koncentrált kapacitások kialakításával lehet hatékonyan megteremteni.
5. Ehhez ma Magyarországon adottak a feltételek.

A cikk a belőle levonható következtetésekkel együtt is alapvetően problémafelvető és nem problémamegoldó céllal készült. Ahhoz, hogy a felvetett problémákat – a helyükön – kezelni lehessen további feladatokat, vizsgálatokat kell végrehajtani. Mindenekelőtt szükséges a jogi háttér rendezése, vagy legalábbis a törekvés rá. Ugyanis, amint azt a „Felhő alapú rendszerek törvényes ellenőrzési problémái”[53], valamint a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II.” című cikkek bemutatták, az alkalmazásszolgáltatóval való együttműködés az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési forma, így ez kikerülhetetlen, ugyanakkor ennek jogi szabályozottságában lelhető fel a legtöbb hiány. Mindemellett a koncentráltság erősítéseként – a hírközlési és postai szolgáltatók kizárólagos ellenőrzéséhez[54,55] hasonlóan – a kizárólagosság jogszabályban rögzítését is meg kell fontolni. Másodszor meg kell vizsgálni a koncentráltan kialakítandó, több adatforrást alkalmazó felderítés és az így keletkező adatok összefuttatását, korreláltatását is biztosító fúziós feldolgozás technikai lehetőségeit. Mindezt úgy, hogy számba kell venni a lehetséges új, eddig nem

[53] *KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. 2013. március, Hadmérnök, VIII. Évfolyam 1. szám. pp. 233 – 241. ISSN 1788-1919.*

[54] *180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400180.KOR. [1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV. Letöltés ideje: 2016. 01. 04.]*

[55] *9/2005. (I. 19.) Korm. rendelet a postai szolgáltatók, a postai közreműködők és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének részletes szabályairól. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500009.KOR. 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV. Letöltés ideje: 2016.. 01. 05.*

ellenőrzött adatokat, adatforrásokat, különös tekintettel a kísérő és egyéb metaadatokra.

Felhasznált irodalom

- BALOGH Péter: As elektronikai támogatás és a SIGINT helyzete a Magyar Honvédségben. Felderítő Szemle, XII. évfolyam. 1. szám, 2013. szeptember-október, pp.: 58-99. ISSN 1588-242X.
- BAUMGÄRTNER, Maik - BLOME, Nikolaus - GUDE, Hubert - ROSENBACH, Marcel - SCHINDLER, Jörg - SCHMID, Fidelius: Spying Close to Home: German Intelligence Under Fire for NSA Cooperation. 2015. 04. 24. http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html. Letöltés ideje: 2016. 01. 02.
- BARTOLITS István: A 21. század hírközlési trendjei, A SIGINT a XXI. század kihívásainak tükrében. Felderítő Szemle, VI. évfolyam. 2007. február pp.: 49-61. ISSN 1588-242X.
- DAJKÓ Pál: A Google továbbra sem ad ki adatokat a magyar kormánynak 2013. 01. 24. http://itcafe.hu/hir/google_atlathatosag_transparency.html. Letöltés ideje: 2013. 02. 09.
- DOBÁK Imre - KOVÁCS Zoltán: Új technológiák hatása a hírszerzésre. In: A nemzetbiztonság általános elmélete. Szerk.: Dobák Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2014. pp. 206-220. ISBN: 978-615-5305-49-8
- GELLMAN, Barton - LINDEMAN, Todd: Inner workings of a top-secret spy program. 2013. 06. 29. https://www.washingtonpost.com/apps/g/page/national/inner-workings-of-a-top-secret-spy-program/282/. Letöltés ideje: 2013. 09. 15.
- HAIG Zsolt – KOVÁCS László – VÁNYA László – VASS Sándor: Elektronikai hadviselés. Budapest. Nemzeti Közszolgálati Egyetem, 2014. ISBN 978-615-5305-87-0
- HAIG Zsolt – KOVÁCS László – MUNK Sándor – VÁNYA László: Az infokommunikációs technológia hatása a hadtudományokra. Budapest : Nemzeti Közszolgálati Egyetem, 2013. ISBN 978-615-5305-02-3.
- HAIG Zsolt: Információ - társadalom - biztonság. Budapest. NKE Szolgáltató Kft., 2015. ISBN 978-615-5527-08-1
- KOVÁCS László: Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben. Doktori (PhD) értekezés. ZMNE, Budapest, 2003.
- KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. 2013. március, Hadmérnök, VIII. Évfolyam 1. szám. pp. 233 – 241. ISSN 1788-1919.

- KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 184 – 197. ISSN 1788-1919.
- KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 198 – 210. ISSN 1788-1919.
- KOVÁCS Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-375
- POITRAS, Laura – GELLMAN, Barton: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. 2013. 06. 07. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Letöltés ideje: 2013. 06. 28.
- MACASKILL, Ewen – BORGER, Julian – HOPKINS, Nick – DAVIES, Nick – BALL, James: GCHQ taps fibre-optic cables for secret access to world's communications. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Letöltés ideje: 2013. 07. 05.
- MACASKILL, Ewen – DANCE, Gabriel: NSA Files: Decoded. 2013. 11. 01. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Letöltés ideje: 2014. 02. 17.
- MACASKILL, Ewen – BORGER, Julian – HOPKINS, Nick – DAVIES, Nick – BALL, James: Mastering the internet: how GCHQ set out to spy on the world wide web. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Letöltés ideje: 2013. 07. 05.
- MUNK, Sándor: A kommunikáció fogalomrendszerének keretei az integrálódó információs technológiák korában. In: Kommunikáció 2009. Budapest. ZMNE, 2009. pp. 51-64. ISBN 978-963-7060-70-0
- PEREZ, Juan Carlos: Google tightens HTTPS protections in Gmail in light of government snooping. 2014. 03. 20. http://www.pcworld.com/article/2110480/google-tightens-https-protections-in-gmail-in-light-of-government-snooping.html. Letöltés ideje: 2015. 12. 28.
- SALLAI Gyula – ABOS Imre: A távközlés, információ- és médiatechnológia konvergenciája. Magyar Tudomány. Infokommunikációs hálózatok. 168. Évfolyam. 2007. július pp. 844-851. ISSN 1588-1245
- SALLAI Gyula: Defining Infocommunications and Related. Acta Polytechnica Hungarica. 9. Évfolyam 6. szám – 2012. pp. 5-15. ISSN 1785-8860
- WAWRO, Alex: A simple guide to Deep Packet Inspection. 2012. 02. 01. http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/. Letöltés ideje: 2013. 06. 28.

- WINNETT, Robert: Spy agencies win millions more to fight terror threat. 2013. 06. 25. http://www.telegraph.co.uk/news/politics/spending-review/10142443/Spy-agencies-win-millions-more-to-fight-terror-threat.html. Letöltés ideje: 2016. 01. 02.

Egyéb források:

- Hacking Team - Remote Control System - Budgetary Proposal. 2015. 04. 14. https://www.documentcloud.org/documents/2157711-dany-galilelo-budgetary-proposal-150414.html. Letöltés ideje: 2016. 01. 02.
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV. Letöltés ideje: 2013. 07. 01.
- 180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400180.KOR. Letöltés ideje: 2016. 01. 04.]
- 9/2005. (I. 19.) Korm. rendelet a postai szolgáltatók, a postai közreműködők és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének részletes szabályairól. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500009.KOR
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV. Letöltés ideje: 2016.. 01. 05.
- NSA slides explain the PRISM data-collection program. washingtonpost.com. 2013. 06. 06. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Letöltés ideje: 2013. 06 28.
- Budget of the U.S. National Security Agency in line with the U.S. National Intelligence Program for fiscal years 2011 to 2017 (in billion U.S. dollars). http://www.statista.com/statistics/283545/budget-of-the-us-national-security-agency/. Letöltés ideje: 2016. 01. 02.
- https://www.otpbank.hu/portal/hu/OTPdirekt/Home. Letöltés ideje: 2013. 10. 27.
- https://www.paypal.com/hu/webapps/mpp/home Letöltés ideje: 2013. 10. 27.
- http://eu.battle.net/wow/en/. Letöltés ideje: 2013. 10. 27.
- http://office.microsoft.com/hu-hu/business/. Letöltés ideje: 2013. 10. 27.
- http://www.adobe.com/hu/products/photoshop.html. Letöltés ideje: 2013. 10. 27.
- dropbox.com. https://www.dropbox.com/. Letöltés ideje: 2014. 03. 14. https://maps.google.hu/maps?hl=hu&tab=wl. Letöltés ideje: 2013. 10. 27.