Jobbágy Szabolcs – Sándor Miklós
jobbagy.szabolcs@zmne.hu – sandor.miklos@zmne.hu

A MINŐSÍTETT ADATOK VÉDELMÉNEK JOGI SZABÁLYOZÁSA

Absztrakt

Mindenki számára köztudott, hogy a saját maga határait feszegető, a lehetetlent nem ismerő, megállíthatatlanul dübörgő információs társadalom mindennapjainak a szerves, tudatos és aktív részesei vagyunk. Az ezt átívelő információs szupersztráda alappilléreit megtestesítő információ nélkül elképzelhetetlen ennek a pillanatról-pillanatra megújuló infokommunikációs forradalomnak a léte. Lényegi mivolta abban gyökerezik, hogy az információ mindenki számára a megfelelő módon, a megfelelő mennyiségben és minőségben, a szükséges mértékben, a kellő időben és helyen a rendelkezésére álljon. Ebben a milieu-ben az információt a felfokozott jellegéből adódóan azonban nem szabad magára hagyni, védeni kell a rosszakaratú támadások, az illetéktelen és jogosulatlan hozzáférésekkel szemben.
A szerzők a cikkben alapul véve és elemezve a „Minősített adatok védelméről szóló 2009. évi CLV. törvényt" röviden általános kitekintést próbálnak nyújtani az információbiztonságnak, az információvédelemnek, mint egyre markánsabban megjelenő és érvényesülni kívánó, a híradást és informatikát vagy komplex értelemben az új keletű megnevezéssel illetett infokommunikációt és ennek a technológiai alapját megtestesítő infokommunikációs rendszereket-hálózatokat egyaránt akarva-akaratlan és nélkülözhetetlenül átható szakterületnek a hazai szabályozására.

It is common knowledge that we all are integral, conscious and active participants in the everyday life of unstoppably booming information society, which keeps trying to go beyond its limits and for which nothing is impossible. Information, embodying the base of the information superhighway spanning over it, is indispensable for the existence of this infocommunication revolution, renewing itself every single moment. Its essence is that information should be made available for everyone in the proper way, in the proper amount and quality, to the desired extent and at the proper place and time. In this environment, due to its intense nature, information must not be left alone but should be protected against any ill-meant attacks or unauthorised and illegal access.
Taking 'Act No. CLV of 2009 on the protection of qualified data' as their starting-point and analysing it in their article, the authors strive to give a brief and general overview of the national regulation of information security or protection as a more and more markedly present and prevalent field, unavoidably and indispensably penetrating both telecommunications and IT, or in a complex sense and with their newly-coined common name, infocommunication, as well as the infocommunication systems and networks providing the technological base of the former.

Kulcsszavak: *információs társadalom, infokommunikáció, információ, információbiztonság, minősített adat, bizalmasság, sértetlenség, rendelkezésre állás, elektronikus információbiztonság ~ information society, infocommunication, information, information security, classified data, confidentiality, integrity, availability, electronic information security*

ELŐSZÓ

Napjainkban a társadalmi fejlődés fokozatainak harmadik nagy szignifikáns korszakát, ciklusát éljük, melyet az információs társadalom[1] kifejezéssel illet a releváns szakirodalom. Ennek a típusú társadalmi szerveződésnek az alapvető alkotóeleme, legfontosabb lényegi meghatározója az információ[2], mely egy óriási jelentőséggel bíró „érték", mellyel rendelkezni, melynek birtokosának lenni, pedig „hatalom". [1][2][3][4]

Ezen egyszerű okból kifolyólag azonban nem csak az információ értékének, jelentőségének a súlya, hanem a vele szemben megnyilvánuló támadások száma is ugrásszerűen megnőtt és folyamatosan növekvő tendenciát mutat napjainkban is, mely támadások, illetéktelen információszerzések-hozzáférések, a jogosulatlan behatolások változatos formáinak, minden lehetőséget kiaknázó módjainak tárháza határokat nem ismer. Ugyanakkor a fent említett tevékenységek negatív, destruktív hatásai, az általuk okozott károk volumene is egyre súlyosabb következményekkel jár az egyes személyek, az ország, az információt kezelő rendszerek, ezáltal a katonai infokommunikációs rendszerek biztonságának vonatkozásában is.

Ez egyértelműen megköveteli az információ fokozottabb védelmét, a továbbítására, feldolgozására, tárolására, kezelésére szolgáló infokommunikációs hálózatok[3] [5] biztonsági szintjének fokozását, az információ és az átvitelére szolgáló rendszerek védelmére, a biztonságos továbbításnak a lehetővé tételére predesztinált egyre kifinomultabb, megbízhatóbb és biztonságosabb módszerek, eljárások, technológiák, eszközök és berendezések életre hívását és rendszerbeállítását, a szükséges információk-adatok különböző szintű minősítését, az információbiztonság[4] [6], az információvédelem[5], a minősített adatok[6] [7] kezelésével kapcsolatos eljárások, szabályzó intézkedések, törvények,

1 Információs társadalom: Egy viszonylag új keletű dolog, mely az informatika és a távközlés konvergenciáján, az információ és a tudás szabad létrehozásán, forgalmazásán, hozzáférésén és felhasználásán alapuló társadalmi struktúra kialakításán nyugszik. Legfőbb mozgatórugója az informatikai, a távközlés, a szórakoztató elektronika, és a média külön – külön is hatalmas ütemű fejlődése. A Hadtudományi Lexikon értelmezésében az ipari társadalmak utáni társadalmi formáció, a XXI. századi úgynevezett információs korszak társadalma.

2 Információ: Átvitelre, tárolásra vagy feldolgozásra alkalmas formában kifejezhető hír, ismeretanyag. Az információ lehet jel, adat, szimbólum, kép, hang, stb.

3 Infokommunikációs hálózat: Az infokommunikáció az informatika és a kommunikáció (híradás) integrációja. Az infokommunikációs (híradó-informatikai) rendszer magába foglalja az információ előállítását, gyűjtését, felvételét, tárolását, feldolgozását, törlését, és továbbítását, továbbá az ehhez szükséges berendezéseket, elektronikus eszközöket, üzemeltető és felhasználó személyeket az információ bármely típusát tekintve.

4 Információbiztonság: „Az információbiztonság a katonai szervezetek vezetésének, működésének sikere érdekében az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az adatkezelő képességek megfelelő szintű védettsége."

5 Információvédelem: Az információvédelem fogalmára nagyon egyszerű magyarázattal szolgálhatunk a hozzá szorosan kapcsolódó fogalom, az információbiztonság alappillérére építkezve. E gondolatmenetet végigfuttatva azzal a triviális megfogalmazással élhetünk miszerint, ha az információbiztonságot egy állapotnak tételezzük fel, akkor az információvédelem ennek az állapotnak a megteremtésére, fenntartására és fokozására irányuló tevékenységek és eszközök összessége.

6 Minősített adat: A 2009. évi CLV. a minősített adatok védelméről szóló törvény értelmében megkülönböztethetünk nemzeti és külföldi minősített adatot. A nemzeti minősített adat „…olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti…és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza." A külföldi minősített adat fogalma, pedig „Az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza."

jogszabályok komplex egységének és az információbiztonság-politikának[7] [6] az előtérbe kerülését.

Az egyre fokozottabb veszélynek kitett infokommunikációs rendszerek-hálózatok, a rajtuk keresztül továbbított információk, minősített adatok azonban nem csak a „polgári-civil" szférában vannak jelen az egyre inkább növekvő „információéhség" és az újabbnál-újabb felhasználói igények kiszolgálásának érdekében, hanem a fegyveres erők, a haderők szektorában, mint egyfajta speciális felhasználási szegmensek területén is aktívan képviseltetik magukat a vezetés és irányítási rendszerek, a csapatok vezetésének legfontosabb és alapvető eszközeiként. Ezen elméleti megfontolás alapján érthető, hogy a katonai kommunikációs rendszerek információbiztonságának kérdése is halaszthatatlan és folyamatos megújulást igénylő és egyben megkövetelő kérdéskör. Különösen igaz ez a mai kor modern hadseregeire, hadviselési módjaira, digitális hadszíntereire[8] [8][9][10]. Ebben a speciális, új típusú környezetben az információ, a különféle katonai infokommunikációs hálózatok óriási jelentőséggel bírnak. A digitális hadviselés[9], a hatásalapú műveletek[10] [10], a hálózatközpontú hadviselés[11] [11], mint az „új típusú küzdelem" alapvető alkotóelemeit testesítik meg az ellenség legyőzése, az információs fölény-uralom megszerzése-kivívása, a kitűzött cél, a meghatározott feladat elérése és véghezvitele céljából többek között digitális katonák[12] [12] és információs harcosok[13][10] bevetése, alkalmazása révén.

---

7 Információbiztonsági politika: Az információbiztonsághoz szorosan kapcsolódó fogalom. Tulajdonképpen „Az általa meghatározott felelősségi rend és hierarchizált szabályozás, a saját erőkre, képességekre, környezetre, ellenséges erőkre vonatkozó adatok biztonsági alapelvek szerinti kockázatokkal arányos védelme, valamint a rendszabályok folyamatos pontosítása, hatékonyságuk ellenőrzése, a biztonsági eseményekre való gyors és hatékony reagálás képezi az információbiztonság alapját."

8 Digitális hadszíntér: Egy többdimenziós, digitalizált hadszíntér, ahol magas fokon elektronizált, tudás alapú (knowledge based army), nagy találati pontosságú precíziós (hightech) fegyverzetű hadseregek, digitális katonák, információs harcosok harcolnak. Alapvetően infokommunikációs, multimédiás szolgáltatásokat biztosító harci hálózatokon nyugszik, helyet biztosít a támadó és védelmi információs műveleteknek. „Digitális hadszíntér alatt azt a virtuális teret ért(het)jük, amely magába foglalja a fegyveres küzdelem rendszerének informális elemeit (az elektronikus információszerzés, -továbbítás, -feldolgozás illetve az ennek bénítására és lefogására alkalmazott eszközöket és eljárásokat)."

9 Digitális hadviselés: Napjainkban a harmadik hullámú vagy negyedik generációs hadviselés korszakát éljük, mely a 21. század jellemző hadviselési módja. Legfontosabb jellemzője a globalitás, a dinamikus hadműveletek, a vezetés-irányítási rendszerek (C2-Command and Control) pusztítása, precíziós csapások, digitális és hálózatos hadseregek. Alkalmazására elsőként az I. Öböl háborúban került sor a nemzeti kommunikációs és államigazgatási infrastruktúra ellen intézett digitális, infokommunikációs támadások végrehajtása által.

10 Hatáslapú műveletek (effects-based operations): „A katonai műveletekben alkalmazott hatásalapú megközelítés (effects-based approach) elve szerint a hadszíntéren egymással hálózatba kapcsolt objektumok vannak. Egy kiválasztott központ és a benne található nagyfontosságú célpontok elleni támadás, különböző hatásokat eredményezhet a többi, hozzájuk kapcsolt objektumok működésében is….A hatásalapú műveletekben a korábbi felfogáshoz képest komolyan figyelembe veszik azt a láncreakcióhoz hasonlító elvet, miszerint a kezdeti közvetlen hatással –első csapással- törvényszerűen további közvetett károsító, korlátozó hatásokat lehet elérni, amely a teljes rendszerre különböző mértékű negatív hatást fejt ki. Az előidézett hatások eredőjének, vagyis az összhatás eredményének elemzése és értékelése képezi a hatásalapú műveletek lényegét….A közvetlen és közvetett hatások elve szerint egy rendszer belső – kulcsszerepet játszó – elemeire mért pusztító vagy korlátozó jellegű csapás mind a rendszeren belül, mind, pedig a rendszerek közötti kapcsolatokban másod, harmad és n-edik típusú és erősségű hatásokat vált ki."

11 Hálózatközpontú hadviselés: „A hálózatközpontú hadviselés (NEC- Network Centric Warfare) legfontosabb eleme az információk megszerzésének és felhasználásának radikálisan új módja, amely gyökeresen átalakítja a haderő vezetési rendszerét is, hiszen lehetővé teszi, hogy minden információ a vezetés minden szintjén egy időben álljon rendelkezésre, és ennek megfelelően a döntések mindig a lehető leggyorsabban és a döntés szempontjából optimális szinten születsenek. A NEC lényege, hogy egyetlen integrált rendszerbe foglalja az érzékelőket, a döntéshozókat és a fegyverrendszereket. Alkalmazása során kiemelkedő jelentőségű a koalíciós partnerek közötti minél jobb információ-megosztás, a döntéshozatal felgyorsítása, illetve az, hogy a megfelelő időben a megfelelő katonai eszköz kerüljön bevetésre. Az NEC sokkal több, mint többletfelszerelés: optimalizált parancsnokságra, vezetési struktúrára, illetve átalakított kiképzési rendszerre helyezi a hangsúlyt, hogy a válasz gyors és a körülményeknek megfelelő legyen."

12 Digitális katona: „A digitális katonák (vagyis összfegyvernemi manőverező erők) a digitalizált harcmezőn, elektronizált és informatizált fegyverrel, digitális vezérlésű, igen nagy találati pontosságú ún. precíziós fegyverrel harcolnak az általános hadműveleti terv alapján. Kiképzésükbe és felkészítésükbe beletartozik a számukra

Mielőtt hozzálátnánk a címben megnevezett törvény boncolgatásához, fontosnak tartom összegezvén a fent elhangzottakat tisztázni azt a kérdést, hogy hogyan is kapcsolódik össze az információ, az infokommunikációs hálózat az információbiztonság és a minősített adatok védelmének a kérdésével. A közös csatlakozási pont evidens, hiszen mint azt korábban említettük volt egy fogalmi kitekintő keretében, az információ számtalon formában van jelen az őt továbbítani, feldolgozni, tárolni predesztinált infokommunikációs rendszerben, mint például hang, kép, jelzés és a számunkra, a cikk szempontjából meghatározó jelentőséggel bíró adat formájában. Tehát az adat tekinthető úgy is, mint egy ismeretelem, egy valamilyen információt magában hordozó, az információ, mint értelemmel bíró adat, „infokommunikációs elem", melyet tartalmának függvényében minősíteni, az adathoz való hozzáférést a szükséges és elégséges mértékben korlátozni kell, az adatot védeni kell, és biztosítani kell a bizalmasságát[14], sértetlenségét[15] és rendelkezésre állását[16]. [7][10]

A MINŐSÍTETT ADATOK VÉDELMÉRŐL SZÓLÓ 2009. ÉVI CLV. TÖRVÉNY LÉTREJÖTTÉNEK OKAI

A Sólyom László Köztársasági Elnök Úr és a Dr. Katona Béla Úr az Országgyűlés elnöke által aláírt, a minősített adat védelméről szóló törvényt, mely 2010. április 1.-jén lépett hatályba, alapvetően az állami és közfeladatok zökkenőmentes, zavartalan biztosítása érdekében, a közérdekű adatok megismerésének alkotmányos jogából, valamint ennek a jognak a kizárólag szükséges és arányos mértékű korlátozásából kiindulva alkotta meg az Országgyűlés. A törvény megalkotása időszerű volt több szempontból is, értendő ez alatt az idejétmúlt korábbi szabályozás aktualizálása, egyértelművé tétele, a hiányzó szabályozási részelemek, részterületek, a minősített adatok kezelésével foglalkozó nélkülözhetetlen új intézmények, szervezeti elemek felállítása, létalapjuk és intézményrendszerük megteremtése, a hazai szabályozásnak a szövetségesi rendszerekben működő szabályozásnak és gyakorlatnak való megfeleltetése.

Ennek az új törvénynek a megalkotását az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény szükségessé vált átfogó felülvizsgálata során feltárt hiányosságok tették indokolttá. A felülvizsgálat alkalmával megállapítást nyert többek között, hogy kifejezetten sok a „Szigorúan titkos" és a „Titkos" minősítési jelzéssel ellátott nemzeti minősített adat. Ugyanakkor problémát jelentett bizonyos jogintézmények hiánya is, mint a nemzeti személyi és telephely biztonsági tanúsítványok és a nemzeti iparbiztonsági rendszer, melynek következtében például EU Telephely Biztonsági Tanúsítvány hiányában magyar gazdálkodó szervezetek nem vehettek részt az EU adatok megismerését indokolttá tevő tenderekben. Továbbá a különböző nemzetközi szervezetekben történő szerepvállalásunk, az Euroatlanti régióban elfoglalt helyünk is újabb problémákat, végrehajtandó feladatokat, és megoldásra váró szabályozási kérdéseket vetett fel ezen a téren. Ennek következtében a revízió rávilágított a külföldi, elsősorban NATO és EU, valamint a nemzeti minősített adatok védelmére vonatkozó követelményrendszerek közötti markáns különbözőségekre, mint például az elektronikus információbiztonságra[17] vonatkozó szabályok hiányára, a nemzetközi

rendszeresített számítógépek (palmtopok, laptopok, törzsmunkaállomások, digitálisan vezérlet híradó eszközök, ellenőrző és felderítő eszközök, fegyverek és fegyverrendszerek, stb.) kezelésének mesterfokú elsajátítása.

13 Információs harcos: „Az információs hadszíntéren az információs műveleti terv szerint digitális adatszerző, feldolgozó, továbbító, valamint támadó és védő információs műveleti eszközökkel (fegyverekkel), eljárásokkal harcolnak."

14 Bizalmasság: A minősített adatot csak az arra jogosult személy ismerheti meg, csak ő férhet hozzá. Nem fordulhat elő illetéktelen, jogosulatlan információszerzés vagy a minősített adat nyilvánosságra kerülése.

15 Sértetlenség: A minősített adat tartalmát csak az arra jogosult személy változtathatja meg, illetve az adatot csak ő törölheti. Kiküszöböli annak a lehetőségét, hogy a minősített adatot észrevétlenül módosítsák.

16 Rendelkezésre állás: Lehetővé teszi, hogy az arra jogosult személy számára a minősített adat elérhető, hozzáférhető legyen, egyáltalán, hogy használni tudja azt.

17 Elektronikus információbiztonság: INFOSEC – Information security (Electronic information security). „A távközlési és informatikai, valamint egyéb elektronikus rendszerekben és támogató infrastruktúráiban alkalmazott

szervezetek minősített adatok kezelésére vonatkozó szabályrendszereiben bekövetkezett változások (EU) hazai szabályozásba való integrációjának, átültetésének elmaradására. Az új titokvédelmi törvény hiányában jelentős nehézségekbe ütközött többek között a minősített adatok cseréjével járó két vagy többoldalú biztonsági megállapodások megkötése is, nem volt megfeleltetés a nemzetközi szervezetek gyakorlatában alkalmazott és a nemzeti minősítési szintek vonatkozásában, valamint a Bűntető Törvénykönyv állam és szolgálati titok megsértésére vonatkozó paragrafusai ugyancsak nem álltak összhangban a NATO szabályozással. [7][13][[14]

ALAPVETŐ CÉLOK

A törvény megalkotásával alapvető célul tűzték ki többek között a jogállamiság intézményének alappillérét megtestesítő alapvető jogok tiszteletben tartása, az ország érdekeinek védelme és a nemzetközi kötelezettségvállalásainak maradéktalan teljesítése érdekében, a minősített adatok létrejöttével, kezelésével, a minősítési eljárással, a nemzeti minősített adatok felülvizsgálatával kapcsolatos rendszabályok, a minősített adatok védelme általános szabályainak, az ezt megvalósító személyek és szervezetek körének, a nemzeti iparbiztonsági rendszer főbb eleminek a meghatározását. Szükségessé vált tehát egy egységes követelményrendszer megfogalmazása mind a nemzeti mind a külföldi minősített adatok védelmével kapcsolatban. A törvény megalkotásának indokai között felvonultatott probléma okán, mely a nagyszámú nemzeti minősített adat létére utal, egyértelműen következik, hogy a törvényalkotás egyik alapvető célját testesítette meg ezen adatok volumenének a redukálása. Célként fogalmazható meg többek között a széttagolt szakmai felügyeleti rendszer egységesítése is. [7]

A törvényalkotó természetesen alapul vette a minősített adat kezelésére vonatkozó alapvető kritériumokat, mint a bizalmasság, a sértetlenség és a rendelkezésre állás elvét párhuzamban a szükségesség és arányosság[18], valamint a szükséges ismeret[19] elvének figyelembevételével. [7][10]

ÉRTELMEZŐ RENDELKEZÉSEK

Mint a törvények nagy többségében, és mint az a korábbi 1995. évi LXV. az államtitokról és szolgálati titokról szóló törvényben is tapasztalható volt, ebben az esetben is sor került az egységes értelmezéshez, közös nyelvezethez elengedhetetlenül szükséges fogalomcsokor meghatározására és kifejtésére. Ennek keretében a törvény vonatkozó paragrafusa és annak alpontjai magukba foglalják a minősített adat és az ahhoz szorosan kapcsolódó fogalomtár definiálását, egységes keretbe integrálva a minősített adat kezeléséhez fűződő eljárásokkal, személyekkel, szervezetekkel kapcsolatos definíciókat.

Az információs társdalom „elektronikus íróasztalán" egymás mellé fektetvén a korábbi törvényt és annak utódját, első látásra szembeötlővé válik az a nagyon fontos észrevétel, hogy az aktuális passzus szól, illetve rendelkezik a megértés alapját képező olyan új definíciókról, mint a személyi biztonsági tanúsítványról[20], a telephely biztonsági

rendszabályok összessége amelyek védelmet nyújtanak az előállított, feldolgozott, tárolt, továbbított és megjelenített információk, bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen.

18 Szükségesség és arányosság elve: A közérdekű adatok nyilvánosságának korlátozásával foglalkozik, melynek értelmében az adat nyilvánossághoz fűződő jogát csak a törvényi feltételek teljesülése esetén, a védelméhez szükséges mértékű minősítési szinttel és csak a feltétlenül szükséges ideig lehet korlátozni.

19 Szükséges ismeret elve: Az elv a minősített adat megismeréséről rendelkezik, melyet azon személyek részére tesz lehetővé, akiknek az állami vagy közfeladataik ellátásához feltétlenül szükséges.

20 Személyi biztonsági tanúsítvány: A 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kaphat felhasználási engedélyt."

tanúsítványról[21], és az elektronikus adatkezelő rendszerről[22], mely fogalmak törvényi meghatározása, leszabályozása kvázi az új törvény megalkotása indokainak tárházában jelesen képviseltetik magukat, mint azt korábban említettük volt. Véleményem szerint megemlítendő jelentős különbözősége az értelmező rendelkezéseknek az is, hogy a titokbirtokos[23] fogalmát szétbontva az új törvény vonatkozó paragrafusai különbséget tesznek a minősítő[24], a felhasználó[25] és a közreműködő személye[26] között is. [7][14]

A MINŐSÍTŐK ÉS A MINŐSÍTÉSI ELJÁRÁS SZABÁLYAI

A törvény vonatkozó paragrafusa szabályozza, és egyértelműen meghatározza azon személyek körét, akik feladat és hatáskörükben egy adat vonatkozásában minősítő jogkörrel rendelkeznek. Ezzel párhuzamosan szabályozza magát a minősítés tevékenységét is, beleértve a minősítéssel védhető közérdekek körének meghatározását, az adat minősítésének egyes eseteit, az alkalmazható minősítési szintek megjelölését és a nemzeti minősített adat felülvizsgálatának és felülbírálatának egyes eseteit.

Itt fontos megemlítenünk a törvény hordozta legjelentősebb változások közül néhányat, melyeket a fent nevezett cím alatt csoportosuló vonatkozó paragrafusok hordoznak magukban. Egyik ilyen változás, hogy a minősítők körében a Legfelsőbb Bíróság elnöke mellett az Országgyűlés Igazságszolgáltatási Tanácsának az elnökét is megjeleníti, ebbe a körbe sorolja továbbá a Nemzeti Biztonsági Felügyelet vezetőjét is, ugyanakkor olyan, az 1995. évi LXV. törvényben meghatározott személyek, mint az Országos Egészségbiztosítási Pénztár elnöke vagy az Országos Nyugdíjbiztosítási Főigazgatóság főigazgatója, a jelen törvényben nem kerülnek a minősítők körébe sorolásra.

Ugyancsak markáns eltérés a két törvény között, hogy az utóbbi esetében az egyes minősítési szinteket az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által okozható kár mértéke határozza meg. Ennek megfelelően „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" minősítési szintekről szól, mely szintek már teljes harmóniát mutatnak többek között a NATO-ban alkalmazott minősítési szintekkel[27]. Ugyanakkor ennek folyamodványaként megszűnik az „Államtitok" és „Szolgálati" titok, mint minősítési szint kategória, melyről a korábbi törvény még aktívan rendelkezett, és ezzel egyetemben módosításra kerültek a különböző minősítési szintek érvényességi ideje is. Az 1995. évi LXV. törvény értelmében az akkor megfogalmazott „Államtitok" kategória maximális érvényességi idejét 90 évben, a „Szolgálati titok" kategória érvényességi idejét, pedig 20 évben limitálta a törvényalkotó. Jelen esetben ez oly módon változott meg, hogy a „Szigorúan titkos" és „Titkos" minősítési szint esetén 30 évben, a „Bizalmas" minősítéssel ellátott adat esetén 20 évben, a „Korlátozott

21 Telephely biztonsági tanúsítvány: A 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „az a tanúsítvány, amely meghatározza, hogy a gazdálkodó szervezet milyen legmagasabb minősítésű szintű minősített adat kezelésére alkalmas".

22 Elektronikus rendszer: Az elektronikus adatkezelő rendszer a 2009. évi CLV. törvény értelmező rendelkezések részében foglaltak értelmében „minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese".

23 Titokbirtokos: Az 1995. évi LXV. törvény általános rendelkezések értelmében „a minősítő, valamint az a személy vagy szerv, akinek vagy amelynek a minősített adatot … továbbították".

24 Minősítő: A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „feladat és hatáskörében minősítésre jogosult személy".

25 Felhasználó: A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „az a személy, akinek állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít".

26 Közreműködő személy: A 2009. évi CLV. törvény értelmező rendelkezések részének értelmében „az a természetes személy, aki az állami vagy közfeladatot ellátó szerv feladat- és hatáskörébe tartozó ügyben segítséget nyújt, és ehhez minősített adat felhasználása is szükséges."

27 NATO-ban alkalmazott minősítési szintek: „NATO Cosmic Top Secret", „NATO Top Secret", „NATO Confidential", „NATO Restricted"

terjesztésű" minősítési szinttel védett adat esetén, pedig legfeljebb 10 évben állapította meg az érvényesség idejét a törvényalkotó. Természetesen meghatározott módon, korlátozott formában, de mind a két törvény lehetőséget biztosított és biztosít a különböző minősítési szintek érvényességi idejének a meghosszabbítására. Továbbá az új törvény azonosítja az új minősítési szinteknek megfelelő típusú nemzetbiztonsági ellenőrzések szintjét is, mely „Szigorúan titkos" minősítés esetén „C", „Titkos" minősítés esetén „B", „Bizalmas" minősítés esetén „A" típusú nemzetbiztonsági átvilágítást követel meg. A „Korlátozott terjesztésű" minősítési szint esetén a törvény nem rendelkezik nemzetbiztonsági kérdőív kitöltéséről. [7][14]

KÜLFÖLDI MINŐSÍTETT ADAT

A 2009. évi CLV. törvény vonatkozó paragrafusai kifejezetten a külföldi minősített adatok kezelésére helyezik a hangsúlyt, melyre a korábbi törvényben nem történt intézkedés.

A 2009. évi törvény a 2. számú mellékletében összefoglalja, rendszerezi a különböző nemzetközi szervezetek, mint a NATO, EU, NYEU, EURATOM[28], EUROPOL[29], EUROJUST[30] által alkalmazott minősítési szinteket, és azonosítja az ezeknek megfelelő nemzeti minősítési szinteket. Ha visszagondolunk a korábban említett, a törvény megalkotását szorgalmazó indokokra, célokra, a nemzeti és külföldi minősített adatok jelölésére szolgáló, a hazai és nemzetközi szervezetek gyakorlatában alkalmazott egyes minősítési szintek egymáshoz illesztése, egymásnak való megfeleltetése, harmonizációja ugyancsak időszerű és halasztást nem tűrő ok volt.

Nagyon fontos kiemelni, hogy a törvény rendelkezése értelmében, abban az esetben, ha a nemzeti minősített adat külföldi minősített adatot is tartalmaz, akkor annak minősítési szintje és a minősítés érvényességi ideje nem lehet kisebb és rövidebb, mint a külföldi minősített adat minősítési szintje és annak érvényességi ideje. [7][14]

A MINŐSÍTETT ADAT BIZTONSÁGÁRA VONATKOZÓ SZABÁLYOK

A minősített adatok védelméről szóló törvény a minősített adatok biztonságára vonatkozó szabályok részének első, 10 §-a egy jelentős kritériumot fogalmaz meg a minősített adatok kezelésével kapcsolatban, melynek értelmében minősített adatot kezelni csak a Nemzeti Biztonsági Felügyelet által kiadott engedély alapján lehet, mely szerv új elemként jelent meg korábban a törvénynek a minősítők körét meghatározó paragrafusa alatt. Ezt megelőzően az államtitokról és szolgálati titokról szóló törvény vonatkozó rendelkezése a belügyminiszter felügyeleti jogkörének keretébe helyezte a minősített adatok védelmének szakmai felügyeletét.

A minősített adatokhoz való hozzáférést kizárólagosan a személyi biztonsági tanúsítvány és titoktartási nyilatkozat meglétéhez köti. A személyi biztonsági tanúsítvány kiadása a Nemzeti Biztonsági Felügyelet hatáskörébe tartozó feladat. A minősített adat megismerésével kapcsolatban továbbra is megmarad a megismerési engedély és titoktartási

28 EURATOM: The European Atomic Energy Community - Európai Atomenergia Közösség. Egy nemzetközi szervezet, melyet 1957.-ben alapítottak a második római szerződéssel. A közösség lényege abban áll, hogy a szerződés aláírói egyértelmű szándékukat fejezték ki az atomenergia békés célú felhasználásával kapcsolatban és az atomenergia-iparban történő készséges együttműködésük iránt. Több ügynöksége létezik, többek között Spanyolországban.

29 EUROPOL: The European Police Office - Európai Rendőrségi Hivatal. Az Európai Unió rendvédelmi ügynöksége, melynek legfontosabb célkitűzése egy biztonságosabb Európa megteremtése, segítségnyújtás az Európai Unió tagállamai rendvédelmi szervei részére a nemzetközi bűnözés és terrorizmus visszaszorítása érdekében. Székhelye Hollandia.

30 EUROJUST: The European Union's Judicial Cooperation Unit - Európai Igazságügyi Együttműködési Egység. A szervezet 2002-ben lett létrehozva az EU által azzal a céllal, hogy előmozdítsák az együttműködést az uniós tagállamok igazságügyi hatóságai között a két vagy több uniós tagállamot érintő nyomozati és büntetőeljárások keretében. Székhelye Hollandia.

nyilatkozat intézménye mondhatni a személyi biztonsági tanúsítvány intézményén belül, leszabályozva azokat az eseteket a megismeréssel és felhasználással kapcsolatosan, amikor az érintettnek nem kell rendelkeznie a nevezett tanúsítvánnyal.

Továbbá előírja, hogy minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a személyi[31], fizikai[32], adminisztratív[33] és elektronikus biztonság [10] feltételeket is. Ez önmagában véve nem jelentene merőben új szabályozást, hiszen az előző törvény a titokbirtokos szerv vezetőjének feladat és hatásköre keretében rendelkezik a minősített adatok védelmi rendszerének biztonsági elemeiről, beleértve az imént felvázolt biztonsági feltételeket is, de az új törvény már külön rendelkezik az elektronikus rendszereken kezelt minősített adat és az elektronikus rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának kérdésében is, melyről az 1995. évi LXV. törvényben még nem találunk említést.

Ugyancsak új rendelkezése a törvénynek a személyi biztonsági tanúsítvány intézménye mellett a telephely biztonsági tanúsítvány intézménye is a gazdálkodó szervezetek vonatkozásában, melynek kibocsátását a Nemzeti Biztonsági Felügyelet hatáskörébe utalja. A telephely biztonsági tanúsítvány kibocsátása az iparbiztonsági ellenőrzés lefolytatását követően válik indokolttá abban az esetben, - természetesen, ha kockázati tényezők nem merülnek fel - amikor a minősített adatot kezelő szervnek az állami vagy közfeladata ellátása érdekében gazdálkodó szervezet közreműködését veszi igénybe. [7][13][[14]

A MINŐSÍTETT ADAT VÉDELMÉT ELLÁTÓ SZERVEZETEK ÉS SZEMÉLYEK

A 2009. évi CLV. törvény soron következő V. nagy fejezetében kerülnek meghatározásra a minősített adatok kezelésével kapcsolatban érintett személyek és szervezetek, többek között a már oly sokat emlegetett Nemzeti Biztonsági Felügyelet is. A törvény részletekbe menően szabályozza az érintett szervezet tevékenységi körét, legfőbb feladatát, mely többek között nem más, mint a minősített adat védelmének hatósági felügyelete, a minősített adat kezelésének hatósági engedélyezése és felügyelete, továbbá a nemzeti iparbiztonsági hatósági feladatok ellátása. Korábban az 1995. évi LXV. az államtitokról és szolgálati titokról szóló törvény értelmében a titokbirtokos szerv vezetőjének hatás és feladatkörébe tartozó tevékenység volt a minősített adatok védelméről szóló jogszabályok végrehajtásáról, illetve a hatáskörében keletkezett vagy más szervek által átadott minősített adatok védelmi rendszerének különböző biztonsági elemekkel való kiépítettségéről és működtetéséről történő gondoskodás, mint azt korábban említettük volt.

A felügyelet feladat és tevékenységi körének legfontosabb részét képezi az új törvény által életre hívott személyi biztonsági tanúsítvány, telephely biztonsági tanúsítvány kiadása, a minősített adatok kezelésére szolgáló elektronikus rendszerek használatbavételének engedélyezése, a rejtjeltevékenység hatósági engedélyezésének és felügyeletének biztosítása, a minősített adatok védelmével kapcsolatos bejelentések kivizsgálása, csakhogy néhányat említsünk a legfontosabbak közül. Továbbá korábban említettük volt, hogy az új törvény megalkotásának egyik fontos indokaként jelenik meg a nemzetközi szervezetekkel, szabályozással való harmonizáció, ebből kifolyólag a törvényalkotó a felügyelet

31 Személyi biztonság: „…a minősített információ csak olyan személynek juthat birtokába, aki megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelel, illetve az adott minősítésű információ megismerése számára hivatalos célból szükséges. A személyi biztonság megteremtésének egyik legfontosabb eljárása a nemzetbiztonsági ellenőrzés."

32 Fizikai biztonság: „Azon rendszabályok és tényleges akadályok - …falak,…behatolás jelzők, beléptető rendszerek, stb. – összessége, melyek megfosztják az illetékteleneket a minősített, kritikus információkhoz, dokumentumokhoz, eszközökhöz való hozzáféréstől… és meghiúsítják vagy megakadályozzák a fizikai támadást."

33 Dokumentumbiztonság: „ A titokvédelem tágabb értelmezése, amely azt jelenti, hogy az összes dokumentumot a minősítésének, az érzékenységének, vagyis a titkossági osztályba sorolásának megfelelően kell védeni….A dokumentumbiztonság közvetlenül kapcsolódik az elektronikus információbiztonsághoz, hiszen valamennyi elektronikus adathordozó egyben dokumentumnak is minősül."

tevékenységi körébe utalta a különböző nemzetközi szervezetek vonatkozó szabályzataiban, illetve a minősített adatok védelme tárgyában kötött nemzetközi szerződésekben a nemzeti biztonsági hatóságok számára előírt feladatok ellátását is. [7][14]

MÓDOSULÓ RENDELKEZÉSEK

Mivel a 2009. évi CLV. törvény a minősített adatok védelméről jelentős változást hoz a korábbi 1995. évi LXV. törvény az államtitokról és szolgálati titokról törvény vonatkozásban, ha már csak az új megnevezésekre, tanúsítványokra vagy szervezetekre gondolunk is, ezért elengedhetetlenül szükséges mindazon releváns törvényekről és az őket kő keményen érintő módosító rendelkezésekről megemlékezni, melyeket maradéktalanul harmonizálni szükséges az új törvény tükrében. Részletekbe menően nem kívánunk kitérni e módosító rendelkezések hosszas felsorolására, csupán címszavakban kívánjuk megemlíteni az érintett törvényeket.

A 2009. évi törvény alkotta szabályozás szorosan érinti tehát többek között a „Büntető Törvénykönyvről szóló 1978. évi IV. törvény", „A csődeljárásról és felszámolási eljárásról szóló 1991. évi XLIX. törvény", „Az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény", „A szervezett bűnözés, valamint az azzal összefüggő egyes jelenségek elleni fellépés szabályairól és az ehhez kapcsolódó törvénymódosításokról szóló 1999. évi LXXV. törvény", „Az elektronikus hírközlésről szóló 2003. évi C. törvény", „Az Európai Parlament magyarországi képviselőinek jogállásáról szóló 2004. évi LVII. törvény", „A légi-, a vasúti és a vízi-közlekedési balesetek és egyéb közlekedési események szakmai vizsgálatáról szóló 2005. évi CLXXXIV. törvény", „Az elektronikus közszolgáltatásokról szóló 2009. évi LX. törvény", „Az országgyűlési képviselők jogállásáról szóló 1990. évi LV. törvény", „A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény", „Az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvény", „A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény", valamint „A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény" releváns paragrafusait. [7][14]

FELHATALMAZÁS

A törvényalkotó felhatalmazza a Kormányt, hogy rendelettel szabályozza a törvényben megjelenő, a korábbi törvényhez képest végbemenő legfontosabb változásokat, értendő ezalatt, hogy a Kormány állapítsa meg többek között a Nemzeti Biztonsági Felügyelet részletes feladatait, eljárás és működési rendjét, a minősített adatok kezelésének rendjét, a minősített adat elektronikus kezelésének részletes szabályait, a rejtjeltevékenység engedélyezésének rendjét és a hatósági felügyeletének részletes szabályait, valamint az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályait. [7]

ZÁRÓ RENDELKEZÉSEK

A jogharmonizáció elősegítése érdekében a 2009. évi CLV. törvény a záró fejezetében rendelkezik a két törvény közötti átmeneti időszakban végrehajtandó intézkedésekről, elindított folyamatokról és határidőkről, megszűnő törvényekről és újabb, esetenként minősített többséget igénylő módosító rendelkezésekről is úgy, mint a személyi biztonsági tanúsítvány beszerzésének, a minősített adatok védelmére vonatkozó fizikai és elektronikus biztonsági feltételek megteremtésének a határidejéről, az 1995. évi LXV. törvény az államtitokról és a szolgálati titokról hatályát vesztéséről, és olyan már korábban is említett

esetekről, melyek az új törvény megszületése és hatályba lépése következtében módosulásokon kell, hogy átessenek. [7][14]

REZÜMÉ

Összegezvén a minősített adatok védelméről szóló 2009. évi CLV. törvény legfontosabb passzusait, dióhéjban az alábbi gondolatokat kell felelevenítenünk. Leszögezhetjük, hogy a törvény megalkotása a korábbi szabályozás hiányossága, idejétmúlt volta, a nemzetközi szabályozásban végbemenő változások, a szabályozási rendszerek és törvényi hátterek harmonizációjának szükségessége okán indokolt volt. Olyan új változások következtek be, mint például a különböző minősítési szinteknek az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által okozható kár mértéke által történő meghatározása, az „Államtitok" és „Szolgáti titok" minősítési szintek megszűntetése, a „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" minősítési szintek meghatározása, az egyes szintek maximális érvényességi idejének újralimitálása, a hozzájuk szükséges nemzetbiztonsági átvizsgálási szintek újradefiniálása, a Nemzeti Biztonsági Felügyelet felállítása, hatás, feladat és tevékenységi körének meghatározása, a személyi és telephely biztonsági tanúsítvány fogalmi kategória megalkotása, az elektronikus információbiztonságra vonatkozó szabályok életre hívása, az iparbiztonsági ellenőrzés intézményének megteremtése, csakhogy a legfontosabbakat említsük a teljesség igénye nélkül.

HIVATKOZÁSOK

[1] „Zöld Könyv" A távközlési, média és információ-technológiai szektorok konvergenciájáról és ennek szabályozási kihatásairól. European Comission, Brüsszel, 1997. december 03. (Forrás: http://www.itb.hu/dokumentumok/zold_konyv/index.html#toc /letöltés ideje: 2009.11.10./)

[2] Jobbágy Szabolcs: Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. – In: Hadmérnök A ZMNE Bolyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On - line Tudományos Kiadványa, 2009. március, IV. évfolyam 1. szám (elektronikus) – p. 184-196. (Forrás: http://www.hadmernok.hu/2009_1_jobbagy.pdf /letöltés ideje: 2009.11.10./)

[3] Magyar Hadtudományi Társaság: Hadtudományi Lexikon I. kötet. Szabó József (főszerk.) – Budapest, 1995 – ISBN 963 04 5227 8

[4] Dr. habil Sándor Miklós nyá. ezds – Farkas Tibor fhdgy. – Jobbágy Szabolcs fhdgy.: Híradásszervezés jegyzet a BJKMK Híradó Tanszék BSc, MSc és PhD hallgatói számára – Budapest, ZMNE EEK, 2009 – 109 p.

[5] Muha Lajos: Infokommunikációs biztonsági stratégia. – In: Hadmérnök A ZMNE Bolyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On - line Tudományos Kiadványa, 2009. március, IV. évfolyam 1. szám (elektronikus) – p. 214-224. (Forrás: http://hadmernok.hu/2009_1_muha.pdf - /letöltés ideje: 2009.11.14./)

[6] Magyar Honvédség Öszhaderőnemi Doktrína 3. kiadás (ÁLT/27) – Honvédelmi Minisztérium kiadványa, 2010.

[7] 2009. évi CLV. törvény a minősített adat védelméről – Magyar Közlöny a Magyar Köztársaság Hivatalos Lapja, 2009. december 29. kedd, 194. szám (Forrás: www.nbf.hu/anyagok/jogszabaly/09CLV.doc - /Letöltés ideje: 2010.04.14./)

[8] Dr. Seres György: A digitális hadszíntér határai. – Előadás a Robothadviselés I Konferencián (elektronikus változat), 2001 – 11 p. (Forrás: http://drseres.com/publik/pdf/digit_hun.pdf - /letöltés ideje: 2010.04.06./)

[9] Gácser Zoltán mk. őrgy.: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben. – Doktori PhD értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2008.

[10] Dr. Haig Zsolt mk. alez.: Az információs társadalom információbiztonsága Egyetemi jegyzet. – Budapest, ZMNE EKK, 2009 – 179 p.

[11] Nagy Zoltán: A 21. század fegyveres küzdelmeinek irányai és kihívásai a NATO szemszögéből. –In: Hadtudomány. A Magyar Hadtudományi Társaság folyóirata, 2005. december, XV. Évfolyam, 4. szám (elektronikus) (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_4.html /letöltés ideje: 2010.04.06./)

[12] Várhegyi István – Makkay Imre. Információs korszak, információs háború, biztonságkultúra. – Budapest, OMIKK, 2000 – 296 p. – ISBN 963593 238-3

[13] Zala Mihály: Az új információvédelmi törvény és kihatásai. – Innovációval a Védelemért és a Biztonságért Társaság Innovációs Klub klubnapján elhangzott előadás anyaga, 2010. január 20. (Forrás: http://www.ivb.org.hu/IC-Download.php - /letöltés ideje: 2010.04.17./)

[14] 1995. évi LXV. törvény az államtitokról és a szolgálati titokról – A Magyar Köztársaság Információs Hivatala – (Forrás: http://www.mkih.hu/torvenyek/t9500065/t9500065.htm#kagy1 /letöltés ideje: 2010.04.21./)