Bocsok Viktor, Boldizs Péter Ferenc, Loós Csaba, Major Tamás

A dolgok internete

Technológiai háttér, információbiztonsági és adatvédelmi aspektusok

Absztrakt

Az információs és távközlési technológiák fejlődésével és elterjedésével, az internet közművesedésével a dolgok internete (IoT), illetve annak alapja, a gép-gép közötti (M2M) kommunikáció az infokommunikációs iparág egyik meghatározó, tematizáló kérdéskörévé vált. A rohamléptékű technológiai fejlődés az eszközök összekapcsolásában rejlő kétségtelen előnyök ellenére számos kitettséget eredményez, melyeket kezelni kell. Jelen tanulmányban röviden vázoljuk az IoT fogalmi-technológiai hátterét, illetve bemutatjuk a jelenséggel összefüggésben felmerülő adatbiztonsági (műszaki és jogi) kérdéseket, a fenyegetéseket és az azokra adható lehetséges válaszokat. A személyes adatok mellett vállalati információk, üzleti titkok, vagy akár minősített adatok is kezelhetőek a dolgok internetén. A minősített adatok kezelése az elektronikus adatkezelő rendszerek vonatkozásában kellően szabályozott, míg a vállalati információk, üzleti titkok elektronikus kezelése tekintetében a szerződéses szabadság elve érvényesül. E helyütt alapvetően az információbiztonság és az adatvédelem kérdéskörét jártuk körül, így az előzőekben említett két témakör mélységi vizsgálata nem képzi tanulmányunk tárgyát (noha az általános információbiztonsági követelmények esetükben is azonosak a cikkünkben kifejtettekkel).

Bevezetés

Az Internet of Things (dolgok internete) megnevezést Kevin Ashton, a Procter & Gamble brand managere használta elsőként a kilencvenes évek végén, egy vállalati prezentáció címeként. A hangzatos megnevezés jól illeszkedik az informatikai gondolkodást tematizáló szlogenek (buzzword-ök) sorába[1], ugyanakkor meglehetősen pontosan írja le a kifejezés takarta jelenséget. A tárgyak, rendszerek, eszközök, illetve a tárgyak, rendszerek, eszközök és emberek közötti kommunikáció nem előzmények nélküli, már az internet megjelenése előtt is működtek az összekapcsolt, hálózatba kötött eszközök közötti, külső beavatkozást nem igénylő adat- és információcserét biztosító, valamint az eszközök felől az emberek felé irányuló, az eszköz által kezdeményezett közléseket támogató rendszerek.[2] A címadással Ashton annak a felismerésének adott hangot, hogy a világhálón folyó információcserében az emberiség a gépek mögött a képzeletbeli dobogó második fokára szorul vissza[3].

Lassan meghatározóvá válik az az álláspont, amely az internetre, illetve az internetes szolgáltatásokat kiszolgáló infrastruktúrára, így a szélessávú adatátviteli csatornákra, az elosztott számítási kapacitások, szoftverek használat alapú elérését lehetővé tévő felhőre (cloud) a víz, villanyáram és egyéb erőforrások körébe tartozó közműszolgáltatásként tekint[4]. Ez a jelleg, valamint az informatizáltság fokozódása, az informatika új területeken való megjelenése, a hálózatok bővülése, az adatátvitel és -tárolás fajlagos költségeinek csökkenése, a fejlesztési ciklusok rövidülése, az egyre újabb technológiák és felhasználói elvárások megjelenése a kétségtelen üzleti-gazdasági előnyök mellett új információ- és informatikai biztonsági kihívások megjelenését és a kitettségek számának, az okozható kár mértékének növekedését is eredményezte.

Az IoT fogalmi-technológiai háttere

Az IoT információ- és adatbiztonsági vetületeinek bemutatása megkívánja a témakör tartalmának, határainak kijelölését, fogalmi hátterének megvilágítását. Fontos tehát tisztáznunk azt, mit is értünk a dolgok internete kifejezés alatt, ez pedig az IoT technológiai alapjának megvilágítását is igényli. Terjedelmi korlátokra, valamint a szaktetületen jelenlévő definíciós kavalkádra, a konszenzus hiányára[5] tekintettel e helyütt csak rövid áttekintést adhatunk. Jelen tanulmánynak nem tárgya a definíciók összevetése, vagy a meghatározási próbálkozások feletti ítéletalkotás, ezért a témánk szempontjából leginkább járhatónak tűnő utat választjuk és ott, ahol nincs számunkra megfelelő, kiválasztható fogalom, alkotunk egyet.

A dolgok internetének legjelentősebb alapeleme, szolgáltatási rétege a „dolgok" összekapcsolását, az adatátvitelt, a gép-gép közti kommunikációt biztosító technikai megoldás, átviteli csatorna, melyet a távközlési szaknyelv az M2M (machine-to-machine) megnevezéssel jelöl.[6] Néhány szerző egyenlőségjelet tesz az IoT és az M2M között[7], álláspontunk szerint azonban az M2M és a dolgok internete – mivel utóbbinak maguk a kommunikáló eszközök, rendszerek, alkalmazások és szolgáltatások is a részét képezik – nem tekinthető ekvivalens fogalmaknak, az M2M az IoT szükséges (elő)feltétele, részeleme.[8]A magunk részéről M2M-nek tehát az aktív vég- és köztes berendezések közötti, vezetékes és vezeték nélküli adatkapcsolatokat tekintjük, melyek lehetővé teszik az érintett eszközök közötti információáramlást. Meghatározásunk tágnak tűnhet, mivel nem tekintjük szükséges elemnek ezen kommunikáció teljes vagy részleges automatizáltságát, emberi beavatkozástól mentességét. Ugyanakkor ha ezt tennénk, az M2M kizárólag az autonóm rendszerek primátusa lenne, ezek számossága azonban ma még elenyésző. A kellően tág meghatározás biztosítja számunkra annak lehetőségét, hogy ne kelljen az emberei beavatkozás határait felrajzolnunk (önmagában az adott rendszerelem hálózatba kötése már emberi beavatkozás). Meglátásunk szerint annak megkövetelése, hogy az eszközök aktív félként vegyenek részt a kommunikációban elegendő ahhoz, hogy tisztán M2M adatkapcsolatról beszéljünk.

A dolgok internetére tehát az M2M-et magába olvasztó, azt egyfajta adatátviteli infrastruktúraként használó kategóriaként tekintünk. Az ENSZ távközléssel foglalkozó szakosított szerveként működő ITU (International Telecommunication Union) és az EU részvételével létrehozott IERC (European Research Cluster on the Internet of Things) közösen kidolgozott meghatározását alapul véve az IoT megfogalmazásunkban adatgyűjtésre, -feldolgozásra, -továbbításra alkalmas, nagy varianciát mutató infokommunikációs eszközök olyan, az internettől nem elkülönülő, azt adatátviteli csatornának használó, globális, dinamikus hálózata, mely szabványos és interoperábilis adatkapcsolatokon, protokollokon keresztül biztosítja az eszközök egymás közti, valamint az eszközök és természetes személyek közti információáramlást, függetlenül ez utóbbi céljától és tartalmától. A részes eszközök ugyancsak az IoT elemei. Több fogalmi meghatározás az eszközök összekapcsolását biztosító protokolt a TCP/IP adatkapcsolattal, az ún. internet réteggel azonosítja. Magunk részéről ezt indokolatlan megkötésnek, szűkítésnek tartjuk, hiszen ez esetben kizárnánk a fogalomkörből mindazon hálózatokat, melyek kommunikációjuk során nem, vagy nem kizárólag a TCP/IP protokollstruktúrát használják.[9] Véleményünk szerint az IoT fogalomkörének mindazon hálózatok eleget tesznek, melyek legalább egy olyan interfészszel rendelkeznek, amellyel

biztosított a TCP/IP protokollstruktúrához való illeszkedés. Számos definíció at IoT-vel szembeni, további követelményként jeleníti meg a hálózatba kapcsolt készülékek önkonfigurációs képességét. A magunk részéről ezt sem tekintjük szükségszerű elemnek, mivel a dolgok internetének körébe olyan eszközök is beletartozhatnak, melyek nem rendelkeznek ezen tulajdonsággal. Önmagában az eszközök fizikai létezését sem tekintjük lényeges követelménynek, meglátásunk szerint a virtuális számítógépek és az önálló kommunikációra képes alkalmazások, algoritmusok ugyanúgy a halmaz részegységei, mint fizikailag létező társaik.[10] Az ITU Y.2060 számú ajánlása (Overview of the Internet of Things) az IoT lényegi fogalmi elemének tekinti annak legnagyobb hozzáadott értékét, a dolgok internete által elérhetővé tett új, fejlett szolgáltatásokat is. A magunk részéről ezt, az üzleti szemléletű foglami elemet sem tekintjük szükségszerűnek, hiszen számos, mára már hagyományosnak tekinthető szolgáltatás (így például a távfelügyeleti és nyomkövető rendszerek) is az IoT részét képezik, a dolgok internete nem csak az ún. okos eszközök összefoglaló megnevezése, halmaza.

Fontos megjegyezzük, hogy az ember-gép kommunikáció iránya, illetve természete befolyásolja, hogy egy adott ember-gép adatkapcsolatot, információátvitelt az IoT részének tekintünk, vagy sem. Meglátásunk szerint alapvetően minden olyan információcsere e körbe sorolandó, amely a gép aktív részvételét igényli, így a gép által az ember felé kezdeményezett kommunikáció mindenképp e körbe sorolandó. A fordított esetre, az ember által kezdeményezett kommunikációra azonban csak akkor alkalmaznánk az IoT kifejezést, ha a gép a kommunikáció aktív részeseként jelenik meg, tehát az ember kezdeményezte „párbeszéd" kétoldalúvá válik. A gép-gép közti kapcsolatokat a két passzív eszköz közti passzív adatáramlást is ideértve a dolgok internete részelemeként azonosítjuk.

Az IoT megjelenését a robbanásszerű technológiai fejlődés – és nem meglepő módon - az M2M tartalmi bővülése, az adatátviteli kapacitások bősége, az egy bit átvitelére eső fajlagos költség drasztikus csökkenése indukálta. A kategória elképesztő varianciát mutat, az aktív (szoft)szenzorok, aktuátorok és hálózataik, a telemetriai és telematikai rendszerek[11] éppúgy részét képezik, mint a különböző nyomkövető, azonosító eszközök és alkalmazások, vagy maguk az átviteli protokollok, a sor szinte a végtelenségig folytatható. Az IoT meghatározó fejlesztési területeit[12] elsősorban a ma divatosan okos jelzővel kiegészített, magasan informatizált, illetve automatizált ágazatok, így az ún. okos közlekedés (ezen belül is a közlekedésszervezés, útvonaloptimalizálás és a járműinformatika), az okos energetika (elsősorban a távmérőhálózatok és erőforrás menedzsment rendszerek), az integrált ipari (gyártói és logisztikai), mezőgazdasági munkafolyamat és erőforrás menedzsment (workflow és workforce) rendszerek, az e-egészségügyi távdiagnosztikai és biztonságtechnikai távfelügyeleti alkalmazások és rendszerek, az e-pénzügyi alkalmazások és megoldások, valamint az e-kormányzati szolgáltatások képezik.

A virtualizációs technológián alapuló cloud, vagy számítási felhő sem szükségszerű része a dolgok internetének, ugyanakkor a szakirodalom több helyütt fontosnak tartja a két tárgykör együttes tárgyalását. Az infokommunikációs rendszerek már említett közmű jellegűvé válására, valamint a virtuális eszközök és az – akár felhőből futtatható – alkalmazások IoT körébe vonására tekintettel, a dolgok internete technológiai hátterének részelemeként mi is indokoltnak látjuk a technológia lényegének összefoglalását.[13] A cloud mint fogalom

számtalan meghatározása lelhető fel a szakirodalomban, illetve a felhő létsíkján, a világhálón.[14] Anélkül, hogy e helyütt – a tanulmány tárgyától eltérve – hosszas terminológiai elemzésbe bocsátkoznánk, magunk is megpróbálkozunk egy, a lényegi ismérveket a jogi problémafelvetés szempontjából megragadó definíció rögzítésével. Értelmezésünkben a felhő szolgáltatás a szolgáltató hálózaton keresztül elérhető, magas rendelkezésre állású, a felhő üzemeltetésére (is) dedikált informatikai infrastruktúrájának[15] igény, illetve használat alapú ingyenes, vagy visszterhes bérleti konstrukció keretében, interneten keresztül történő megosztása. A felhő a felhasználók, fogyasztók nagyobb tömegét (publikus felhő), vagy meghatározott fogyasztót (privát felhő) szolgálhat ki.[16] Az erőforrás megosztás jelentkezhet infrastruktúra (IaaS), platform (PaaS), vagy szoftver, mint szolgáltatás (SaaS), továbbá mindezek kombinációja formájában. A számtási felhő számos előnyéből kiemelkedik a nagyfokú skálázhatóság, a szükségletekhez igazodó („on-demand") erőforrás-allokáció lehetősége és a tárolt adatok, információk, használt alkalmazások könnyű elérhetősége, magas rendelkezésre állási szintje. A felhő szolgáltatás jogi szempontból – a kifejezetten táv- és hírközlési célú szolgáltatási kör kivételével[17] – az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény hatálya alá tartozó információs társadalommal összefüggő szolgáltatás, vagyis olyan, elektronikus úton, távollevők részére ingyenesen, vagy ellenérték fejében nyújtott szolgáltatás, melyhez az igénybevevő egyedi hozzáféréssel rendelkezik. A visszterhes szolgáltatás a szolgáltató szempontjából az információs társadalommal összefüggő szolgáltatáson belül elektronikus kereskedelmi szolgáltatásnak minősíthető. A felhő alapú szolgáltatási konstrukció és az alapját képező virtualizációs technológia számos jogi természetű[18] kérdést vet fel, melyek megválaszolása alapvetően határozza meg a technológia alkalmazhatóságát, illetve az alkalmazhatóság kereteit. Tanulmányunk tárgyához igazodva e kérdéskörből – kis kitekintésként – a felhő adatvédelmi sajátosságait emeljük ki.[19]

A számítási felhő szempontjából kiemelt jelentőségű a személyes adatok védelme, tekintve, hogy a felhőben számos szolgáltató kezel, illetve dolgoz fel tömegesen személyesnek minősülő adatokat. A felhő jó példája a technológiai fejlődés eredményezte adatvédelmi kihívásoknak, a normatív szabályozás infokommunikáció által indulkált módosulásának.[20] Az adatvédelem egyik központi kérdése az adatkezelő és az adatfeldolgozó elhatárolása, mely biztosítja az adatvédelmi szabályok betartásáért felelős azonosíthatóságát és támogatja az érintett jogérvényesítését.[21] A felhő egyik – adatvédelmi szempontú – hiányosságának az adatkezelői és feldolgozói szerepkör elkülöníthetőségének, illetve a feldolgozási láncolatok átláthatóságának (az adatot ki, mikor és milyen folyamat keretében, milyen módon kezeli) hiányát szokás felemlíteni.[22] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) definiálja, ki tekintendő adatkezelőnek, illetve feldolgozónak, meghatározza továbbá az adatkezelés és a feldolgozás tartalmát is. Az adatkezelés az adaton végzett műveletek összességét jelenti,[23] míg utóbbi körbe – az alkalmazott eszközöktől és módszerektől függetlenül – az adatokkal végzett technikai intézkedések tartoznak, a puszta infrastruktúra biztosítása, illetve birtoklása tehát nem tekinthető adatfeldolgozásnak.[24] Bonyolítja a helyzetet, hogy a felhő alapú szolgáltatások esetében sokszor keverednek a szerepkörök, az adatfeldolgozók bizonyos adatok tekintetében adatkezelőként működnek,[25] mely adott esetben az Infotv. 10. § (3) bekezdésében rögzített saját célú adatfeldolgozás tilalmának megsértését eredményezheti.[26] Meglátásunk szerint a felhő alapú szolgáltatások elterjedését akadályozó al-, vagy másként további adatfeldolgozás

tilalmának felülvizsgálatához hasonlóan[27] életszerűbb lenne az Infotv. rendelkezéseinek releváns gyakorlathoz igazítása, a 10. § (4) bekezdésében rögzített tilalom[28] törlése, vagy garanciális elemekkel való bővítése.[29] A magunk részéről az adatkezelő és adatfeldolgozó külön jogalanyiságát sem követelnénk meg.[30] A felhő vonatkozásában, az adatvédelem kapcsán az adatkezelő és adatfeldolgozó elhatárolásának nehézségei mellett a technológia sajátosságaiból adódó – elsősorban műszaki, adatbiztonsági – kockázatokat szokás kiemelni, így a szolgáltatónak való kiszolgáltatottságot, a „beszorulás" lehetőségét (lock-in)[31], a virtualizációból, izolációs hibákból adódó sérülékenység, az esetleges adatkeveredés, az eltérő szolgáltatási rétegek kompromittálódásának lehetőségét,[32] a szolgáltatási rétegekre irányadó adatvédelmi irányelvek megismerése problémásságát,[33] a felejtéshez való jog[34] érvényesíthetőségének nehézségeit, az adatok feletti rendelkezés elvesztésének lehetőségét, az adatkezelés folyamata feletti érintetti ellenőrzés korlátozottságát (loss of governance),[35] valamint a szolgáltatások határokon (és nemzeti szabályozásokon) átnyúló jellegét. A fenti kockázatokat a szabályozás módosításával, egységesítésével, az érintettel kötendő adatvédelmi megállapodások kötelező tartalmának megállapításával, a szolgáltatók önszabályozásával,[36] illetve az adatbiztonságot szavatoló technológiai védelmi és szervezési intézkedések bevezetésével lehet és kell kezelni. Természetesen a fent tárgyalt kitettségek kizárólag azon adatok vonatkozásában merülnek fel, melyek személyes adatnak minősülnek, így kapcsolatuk az érintettel az adatkezelő által helyreállítható.[37] Nem vitatva azt a tényt, hogy a számítási felhő valóban adatvédelmi kihívást jelent, a „hagyományos" adatfeldolgozási tevékenység kiszervezésével szemben lényeges különbséget csupán a körben vélünk felfedezni, hogy a felhő az interneten, hálózati infrastruktúrában működik, amely az adatáramlást lényegesen könnyebbé, a tényleges feldolgozási tevékenység pontos (fizikai) helyének és folyamata alakulásnak (a feldolgozás lépéseinek) meghatározását pedig nehezebbé teszi.

A fentieket összegezve a dolgok internetét adatgyűjtésre, -feldolgozásra, -továbbításra szolgáló fizikai és – a számítási felhőben működő – virtuális eszközök az internetet adatátviteli csatornaként használó globális, dinamikus hálózataként azonosítjuk, mely szabványos, interoperábilis adatkapcsolatokon, protokollokon keresztül valósítja meg az eszközök egymás közti aktív és passzív (M2M), valamint az eszközök és személyek közti aktív kommunikációt. A hálózat részeként definiáljuk magukat a kapcsolódó eszközöket is.

Információbiztonsági aspektusok

A releváns fogalmi-technológiai háttér – kis kitekintéssel történő – tárgyalása után további vizsgálódásunkat az IoT információ- és adatbiztonsági vetületei irányában folytatjuk. Mielőtt azonban elmélyednénk a kérdésben, tisztáznunk szükséges az információbiztonság, az informatikai biztonság, az adatvédelem és az adatbiztonság fogalmak tartalmát és kapcsolódási pontjait.

A biztonság általánosan megfogalmazva nyugalmi állapot, fenyegetettségmentesség, illetve a fenyegetettségekkel szembeni védettség megfelelő szintje. Az információbiztonság az ISO mértékadó, a témakört feldolgozó 27000-es szabványcsaládja értelmében az információ, azaz az új ismeretet hordozó adat bizalmasságának, sértetlenségének és rendelkezésre állásának[38] megőrzését, illetve, egyéb olyan tulajdonságokat jelöl, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság. A fogalom nem tartalmaz megkötést az információ

formátuma, illetve megjelenési formája tekintetében. Az informatikai biztonság ennél szűkebb kategória, mivel kizárólagosan az informatikai rendszerek számára értelmezhető adatok (és maguk a rendszerek) bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését értjük alatta.[39] Kommunikációelméleti oldalról az adat az információ részegysége, építőköve, ugyanakkor az információbiztonság és az adatvédelem bár illeszkedő, de nem szinoním fogalmak. Az adatvédelem a nemzetközileg használt – és ezzel egyezően a hazai – terminológiában a személyes adatok védelmét, a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapjáról elérhető megfogalmazás[40] alapján a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét jelenti. Az információbiztonsághoz hasonlóan a fogalom nem tartalmaz megkötést az adat megejelenési formája vonatkozásában. Az adatbiztonság fogalmának meghatározása érdekében az Infotv. vonatkozó passzusához[41] nyúlunk vissza, mely alapján a terminus technicus a személyes adatokhoz való jogosulatlan hozzáférést, az adatok megszerzését, továbbítását, nyilvánosságra hozatalát, megváltoztatását, törlését vagy megsemmisítését, felhasználását, véletlen megsemmisülését és sérülését, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válását, valamint minden az adat bizalmasságát, sértetlenségét és rendelkezésre állását sértő vagy veszélyeztető cselekmény és esemény bekövetkezését kizáró, megakadályozó szervezési és technikai megoldások, eljárások eredményeként előálló olyan állapotot jelöl, melyben biztosított az adatok, valamint az érintett magánszférájának fenti kitettségekkel szembeni védelme. E körben sem meghatározott a védendő személyes adatok megjelenési formája. Az elektronikus formában létező adatok tekintetében, az adatbiztonság körében a jogszabály további követelményként rögzíti a különböző nyilvántartásokban kezelt adatok törvényi felhatalmazás hiányában történő összekapcsolhatóságának kizárását. A hivatkozott szakasz (5) és (6) bekezdései további adatbiztonsági követelményeket támasztanak az automatizált adatkezeléssel szemben. [42] Fontos megjegyezzük, hogy a fenti kategóriák közül az adatvédelem jogi, míg az információ-, informatikai és az adatbiztonság technológiai jellegű védelmet jelent.

Az (új) infokommunikációs technológiák sokszor természetükből adódóan sajátos (információ) biztonsági kihívásokat hordoznak, ez alól az IoT sem tekinthető kivételnek, így vonatkozásában is felmerülnek mindazon kitettségek, melyek a hálózatba szervezett informatikai és – informatikai eszközökön alapuló – távközlési rendszerek tekintetében jelentkeznek. Az e körben felmerülő, eltérő indíttatású, de hasonló károkozásra képes, jellemzően aszimmetrikus[43] fenyegetések közé többek között a kiberbűnözés, a továbbított, illetve feldolgozott információk megszerzését célzó ipari/gazdasági kémkedés, az adatok manipulációját, törlését célzó szabotázs, a kiberterrorizmus, valamint a hacktivista mozgalmak tartoznak. A kiberbűnözés fogalmába a hekkertámadások – a szolgáltatásmegtagadással járó DDoS támadásoktól, [44] az információs rendszereket érintő célzott információszerző, törekvéseken,[45] a személyazonosság ellopását célzó, adathalász bűncselekményeken[46] át a vírusok, egyéb kártevők, malware-k terjesztéséig és felhasználásáig[47] terjedő – széles körét beleértjük. Az ipari, illetve gazdasági kémkedés célja gazdasági versenyelőnyt biztosító információk megszerzése, háttere állami és vállalati egyaránt lehet. Az akár személyes, vagy különleges, így például egészségügyi adatokat tartalmazó, piaci értékkel bíró adatbázisok[48] megszerzése éppúgy kellően motiválható lehet egy ipari kém számára, mint mondjuk a vezető beosztású munkavállalók jogellenes befolyásolását célzó információk, személyes adatok

megszerzése.[49] A szabotázs jellemzően az adatok integritásának sérülését eredményező szándékos magatartás, mely például az adatbázisok adattartalmának módosításával, részleges törlésével ugyancsak jelentős károkat okozhat egy társaság működésében, vagy akár egy adott személy életében.[50] A kiberterrorizmus, valamint a hacktivista tevékenységek[51] leginkább céljukat tekintve különíthetőek el a kiberbűnözésen belül. E tevékenységek mögött jellemzően a nemzetközi szervezetek, államok, illetve szerveik befolyásolásának szándéka húzódik meg.

Természetesen nem csak szándékos magatartások veszélyeztethetik az információbiztonságot, hasonló kitettségként jelentkeznek a természeti csapások, sztrájk, vagy – okától függetlenül – a szolgáltatás, illetve ellátási lánc kiesések, a programozási, paraméterezési, üzemeltetési hibák, kompatibilitási, interoperabilitási [52] problémák is. Sajátos, technológiai eredetű kitettségek adódnak az IoT jellemzőiből, illetve a dolgok internetének alapját képező M2M technológiából. Problémát jelenthet a mobileszközök, kommunikációs interfészek beágyazottsága, [53] illetve az ennek következtében jelentkező szervizelési, hibajavítási, fejlesztési nehézségek felmerülése. Ugyancsak gondot okoz a mobileszközök jelentős hányadának a hálózati betáplálásnál alacsonyabb feszültségigénye, a saját áramforrások korlátos energiatárolási kapacitása, valamint az eszközök egy részének limitált funkcionalitása. Az elképesztő fejlődés eredményezte heterogén eszközháttér bizonyos szempontból növeli a védekezés hatékonyságát, több rendszer ismeretét követelve meg egy támadótól, [54] ugyanakkor viszont az üzemeltetés mellett a biztonságot is veszélyeztető kompatibilitási problémákat okozhat, hiszen a beszállítók varianciájából adódóan akár egy adott készüléktípus generációi is jelentős műszaki eltéréseket hordozhatnak. A heterogenitás kizárja az egyenszilárdságú védelem [55] elérését, megnehezíti a rendszerek megfelelő megerősítését (patch- és frissítés menedzsmentjét,[56] mely különösen az IoT szempontjából igen releváns ipari folyamatirányító- és vezérlőrendszerek [57] esetében jelent komoly termelésfolytonossági kihívást), az adatkapcsolatok rétegzettsége okán ráadásul adott esetben a mélyebb rétegekhez, az azokhoz tartozó alkalmazásokhoz, adatátviteli csatornákhoz való hozzáférés is elegendő (gondoljunk csak bele, milyen kitettséget jelenthet egy alsószintű alkalmazás 0. day hibája,[58] vagy nem megfelelő frissítése). A számítási felhőnél már említett transzparnecia-hiány, valamint a virtualizációból adódó biztonsági problémák ugyancsak kezelendőek, ahogyan az adatátviteli utak kockázatarányos védelmét, biztonsági megfelelőségét is szavatolni kell, szükség esetén a titkosítását is meg kell oldani (hiszen az eszközök közötti kommunikáció lehallgatása, vagy akárcsak megfigyelése[59] igen jelentős veszélyforrás). Távközlési szempontból további, áttételesen az információbiztonságot is befolyásoló kihívást jelent a csatlakozó eszközök számossága, mely azonosítási, címzési (számozási) problémákhoz[60] vezethet, illetve a több országon, régión átnyúló, a piacok töredezettségéből és szigetszerűségéből eredő interoperabilitási és roaming problémák. Természetesen a jelzett információbiztonsági kitettségek nem eredményezhetik a IoT teljes kiesését, vagy lebénulását, mint ahogyan az sem tekinthető nagy bekövetkezési valószínűségű kockázatnak, hogy valaki a teljes internetet megbénítsa. Az egy felhasználási fókuszba tartozó, összekapcsolt rendszerek, vagy az egyes eszközök és hálózataik esetében a felvázolt fenyegetettségek azonban reális kockázatként értékelhetők.

Az IoT egyes részhalmazainak interdependenciájára,[61] a rész-egész, illetve a leggyengébb láncszem elvek érvényesülésére,[62] a kitettségek átgyűrűző hatására, azaz a dominó hatás bekövetkezésének lehetőségére tekintettel érdemes megvizsgálni az érintett infrastruktúrák

kritikusságának kérdését. Mint a fogalmi meghatározásból láthattuk, bármely olyan infokommunikációs hálózat, rendszer, illetve eszköz a dolgok internetének részét képezheti, amely adatgyűjtésre, feldolgozásra, továbbításra alkalmas, szabványos és interoperábilis adatkapcsolatokon, protokollokon keresztül biztosítja az eszközök egymással és természetes személyekkel bonyolított információcseréjét. Ebben a körben olyan részelemek is megtalálhatóak, melyek a védelemtudomány és a jog meghatározása szerint ún. kritikus infrastruktúrának (létfontosságú rendszernek, vagy rendszerelemnek), pontosabban kritikus információs infrastruktúrának minősülhetnek.[63]

Az európai és nemzeti jogrendben a létfontosságú rendszerré, vagy rendszerelemmé minősítésnek természetesen jogszabályi feltételei vannak, azaz hazánkban a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben foglalt feltételeknek teljesülnie kell. A hivatkozott norma rendelkezéseinek megfelelően a létfontosságú rendszerelemként kijelölt infrastruktúra elemeknek (legalább) az érintett ágazatok egyikébe kell tartozniuk, azaz meg kell felelniük az ún. ágazati kritériumoknak, [64] továbbá elengedhetetlenül szükségesnek kell lenniük a létfontosságúnak tekintett társadalmi feladatok [65] ellátásához. Tartalmi szempontból a rendszerelem kritikussága elsősorban potenciális kiesésének – emberi életre, egészségre, a gazdasági és társadalmi folyamatokra, a természetre és az épített környezetre – gyakorolt hatásában jelenik meg. Fontos tényező továbbá a kiesés (működési zavar, vagy szolgáltatás lehetetlenülés) térbeli és időbeli kiterjedtsége is.[66]

Miért fontos a kritikus infrasturktúrákra irányadó szabályozás említése? A jogszabály az üzemeltetők számára előírja a kritikus infrastruktúrák védelmének kötelezettségét, mely védelem a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség[67] enyhítésére vagy semlegesítésére irányuló tevékenységek összességét jelenti. Az állam a védettséget szükség esetén az adott rendszerelem létfontosságúvá minősítésével (a kijelölés kikényszerítésével), adminisztratív kötelezettségek előírásával (szabályozók, eljárásrendek, intézkedések megkövetelésével), bírság kiszabásával ki is kényszerítheti. A védelem a dolgok internete létfontosságúnak minősített elemeit is megilleti.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) célként fogalmazza meg a hatálya alá tartozó[68] elektronikus információs rendszerek és az azokban kezelt, tárolt és feldolgozott adatok zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítását, valamint az ún. PreDeCo elv [69] érvényesítésével a lehetséges biztonsági események (incidensek) bekövetkezésének megelőzését, a rendszerek védettségének folyamatos fenntartását és a már bekövetkezett biztonsági események kezelését. A törvény biztonsági eseménynek mindazon nem kívánt vagy nem várt eseményeket, vagy azok sorozatát tekinti, amelyek az elektronikus információs rendszerekben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéznek elő, és amelyek hatására az elektronikus információs rendszerben kezelt, tárolt adatok és információk bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. A norma hatálya az állami szervekre és rendszereikre, az ún. nemzeti elektronikus adatvagyonra, [70] az ezt kezelő rendszerekre, illetve a korábban tárgyalt, létfontosságú rendszerelemnek minősített rendszerekre, valamint a közösségi vagy nemzeti

forrásból megvalósított beruházásokra terjed ki. A kockázatarányos és költséghatékony védelem érdekében a rendszereket biztonsági osztályba kell sorolni[71] a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, illetve gondoskodni kell azok besoroláshoz illeszkedő adminisztratív, fizikai és logikai védelméről. A jogszabály elektronikus információs rendszernek többek között az adatok, információk kezelésére használt eszközöket, számítástechnikai rendszereket és hálózatokat, eljárásokat, valamint az ezeket kezelő személyek együttesét tekinti. A rendszerek körében nevesítetten megjelennek az automatizálási, vezérlési és ellenőrzési (adatgyűjtő, távmérő, távérzékelő és telemetriai) azaz a dolgok interneteként azonosított rendszerek is.

Az Ibtv. az adatkezelő, adatfeldolgozó, illetve az adatkezelés és feldolgozás fogalmát az Infotv-ből emelte át, a norma személyi hatályát rögzítő szakasz[72] (2) bekezdése azonban – egyfajta adatkezelői láncolatot felállítva[73] – kissé nehezíti a tisztánlátást. Az Ibtv. iktatta ki az Infotv-ből a további adatfeldolgozás tilalmát, megjegyzendő ugyanakkor, hogy a (2) bekezdés b) pontjában rögzített hatásköri rendelkezés megfogalmazása alapján az adatkezelés is kiszervezhető. Az adatkezelés, mint tevékenység az adatkezelés céljának meghatározását, valamint az adatkezelésre vonatkozó döntések összességének meghozatalát, végrehajtását fogja össze. A döntésekhez kapcsolódó technikai feladatok végrehajtása már az adatfeldolgozás körébe tartozik, ugyanakkor az adatkezelés az adatfeldolgozást is magában foglalhatja, az adatfeldolgozó igénybevétele nem szükségszerű, kötelező elem. Az Infotv. ismeri és lehetővé teszi az együttes adatkezelést,[74] ez azonban a döntéshozatalban még akkor is párhuzamosságot, közös akaratot és nem alá-fölé rendeltséget, a döntési jog átruházását jelenti, ha a cél és mód meghatározásában az együttes adatkezelők eltérő arányban is részt vehetnek, vagy adatkezelési kapcsolatuk laza, eseti. Indokolt lenne a jogszabályhely Infotv-hez igazítása, ez azonban szükségessé teszi annak vizsgálatát, hogy a hatásköbe vont szervezetek esetében meghatározható-e közös adatkezelési cél.[75] Amennyiben nem, úgy – a releváns gyakorlatot is figyelembe véve[76] – az adatkezelés minden szervezet esetében önállónak, az együttműködés pedig a két fél közti adatátadásnak minősül. [77]

Az Ibtv. kiemelt jelentőséget tulajdonít a személyes adatokat kezelő rendszerek, illetve az adatállományok technikai védelmének, adatbiztonsági megfelelőségének. A törvény 16. § (4) bekezdése alapján a kormányzati eseménykezelő központ[78] személyes adatok sérülésével járó súlyos biztonsági esemény[79] bekövetkezése, vagy az ezzel közvetlenül fenyegető helyzet fennállása esetén az adatkezelőket, illetve feldolgozókat kötelezheti az esemény megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedések megtételére. Az információbiztonsági (technológiai) és adatvédelmi (jogi) aspektusok illeszkedésének példájaként – és az IoT eddig nem tárgyalt adatvédelmi vetületeire való átvezetésként – meg kell említenünk az Infotv. egyik új jogintézményét, a 2015. október 1-től hatályba lépő rendelkezésekkel törvénybe illesztett adatvédelmi incidens fogalmát. Az adatvédelmi incidens voltaképp az adatbiztonság követelményének[80] sérülését, a személyes adat jogellenes kezelését vagy feldolgozását jelenti. Az incidens bekövetkezéséhez önmagában az adatkezelés jogellenessége elegendő, nem szükséges, hogy az érdeksérelmet, illetve kárt okozzon, vagy, hogy haszonszerzési célra irányuljon. Az új jogintézmény kiegészíti a személyes adatok védelmének rendszerét, előírva a személyes adattal visszaélés[81] törvényi tényállását ki nem merítő incidensek nyilvántartásának, illetve az érintett tájékoztatásának kötelezettségét is (tekintve, hogy a büntetni rendelt cselekmények is

adatvédelmi incidensek).[82] Az incidensek és az elhárításukra tett intézkedések nyilvántartása megkönnyíti az érintett esetleges kártérítési, illetve sérelemdíj megfizetésére irányuló igényének érvényesítését.[83] Az adatvédelmi incidens kategóriája bővebb a korábban már említett, Ibtv. szerinti biztonsági esemény (azaz a voltaképpeni informatikai incidens) körénél, mivel előbbi az adatbiztonsági szempontból nem kifogásolható, de jogellenes[84] adatkezelésre is kiterjed. Az eltérést a szabályozási célok és irányultság különbözősége eredményezi.

Adatvédelem és a dolgok internete

Az infokommunikációs hálózatok igénybevételével történő, akár földrajzi határokat átlépő kommunikáció, adattovábbítás, -tárolás és -feldolgozás kapcsán szükségszerűen viszgálandó az adatvédelem kérdésköre. Szakcikkünkben – a tárgykörök illeszkedése okán – több helyütt tárgyaltunk már adatvédelmi kérdéseket, így kitértünk az adatkezelő és az adatfeldolgozó, illetve az adatkezelés és adatfeldolgozás elhatárolására, bemutattuk továbbá az Infotv. egyik új jogintézményét, az adatvédelmi incidenst. Tanulmányunk fókuszára tekintettel azonban az IoT adatvédelmi vetületei még további vizsgálatot, illetve kifejtést igényelnek.

Ahogyan azt a foglami meghatározások is mutatják, a dolgok internete esetében az információcsere folyamatában közlő félként többnyire nem természetes személyek, hanem eszközök, gépek vesznek részt, sőt maga az információs folyamat is jellemzően automatizált, nem igényel közvetlen emberi beavatkozást. Ez ugyanakkor nem jelenti azt, hogy a gépek közti kommunikációban nem kerülhet sor személyes adatok (akár különleges, vagy egészségügyi adatok) kezelésére, feldolgozására, még akkor sem, ha az Infotv. a természetes, vagy jogi személyeket, jogi személyiséggel nem rendelkező szervezeteket tekinti adatkezelőnek. A fenti kitétel, mivel az adatkezelő az, aki az adatkezelés célját meghatározza, alapvetően nem kellene, hogy problémát jelentsen, ugyanakkor a jogalkotó a fogalmat az adatkezelési döntések meghozatalával és végrehajtásával is kibővíti, mely feladatokat ma már egy gép (nem is feltétlenül mesterséges intelligencia), akár külső, közvetlen emberi beavatkozás nélkül, önállóan, vagy más adatkezelőkkel együttesen is képes megvalósítani. Az adatkezelés törvényi fogalmában szereplő „adatokon végzett bármely művelet” kitétel tekintetében a norma szövege nem ad iránymutatást. A korábbi adatvédelmi törvény indokolása szerint az adatkezelés az elképzelhető intézkedések teljes vertikumát átfogja, a jogszabály a technológiasemleges, tevékenység-központú megközelítéssel annak lehetőségét kívánja kizárni, hogy technikai megoldásokkal, újításokkal megkerülhető legyen a rendelkezések betartása. Mint látjuk, bár nem taxatív felsorolásról beszélünk, a törvényszövegben a jogalkotó néhány intézkedést kiemelt. A kiemelés az adat életciklusát alapvetően befolyásolni képes, illetve az adat integritása, vagy az adattest tulajdonosa (az érintett) által az adatkezelésre kifejthető befolyás szempontjából jelentős kockázatot hordozó intézkedéseket fogja át. Az adatkezelő feladatát képező adatkezelés definíciója[85] hivatkozott példálózó, nem konjunktív felsorolása körében több olyan elemet is rögzít, melyeket a technika jelen állása szerint is képesek eszközök autonóm módon végrehajtani.[86] E helyütt ismét felmerül a kérdés, mit tekintünk közvetlen emberi beavatkozástól mentes működésnek. A közvetett beavatkozás könnyen értelmezhető, az eszközöket emberek kötik hálózatokba és paraméterezik, az algoritmusokat is emberek írják, ugyanakkor a Neumann-elvek szellemében már a programokat is közvetlen emberei beavatkozás nélkül működő autonóm egységeknek

tekinthetjük.[87] Be kell lássuk, napjainkra az eszközök kiléptek az adatfeldolgozás, azaz a technikai feladatellátás szerepköréből.

Ezen körülmény az Infotv. adatkezelő fogalmának felülvizsgálatát, kibővítését teszi szükségessé. Meglátásunk szerint az adatkezelő fogalmának jelenlegi tartalmát – a jogi felelősség érvényesíthetősége, illetve a jogi védelem biztosítása érdekében – indokolt kiterjeszteni azon természetes, vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre is, akik az adatkezelés céljának meghatározására, illetve az adatkezelést érintő döntések meghozatalára és végrehajtására, adatfeldolgozókkal történő végrehajtatására önállóan vagy másokkal együtt alkalmas és képes berendezést, információtechnológiai eszközt, vagy rendszert üzemeltetnek,[88] adatkezelésre alkalmas ilyen berendezéssel, eszközzel vagy rendszerrel rendelkeznek, üzemeltető, vagy rendelkezési jogosult hiányában pedig aki(k)nek az érdekében a berendezés, eszköz vagy rendszer működik. A berendezés, eszköz, illetve rendszer üzemeltetője, rendelkezési jogosultja, vagy az, akinek érdekében a berendezés, eszköz, vagy rendszer működik, a berendezés, eszköz, illetve rendszer által hozott adatkezelői döntésekért, intézkedésekért úgy felel, mintha maga járt volna el, továbbá – amennyiben a berendezés, eszköz vagy rendszer arra önállóan nem képes[89] – köteles mindazon intézkedések végrehajtására, melyeket az Infotv. az adatkezelő számára előír. Az adatvédelmi nyilvántartásra irányadó rendelkezések [90] ugyancsak kibővítendőek, az adatkezelést végző eszköz azonosításra alkalmas adatainak, illetve azon technikai intézkedésnek a megjelölésével, amelyek biztosítják, hogy az elektronikusan kezelt adatállományok, nyilvántartásban tárolt adatok – törvény eltérő rendelkezése hiányában – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. A nyilvántartásba vételt az üzemeltető, ennek hiányában a rendelkezési jogosult, illetve az köteles kezdeményezni, akinek érdekében a berendezés, eszköz vagy rendszer működik.

A dolgok internetéhez tartozó adatgyűjtő eszközök, szenzorok működésük során több adatforrásból gyűjthetnek adatokat. Ezen adatok lehetnek passzív[91] és aktív gépi, ezen belül is ember üzemeltette, vagy autonóm működésű gépek [92], illetve közvetlenül ember által generált[93] adatok. Az adatvédelem – és jelen szakcikkünk – szempontjából természetesen csak az lényeges, hogy ezen adatkörből mi minősül személyes adatnak. Az Infotv. a személyes adatok körét széles körben határozza meg, az érintettel kapcsolatba hozható adatok teljességét (értve ez alatt az egyén azonosságára jellemző ismereteket is), valamint az azokból levonható következtetéseket[94] egyaránt e kategóriába sorolja be.[95] A személyes adatok terjedelmének jogszabályi meghatározása erősíti azon megállapításunkat, hogy a dolgok internete tárgyalása szempontjából indokolt az adatvédelmi kérdések tisztázása (több helymeghatározó, illetve telematikai rendszer gyűjt olyan adatokat, melyekből természetes személyekre vonatkozó következtetések vonhatók le, az e-egészségügyi rendszerekről nem is beszélve). Az Infotv. értelmében az adat mindaddig megőrzi személyes minőségét, amíg kapcsolata az érintettel az adatkezelő által helyreállítható, azaz az adatkezelő rendelkezik a helyreállítás technikai lehetőségével. Több technológiai, illetve eljárásrendi megoldás is létezik, melyekkel a dolgok internetén is biztosítható az érintettel való kapcsolat helyreállíthatóságának kizárása. Az eljárásrendi megoldások körébe tartozik például a kapcsolati kódok képzésével történő adatfelvétel, rögzítés és tárolás,[96] míg technológiai megoldás lehet az adatok anonimizáló algoritmusokkal történő átdolgozása,[97] vagy az adatállományok aggregálása.[98] Az érintettel való összekapcsolás lehetőségének kizárása esetén az adat elveszti személyes jellegét, így már

nem igényli a személyes adatok megóvásához fűződő jogi védelmet.

Nem lennénk kellően körültekintőek, ha nem jeleznénk, hogy az Infotv. a már tárgyalt adatbiztonsági követelmények mellett – technológiasemlegességre törekedve – a gépi adatfeldolgozás kérdését (automatizált adatfeldolgozás megnevezésel[99]) is szabályozza. A norma rendelkezései értelmében az automatizált adatfeldolgozás során az adatkezelőknek és -feldolgozóknak olyan intézkedéseket kell bevezetnie, melyekkel megakadályozható a jogosulatlan adatbevitel, a rendszerek adatátviteli berendezés segítségével történő jogosulatlan használata, ellenőrizhető és megállapítható az adattovábbítások (lehetséges) címzettje, az adatok bevitelének időponjta és az adatrögzítő személye, biztosítható a rendszerek üzemzavar esetén történő helyreállíthatósága, valamint a fellépő hibák rögzítése. A dolgok internete fogalommeghatározása alapján az IoT körébe az automatizált adatfeldolgozás rendszerei besorolhatók.

Tényként rögzíthető, hogy az adatok – különösen az elektronikus formában létező adatok – és információk kompromittálódása nagyfokú látenciával párosulhat, hiszen az adat, illetve az információ az az erőforrás, melynek integritása, bizalmassága úgy is megsérthető, hogy a rendelkezésre jogosult azt nem, vagy nem azonnal észleli. Ezen sajátosságra is tekintettel írja elő a jogszabály az adatkezelőnek, illetve tevékenységi körében az adatfeldolgozónak az adatok biztonságáról való gondoskodás, valamint mindazon technikai és szervezési intézkedések megtételének és mindazon eljárási szabályok kialakításának kötelezettségét, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat az információbiztonság hármas követelményével (bizalmasság, sértetlenség, rendelkezésre állás) megegyezően különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen kell védeni. Mint arra már kitértünk, az elektronikusan kezelt adatállományok esetében megfelelő technikai megoldással azt is biztosítani kell, hogy a nyilvántartásokban tárolt adatok – törvény eltérő rendelkezése hiányában – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. Az Infotv. az adatbiztonsági követelményekre irányadó fenti előírások körében fogalmazza meg az ún. privacy by design, a tervezésbe épített adatvédelem követelményét. A jogintézmény értelmében az érintettek magánszférájának védelmét szavatoló adatvédelmi biztosítékokat már a termékek, szolgáltatások, működési struktúrák (így az IoT) és eljárások megtervezésekor érvényesíteni kell.[100]

Az információs hálózatok igénybevételével történő adatkezelés kiemelt – a számítási felhőnél már említett – kockázata az adatok feletti rendelkezés (a tiltakozás, felejtés joga) elvesztésének lehetősége. Az IoT sajátosságából adódóan ténylegesen előfordulhat, hogy az adatokat egyidejűleg akár több példányban, eltérő földrajzi elhelyezkedésű és jogi berendezkedésű, kultúrájú országban, vagy akár kontinensen működő eszközök, illetve rendszerek kezelik, tárolják, érik el, dolgozzák fel. Megvan tehát annak a lehetősége, hogy az Unió, vagy az Európai Gazdasági Térség egyik részes államában, így hazánkban működő telemetriai eszköz, szenzor által gyűjtött adat, több ország aktív adattovábbító, -elosztó berendezésén keresztül, egy, az Egyesült Államokban működő adatfeldolgozó berendezés útján orosz, kínai, esetlegesen észak-afrikai, vagy ausztrál szerverre, az ott lévő adatállományba kerül feltöltésre.[101] Mivel a terület mellett az időbeliség is folyamatosan

változhat, azaz adott időpillanatban más és más lehet az adat státusza, feldolgozottsága és tárolási helye, meglehetősen körülményes, vagy éppen lehetetlen az adattulajdonos (érintett) rendelkezési jogosultságának egyenszilárdságú gyakorlása, az előzetes tájékoztatáshoz való jog érvényesítése. A hatályos magyar adatvédelmi norma megoldást ad e problémára, mivel a személyes adatok védelmére irányadó szakaszainak hatálya, annak módjától függetlenül a Magyarország területén folytatott valamennyi adatkezelésre és feldolgozásra kiterjed. A törvényi előírásokat abban az esetben is alkalmazni kell, ha az adatfeldolgozás során belföldi eszközt vesznek igénybe, kivéve, ha a berendezés, vagy eszköz kizárólag az EU-n átmenő adatforgalom megvalósítására szolgál.

Mint azt a cloud esetében is láttuk, az adatkezelési folyamatok átláthatóságának, illetve az átláthatóság hiányának kérdése valamennyi internet alapú infrastruktúrát használó megoldás, alkalmazás tekintetében felmerül, ez alól az IoT sem képez kivételt. A korábban tárgyalt információbiztonsági kockázatok érintett általi átlátása, az adatkezelési megbízás, illetve hozzájárulás megadásának előfeltétele kell legyen, mely az adatkezelőtől elvárható, annak tájékoztatási kötelezettsége körébe esik. E helyütt érdemes visszanyúlni a már hivatkozott automatizált adatfeldolgozással hozott döntésre irányadó szabályozásra, illetve az érintettek jogainak érvényesítésére vonatkozó törvényhelyre.[102] Az érintettet kérelmére tájékoztatni kell kezelt, illetve feldolgozott adatairól, az adatforrásokról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az igénybe vett adatfeldolgozóról, annak tevékenységéről, a bekövetkezett adatvédelmi incidensekről, adattovábbítás esetén annak jogalapjáról és címzettjéről, továbbá az automatizált adatfeldolgozás keretében alkalmazott módszerről, annak lényegéről. A fenti tájékoztatási kötelezettséget a dolgok internete körébe tartozó, adatkezelést végző gép esetében a berendezés, eszköz, illetve rendszer üzemeltetőjére, rendelkezési jogosultjára, vagy arra érdemes telepíteni, akinek érdekében a berendezés, eszköz, vagy rendszer működik, azzal, hogy a tájékoztatás az adatkezelést végző eszköz útján is teljesíthető.[103]

Összegzés

A dolgok internete, azaz az adatgyűjtésre, -feldolgozásra, -továbbításra szolgáló fizikai és – a számítási felhőben működő – virtuális eszközök az internetet adatátviteli csatornaként használó globális, dinamikus hálózata, a virtualizáció és az ún. okos eszközök térhódítása, a felhő-technológia elterjedése az információbiztonság és az adatvédelem szempontjából számos, szakcikkünkben is bemutatott kockázat és kitettség kezelését, legalábbis a kockázat, a bekövetkezési valószínűség és a kármérték csökkentését igényli. A technológiai és adatbiztonsági kockázatok kezelése az információbiztonság hagyományos területe, a jogi eszközrendszer e körben a biztonsági elvárások, követelmények kikényszerítésére korlátozódik. Az adatvédelem a jelentős asszimetria miatt is jogi kategória, az érintettek érdekeinek védelmét az információbiztonsági kitettségek mellett ugyanis az adatkezelők, feldolgozók által alkalmazott eljárásokkal, megoldásokkal szemben is biztosítani kell. A hatályos – az EU többször hivatkozott 95/46/EK számú adatvédelmi irányelvével ekvivalens – adatvédelmi szabályozásunk technológiasemlegesen, egyértelmű követelményeket támasztva rendezi az adatkezelőket és feldolgozókat terhelő kötelezettségeket, úgy véljük azonban, hogy az adatkezelői minőség jelenlegi formában történő meghatározása nem felel meg a gépi adatkezelés térhódításának, a dolgok internete sajátosságainak, a fogalmat álláspontunk szerint ki kell terjeszteni az adatkezelést végző berendezésekre, eszközökre és rendszerekre is.

A hatályos 95/46/EK irányelv elfogadása óta közel húsz év telt el.[104] Az irányelv fő célkitűzése a tagállamok adatvédelmi szabályozásának egységesítése volt két vívmány, az adatok (pontosabban a személyek és szolgáltatások) szabad áramlásának biztosítása, illetve a személyek alapvető jogainak védelme közötti egyensúly megteremtése érdekében. Az elfogadása óta eltelt időszakban bekövetkezett technológiai változások, az adat, mint erőforrás jelentőségének felértékelődése, a keletkező, feldolgozott és tárolt adatmennyiség megnövekedése a norma újragondolását tette szükségessé. A Bizottság 2012. január 25-én tette közzé az irányelv átfogó módosítását, egy korszerűbb, egységesebb keretszabályozás megteremtését célzó rendelettervezetét. A módosítási szándék komolyságát, illetve a jogterület jelentőségét már a szabályozás tervezett formája is mutatja, a pusztán célkitűzéseket rögzítő, de a megvalósítás módját a tagállamokra bízó irányelvet egy közvetlenül és elfogadását követően azonnal hatályosuló, a tagállami szabályozást kiváltó jogi eszköz, a rendelet válthatja fel. Az egységesebb és koherensebb szabályozást tartalmazó, az interneten történő adatkezelést központi kérdésként kezelő új norma már törekszik a technológiai fejlődésből eredő kihívások,[105] megválaszolandó kérdések rendezésére, a 29. cikk szerinti Munkacsoport a tagállami szakértők bevonásával folyamatosan dolgozik az új technológiák sajátosságai által generált szabályozási feladatokon. Az új, sokat bírált adatvédelmi irányelv elviekben képes lehet a ma még nyitott kérdések rendezésére, jelenleg azonban még az Unió sem adott választ a gépek átalakuló szerepére, adatkezelői minőségben való megjelenésére.

[1] ld. https://en.wikipedia.org/wiki/List_of_buzzwords

[2] Igaz ez még akkor is, ha ezek alapvetően egy irányban kommunikáltak és a végberendezések működésének jelzésére, visszajelzésére szolgáltak.

[3] Egyes becslések szerint jelenleg már mintegy 25 milliárd eszköz kommunikál az interneten, míg 2020-ra az 50 milliárdos határt is átlépjük. A nagy múltú, nemzetközi befektetési bankház, a Goldman Sachs az IoT-t egyenesen a jövő IT megatrendjének (http://www.goldmansachs.com/our-thinking/pages/internet-of-things), míg a meghatározó piackutató vállalat, a Gartner 2015 egyik legmeghatározóbb technológiai stratégiai irányának (http://www.gartner.com/smarterwithgartner/gartners-top-10-strategic-technology-trends-for-2015) tekinti.

[4] ld. Gautam Shroff Enterprise Cloud Computing; Technology, Architecture, Applications című munkáját (Cambridge University Press, G. Shroff 2010.). Shroff a számítási felhőt a vállalati informatikát forradalmasító, az IT szolgáltatásokat „közművesítő" jelenségnek tekinti.

[5] Az IoT vonatkozásában külön definícióval állt elő az ITU (Recommendation ITU-T Y.2060, Overview of the Internet of things), a témakörre – az ITU fogalom kidolgozásába egyébiránt bevont – klasztert (IERC European Research Cluster on the Internet of Things) dedikáló EU (Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, European Comission Final Report, 2014), illetve az OECD is (Machine-to-Machine Communications, Connecting Billions Of Devices, DSTI/ICCP/CISP(2011)4/FINAL Report), noha utóbbi dokumentum párhuzamosítja az M2M és az IoT fogalmakat.

[6] Az M2M, mint megoldás évtizedes múltra tekint vissza a távközlésben, a hagyományos távközlési csatornák bővülése, átalakulása ezt a fogalmat is új, bővebb tartalommal töltötte meg. Mint arra a Budapesti Műszaki és Gazdaságtudományi Egyetem Nemzeti Média és Hírközlési Hatóság felkérésére készített előkészítő tanulmánya (Dr. Sallai Gyula, Dr. Abos Imre, Dr. Kósa Zsuzsanna, Dr. Adamis Gusztáv: Felmérés előkészítő tanulmány az M2M alkalmazások számozási kérdéseiről, Budapest, 2012. http://nmhh.hu/tart/index/368/Tanulmanyok_felmeresek [2015.06.30.]) is rámutat, az M2M megjelenését indukáló egyik forrás a távközlési hálózatokon belül működő terhelés-elosztó, adaptív forgalomirányító rendszerek, a másik pedig az irányítástechnika, az ipari folyamatszabályozási rendszerek, a gépek, gyártósorok közti jelátvitel volt. Az M2M korábban tehát egyfajta peer-to-peer, két végpont közötti, direkt kapcsolatot jelentett. Ma már kis szűkítéssel minden olyan kommunikációt e körbe sorolunk – legyen az bárminemű adatátvitel – melyben a kommunikáció két berendezés, azaz gép között zajlik, függetlenül attól, hogy a köztük lévő kapcsolat közvetlen, vagy központi csomóponton áthaladó, közvetett. Egyes megfogalmazások a gép által humán fogadó felek felé kezdeményezett kommunikációt is az M2M körébe sorolják, de a betűszavak világában mi ezt inkább meghagynánk az M2H (Machine-to-Human) kategóriájának. Az M2M átalakulása a vezeték nélküli, mobilkommunikációs eszközök és csatornák elterjedésének, a félvezető ipar fejlődésének, a lefedettség növekedésének és a bővülő kapacitások kihasználatlanságának együttes eredménye.

[7] Mint például Wu, Geng, Talwar Shilpa, Johnsson Kerstin, Himayat Nageem, JohnsonD. Kevin: M2M: From mobile to Embedded Internet, Communications Magazine, IEEE 2011/49 p. 36-43.

[8] Állásfoglalásunk erősíti, hogy a téma feldolgozására komoly erőforrásokat fordító, a távközlési ágazat összehangolását világméretű szinten biztosító ITU a távközlés világméretű szabványosítására (ITU-T) irányuló tevékenysége keretében külön munkacsoportok felállításával, önálló keretszabályozás és szabványok kidolgozásával kívánja definiálni és szabályozni a két jelenséget, fogalomkört.

[9] A TCP/IP hivatkozási modell még az internet esetében is csak azt követeli meg, hogy a host-nak csatlakoznia kell egy olyan hálózathoz, amely az IP-csomagok fogadására és továbbítására alkalmas protokollal rendelkezik.

[10] Az adott eszköz megszemélyesítése sem feltétlen követelmény, noha a címzett azonosságának ismerete a kommunikáció szükséges eleme és jelentősen megkönnyíti a későbbi bizonyítást.

[11] Az IoT fejlődésében komoly katalizáló szerepet betöltő telemetria lényegében az intelligens távmérés megnevezése, a telemetrikus rendszerek tehát olyan intelligens távmérő rendszerek, melyek mérőeszközök távoli leolvasására, távolról vezérelt mérések végrehajtására, a mért adatok összegyűjtésére, illetve továbbítására szolgálnak. A telemetrikus, vagy távmérőhálózat tehát az IoT azon része, amely a mérőeszközöket, szenzorokat, a mért adatok fogadását, feldolgozását végző központi egységeket és az ezek között húzódó adatátviteli csatornát foglalja magában. A telematikát, mint szakkifejezést a szaknyelv elsődlegesen az intelligens járműirányításra, azaz a járművek irányítástechnikai eszközökkel történő távoli vezérlésére, az irányítási folyamat (hurok) távközlési eszközrendszerrel történő megvalósítására használja. Az irányítási folyamat az irányított rendszerre vonatkozó jelek szenozorok útján történő összegyűjtését, az összegyűjtött jelek alapján történő ítéletalkotást, a beavatkozási pont meghatározását, a beavatkozást és a visszacsatolást fogja át.

[12] Bővebben lásd: Aguzzi, Stefania, Bradshaw, David, Canning, Martin, Cansfield, Mike, Carter, Philip, Cattaneo, Gabriella, Gusmeroli, Sergio, Micheletti, Giorgio, Rotondi, Domenico, Stevens, Richard: Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, European Comission Final Report, 2014. http://ec.europa.eu/digital-agenda/en/newsroom/publications/network-technologies [2015.07.10.]

[13] A cloud technológia rövid bemutatását a műszaki-informatikai átfedések mellett a felhő technológia katalizáló szerepe, valamint a jogi sajátosságok hasonlósága, azonossága is indokolja. Az IoT és a számítási felhő vonatkozásában is elsődleges kérdés a személyes adatok védelme és az információbiztonság.

[14]Az egyik leggyakrabban hivatkozott meghatározás az amerikai szabványügyi intézet (NIST) definíciója. A NIST megfogalmazásában a cloud computing az erőforrások migrációja egy olyan közös, megosztott, harmadik fél által működtetett erőforrású infrastruktúrába, amelyből az ügyfelek az interneten keresztül technológiai szolgáltatásokat érhetnek el. Az Európai Unió Bizottsága Unleashing the Potential of Cloud Computing in Europe című vitairatában (COM(2012)529 final) maga is ad egy meghatározást: *„ 'Cloud computing' in simplified terms can be understood as the storing, processing and use of data on remotely located computers accessed over the internet. This means that users can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can get to their data from anywhere with an internet connection."*

[15] Informatikai infrastruktúra alatt értve a szolgáltató szervereit, hálózati eszközeit, adattároló- és rögzítő berendezéseit, operációs- és egyéb rendszerszoftvereit, felhasználói szoftvereit, illetve a szoftverek esetében azok használati jogát.

[16] Természetesen ún. hibrid megoldás is létezik, a felhasználók, vagy fogyasztók a privát és publikus felhőt kombináltan is igénybe vehetik.

[17] Az ilyen jellegű szolgáltatások – kiemelten a hozzáférés-szolgáltatások – elektronikus hírközlési szolgáltatásnak minősülnek, és az elektronikus hírközlésről szóló 2003. évi C. törvény hatálya alá tartoznak.

[18] Többek között adatvédelmi, szerzői és polgári jogi, büntető- és polgári eljárásjogi, pénzügyi, illetve bankjogi kérdéseket.

[19] A téma jelentőségét mutatja, hogy az egyének személyes adatainak védelmét alapjogként kezelő – épp ezért az adatvédelmi szabályozás egységesítése felé tartó – Európai Unió több fóruma is kiemelten foglalkozik a számítási felhő működésének, igénybevételének adatvédelmi kockázataival. Az Unió a felhő lényegében a virtuális és földrajzi határokat átlépő adattovábbítás, tárolás és feldolgozás lehetőségét, a globalizálódó adatáramlást látja. Az Unió adatvédelmi joganyagával kapcsolatban bővebb tájékoztatást ad dr. Oros Paulina és dr. Szurday Kinga Adatvédelem az Európai Unióban című munkája, In.: Európai Füzetek 35., Szakmai összefoglaló a magyar csatlakozási tárgyalások lezárt fejezeteiről, Budapest, 2003.

[20] Az adatvédelmi szabályanyag technológiakövető változására példaként ld. Könyves Tóth Pál Az adatvédelmi törvény metamorfózisai című munkáját (In. Fundamentum 14. évfolyam 2. szám, Budapest, 2010)

[21] Ti. a felelősség kérdésének tisztázásával egyértelművé válik, kivel szemben léphet fel jogainak védelmében az érintett. Az adatvédelmi szabályok elsődleges címzettje is az adatkezelő.

[22] Az adatfeldolgozási láncolatok kialakulásának oka a felhőszolgáltatások rétegzettsége, a fizikai infrastruktúra, az azon húzódó virtualizációs alapréteg és az e felett futó szolgáltatási réteg elkülönülésének lehetősége. Egy felhő alapú szolgáltatás esetében előfordulhat, hogy mindhárom réteg szolgáltatója aktív adatfeldolgozói intézkedéseket tesz.

[23] Az Infotv. az adatkezelés fogalma alatt az alkalmazott eljárástól függetlenül az adatokon végzett bármely műveletet, azok összességét, így különösen az adatgyűjtést, felvételt, rögzítést, rendszerezést, tárolást, megváltoztatást, felhasználást, lekérdezést, továbbítást, nyilvánosságra hozatalt, összehangolást vagy összekapcsolást, zárolást, törlést és megsemmisítést, az adatok további felhasználásának megakadályozását, fénykép-, hang- vagy képfelvétel készítését, valamint a személy azonosítására alkalmas fizikai (biometrikus) jellemzők rögzítését érti (ld. Infotv. 3. § 10. pont)

[24] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény nem rögzítette ennyire egyértelműen az adatfeldolgozás határait, a technikai intézkedés adatokhoz kötése a normát felváltó Infotv-ben jelent meg elsőként. Ez azt is jelenti, hogy számos felhőszolgáltatás (jellemzően IaaS, PaaS) kiesik vizsgálatunk köréből, mivel a pusztán a környezetet, infrastruktúrát biztosító szolgáltató nem minősül adatfeldolgozónak.

[25] Adott intézkedéseik kihathatnak az adatkezelés lényeges körülményére, így például az adat törlésére vagy módosítására, mely már adatkezelői hatáskör.

[26] Az Infotv. 10. § (3) bekezdése értelmében az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni. Ezen rendelkezés ütközést eredményezhet a gyakorlattal, a napjainkban meghatározó piaci modell ugyanis az adatok nyers, vagy feldolgozott formában történő értékesítésén alapszik, az alapszolgáltatásokért sokszor adataival (azok felhasználásának engedélyezésével) fizet a felhasználó. Jogi szempontból a személyes jellegüktől megfosztott adatokkal (így pl. aggregátumokkal) való, valamint az érintett megfelelő tájékoztatásán és hozzájárulásán alapuló kereskedés nem sérelmes, azonban egyértelműen ütközik az Infotv. hivatkozott passzusába.

[27] A további adatfeldolgozás tilalmát, azaz több adatfeldolgozó egy adatkezelési folyamatban igénybevételének lehetőségét az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) 28. § (2) bekezdésével módosított Infotv. 2013. július 1-től teszi lehetővé.

[28] A passzus értelmében adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

[29] Ilyen garanciális elem lehet az érintett kifejezett előzetes hozzájárulásának megkövetelése, esetlegesen a törvényhely pontosítása azzal, hogy a rendelkezés a személyes jellegétől megfosztott adatok esetében nem alkalmazandó.

[30] E gondolatra az IoT adatvédelmi aspektusai tárgyalása keretében még visszatérünk.

[31] Ez a kitettség alapvetően a technológiák kompatibilitásának, illetve interoperabilitásának hiányából eredhet és jellemzően az érintett által informatikai rendszerekben kezelt – saját – személyes adatokhoz való hozzáférés korlátjaként jelentkezik. A gyártók sokszor törekednek arra, hogy az egy adott rendszerben kezelt, illetve feldolgozott adatok más rendszerekben ne, vagy ne könnyen legyenek hozzáférhetőek, kezelhetőek, illetve feldolgozhatóak.

[32] A felhőben általában egy szolgáltató megosztott infrastruktúráján, több ügyfél számára folyik az adatkezelés, illetve feldolgozás, ami felveti annak kockázatát, hogy az egyik ügyfélnél bekövetkező incidens az adott infrastruktúrán lévő többi ügyfél rendszereit is érinti. Ennek kockázata valós, de ma már csekély, a rendszerek kialakítása során ezen kitettség jellemzően megfelelő figyelmet kap. Ugyancsak kockázatként merülhet fel a szolgáltatás rétegeinek (alapinfrastruktúra, virtualizációs réteg és szolgáltatási réteg) nem megfelelő védelme, elégtelen lehatárolása, mely esetben egy mélyebb rétegen keresztül felmerülő incidens eredményezheti az adatbiztonsági követelmények sérelmét.

[33] E helyütt visszautalnánk azon megállapításunkra, hogy adott esetben az eltérő szolgáltatási rétegek üzemeltetői is a feldolgozási lánc részesei lehetnek.

[34] A felejtéshez való jog az érintett rendelkezési jogának része, több, mint a törléshez való jog. Az internet sajátosságaiból adódóan uganis egy adott adat egyidejűleg több változatban, időállapotban, példányban is létezhet. Tipikusan ilyen a keresőoldalak „tárolt változat" elérését biztosító funkciója. Önmagában tehát az adott adat törlése nem elegendő, annak valamennyi példánya „elfelejtése" szükséges.

[35] Az adatok feletti érintetti kontroll elveszthetősége a gépi adatkezelések sajátossága, mivel technológiai és bizonyos adatbiztonsági (rendelkezésre állás) okokból a rendszerek, szoftverek és algoritmusok nem egyszer folyamataik részeként duplikálják az adatot, sértik meg annak integritását (kiemelik bizonyos részeit, törlik, vagy éppen hozzáfűznek).

[36] 2014. július 30-tól a szolgáltatók önszabályozás keretében a Nemzetközi Szabványosítási Szervezet, az ISO 27000-es szabványcsaládjába (információbiztonság) tartozó 27018 szabvány bevezetésével is élhetnek. A kifejezetten a felhő alapú technológiák adatvédelmi szabványa alapján működő szolgáltatók vállalják, hogy az ügyfél erre vonatkozó kifejezett előzetes utasítása hiányában nem használják fel azok személyes adatait reklám- és marketing célokra, emellett az ügyfél számára teljes ellenőrzést biztosítanak adatai használata felett. A szabvány alapján a szolgáltatónak tájékoztatnia kell ügyfelét az adatok fizikai elhelyezkedéséről és mindazon alvállalkozóiról, amelyek részt vesznek az adatkezelésben (a szabvány szóhasználata nem alkalmazkodik az adatvédelmi szabályozás adatkezelő, adatfeldolgozó megosztásához). Az alvállalkozók szabványkövető működéséért is a szolgáltató felelős. Személyes adat jogosulatlan megismerésével járó incidens esetén a szolgáltató tájékoztatni köteles az érintett ügyfeleket, továbbá dokumentálni kell az eseményt és az elhárításra tett lépéseket is (hasonlóan az Infotv. októbertől hatályos adatvédelmi incidens esetén követendő eljárásához). A szabványt bevezető szolgáltató évente külső audit alá kell vesse magát.

[37] Az Infotv. 4. § (3) bekezdése értelmében: *„A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek."* A jogszabály tehát követelményként határozza meg a helyreálllításhoz szükséges technikai feltételek meglétét. E körben indokolt lenne annak átgondolása, hogy a feltételek tényleges rendelkezésre állása helyett a helyreállítás lehetőségének megléte, a technikai megoldás adatkezelő általi elérhetősége nem lenne-e megfelelőbb a személyes adatok jogi védelmben részesítése szempontjából. Természetesen az adatkezelő általi helyreállíthatóság akkor is megvalósul, ha a helyreállítást az adatkezelő az igénybevett adatfeldolgozó útján valósítja meg, meglátásunk szerint ugyanakkor a helyreállításhoz szükséges technológia elérhetősége a jelen szabályozás alapján önmagában nem elegendő.

[38] Az Ibtv. fogalomhasználatát alapul véve a bizalmasság azt jelenti, hogy az információt kizárólag az arra jogosultak és csak a jogosultságukhoz igazodó mélységben ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A sértetlenség annak bizonyosságát jelenti, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, feldolgozási módszereikkel együtt pontosak és teljesek, az adat hiteles, az elvárt forrásból származik, származása ellenőrizhető, azaz letagadhatatlan. Rendelkezésre állás alatt pedig az adat arra jogosult személy számára való korlátozásmentes elérhetőségét, felhasználhatóságát értjük.

[39] Az Ibtv. értelmező rendelkezései körében rögzíti az elektronikus információs rendszer biztonságának fogalmát is, mely az elektronikus információs rendszer olyan állapotát jelöli, amelyben annak védelme, elemeinek sértetlensége és rendelkezésre állása, valamint a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása zártan, teljes körűen, folytonosan és a kockázatokkal arányos módon biztosított. (ld. Ibtv. 1. § (1) bek. 15. pontja)

[40] http://www.naih.hu/adatvedelmi-szotar.html [2015.08.19.]

[41] ld. Infotv. 7. §

[42] 7. § (...) *„(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja*
a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.
(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek."

[43] Az aszimmetria e körben az infrastruktúrák támadásához, veszélyeztetéséhez szükséges erőforrások védelmi igényekkel szembeni aránytalanságára utal.

[44] A DDoS (Distributed Denial of Service) támadás lényege egy adott informatikai szolgáltatás, így például egy adatbázis, portál – annak túlterhelésével történő – teljes vagy részleges megbénítása, működésének befolyásolása. DDoS támadás esetén a támadó – jellemzően célalgoritmusok, illetve eltérített és hálózatba szervezett számítógépek (ún. botnetek) igénybevételével egyidejűleg, vagy rövid időközökkel nagyszámú, aránytalanul nagy számítási kapacitást, vagy sávszélességet igénylő lekérdezést címez az adott szolgáltatáshoz, mely a terhelés következtében összeomlik, más felhasználók számára elérhetetlenné válik. Az egyik legnagyobb ilyen jellegű támadás a 2013. márciusában a Spamhouse nevű szervezetet érte (az incidensről bővebben ld.

http://www.nsfocus.com/SecurityView/Analysis%20of%20DDoS%20Attacks%20on%20Spamhaus%20and%20recommended%20solution-EN-20130510.pdf [2015.08.12.])

[45] Célzott információszerző törekvés alatt az egy konkrét szervezetre, rendszerre, vagy információra irányuló hekkertámadásokat értjük. Ezek jellemzően kifinomultabbak a világhálón napi rendszerességgel, tömegesen előforduló, véletlenszerűen (jellemzően sérülékenység, biztonsági rés alapján) kiválasztott célpontokra irányuló támadásoknál, nem egy esetben speciális, egyedi támadóeszköz (algoritmus) igénybevételével történnek. (Ld. pl. a the fappening néven elhíresült esetet, mely során hekkerek egy adott gyártó termékének sérülékenységét kihasználva ismert emberek személyes adatait szerezték meg)

[46] A személyiséglopás (identity theft), illetve az adathalászat elsősorban más bűncselekmények, így kifejezetten a csalás eszközcselekményeként jelenik meg, céljuk a sértett(ek) személyes adatainak megszerzése, annak érdekében, hogy azzal az elkövető, vagy más visszaélést követhessen el. Hatályos büntető törvénykönyvünk, a 2012. évi C. törvény (Btk.) 219. §-ban a „raktárra" történő személyes adatgyűjtést is büntetni rendeli, amennyiben annak célja jogtalan haszonszerzés, vagy az adatkezelés jelentős érdeksérelmet okoz. A tiltott adatszerzés (422. §) ugyancsak sui generis bűncselekmény, így a tényállási elemek megvalósulása esetén a személyiséglopás, illetve adathalászat önmagában is büntetendő.

[47] E körben legeklatánsabb példaként a Duqu kártevőre hivatkozhatunk, amelyet kiejezetten információszerzési céllal készítettek. (bővebben ld.: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf [2015.08.12.])

[48] Mint pl. ügyfélllisták, orvosi-kutatási adatbázisok, adatállományok.

[49] A nemzetbiztonsági (és e körben nemzetgazdasági) szempontból érzékeny, fontos és bizalmas munkakört betöltő személyek jogellenes befolyásolása megelőzésének szükségességét a jogalkotó is felismerte, amikor az ezen személyek tevékenysége ellen irányuló, illetve a tevékenységükhöz kötődő védett információk jogellenes megszerzését célzó leplezett törekvések felderítése és elhárítása érdekében bevezette a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben szabályozott nemzetbiztonsági védelem és ellenőrzés intézményét. Gondoljunk csak bele, mekkora kitettséget jelenthet egy vállalat számára, ha vezető beosztású munkatársa a szexuális életére vonatkozó különleges személyes adataival zsarolhatóvá válik, vagy milyen hatással járhat egy fúzióra, felvásárlásra, esetleg részvényárfolyamra, ha a vállalat befolyással rendelkező tulajdonosának, vezető tisztségviselőjének egészségügyi személyes adata idő előtt, vagy nem kívánt módon nyilvánosságra kerül.

[50] Nem szükséges kifejtenünk, mekkora károkat okozhat mondjuk az egészségügyi adatok akár részleges módosítása az érintett gyógyászati ellátásában, vagy a bűnügyi személyes adatok manipulációja egy adott munkakör betöltésénél.

[51] A kiberterrorizmus, illetve az ún. hacktivista mozgalmak mögött jellemzően valamilyen cél kikényszerítésének szándéka, annak elérése áll, hogy a célzott nemzetközi szervezet, állam, illetve annak szervei valamit tegyenek, ne tegyenek, vagy éppen eltűrjenek. Ez a cél megvalósulhat személyes adatokat tartalmazó, a közigazgatás működése szempontjából jelentős adatbázisok integritásának támadásával, az adatok törlésével, vagy elérhetőségének akadályozásával is (a tárgyban ld. az Észak-atlanti Szerződés Szervezete [NATO] tematikus portálját, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm [2015.08.15.]). A hacktivista mozgalmak körébe a szakirodalom az Anonymous hackercsoporthoz hasonló szerveződéseket sorolja, melyek adott esetben társadalmilag hasznos (vagy hasznosnak vélt) cél elérése érdekében élnek a kiberbűnözés eszközrendszerével. A kiberterrorizmus és a hacktivista mozgalmak jelentette fenyegetéseket a NATO és hazánk is stratégiai szinten kezeli (ld. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm. határozat). A témáról bővebben ld. Kovács László: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. In. Hadmérnök VII. évfolyam 2. pp. 302-311., Budapest, 2012.

[52] A kompatibilitás elsődlegesen az infokommunikációs eszközök, rendszerek egymással való helyettesíthetőségét, míg az interoperabilitás az eszközök, rendszerek együttműködését, a kommunikációt lehetővé tévő illeszthetőségét jelenti.

[53] A beágyazott rendszerek olyan rendszerek, amelyeket feladat-specifikusan, céleszközként történő működésre és nem általános célokra terveztek és optimalizáltak. Nem ritkán egy nagyobb rendszer specifikus részegységei.

[54] E helyütt utalnánk vissza a cloud kapcsán, a szolgáltatási rétegekkel összefüggésben felvázolt biztonsági kockázatra. Az eszközök (értve ez alatt a szoftvereket is) heterogenitása jelentette biztonsági előnyök az alattuk húzódó, közös szolgáltatási réteg sérülékenysége esetén elveszhetnek.

[55] Egyenszilárdnak azt a rendszert nevezzük (rendszer alatt értve az eszközökön felül azok kapcsolatait, üzemeltetőit és folyamatait is), melyeknek valamennyi eleme azonos szintű védettséget valósít meg.

[56] A patch-menedzsment a szoftverek (operációs rendszerek és alkalmazások) frissítéseinek, azaz az önálló szoftvernek nem minősülő javítások és verziók telepítését jelenti.

[57] Az ipari folyamatirányító és vezérlő rendszerek speciális, többségében számítógép vezérelte célrendszerek, melyek gyártási, ipari folyamatok felügyeletét és vezérlését teszik lehetővé. Legelterjedtebb formái az ún. SCADA (Supervisory Control and Data Acquisition) rendszerek.

[58] Az ún. 0. day hiba egy szoftver, vagy rendszer olyan, esetlegesen a gyártó előtt is ismeretlen hibáját jelenti, amely még nem került kipublikálásra, illetve javításra.

[59] Gondoljunk bele, egy okos otthon távmérő eszközei kommunikációjának megfigyeléséből látható, hogy az adott háztartás fogyasztott-e bármilyen erőforrást, amelyből arra vonatkozóan is tehető megállapítás, hogy a ház lakói éppen otthon tartózkodnak-e.

[60] Az azonosítók forgalmat lassító, a kezelést nehezítő hosszúságúvá válásához, vagy elfogyásához.

[61] Az interdependencia az elemek, részhalmazok kölcsönös függőségét, összehangolt viselkedését jelenti, azaz azt, hogy a részhalmazokban bekövetkező folyamatok, a részhalmaz viselkedése ki- és visszahat a másik részhalmazra.

[62] A rész-egész, illetve leggyengébb láncszem elve azt jelenti, hogy egy adott rendszerelem, eszköz védettségét önmagában és a rendszer részeként is értékelni kell, valamint, hogy az összekapcsolt eszközök biztonságának szintjét a leggyengébb védelemben részesülő elem védelmi szintje határozza meg.

[63] Az infokommunikációs technológiákat, illetve az azok azonosítási és kijelölési eljárás során alkalmazott ágazati és horizontális kritérumoknak megfelelő elemeit az irányadó nemzetközi és hazai szabályozás részben saját jogon (az infokommunikációs technológiák, mint ágazat részét képező szinte valamennyi alágazat, azaz az információs rendszerek és hálózatok, az internet-infrastruktúra és hozzáférés, az eszköz-, automatikai és ellenőrzési rendszerek, a vezetékes és mobil távközlési szolgáltatások, a rádiós távközlés és navigáció, a műholdas távközlés és navigáció, valamint a kormányzati informatikai, elektronikus hálózatok körében), részben a többi létfontosságú infrastruktúra ágazat részét képező technológiai irányítási és vezérlési rendszerek körében szabályozni rendeli.

[64] Kritériumok mindazon szempontok, illetve a szempontokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, rendszerelem megzavarása vagy megsemmisítése által kiváltott hatásra vonatkoznak (hatás alapú megközelítés).

[65] A jogszabály értelmében létfontosságú társadalmi feladat különösen az egészségügy, a lakosság személy- és vagyonbiztonsága, valamint a gazdasági és szociális közszolgáltatások biztosítása.
[66] Vagyis az, hogy az adott rendszerelem, infrastruktúra kiesésének hatása mekkora földrajzi területen és időtávon érvényesül.
[67] A fenyegetettség az informatikai biztonsági szaknyelvben azt az állapotot jelöli, amelyben fennáll a bizalmasság, a sértetlenség vagy a rendelkezésre állás sérülésének veszélye. Az Ibtv. 1. § (1) bekezdése alapján a kockázat a fenyegetettség mértéke, amely egy adott fenyegetés bekövetkezési valószínűségének és a bekövetkezés által okozott kár nagyságának függvénye, míg a sérülékenység a rendszer olyan hiányossága, vagy tulajdonsága, amelyen keresztül a fenyegetés megvalósulhat.
[68] ld. az Ibtv. 2. §-át.
[69] A PreDeCo védelem-tervezési elv a védelmet három egymásra épülő, egymást kiegészítő elemből, a megelőző (preventív), felismerő (detektív) és az elhárító (korrektív) kontrollokból építi fel.
[70] ld. 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
[71] A besorolás kritériumait az Ibtv. 7. §-a, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet rögzíti.
[72] Ibtv. 2. §
[73] Az Ibtv. 2. §-a értelmében:
„(2) E törvény rendelkezéseit kell alkalmazni:
a) az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők,
b) a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,
(...)
elektronikus információs rendszereinek védelmére.”
[74] Erre utal az adatkezelő fogalmának meghatározásánál (Infotv. 3. § 9. pont) a „másokkal együtt” kitétel.
[75] Természetesen azt is meg kell vizsgálni, hogy a szabályozás finomhangolása nem eredményezi-e valamely, az Ibtv. által védendő érdek sérülését, védendő szervezet, adatbázis, vagy adatállomány szabályozási körön kívül kerülését.
[76] ld. a NAIH-2298-23/2013/H. számú határozatát (http://www.naih.hu/files/2298_2013_H_HATAROZAT_anonim.pdf [2015.08.12.])
[77] Az EU általános adatvédelmi irányelve, az Európai Parlament és a Tanács az egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról szóló 95/46/EK irányelv az EU tagállamok adatvédelemért felelős hatóságainak, felügyeleti szerveinek, az EU adatvédelmi főhatóságának, illetve a Bizottság képviselőjének részvételével életre hívott egy új, független tanácsadó, véleményező és konzultatív testületet, a jogalapot teremtő cikkelyről 29. cikk szerinti Munkacsoportnak nevezett grémiumot. A Munkacsoport az egyének védelmét hivatott biztosítani a személyes-adat feldolgozás során. A Munkacsoport 2010. február 16-án elfogadott 1/2010. számú, az adatkezelő és az adatfeldolgozó fogalmát tárgyaló véleményében részletesen foglalkozik a többes (együttes) adatkezelés tartalmával és értelmezésével.
[78] A polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter felügyelete alatt működő kormányzati eseménykezelő központ (CERT) feladata a globális kibertér irányából érkező, valamint az állami és önkormányzati elektronikus információs rendszerek működését biztosító infokommunikációs infrastruktúrát, a hatáskörbe tartozó szervek nyílt elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelése, megelőzésük elősegítése.
[79] Az Ibtv. 1. § (1) bek. 41a. pontja alapján: *„súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.”*
[80] ld. Infotv. 7. §
[81] ld. Btk. 219. §:
„(1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva
a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
b) az adatok biztonságát szolgáló intézkedést elmulasztja,
vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
(2) Az (1) bekezdés szerint büntetendő az is, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti.
(3) A büntetés két évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges adatra követik el.
(4) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.”
[82] ld. Infotv. 15. §
„(1) Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.
(1a) Az adatkezelő – ha belső adatvédelmi felelőssel rendelkezik, a belső adatvédelmi felelős útján – az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.”
[83] ld. Infotv. 23. §-a. E helyütt jegyezzük meg, hogy az Infotv. 23. §-az adatvédelmi incidens fogalmának bevezetése után már indokolatlanul szerepelteti külön a jogellenes adatkezelés és az adatbiztonsági követelmények megsértésének esetét, elegendő lenne csupán az incidensre hivatkozni, mivel meglátásunk szerint az a büntetőjogi igényérvényesítés mellett sem zárja ki a polgári jogi igények érvényesítését.
[84] Így például jogalap nélküli, azaz a törvényi felhatalmazás nélkül, vagy az érintett hozzájárulása hiányában, esetlegesen annak visszavonása után folytatott adatkezelés.

[85] A 95/46/EK irányelve az Infotv-el közel egyező módon ragadja meg az adatkezelő fogalmát, adatkezelő alatt az a természetes vagy jogi személyt, hatóságot, intézményt vagy bármely más szervet értve, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját.
[86] Így például portálrendszerek, szenzorhálózatok és a mögöttük futó vezérlő algoritmusok hoznak önálló döntéseket személyes adatok felvételéről, módosításáról, törléséről, határozzák meg, hogy milyen célra és módon kerüljenek az adatok rögzítésre, esetlegesen maguk szereznek be (töltenek, hívnak le) adatokat adatbázisokból, adatállományokból.
[87] ld. a tárolt program elve.
[88] Már ma is elérhetőek olyan integrált, szenzorhálózatokból és központi elemzést végző eszközökből álló gépjárműinformatikai rendszerek, melyek egy meghatározott esemény bekövetkezése esetén képesek önálló döntést hozni az érintetthez köthető adatok rögzítéséről és a rögzített adatok felhasználási célokhoz kötött (pl. lízing célra a jármű használati, helymeghatározási adatai, biztosítási célra a sebesség adatok, baleset közeli helyzetekre vonatkozó információk), disztributált továbbításáról.
[89] Előfordulhat olyan intézkedés, melyet az adott eszköz maga is képes végrehajtani, így például képes lehet az adatvédelmi incidensek önálló naplózására, ezáltal a kapcsolódó nyilvántartási kötelezettség teljesítésére, vagy az érintettek elektronikus úton, üzenetek automatizált kiküldésével történő tájékoztatására.
[90] ld. Infotv. 65. § (1) bekezdése.
[91] Passzív például egy környezeti tényezőt mérő szenzor, vagy mondjuk egy személy szívritmusának mérésére használt eszköz.
[92] E körbe tartoznak például a járművek, informatikai eszközök, így mondjuk a határvédelmi tűzfalak működése, illetve a képalkotó (egészségügyi) diagnosztikai eszközök működése során keletkező adatok. Utóbbiak részben már önállóan is képesek az adatok részleges kiértékelésére, következtetések levonására, adatbázisba rendezésére, összevetésére, továbbítására is.
[93] Az online szféránál maradva például blog, vagy fórumbejegyzések.
[94] Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény a fent hivatkozott adatkört (a levonható következtetések tartalmát) a különleges adatnak minősülő egészségügyi adatok meghatározása körében az egyénre vonatkozó leképzett, származtatott adatokkal tölti ki. A jogszabály 3. § a) pontja értelmében *„egészségügyi adat: az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (pl. magatartás, környezet, foglalkozás).”*
[95] Megjegyezzük, a törvény személyes adat definíciója ekvivalens az EU általános adatvédelmi irányelvének fogalom meghatározásával, melynek rendelkezése szerint az azonosított, vagy azonosítható természetes személlyel kapcsolatban hozható bármely információ személyes adatnak minősül.
[96] Ezt a megoldást választotta a jogalkotó a már hivatkozott 1997. évi XLVII. törvény esetében is. A norma kapcsolati kód alkalmazásának előírásával biztosítja a betegre és az egyes ellátási eseményekre, betegutakra vonatkozó adatok személyazonosításra alkalmatlan összekapcsolását. A jogszabály a kapcsolati kódok képzésére vonatkozó előírásokat is tartalmaz, előírja, hogy a kapcsolati kód nem származtatható személyazonosító adatból és nem lehet azzal azonos.
[97] Az anonimizálás a személyes adat érintetthez köthetőségének oly módon történő megszüntetése, melynek eredményeként kizárható a kapcsolat helyreállítása, illetve a helyreállítás kockázata elhanyagolható. A validálás a visszaállíthatóság kizárásának visszaellenőrzését, igazolását jelenti. A személyes adatok anonimizálásának kockázatairól bővebben ld. Dr. Alexin Zoltán: Kockázatokat rejt az egészségügyi adatok anonimizálása című munkáját, In.: IME Informatika és Menedzsment az Egészségügyben, Az egészségügyi vezetők szaklapja Budapest, 2014. év XIII. szám, pp. 68-72., míg az egészségügyi adatok kódolásáról, pszeudonimizálásáról (a kapcsolati kód felett a páciens rendelkezik), illetve anonimizálásáról dr. Hanti Péter Kommentár az egészségügyi és az adatvédelmi törvényhez című könyvét, Budapest, 2013.
[98] Aggregálás alatt e körben az adatok személyes jellegének végleges törlésével történő összevonását értjük.
[99] ld. Infotv. 11. §
[100] ld. Infotv. 7. § (1) bek.: *„Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.”*
[101] A jelenség nem ismeretlen a jogalkotók előtt, az Infotv. több passzusa is szabályozza a kérdést. A problémát az EU szabályozó hatóságai is felismerték, és kezelték, így például a 95/46/EK európai parlamenti és tanácsi irányelv alapján az Európai Bizottság 2010. február 05-én, 2010/87/EU számon bocsátott ki határozatot a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről, ld. Official Journal of the European Communities L 39, Volume 53, 12 february 2010. A kérdést az adatvédelmi irányelv módosítása az extraterritoriális hatály bevezetésével részlegesen (szolgáltatásnyújtás, nyomkövetés) rendezni fogja.
[102] ld. Infotv. 13. fejezet
[103] Az adatkezelést végző eszközök – akár ún. gépi tanulási megoldások alkalmazásával – felprogramozhatóak úgy, hogy a tájékoztatási kötelezettségnek valamilyen információs felületen (így mondjuk egy portálon) keresztül, vagy önállóan generált elektronikus üzenet formájában közvetlenül maguk tegyenek eleget.
[104] Még hosszabb ez az idő, ha figyelembe vesszük, hogy az irányelv tervezetét a Bizottság már több mint húsz éve, 1990. szeptember 13-án készítette el.
[105] A tervezet az adatvédelmi szabályozás hatályát tekintve szakít a territoriális elvvel, az adatkezelő honosságától függetlenül az Unió területén lakó személyeket érintő valamennyi adatkezelést szabályozni kívánja (extraterritoriális hatály). A megoldás tiszta viszonyokat teremthet, biztosíthatja azon, jelenleg érvényesülő nehézkes gyakorlat kiváltását, mely szerint az adat életciklusával érintett minden szereplő vonatkozásában illetékes adatvédelmi hatóságnak jóvá kell hagynia az adatkezelési megállapodást.