HADMÉRNÖK

XI. Évfolyam 4. szám - 2016. december

Kovács Zoltán
zkovacs.24@gmail.com

BIZTONSÁG VS. TÖRVÉNYES ELLENŐRZÉS AZ INTERNET ALAPÚ KOMMUNIKÁCIÓBAN - ELLENTÉTES VAGY EGYMÁSSAL MEGFÉRŐ KÖVETELMÉNYEK? II.

Absztrakt

A cikksorozat első része összefoglalta a kommunikáció változását, a változások hatását a szolgáltatói modellre és a törvényes ellenőrzésre. Rámutatott azokra a jogi hiányosságokra, problémákra, amelyek hatással vannak az internet alapú kommunikáció törvényes ellenőrzésének hatékony ellátására, majd nemzetközi kitekintéssel bemutatta az ellenőrzésére jelenleg rendelkezésre álló, jellemző technikai eszközöket és azok főbb tulajdonságait. A második rész rávilágított a hazánkban újonnan hatályba lépett jogszabályok adta lehetőségekre, pontosítva annak kereteit, valamint ismerteti, hogy milyen hatásai lehetnek a kommunikáció biztonságára.

The first part of this article series has summarized the changes of communication and the effects of these changes on the service-provider model and on the lawful monitoring. That article has pointed out the insufficiencies and problems of the current laws which affect the lawful monitoring of the internet-based communication, then described the currently and typically used possible technical solutions of lawful monitoring, and their major characteristics with an international view. The second part of this article series is highlighting the possibilities given by the Hungarian law that entered into force nowadays, on lawful monitoring of the application service providers, specifying its frames, and describing its effects on the security and privacy of communication.

Kulcsszavak: *hírközlés, kommunikáció, alkalmazásszolgáltató, törvényes ellenőrzés ~ electronic communication, communication, application service provider, lawful monitoring*

BEVEZETÉS

A cikksorozat első része, elsősorban a „Felhő alapú rendszerek törvényes ellenőrzési problémái”, a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. – II.”, valamint az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből” című cikkek alapján összefoglalta a kommunikáció, és ezáltal a szolgáltatói modell változását, bemutatta az internet alapú kommunikációs rendszerek törvényes ellenőrzésére alkalmazható jellemző módszereket, azok főbb előnyeit, hátrányait. Mindezt úgy, hogy erre alapozva bemutathatók legyenek a hazánkban 2016-ban elfogadott új szabályozás keretei és hatásai. Jelen cikk ezt teszi meg, megvizsgálva, hogy az új jogszabály milyen kötelezettségeket ró a felhasználókra, a gyártókra/fejlesztőkre, valamint az alkalmazásszolgáltatókra, bemutatja az általa biztosított jogi garanciákat, de körül járja a betarthatósággal kapcsolatos kérdéseket is.

A MAGYARORSZÁGI TV. SZABÁLYOZÁS ÉS ANNAK HATÁSAI

Az internet alapú szolgáltatások – ezek közül is kiemelten a kommunikációt lehetővé tevők – törvényes ellenőrzésében mérföldkőnek tekinthető a hazánkban 2016-ban hatályba lépett szabályozás. A terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény [1] ugyanis többek között módosította az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényt (Ekertv.). [2] Ennek keretében bevezette az alkalmazásszolgáltató fogalmát, definiálta a Magyarország területére irányuló szolgáltatásokat, valamint előírta a titkosított kommunikációt biztosító alkalmazásszolgáltatóknak, hogy megkeresés esetén tegyék lehetővé az erre feljogosított szervezetek számára a kommunikáció tartalmához és az annak kapcsán keletkező vagy kezelt meta adatokhoz való hozzáférést. Kötelezővé tette számukra továbbá a továbbított küldeményekkel, közlésekkel kapcsolatosan keletkező vagy kezelt meta adatok, azok keletkezésétől számított 1 éven át történő megőrzését is. Az ehhez szorosan kapcsolódó, a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Korm. rendelet [3] pedig rögzíti a szolgáltatók és a törvényes ellenőrzést végzők közötti együttműködésének részletszabályait.

A szabályozás keretei és hatásai

A sajtóban a jogszabályok kihirdetése előtt számos találgatás látott napvilágot, majd a kihirdetés után is lehetett olvasni kissé félreértelmezett interpretálásokat a szolgáltatók, de akár a felhasználók szerepéről, kötelezettségeiről, sőt az ellenőrzés kialakítása okán a kommunikáció biztonságának csökkenéséről is. Éppen ezért érdemes áttekinteni mire ad pontosan lehetőséget ez a szabályozás, mit tesz lehetővé és mit nem, valamint, hogy miben jelent előrelépést a korábbiakhoz képest.

Először is az említett szabályozás nem vonatkozik a titkosított kommunikáció felhasználóira, azaz irányukba semmilyen kötelezettséget vagy büntetést nem eszközöl. Másodszor pedig a titkosított kommunikáció kapcsán is csupán a szolgáltatókkal – és nem a gyártókkal, fejlesztőkkel vagy eladókkal (!) – foglalkozik, azaz azokra érvényes akik a kommunikáció felépítése és/vagy végrehajtása során érdemi tevékenységet látnak el. Így nem vonatkozik olyan gyártó és/vagy fejlesztő és/vagy értékesítő cégekre sem, akik csupán végpont-végpont titkosítást biztosító szoftver és/vagy hardver termékeket biztosítanak a felhasználók részére. Ez utóbbi esetben ugyanis mindkét kommunikáló félnek ugyanazt a titkosító eszközt kell alkalmaznia és ugyanazt – vagy legalábbis kompatibilis – harmadik fél

által nyújtott kommunikációs csatornát kell igénybe vennie, a tikosított kommunikáció kapcsán pedig nincs központi azonosítás, azaz így a kommunikáció kizárólag úgy tud megvalósulni, hogy a felek azt előre egymással egyeztették.

Ugyanakkor ez a szabályozás vonatkozik minden olyan kommunikációs szolgáltatóra, amelyik központilag biztosítja a titkosított kommunikáció lehetőségét minden oda beregisztrált felhasználó számára, a felhasználáshoz pedig megfelelő azonosítás szükséges.

A kötelezettség ilyetén történő meghatározásának a logikája megegyezik a jelenlegi hírközlési szolgáltatóknál alkalmazottal, amely előírja egyrészt a törvényes ellenőrzés biztosításának kötelezettségét, másrészt tiltja olyan új szolgáltatás bevezetését vagy a meglévők olyan átalakítását, amely azt ellehetetleníti, ugyanakkor engedi az egyedi, a felhasználó által alkalmazott végpont-végpont titkosítás használatát.

Ez az előírás viszont azt is jelenti, hogy azok a szolgáltatók, akik ma úgy nyújtanak titkosított kommunikációs szolgáltatást, hogy jelenleg nem biztosítják a kommunikáció tartalmához való hozzáférést, vagy át kell, hogy alakítsák működési struktúrájukat, vagy hazánkban nem nyújthatják szolgáltatásukat. Ez pedig amellett, hogy a hazánkban infrastruktúrával is jelenlévő hírközlési szolgáltatókkal e tekintetben versenyegyenlőséget teremt, lehetővé teszi a törvényes ellenőrzést az arra feljogosított szervek számára.

Érdemes ugyanakkor azt is megvizsgálni, hogy okozhatja-e ez a fajta új jogi szabályozás a kommunikáció biztonságának romlását a felhasználó szemszögéből. Ehhez először is elemezni kell az említett jogszabályok hatásait a kommunikációra biztonságára, majd ezeket össze kell vetni azoknak az egyéb technikai lehetőségeknek a hatásaival, amelyek adott esetben a törvényes ellenőrzést végzők rendelkezésére áll(hat)nak.

A szabályozás hatása a kommunikáció biztonságára

Tekintsük egy példát a klasszikus hírközlés világából. A rádiótelefonok hazai elterjedésekor az első telepített rendszer az NMT 450 volt. Ez a hangátvitelre titkosítás nélküli FM modulált jelet használt, [4] amely egy megfelelő vevő segítségével bárki által lehallgatható volt. Ilyen vevővel bármelyik rádióamatőr rendelkezhetett, de néhány tízezer forintnak megfelelő összegért ezeket bárki engedély nélkül megvásárolhatta, akár hazánkban is. Ehhez képes a mai GSM hálózatok ma már erős (jobbára A5.1 vagy A5.3) titkosítást alkalmaznak a levegőinterfész lehallgatás elleni védelmére. [5] Ezeket ma sokkal biztonságosabbnak tekintjük, mint a régi NMT rendszert, pedig azzal is tisztában vagyunk, hogy a GSM rendszerek esetében is biztosított a törvényes ellenőrzés lehetősége. Ez azt mutatja, hogy úgy lehetett növelni a kommunikáció biztonságát a felhasználó szempontjából, hogy ugyanakkor nem csorbult a törvényes ellenőrzéshez fűződő érdek sem.

Természetesen felmerülhet a kérdés, hogy a hazánkban bevezetett jogi szabályozásnak vannak-e negatív hatásai, azaz a felhasználó szemszögéből a kommunikáció továbbra is elég biztonságosnak tekinthető-e.

A felhő alapú rendszerek, így a kommunikációt (is) biztosítók esetében az egyik kiemelten kezelt probléma a szolgáltató kémkedése, valamint harmadik felek (pl. szolgáltató beszállítói, partnerei) hozzáférése a felhasználó adataihoz, [6] információihoz. Sőt, ennek a kérdésnek a vizsgálata kapcsán arra is külön is érdemes kitérni, hogy – az általában külföldi – felhőszolgáltató hogyan és melyik ország szervei számára biztosítja még az ellenőrzés lehetőségét. Nézzük meg például a Gmail esetét. A Gmail-t biztonságosnak tekintjük, hiszen már bejelentkezéstől erős SSL titkosítást használ, és több eszközt is biztosít (pl. ki mikor milyen IP címről, eszközről stb. fért hozzá utoljára a fiókunkhoz, figyelmeztető emailt küld, ha szokatlan bejelentkezést észlel pl. új mobil eszközről stb.), amellyel támogatja kommunikációnk biztonságát. [7] Ugyanakkor már a Google-al kötött szerződésben is szerepel, hogy hozzáfér leveleinkhez, azokat – persze csupán a szolgáltatás fejlesztése érdekében – elemzi és felhasználja. [8] Ráadásul a Snowden által közzétett anyagokból azt is

tudjuk, hogy 2009-ben a Google is csatlakozott az ún. „Prism” programhoz, amelynek keretében – több más szolgáltatóval, pl. Microsoft, Facebook, Apple stb.) együtt biztosították az Egyesült Államok szolgálatai részére a hozzáférést a rendszereiken tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.). [9] [10] Joggal merülhet fel akkor a kérdés: a felhasználó szemszögéből nézve ez így mennyire biztonságos szolgáltatás? De úgy is feltehetjük a kérdést: ront-e bármit is a biztonságon az, ha az arra illetékes hazai szolgálat egyértelmű és szigorúan betartott és betartatott törvényi előírásoknak megfelelően fér hozzá az általa jogosan igényelt információkhoz?

Ehhez érdemes tovább vizsgálni a szolgáltatói együttműködés adta kereteket. Az egyik ilyen kitétel, hogy a hazai jogszabályok által előírtak mellett nincs szükség az átviteli út titkosításának kikényszerített gyengítésére. Ez azt jelenti, hogy nem kell olyan hátsó kaput, mesterkulcsot vagy gyengített titkosítást alkalmazni, amelyek lehetővé tehetik a szolgálatok számára a szolgáltatók bevonása nélkül is az információkhoz való hozzáférést. Ez a megoldás ugyanis valóban adna egyfajta technikai megoldást az ellenőrzésre[1], de ez azzal a veszéllyel is járna, hogy más, illetéktelen titkosszolgálatok, bűnözők, konkurens cégek stb. is könnyebben hozzáférhetnének a felhasználó adataihoz, információihoz, amely valóban jelentősen gyengíthetné a biztonságot.

A másik ilyen kitétel, hogy így nincs szükség a felhasználó által használt hardver eszközök (pl. okostelefon, notebook stb.) kikényszerített gyengítésére, hátsó kapu beépítésére. Ez szintén adhatna egyfajta technikai megoldást[2] a törvényes ellenőrzésre feljogosított szolgálatok részére, sőt nem csak a kommunikáció tartalmához, hanem akár az eszközön tárolt egyéb adatokhoz is hozzáférést biztosítana, ugyanakkor ugyanúgy rendelkezne azokkal a hátrányokkal, mint a fenti megoldás. Azaz az eszköz elvesztése, ellopása, de akár távoli hozzáférése esetén mások is könnyen hozzájuthatnának ezekhez az információkhoz, vagy telepíthetnének rá kémprogramokat. [11]

A szolgáltató együttműködése így talán a legkisebb veszélyforrásnak tekinthető, mindazok ellenére, hogy ily módon fennáll a veszélye a szolgáltató kémkedésének, vagy egy partnere illetéktelen hozzáférésének. Ez ugyanis jogi és adminisztratív úton kezelhető, azaz előírhatók a szolgáltató számára olyan rendelkezések, amelyek ennek kizárását szolgálják. Ráadásul ezek betartása, valamint a betartás bizonyítása a szolgáltatóknak is érdeke. Azok a szolgáltatók ugyanis, akik elvégeztetnek egy erre vonatkozó auditot, tanúsítással rendelkeznek arról, hogy náluk szabályozott és ellenőrzött módon zárták ki a fent említett problémát, és annak eredményeit közzé is teszik, versenyelőnyt szereznek azokkal szemben, akik nem tudnak hasonlót felmutatni. Ez a metódus a felhő alapú rendszerek esetében már elfogadottnak tekinthető, erre bevált formák és eljárások vannak, az auditorok pedig rendelkeznek a kellő tudással egy ilyen típusú átfogó vizsgálat elvégzéséhez. Ezért a szolgáltatók – a biztonság szem elé kerülésével – érdekeltek lesznek abban, hogy így járjanak el.

Arra, hogy a felhasználók számára valóban a szolgáltatók és a törvényes ellenőrzést végző szervezetek közötti együttműködés biztosítja a legkisebb kockázatot, további érvek is felsorakoztathatók.

---

[1] lásd „Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban – ellentétes vagy egymással megférő követelmények? I”.: pl. mély csomagvizsgálat (DPI), közbeékelődéses ellenőrzés (MitM)

[2] lásd feljebb: pl. aktív ellenőrző eszközök (kémprogramok), valamint pl. FBI-Apple vita. Ez utóbbi esetében két, az Iszlám Állammal szimpatizáló terrorista 14 embert ölt meg egy egészségklinikán az egyesült államokbeli San Bernandinóban. A rendőrség által begyűjtött bizonyítékok között volt az egyik támadó jelkódos zárral védett iPhone 5C típusú mobiltelefonja, amelynek feltörését kérte az FBI az Apple-től. A cég ezt megtagadta, majd egy, az ügyön túlnövő vita alakult ki az adatvédelemről. Bár bírósági végzés is született arról, hogy az Apple-nek segítenie kell, végül egy – vélhetőleg – izraeli cég törte fel a telefont és tette a rajta lévő adatokat elérhetővé az FBI számára. [22]

Az első, hogy a felhasználó számára így ismert és tudott az együttműködés ténye, amely ráadásul a hírközlési szolgáltatók viszonylatában már elfogadott gyakorlat is. Korábban éppen a Snowden botrány kapcsán derült fény arra, hogy például a legjelentősebb alkalmazásszolgáltatók tagadták, vagy kerülték a válaszadást az egyesült államokbeli nemzetbiztonsági szolgálatokkal és rendvédelmi szervekkel való együttműködésre, mégis lehetőséget biztosítottak számukra a felhasználók adataihoz való hozzáférésre. [12]

A második, hogy azok a szolgáltatók, akik a korábban már jelzett auditot végrehajtják, és annak eredményeit közzéteszik, azt is bizonyítják a felhasználóknak, hogy csak azokkal az ellenőrzést végző szolgálatokkal állnak kapcsolatban, akikről a felhasználó is tud. A felhő alapú szolgáltatások esetében ugyanis mindig is kiemelten kezelendő kockázat volt, hogy a szolgáltató kivel osztja, oszthatja meg a felhasználó adatait, így például a szolgáltató honos országában, vagy akár az adatközpontjainak országában is. [13] Amennyiben ez nem tisztázott a felhasználó számára, akkor ez is csökkentheti a kommunikációja biztonságát.

A harmadik, hogy arra egyébiránt sincs garancia, hogy egy szolgáltató vagy gyártó nem épít-e be tudatosan valamilyen hátsó kaput, amellyel akár saját maga, akár egy harmadik fél számára biztosíthatja a hozzáférést a felhasználó adataihoz. Erre több alkalommal is felmerült a gyanú olyan neves gyártók esetében, akik biztonságosnak hirdették termékeiket. [14] [15] [16]

Kikényszeríthetőség

A hazai szabályozás kapcsán felmerült már a kérdés, hogy ki lehet-e egyáltalán kényszeríteni az alkalmazásszolgáltatók együttműködését. Erre talán az adózással és a szerencsejátékok szabályozásával kapcsolatos példákat érdemes megemlíteni. Az alkalmazásszolgáltatók adóztatására már 2014-ben T/264 számon javaslat érkezett, [17] amelyet az Országgyűlés még abban az évben el is fogadott. [18] Az így hatályosított törvényben megfogalmazottak alapot és precedenst teremtettek az internet-technológiára épülő szolgáltatások, így az alkalmazásszolgáltatók „bekényszerítésére” a magyar jogrendbe. Ugyanakkor az adóztatás szempontjából is érdekes – és a későbbiekben megoldandó – feladatként jelentkezik a szankcionálás kérdése. Nagy kérdés ugyanis, hogy milyen eszközökkel lehet kikényszeríteni az együttműködést, vagy hogyan lehet büntetni az az alól kibújókat. Erre lehet példa az interneten nyújtott sportfogadások, szerencsejátékok esete. Itt a NAV[3] már blokkoltatja azokat az online fogadási szolgáltatást nyújtó oldalakat, amelyek nem tesznek eleget a magyar jogszabályokban megfogalmazottaknak. [19] Megjegyzendő azonban, hogy az itt egyébként működő szankcionálási rendszert is meg kívánták erősíteni az illetékesek, amelynek érdekében törvényjavaslatot terjesztettek be, [20] amelyet azóta az Országgyűlés el is fogadott, a rendelkezési pedig már hatályba is léptek. Ennek főbb elemei, hogy a kiszabható pénzbírságot a tízszeresére emelték, valamint bevezették a pénzügyi blokkolást is. Ez utóbbi azt akadályozza meg, hogy az illegális szerencsejáték szervező bankszámlájára megérkezzen a játékos által átutalt összeg, az átutalást ebben az esetben ugyanis a pénzforgalmi szolgáltató nem teljesítheti.

A szankcionálásra a törvényes ellenőrzés kapcsán jelenleg az Ekertv. – ismételhető módon – pénzbírság kiszabását biztosítja. Ennek gyakorlati betarthatósága, esetlegesen más elemekkel pl. a szerencsejátékokhoz hasonló módon blokkolással, történő kiegészítése még a jövő zenéje. Ugyanakkor meg kell jegyezni, hogy a szankcionálás kérdése az adózás esetében sem kristályosodott még ki teljesen, és ez ugyanúgy kérdéseket vet fel a törvényes ellenőrzés kapcsán is. Mindazok mellett, hogy az interneten nyújtott sportfogadások, szerencsejátékok esetében Magyarországon már kialakult egyfajta működő megoldás, célszerű egyrészt

[3] NAV: Nemzeti Adó- és Vámhivatal

megvizsgálni a külföldi ilyen célú megoldásokat, másrészt egyeztetéseket folytatni arról, hogy magasabb pl. EU szinten hogyan lehet a kérdésben egységesen fellépni.

Jogi garanciák

További kérdésként merülhet fel, hogyan lehet, vagy lehet-e bármilyen garanciát adni arra, hogy a törvényes ellenőrzést végző szolgálatok csak ahhoz az információhoz férnek hozzá, amelyekre engedélyt kaptak? Erre jogi garanciát nyújt a nagyon szigorú hazai szabályozás. Ez már a hírközlési szolgáltatók esetében is kizárólag ún. külső, azaz bírói vagy igazságügy miniszteri engedély megléte esetén tette lehetővé a kommunikáció tartalmához való hozzáférést, valamint kizárta a szűrő-kutató jellegű ellenőrzés lehetőségét. A jelenlegi szabályozás ezt konzekvensen fenntartja. Ráadásul a 185/2016. (VII. 13.) Korm. rendelet lehetőséget biztosít a szolgáltató számára, hogy jogi képviselőjével megvizsgáltassa az adatigénylés jogszabályok szerinti megfelelőségét. Ezek pedig megfelelő garanciális elemek mind a felhasználó, mind a szolgáltató számára.

ÖSSZEGZÉS

Összességében megállapítható, hogy a kommunikáció változása a szolgáltatói modell és a törvényes ellenőrzés változását is magával hozta. Az is megállapítható, hogy jelenleg több féle technikai megoldás létezik a törvényes ellenőrzés végrehajtására, ám a szolgáltatóval való együttműködés megkerülhetetlen. A Magyarországon 2016-ban életbe lépett jogi szabályozás mindenképpen előremutató, mondhatni példaértékű, hiszen mások csak most keresik a problémára a megfelelő megoldást. Jól mutatja ezt a német és a francia belügyminiszter által kiadott közös közlemény is, amelyben deklarálják, hogy a terrorizmus elleni küzdelem okán olyan megoldást kell találni a titkosított kommunikáció lehallgatására, amelyik biztosítja az adatokhoz való hozzáférést a felhasználók magánszférájának védelme mellett. Mindezt úgy, hogy a szabályozás minden szolgáltatóra egyforma kötelezettségekkel, egyforma feltételekkel terjedjen ki, függetlenül azok székhelyétől. [21] Azaz egyfajta, a magyar szabályozásnak megfelelő megoldást javasolnak, ám ennek tényleges megvalósításától még messze vannak.

Megállapítható az is, hogy az új hazai szabályozás teremtette lehetőség mindamellett, hogy a felhasználó szempontjából nézve a kommunikáció biztonságára a legkisebb veszélyforrásnak tekinthető, költséghatékonyan képes biztosítani a törvényes ellenőrzést. Ráadásul oly módon, hogy ahhoz megfelelő jogi garanciákat is csatol.

Ugyanakkor megállapítható az is, hogy a kikényszeríthetőség további megoldandó kérdéseket vet fel, amelyek hatékony megoldásához célszerű megvizsgálni egyrészt a hazai és a külföldi már kialakult és működő megoldásokat, másrészt egy magasabb pl. EU szintű egységesen fellépés lehetőségét.

Felhasznált irodalom

[1] 2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600069.TV&timeshift=fffffff4&txtreferer=00000001.TXT Letöltés ideje: 2016. 09. 25.

[2] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv Letöltés ideje: 2016. 09. 25.

[3] 185/2016. (VII. 13.) Korm. rendelet a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600185.KOR Letöltés ideje: 2016. 09. 25.

[4] Ketterling, Hans-Peter A.: Introduction to Digital Professional Mobile Radio. Artech House. Norwood. 2004. ISBN 1-58053-173-3 https://books.google.hu/books?id=nZ5ISTkagOQC&pg=PA85&dq=nmt+450+modulation&hl=hu&sa=X&ved=0ahUKEwjPktaQuazPAhVI0xoKHY84APEQ6AEIVjAG#v=onepage&q=nmt%20450%20modulation&f=false Letöltés ideje: 2016. 09. 25.

[5] GSM Association Specification for A5/3. http://www.3gpp.org/ftp/tsg_sa/wg3_security/tsgs3_13_yokohama/docs/pdf/s3-000362.pdf Letöltés ideje: 2016. 09. 25.

[6] Chow, Richard – Golle, Philippe – Jakobsson, Markus – Shi, Elaine – Staddon, Jessica – Masuoka, Ryusuke – Molina, Jesus: Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security ACM. New York, NY, USA 2009. pp. 85-90. ISBN: 978-1-60558-784-4 http://www.parc.com/publication/2335/controlling-data-in-the-cloud.html. Letöltés ideje: 2011. 11. 05.

[7] Biztonsági tippek a Gmail használatával kapcsolatban. https://support.google.com/mail/answer/7036019?co=GENIE.Platform%3DDesktop&hl=hu Letöltés ideje: 2016. 09. 25.

[8] Google Általános Szerződési Feltételek (Utolsó módosítás: 2014. április 14.) https://www.google.com/intl/hu/policies/terms/ Letöltés ideje: 2016. 09. 25.

[9] 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.

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

[11] Yadron, Danny: Government keeping its method to crack San Bernardino iPhone 'classified'. https://www.theguardian.com/technology/2016/mar/22/apple-fbi-san-bernardino-iphone-method-for-cracking Letöltés ideje: 2016. 09. 25.

[12] Gyurkity Péter: Mindenki a megfigyelt felhőbe igyekszik. 2013. 06. 10. https://sg.hu/cikkek/97838/mindenki-a-megfigyelt-felhobe-igyekszik. Letöltés ideje: 2016. 09. 25.

[13] Cloud Computing: Benefits, risks and recommendations for information security. 2009. 11. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment. Letöltés ideje: 2014. 11. 12.

[14] Sullivan, Nick: How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer. 2014. 01. 06. http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/ Letöltés ideje: 2016. 09. 27.

[15] Zetter, Kim: Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors 2012. 12. 18. https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ Letöltés ideje: 2016. 09. 27.

[16] Afonin, Oleg: iOS 10: Security Weakness Discovered, Backup Passwords Much Easier to Break. 2016. 09. 23. http://blog.elcomsoft.com/2016/09/ios-10-security-weakness-discovered-backup-passwords-much-easier-to-break/ Letöltés ideje: 2016. 09. 27.

[17] http://www.parlament.hu/irom40/00264/00264.pdf. Letöltés ideje: 2014. 07. 01.

[18] 2014. évi XXXIII. törvény az egyes pénzügyi tárgyú törvények módosításáról. http://www.complex.hu/kzldat/t1400033.htm/t1400033.htm#kagy1. Letöltés ideje: 2015. 03. 29.

[19] Ezeket a szerencsejáték-oldalakat kapcsolta le a NAV. 2014. 06. 28. http://www.napi.hu/ado/ezeket_a_szerencsejatek-oldalakat_kapcsolta_le_a_nav.583212.html. Letöltés ideje: 2014. 07. 01.

[20] T/12250. számú törvényjavaslat egyes törvényeknek a tiltott szerencsejáték megakadályozásával összefüggő módosításáról. http://www.parlament.hu/irom40/12250/12250.pdf Letöltés ideje: 2016. 09. 27.

[21] Ein Beitrag zur Erhöhung der inneren Sicherheit in Europa http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/eckpunkte-der-europaeischen-zusammenarbeit-innere-sicherheit.pdf?__blob=publicationFile Letöltés ideje: 2016. 08. 25.

[22] Nakashima, Ellen: FBI paid professional hackers one-time fee to crack San Bernardino iPhone 2016. 04. 12. https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html Letöltés ideje: 2016. 09. 25.