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? I.

Absztrakt

A cikksorozat összefoglalja a kommunikáció változását, a változások hatását a szolgáltatói modellre és a törvényes ellenőrzésre. Rámutat azokra a jogi hiányosságokra, problémákra, amelyek hatással vannak az internet alapú kommunikáció törvényes ellenőrzésének hatékony ellátására, majd nemzetközi kitekintéssel bemutatja az ellenőrzésére jelenleg rendelkezésre álló, jellemző technikai eszközöket és azok főbb tulajdonságait. Rávilágít a hazánkban újonnan hatályba lépett jogszabályok adta lehetőségekre, pontosítva annak kereteit, valamint ismerteti, hogy milyen hatásai lehetnek a kommunikáció biztonságára. Az első rész a kommunikáció, a szolgáltatói modell változásának és a törvényes ellenőrzés lehetőségeinek a téma szempontjából lényeges elemeit foglalja össze.

This article series summarizes the changes of communication and the effects of these changes on the service-provider model and on the lawful monitoring. This article series points out the insufficiencies and problems of the current laws which affect the lawful monitoring of the internet-based communication, then describes the currently and typically used possible technical solutions of lawful monitoring, and their major characteristics with an international view. It highlights the possibilities given by the Hungarian law that entered into force nowadays, on lawful monitoring of the application service providers, specifies its frames, and describes its effects on the security and privacy of communication. The first part of this article series is reviewing and summarizing the changing of the communication and the service provider model, as well as the possible technical solutions of lawful monitoring, which are relevant to the subject.

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

BEVEZETÉS

Napjaink egyik legtöbbet vitatott kérdése az internet alapú szolgáltatások – ezek közül is kiemelten a kommunikációt lehetővé tevők – törvényes ellenőrzése. Érdemes ugyanakkor megemlíteni, hogy a hibrid hadviselés szempontjából is komoly jelentőség tulajdonítható az internet és a mobil kommunikáció egyes területeinek. [1] A viták fő oka az, hogy miközben a kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek, addig az azok ellenőrzését szabályozó törvények jellemzően nem követik azokat. A jogszabályi lemaradás természetesnek mondható, hiszen ez szinte minden új, a nemzetbiztossági szolgálatok és a rendvédelmi szervek által ellenőrizni kívánt technológia esetében hasonló módon megy végbe. A hosszabb távon is megfelelő törvényi szabályozáshoz ugyanis célszerű nem egy-egy szolgáltatásra kihegyezett, hanem általánosan érvényes szabályokat leírni, amelyhez azonban több feltételnek is teljesülnie kell. Először is ismerni kell, melyek azok a technológiák, amelyek felhasználása eléggé elterjedt ahhoz, hogy azokat a szabályozó mindenképp lefedje. Ezáltal a jogszabályokat oly módon kell megfogalmazni, hogy ezekre valóban ki is terjedjen a hatályuk. Másrészt ezen technológiák már műszakilag kellőképpen kiforrottak kellenek legyenek ahhoz, hogy egy-egy műszaki változtatás várhatóan ne lehessen olyan hatású, hogy a frissített rendszerre már nem érvényesíthető a leírt jogszabály, így az ne okozhassa a törvényes ellenőrzés ellehetetlenülését. Az ugyanis a kezdeti, mondhatni bevezetési fázisban lévő kommunikációs szolgáltatásoknál jellemző, hogy sokszor egy-egy új szoftver verzió kiadásával gyökeres változásokat eszközölnek a készítők, többször teljesen új technológiai alapra helyezve a szolgáltatást, akár úgy is, hogy a korábbi verziók kompatibilitását sem biztosítják.

Az internet alapú, ezek közül is kiemelten a kommunikációt lehetővé tevő szolgáltatások törvényes ellenőrzése minden országban kihívást jelent. Egyrészt azért, mert az elektronikus úton folytatott kommunikáció ma már jóval tágabb értelemben értelmezhető fogalom, mint a hagyományos hírközlés, hiszen lehetőségei, a kommunikációs formák száma messze meghaladják ez utóbbiét. Ennek következtében rengeteg olyan új rendszer, technológia jelent, jelenik meg, amelyek törvényes ellenőrzését az arra feljogosított szolgálatoknak meg kell, vagy legalábbis meg kellene oldani. Másrészt pedig azért, mert strukturális átalakulás is zajlik, amelyben a – korábban mindenki által elfogadott és már jól szabályozott ellenőrzési módszereket is tartalmazó – klasszikus hírközlési szolgáltatói modellt egyre inkább felváltja az infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modell. Ez utóbbi esetében azonban nincsenek egységes, mindenki által elfogadott törvényes ellenőrzési módszerek és szabályzók.

A törvényes ellenőrzés kialakítását alapvetően három – egymással szorosan összefüggő – probléma nehezíti. Az egyik, a már említett jogi szabályozás hiányosságaiban keresendő. A hatályos jogszabályok ugyanis nem, nem teljes mértékben vagy csak erős „beleértéssel” teszik lehetővé az említett rendszerek ellenőrzését, mindenki – vagy legalábbis a fejlett demokráciával rendelkező országok – által elfogadott, irányadó szabályozók pedig nincsenek. A másik a technikai megoldások hiánya, vagy a meglévők hiányossága jelenti, hiszen sokszor vagy még nincsenek meg azok a technikai eszközök, amelyekkel az új technológiák törvényes ellenőrzését egyáltalán végre lehet hajtani, vagy a meglévők technikailag korlátozottan képesek az elvárt – és a hírközlés-ellenőrzésnél már megszokott – feladatok elvégzésére. A harmadik nagy problémát pedig az okozza, hogy a hírközlés ellenőrzésnél régóta kialakult és elfogadott rend, miszerint az infrastruktúrával és szolgáltatással az adott országban egyaránt jelen lévő szolgáltató együttműködik a nemzetbiztonsági és bűnüldöző szervekkel, ebben az esetben nem, vagy nem teljes mértékben működik.

A fenti problémakör kezelésére 2016-ban Magyarországon megszületett egy merőben új jogi szabályozás. Ez azonban újszerűsége okán meglehetősen sok vitát váltott ki és félreértést okozott, főleg abban, hogy az egyes szereplőknek, beleértve a felhasználót is milyen

kötelezettségei vannak, és adott esetben annak megszegése hogyan szankcionálható. Mindehhez még hozzájárult a nemzetközi sajtóban fellángolt vita arról, hogy az ellenőrzés biztosítása az arra feljogosított szolgálatok számára milyen esetben és hogyan okozza, okozhatja a kommunikáció biztonságának romlását. Éppen ezért célszerű megvizsgálni, hogy milyen módszerek állnak a titkos információgyűjtést végző szervezetek rendelkezésére, és azok alkalmazása során milyen buktatókba ütköztek, valamint azt is, hogy a nemrégiben elfogadott hazai szabályozás milyen hatással van, lehet egyrészt a törvényes ellenőrzésre, másrészt a felhasználó szemszögéből nézve a kommunikáció biztonságára.

A KOMMUNIKÁCIÓ ÉS A SZOLGÁLTATÓI MODELL VÁLTOZÁSA

A „Felhő alapú rendszerek törvényes ellenőrzési problémái”, [2] a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. és II.” [3] [4] valamint az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből” [5] című cikkek részletesen megvizsgálták és leírták az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére szolgáló lehetőségeket, azok előnyeit, hátrányait, valamint definiálták a jelenlegi hírközlési modellt potenciálisan felváltó infrastruktúra-, alkalmazás- és tartalomszolgáltatói modellt, pontos meghatározásokat adva annak egyes szereplőire. Fenntartva és elfogadva az ott leírtakat az alábbiak röviden összefoglalják a jelen cikk témájának kibontásához szükséges, az említett cikkekben megjelenített főbb elemeket.

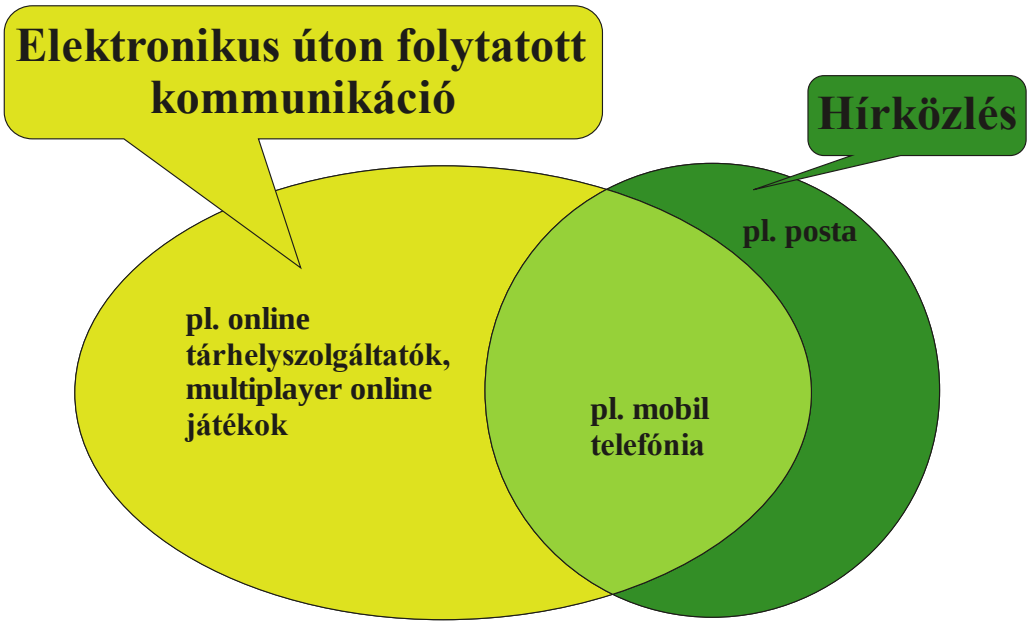
A kommunikáció változása

A kommunikáció formái, lehetőségei az internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. Ebben nagy szerepük van az internet-technológiára épülő szolgáltatásoknak. Ezek azok a mindenki számára elérhető, meglévő eszközeivel (pl. notebook, okostelefon stb.), akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

Az említett rendszerek azonban 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 szervezet biztosítja a felhasználó számára. Sőt, ezek a legtöbb esetben nem is tudnak egymásról, nincsenek semmilyen kapcsolatban egymással. Így a korábbi hírközlés helyett ma már sokkal inkább elektronikus úton folytatott kommunikációról beszélhetünk.

Az elektronikus úton folytatott kommunikáció megnevezés teljesen tudatos szóhasználat. Napjainkban ugyanis az említett fogalom alatt nem csak a hírközlő rendszereken folytatott kommunikációt értjük, hanem minden olyan kommunikációs lehetőséget, formát, amely lehetővé teszi két – vagy adott esetben több – fél között információk, adatok áramlását, cseréjét. Ez pedig messze túlmutat nemcsak a hírközlés, de a kifejezetten kommunikáció céljából kifejlesztett internet alapú rendszereken is.

Húsz évvel ezelőtt a hírközlés teljes egészében lefedte az elektronikus úton folytatott kommunikációt, ez utóbbi a hírközlés mintegy részhalmazát képezte. Mára ez a kép jelentősen megváltozott. Ha ábrázolnánk, akkor talán az 1. ábra megfelelően szemléltetné a kettő kapcsolatát. A területek nagyságával az egymáshoz képesti jelentőséget is szemléltetni kívántam.



1. ábra. Az elektronikus úton folytatott kommunikáció és a hírközlés viszonya

Ma az elektronikus úton folytatott kommunikáció lehetőségei messze meghaladják a hagyományos hírközlését. A végeredmény szempontjából ugyanis nincs különbség a között, hogy megírok és elküldök egy elektronikus levelet, vagy megírás után a piszkozatok közé teszem, de a másik félnek megadom a postafiók eléréséhez szükséges felhasználónevet és jelszót. Hiszen ez utóbbi esetben is hozzáfér, olvashatja ugyanazt az üzenetet. De itt még legalább a „levélszerűség" megvan, a „hagyományos" hírközlési forma fellelhető. Ha a továbbítani szánt információkat azonban egy felhő alapú tárhely szolgáltatónál kialakított fiókba helyezem el fájlként, majd ennek adom meg a belépéshez szükséges adatait a másik félnek, akkor a végeredmény ugyanaz: „A" felhasználótól „B" felhasználóhoz eljutott az információ. Ez a forma azonban már „nyomokban sem tartalmaz" hagyományos hírközlést. Ugyanilyen jellegű példa a multiplayer online játékok esete. Ezeket nem azért fejlesztették ki, hogy a felhasználók kommunikálni tudjanak egymással, az csak egy kiegészítője, hozadéka a játékoknak. Ugyanakkor tényszerűen vizsgálva, a végeredményt tekintve itt sincs különbség a játék során folytatott beszélgetések, chatelések és egy kifejezetten erre szakosodott hírközlő rendszeren folytatott beszélgetés vagy üzenetküldés között.

Az internet-technológiára épülő, azokon belül is elsősorban a kommunikációs szolgáltatások törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, ugyanakkor a törvényes ellenőrzést végző szervek több, már említett jogi és technikai problémával is szembesültek, szembesülnek. A törvényes ellenőrzést végző szervezeteknek alapvetően az a feladata, célja, hogy a kijelölt célszemélyek kommunikációját lehetőség szerint teljes mértékben ellenőrizzék függetlenül annak formájától, a felhasznált technológiától. Az ehhez megfelelő, hatékony törvényi szabályozás megalkotásához és technikai eszközrendszerek kialakításához azonban figyelembe kell venni a szolgáltatói modell változását is.

A szolgáltatói modell változása

Megállapítható, hogy a klasszikus hírközlési szolgáltatói modell egyre inkább eltűnik, helyét új szolgáltatói struktúra veszi át, és ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre az, hogy a hírközlési hálózatot – vagy célszerűbb megfogalmazással internetelérést – és a tényleges kommunikációt más szolgáltatató biztosítja. Ennek a leírására a korábbi hírközlési szolgáltatói modell helyett az azt potenciálisan felváltani képes infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt célszerű

alkalmazni, amely teljes körűen képes leírni mind a jelenlegi helyzetet, mind a korábbi hírközlési modellben szereplőket, valamint azok feladatait.

Fel kell azonban tenni a kérdést, hogy mit is takarnak az infrastruktúra-, alkalmazás-, és tartalomszolgáltató fogalmak. Ezekre részletes választ ad az „Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből” című cikk, [4] definíciós javaslatot is adva mindhárom szolgáltatóhoz. Mindezeket továbbiakban is fenntartva, röviden és egyszerűsítetten az alábbiak szerint fogalmazhatók meg az egyes említett szolgáltatók – a téma szempontjából – lényegi tulajdonságai:

Tartalomszolgáltató: kizárólag egyirányú információáramlást szolgál, azok tartalmára a fogyasztónak semmilyen befolyása nincs, a felhasználó „passzív” fogyasztó, a szolgáltató a tartalomért szerkesztői felelősséggel tartozik. Nem tekinthetők tartalomszolgáltatásnak a magáncélú vagy szűk, meghatározott körben elérhető tartalmak. Sem a szolgáltató, sem a felhasználó a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen. A szolgáltatás Magyarországon elérhető és igénybe vehető, függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e.

Alkalmazásszolgáltató: az információáramlás ebben az esetben többirányú, a felhasználó aktív, tevékeny résztvevő, az információk adattartalmára befolyással rendelkezik. Sem a szolgáltató, sem a felhasználó a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen. A szolgáltatás Magyarországon elérhető és igénybe vehető, függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e.

Infrastruktúraszolgáltató: valamilyen infokommunikációs rendszert üzemeltet és azon keresztül internetelérést biztosít, akár úgy is, hogy más szolgáltatótól vásárolt interneteléréshez biztosít harmadik félnek (feleknek) hozzáférést. Sem a szolgáltató, sem a felhasználó a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen. A szolgáltatás Magyarországon elérhető és igénybe vehető, függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e.

Vegyes szolgáltatások: Természetesen előfordulhat, hogy valamely cég vegyes szolgáltatást nyújt. Ma például egy internetszolgáltató internetelérést és például e-mail-ezési lehetőséget is biztosíthat, vagy egy online tartalomszolgáltatással foglalkozó cégnél, például egy internetes újságnál pedig lehetőséget biztosíthatnak kommentek írására, ezen keresztül pedig kommunikáció megvalósítására is. Ezekben az esetek is kezelhetőek a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkben [2] bemutatott hármas tagozódásban szereplő tartalom-, alkalmazás-, és infrastruktúraszolgáltató modellel.

A törvényes ellenőrzés kapcsán a három szolgáltatónak eltérő kötelezettségei származnak. Míg a tartalomszolgáltatónak alig, az infrastruktúra szolgáltatónak korlátozott (elsősorban előfizetői adatszolgáltatási), addig az alkalmazásszolgáltatóknak – a hagyományos hírközlési szolgáltatóhoz hasonlóan – szinte teljes körű (például az összes felhasználói adat, így bejelentkezési IP címek, felhasználónevek, valamint az általa nyújtott szolgáltatás kapcsán keletkező tartalmak, így e-mailek, hangkommunikáció, chat, stb.) információ-, és adatelérést kell biztosítania az arra felhatalmazott szervezetek számára.

Amennyiben egy cég vegyes szolgáltatást nyújt, akkor a szolgáltatásfajtáknak megfelelően kell a törvényes ellenőrzést lehetővé tennie. Maradva a fent említett példáknál, ha egy mai értelemben vett internetszolgáltató e-mail lehetőséget is biztosít, akkor erre az alkalmazásszolgáltatóknál kialakítandó kötelezettségeket kell figyelembe venni. Ugyanez igaz az online újság esetében is, ahol a fórumok, kommentek esetén már az alkalmazásszolgáltatókra kirótt kötelezettségeket kell teljesíteniük.

Érdemes megvizsgálni a mai hírközlési szolgáltatók helyzetét is. Esetükben a problémakör két részre bontható. Amennyiben internet-szolgáltatást is végeznek, akkor a fent leírtak alapján lehet eljárni. Amennyiben a hagyományos – például vezetékes telefon – szolgáltatásokat nézzük, akkor ott is megjelenik az infrastruktúra-, és alkalmazásszolgáltatás,

csak kizárólagosan egy, azonos és elválaszthatatlan infrastruktúrával és szolgáltatóval. Ebben az esetben is ugyanúgy kezelhető a probléma, mint a fent már leírt egyéb vegyes szolgáltatások esetében.

A fentiek alapján megállapítható, hogy a tartalom-, alkalmazás-, és infrastruktúraszolgáltató modellbe minden szolgáltató egyértelműen besorolható, így törvényes kötelezettségeik is egyértelműen meghatározhatóvá válnak. Igaz ez a mai jogszabályokban leírt hírközlési-, és internetszolgáltatók esetében is.

Mindezek mellett a hírközlési szolgáltató és szolgáltatás fogalmát a továbbiakban is célszerű fenntartani, egyrészt azért, mert így például a hagyományos telefonszolgáltatások a jelenlegi szabályoknak megfelelően a továbbiakban is egyszerűen, mindenki számára vita nélkül elfogadott módon kezelhetők, másrészt pedig azért, mert a nemzetközi jogi szabályozásban ezek törvényes ellenőrzése egy mindenki által elfogadott meghatározás és normarendszer szerint történik.

A TÖRVÉNYES ELLNŐRZÉSI MÓDSZEREK

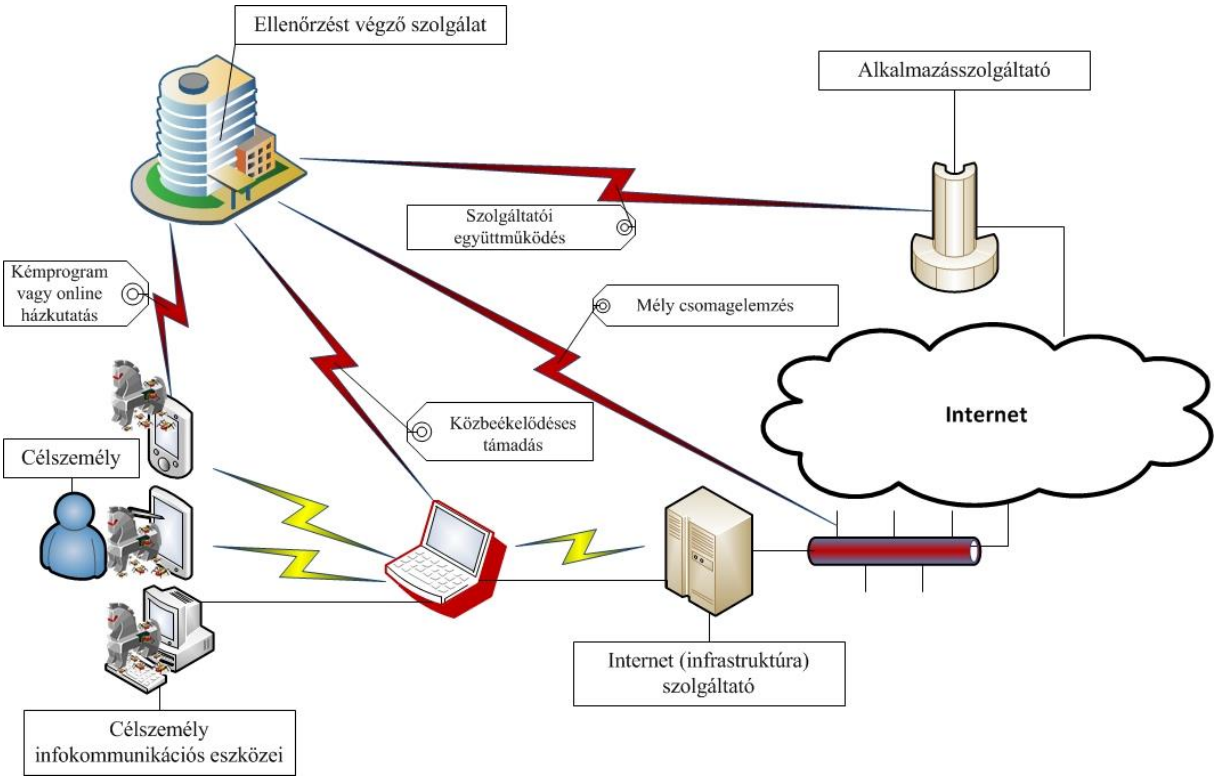
Annak érdekében, hogy tisztázni lehessen, milyen hatása van vagy lehet az erre vonatkozó újonnan hozott hazai jogszabályoknak az internet-technológiára épülő szolgáltatások törvényes ellenőrzésének hatékonyságára, valamint hogy sérülhet-e a kommunikáció biztonsága, célszerű megvizsgálni, hogy a szolgáltatói modell változása milyen hatással van a törvényes ellenőrzésre, milyen jellemző technikai eszközök állnak rendelkezésre annak megvalósításához.

Az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére alapvetően az alábbi négy módszert használhatják az arra felhatalmazott szolgálatok:

a) aktív ellenőrző eszköz,
b) közbeékelődéses ellenőrzés (MitM),
c) mély csomagvizsgálat (DPI),
d) együttműködés a szolgáltatóval.

A módszerek elnevezései önkényesek. Valódi, mindenki által elfogadott magyar megfelelőik vagy nem alakultak ki, vagy az ezekről szóló szakirodalom is többféle megnevezéssel használja azokat. [6] [7]

A fenti módszerekre rendkívül jellemző az alkalmazásukkor használt adatszerző, elfogó eszközök – ebbe bele kell érteni a hardver és szoftver elemeket egyaránt – távolsága a célszemélytől. Ezt jól szemlélteti a 2. ábra.



2. ábra. Az adatszerző, ellenőrző eszközök távolsága a célszemélytől

Aktív ellenőrző eszköz

Az aktív ellenőrző eszközök, vagy közismertebb, a fejezet első részében említett nevükön kémprogramok vagy online házkutatási eszközök esetében a célszemély infokommunikációs eszközére, eszközeire (pl. számítógép, telefon, táblagép stb.) egy speciális „kártékony" szoftvert telepít az ellenőrzést végző szolgálat. Ez sok hasonlóságot mutat a valódi kártékony szoftverekkel, de ebben az esetben ez törvényes célokat szolgál. Talán azt az analógiát lehetne erre alkalmazni, mint amikor egy lőfegyverről beszélünk, amely más értelmet nyer egy bűnöző és mást egy rendőr kezében.

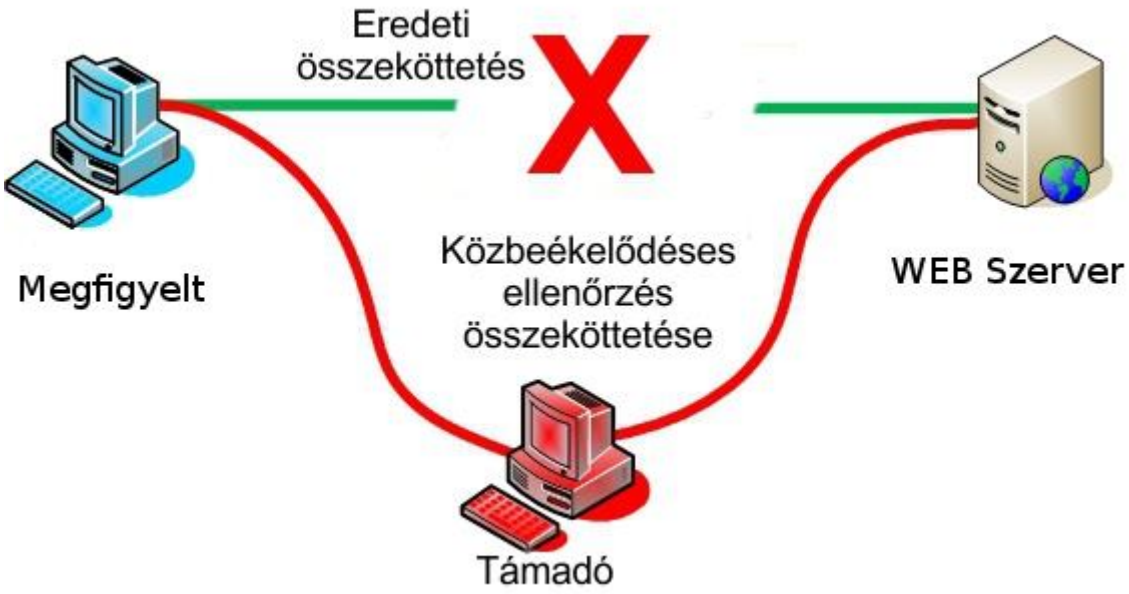
Az aktív ellenőrző eszköz bejuttatása a célszemély eszközére többféle módszerrel is lehetséges, hasonlóan a kiberbűnözők által használt módozatokhoz (pl. elektronikus levél csatolmányaként, fertőzött weboldal segítségével, 0. napi sebezhetőség kihasználásával stb.). A működés során ezek képesek az online kommunikáció elfogására, de billentyűzetleütések rögzítésére, a háttértárban található adatok megszerzésére, vagy akár – ha van – a webkamerával képek készítésére is. Az információkat azután összegyűjtve küldik el az aktív ellenőrző eszköz tulajdonosának. [8] [9] [10] [11] [12]

Az online házkutatásra alkalmas eszközök, azaz kémprogramok természetesen jóval több információt tudnak biztosítani a célszemélyek számítógépéről (pl. tárolt fájlok), a számítógép technikai eszközein keresztül a célszemély tevékenységéről (pl. webkamera képek), mint amit pusztán az elektronikus úton folytatott kommunikációt biztosító alkalmazásszolgáltató – a törvényi feltételek megléte és maximális segítőkész hozzáállás mellett – képes.

A törvényes ellenőrzések során alkalmazott kémprogramokról Németországból szivárgott ki a legtöbb információ, ám – mint bizonyos körülmények között rendkívül hatékony vagy sokszor egyetlen alkalmazható eszközt – más országok titkos információgyűjtésre feljogosított szervei is használják, vagy legalábbis használni tervezik. Ilyen témájú hírek érkeztek Svájc, [13] Franciaország, [14] Ausztria, [15] Hollandia [16] és természetesen az USA [17] [18] [19] [20] és az Egyesült Királyság [21] vonatkozásában is.

Közbeékelődéses ellenőrzés (MitM)

Leegyszerűsítve a dolgot, a közbeékelődéses ellenőrzés esetében az ellenőrzést végző szolgálat úgy hallgatja le a két fél között zajló kommunikációt, hogy a kommunikációs csatornát megszakítja, legyen az vezetékes vagy vezeték nélküli, majd abba, a két kommunikáló fél közé „beállva” mindkettőjük számára a másik félnek adja ki magát. A kapcsolat ezáltal mindkét fél számára zavartalannak tűnik, valójában azonban a teljes forgalom „átfolyik” az ellenőrzést végző eszközén, amellyel az itt zajló kommunikációt lehallgathatja, ahhoz teljes mértékben hozzáfér. Ezt szemlélteti a 3. ábra.



16. ábra. Közbeékelődéses ellenőrzés. (a szerző szerkesztette a [39] alapján)

A sikeres közbeékelődéses ellenőrzéshez több feltételnek is teljesülnie kell. Az ellenőrzést végzőnek hozzá kell férnie a kommunikációs csatornához, képesnek kell lennie annak megszakítására (legyen az vezetékes vagy vezeték nélküli kapcsolat) oly módon, hogy megakadályozza az üzenetek eljutását a valódi címzetthez, majd le kell tudnia hallgatni a rajta küldött üzeneteket. Ez titkosítás nélküli kommunikáció esetében viszonylag egyszerű, de bizonyos esetekben, kis szerencsével és a valódi kommunikáló fél (felek) figyelmetlenségével akár titkosított kommunikáció esetén is megvalósítható. Ezt szemlélteti a 4. ábra.

4. ábra. Példa HTTPS kommunikáció ellenőrzésére. (a szerző szerkesztette a [25] alapján)

Sikeres közbeékelődéses ellenőrzés akkor hajtható végre viszonylag egyszerű eszközökkel és nagy valószínűséggel, ha a célszemélyhez (azaz az egyik kommunikáló félhez) az ellenőrzést végző a lehető legközelebb helyezkedik el. [22] [23] [24] [25] [26] [27]

Érdekes, hogy amíg a többi módszer törvényes ellenőrzésre történő felhasználásáról sok konkrét információ szivárgott ki, addig a MitM-ről ez nem mondható el. Ugyanakkor a

Snowden által kiszivárogtatott anyagokban található információ arra, hogy az Egyesült Államok szolgálatai használták ezt a technológiát is. [28]

Mély csomagvizsgálat (DPI)

A mély csomagvizsgálat azt jelenti, hogy az adatcsomagoknak nemcsak a fejlécét, hanem azok adattartalmát is vizsgálat alá vetik, majd az adattartalom alapján kiszűrik az „érdekes" adatcsomagokat. A szűrés jellege a mély csomagvizsgálat felhasználásának céljától függ, a csomagvizsgálati módszerek azonban technikailag függetlenek attól. [29]

A mély csomagvizsgálatot leggyakrabban három esetben szokták alkalmazni. Az első eset a behatolást észlelő és behatolás-védelmi rendszerekben (IDS/IPS) történő felhasználás. Ezek a rendszerek a csomagok elemzésekor speciális bitmintákat (ismert támadókódokat) keresnek erre dedikált eszközök segítségével, majd a felismert, rosszindulatú kódot tartalmazó csomagokat kiszűrik. [30] A második a hírközlési, internetszolgáltatók rendszereiben történő alkalmazás. Itt az internet protokoll alapú hangátviteli szolgáltatások (VoIP) és a peer-to-peer kapcsolaton alapuló fájlcsere forgalmának blokkolására használják a technológiát. [31] A harmadik a törvényes ellenőrzés, ahol a csomagok vizsgálata alapján dönthető el, hogy az az ellenőrzést végző számára érdekes-e (pl. adott célszemélyhez tartozik-e az email), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását. [32] [33] [34] [35]

Titkosítás nélküli kommunikáció esetén a lehallgatás viszonylag egyszerűen, sőt ebben az esetben, ellentétben a közbeékelődéses ellenőrzéssel, tömegesen is megvalósítható. Ugyanakkor titkosított kommunikáció esetén a tartalomhoz való hozzáféréshez feltétlenül szükséges a titkosítás feltörése, ez pedig hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a kommunikáló felek akár a nyílt forgalmaknál is egyszerű – és sokszor ingyenesen rendelkezésre álló – titkosító szoftvereszközök használatával (pl. HTTPS Everywhere) jelentősen megnehezíthetik vagy akár el is lehetetlenítik az ellenőrzést. [36]

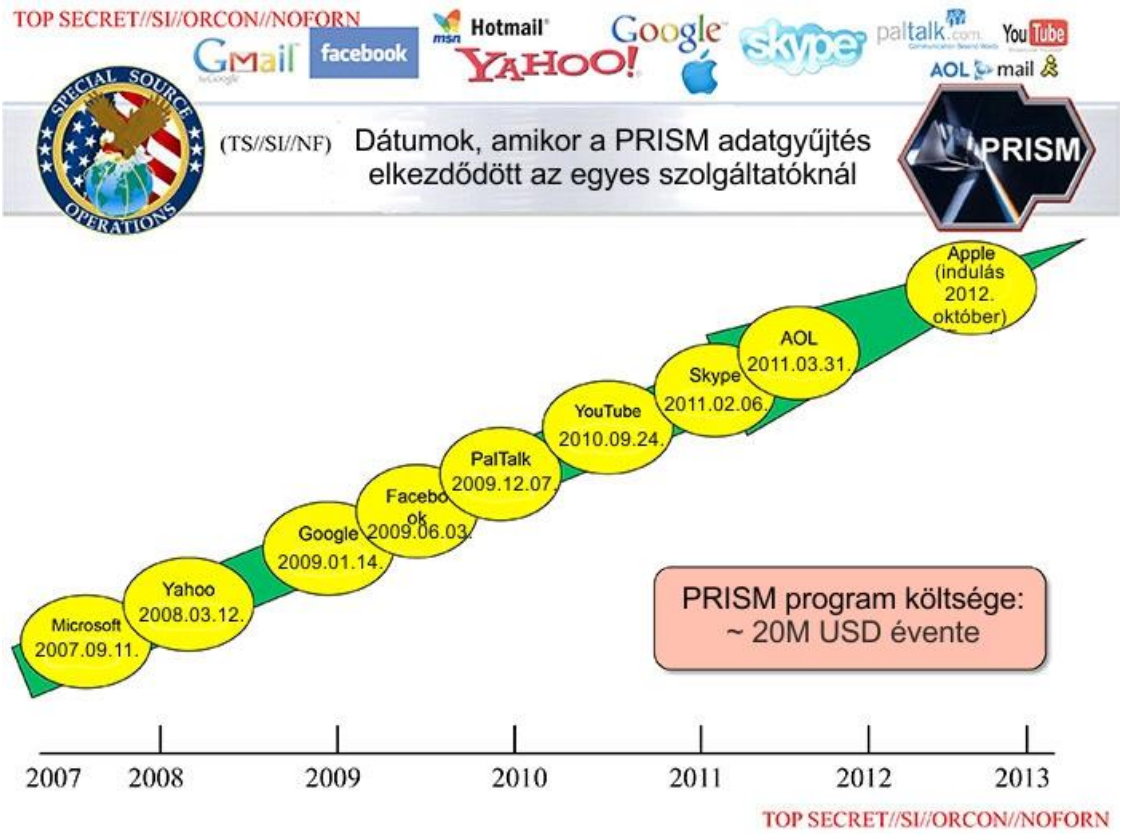
E korlát ellenére az „Öt Szem" országai (USA, UK, Kanada, Új Zéland és Ausztrália) együttműködve használják ezt a technológiát ellenőrzésre, és osztják meg egymás között az így kinyert információkat – a tartalmat és a kísérő ún. metaadatokat egyaránt. [35] [37]

Együttműködés a szolgáltatóval

A szolgáltatóval való együttműködés a hagyományos hírközlési szolgáltatóknál már egy jól ismert és bevált modell szerint működik. Ekkor az ellenőrzést végző szerv eljuttatja a célszemélyhez kapcsolódó releváns adatokat (pl. felhasználónév) a szolgáltató rendszerébe, majd a szolgáltató automatikusan (emberi beavatkozás nélkül) vagy egyedi kiszolgálással (emberi beavatkozással) biztosítja a – rendszerében rendelkezésre álló – kért adatokat, információkat, vagy akár a rajta átfolyó kommunikáció tartalmát is. [34]

Legjellemzőbb példaként itt talán az Egyesült Államok említhető. A Prism programról nyilvánosságra került adatok szerint is. Az ott leírtak szerint 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.) (12. ábra) – szolgáltatónként változó formában és mélységben – férnek hozzá az erre felhatalmazott szolgálatok. [38] Ezt mutatják az 5. és a 6. ábrák.

5. ábra. A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok. [34]



6. ábra. A Prism programban résztvevő szolgáltatók és csatlakozásuk időpontja. [34]

A módszerek összehasonlítása

A fent említett módszerek – a téma szempontjából – legfontosabb előnyei és hátrányai az alábbi táblázatban foglalhatók össze:

1. táblázat. Az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyei, hátrányai.

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
aktív ellenőrző eszköz	• nem csak az éppen folyó forgalmat, hanem a gépen tárolt minden adatot el lehet érni • titkosítás előtti elfogás – azaz a felhasznált titkosítástól függetlenül ellenőrizhető a forgalom	• egyedi ellenőrzés (egy trójai, egy eszköz) • a telepítés problémákba ütközhet • a célszemély minden eszközére kell telepíteni a teljes körű ellenőrzéshez • aktív, ezért működése adott esetben felfedezhető • működése, működő képessége nagymértékben függ a céleszköz beállításaitól, telepített szoftvereitől (pl. vírusirtó, tűzfal) • működése azonnali utasítással nem megszakítható • alapos előkészületek ellenére a képességet egy egyszerű (pl.: vírusellenőrző) frissítés ellehetetlenítheti • jogszabályi háttere nem egyértelmű

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
közbeékelődéses ellenőrzés (MitM)	• bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését (általában SSL, https esetén)	• egyedi ellenőrzés (egy internetforgalomra) • más titkosított forgalmak problémát okozhatnak • viszonylag közel kell menni • több eszköz és netelérés esetén problémás (pl. vezetékes és mobil net) • adott esetben a tevékenység felfedezhető • csak az éppen folyó forgalmat lehet vele megismerni • titkosított forgalom esetében az alkalmazónak szükséges hiteles tanúsítvánnyal rendelkeznie • jogszabályi háttere nem egyértelmű
mély csomagvizsgálat (DPI)	• tömeges – egyszerre több célszemély forgalma is ellenőrizhető • teljesen passzív • tartalom alapú szűrést tesz lehetővé • jogszabályi háttere egyértelmű	• nagy beruházási igény • az egyre növekvő sávszélesség miatt egyre gyorsabb, nagyobb sávszélességű elfogókat kell használni • a titkosítás problémákat okozhat • adott „csatornán” átfolyó forgalmat elemzi, ha nem ott megy a célszemély forgalma, nem fogja el – nem teljes körű • csak az éppen folyó forgalmat lehet vele megismerni

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
együttműködés a szolgáltatóval	• tömeges – egyszerre több célszemély is ellenőrizhető • teljes információkör elérhető, a használt eszközöktől, interneteléréstől függetlenül • nem csak az éppen folyó forgalmat, hanem a szolgáltatónál tárolt minden adatot (pl. piszkozatok) el lehet érni • a szolgáltató által alkalmazott titkosítás nem probléma	• a szolgáltatók nem mindig partnerek, csak jogszabályi alapon működik (hatékonyan) • külföldi szolgáltatók felhasználóinak ellenőrzése esetén ráadásul nemzetközi jogszabályok szükségesek • a célszemély adatait szolgáltató is megismeri – titoktartási, konspirációs gondot okozhat • több szolgáltatót használó célszemélyeknél mindegyikkel együtt kell működni

A fentiek alapján megállapítható, hogy bár az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére technikailag jelenleg többféle módszer is az érintett szolgálatok rendelkezésre áll, ám ezek egyike sem nyújt teljes körű megoldást. Kijelenthető az is, hogy az alkalmazásszolgáltatóval való együttműködés kikerülhetetlen. Ez biztosítja ugyanis, hogy egyszerre több célszemély is ellenőrizhető úgy, hogy az adott szolgáltatáshoz kapcsolódó teljes információkör elérhető az adott szolgálat számára, függetlenül a célszemély(ek) által használt eszközöktől és interneteléréstől. Ez pedig az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési formává teszi.

Ugyanakkor – ahogy korábban Magyarországon is – éppen ennek a módszernek a jogi szabályozottsága kapcsán fellelhető hiányosságok okán, ma a legtöbb ország esetében is kizárólag az alkalmazásszolgáltató jóindulatán múlik, együttműködik-e az ellenőrzést végző szervekkel és teljesíti-e – az egyébként teljesen legális, hatályos és pl. a hírközlési szolgáltatók számára (is) kötelező érvényű bírói végzésben foglaltakat. Éppen ezt a problémát orvosolja, orvosolhatja – az egyébiránt nemzetközi kitekintésben is előremutató – új hazai szabályozás.

ÖSSZEGZÉS

A fentiek alapján megállapítható, hogy a kommunikáció változása a szolgáltatói modell és a törvényes ellenőrzés változását is magával hozta. Bár az elmúlt években megjelent, vagy akár az újonnan megjelenő internet alapú kommunikációs formák törvényes ellenőrzésére az arra felhatalmazott szolgálatok többféle technikai módszerrel, megoldással is rendelkeznek, ám önmagukban ezek egyike sem nyújt teljes körű megoldást. Ugyanakkor a jellemző módszerek előnyeit és hátrányait figyelembe véve elmondható, hogy a szolgáltatóval való együttműködés kikerülhetetlen. Ez utóbbit biztosítják hazánkban a 2016-ban hatályba lépett jogszabályi módosítások. Ezen új szabályozások kereteivel és a – felhasználó szemszögéből megvilágítva – a kommunikáció biztonságára gyakorolt hatásaival foglalkozik a cikksorozat második része.

Felhasznált irodalom

[1] Balog Fatime, Fekete Csanád, Németh András, Németh József Lajos: A hibrid hadviselés különös tekintettel a mobil kommunikációra, in: HADMÉRNÖK X:(4) pp. 120-131. (2015)

[2] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. Hadmérnök. VIII. Évfolyam 1. szám - 2013. március, pp. 233-241. ISSN 1788-1919 Online: http://hadmernok.hu/2013_1_kovacsz.pdf

[3] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 184-197. ISSN 1788-1919 Online: http://hadmernok.hu/133_18_kovacsz_2.pdf

[4] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 198-210. ISSN 1788-1919 Online: http://hadmernok.hu/133_19_kovacsz_3.pdf

[5] Kovács Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2014-4-2.original.pdf (2014.11.27.)

[6] Berta Sándor: Online házkutatásokat indítanának Németországban. 2006. 12. 08. http://sg.hu/cikkek/49079/online_hazkutatasokat_inditananak_nemetorszagban. Letöltés ideje: 2013. 06. 24.

[7] Dajkó Pál: Lebukott az állami kémprogram. 2011. 10. 10. http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html. Letöltés ideje: 2013. 06. 24.

[8] Chaos Computer Club analyzes government malware. 2011. 10. 08. http://ccc.de/en/updates/2011/staatstrojaner. Letöltés ideje: 2013. 06. 24.

[9] Golovanov, Sergey: Spyware. HackingTeam. 2013. 04. 23. http://securelist.com/analysis/publications/37064/spyware-hackingteam/. Letöltés ideje: 2013. 06. 28.

[10] Marquis-Boire, Morgan – Marczak, Bill – Guarnieri, Claudio – Scott-Railton, John: For their eyes only. 2013. 05. 01. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf. Letöltés ideje: 2013. 06. 28.

[11] Rouse, Margaret: spyware. 2006. 10. http://searchsecurity.techtarget.com/definition/spyware. Letöltés ideje: 2013. 07. 16.

[12] Spyware. http://www.spywareguide.com/term_show.php?id=12. Letöltés ideje: 2013. 07. 16.

[13] ehe: Superintendent Trojan. 2006. 10. 09. http://www.h-online.com/security/news/item/Superintendent-Trojan-731613.html. Letöltés ideje: 2013. 06. 28.

[14] Cyberperquisitions. 2008. 02. 28. http://www.lemonde.fr/idees/article/2008/02/28/cyberperquisitions_1016773_3232.html Letöltés ideje: 2013. 06. 28.

[15] Ausztriában törvényes lesz az online házkutatás. 2007. 10. 18. http://sg.hu/cikkek/55658/ausztriaban_torvenyes_lesz_az_online_hazkutatas. Letöltés ideje: 2013. 06. 28.

[16] Berta Sándor: Külföldi szervereket is megtámadhat a holland rendőrség. 2013. 05. 06. http://sg.hu/cikkek/97134/kulfoldi_szervereket_is_megtamadhat_a_holland_rendorseg. Letöltés ideje: 2013. 06. 28.

[17] McCullagh, Declan: FBI remotely installs spyware to trace bomb threat. 2007. 06. 18. http://news.cnet.com/8301-10784_3-9746451-7.html. Letöltés ideje: 2013. 06. 28.

[18] http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf. Letöltés ideje: 2013. 06. 28.

[19] O'Neill, Patrick Howell: Hackers claim to be selling NSA cyberweapons in online auction. 2016. 08. 15. http://www.dailydot.com/layer8/shadow-brokers-nsa-equation-group-hack/. Letöltés ideje: 2016. 08. 28.

[20] Franceschi-Bicchierai Lorenzo: Hackers Say They Hacked NSA-Linked Group, Want 1 Million Bitcoins to Share More. 2016. 08. 15. http://motherboard.vice.com/read/hackers-hack-nsa-linked-equation-group. Letöltés ideje: 2016. 08. 28.

[21] Gardham, Duncan: Government plans to extend powers to spy on personal computers. 2009. 01. 04. http://www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html. Letöltés ideje: 2013. 06. 28.

[22] Sanders, Chris: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1). 2010. 03. 17. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html. Letöltés ideje: 2013. 07. 16.

[23] Sanders, Chris: Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing. 2010. 04. 07. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html. Letöltés ideje: 2013. 07. 16.

[24] Sanders, Chris: Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking. 2010. 05. 05. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html. Letöltés ideje: 2013. 07. 16.

[25] Sanders, Chris: Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking. 2010. 06. 09. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html. Letöltés ideje: 2013. 07. 16.

[26] Fisher, Dennis: What is a Man-in-the-Middle Attack? 2013. 04. 10. http://blog.kaspersky.com/man-in-the-middle-attack/. Letöltés ideje: 2013. 07. 16.

[27] DuPaul, Neil: Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks.

[28] Biddle, Sam: The NSA Leak is Real, Snowden Documents Confirm 2016. 08. 19. https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/ Letöltés ideje: 2013. 07. 19.

[29] Wawro, Alex: What Is Deep Packet Inspection? 2012. 02. 01. http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html. Letöltés ideje: 2016. 09. 28.

[30] Dubrawsky, Ido: Firewall Evolution - Deep Packet Inspection. 2010. 11. 02. http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection. Letöltés ideje: 2013. 06. 28.

[31] BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely. http://berec.europa.eu/doc/2012/TMI_press_release.pdf. Letöltés ideje: 2013. 06. 28.

[32] 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.

[33] Messmer, Ellen: US government's use of deep packet inspection raises serious privacy questions. 2013. 04. 24. http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/. Letöltés ideje: 2013. 06. 28.

[34] 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.

[35] 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.

[36] HTTPS Everywhere. https://www.eff.org/am/https-everywhere. Letöltés ideje: 2013. 06. 28.

[37] 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.

[38] 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.

[39] Man-in-the-middle attack. https://www.owasp.org/index.php/Man-in-the-middle_attack Letöltés ideje: 2013. 07. 16.