SEBESTYÉN ATTILA

AZ INFORMÁCIÓVÉDELEM FELÜGYELETI SZEREPKÖREINEK AKTUÁLIS KÉRDÉSEI

Az informatika, az információ-technológia mindennapjaink meghatározó részesévé vált. A „fejlett gazdaságú" társadalmakban a termelés mozgatórugója az információ. A teljesítőképesség, a hatékonyság mércéje az információval való gazdálkodás képessége. A „technotronikus"[1] kor előtt állunk, amelynek nem csak látható jelei vannak, a köznyelvben is általánosan használt kifejezésekkel azonosítjuk úgy, mint információs társadalom, e-kormányzás, fenntartható fejlődés stb..

A „mindent behálózó informatika", az informatikai rendszerekben tárolt adat a hatékonyság mellett, eddig nem ismert, megfelelően fel nem becsült kockázatot is jelent. Kockázatot, amely a szándékaink megismeréséből, az adataink ellopásából, megváltoztatásából, a hozzáférés, rendelkezésre állás ellehetetlenítéséből fakadó károkozásból következik.

Szinte nincsen olyan nap, amikor ne jelenne meg valamilyen „biztonsági riasztás". Csak néhány szalagcím 2013-2015-ből:

- Heti Világgazdaság (2013. június 11.): Assange: a titkos adatgyűjtést leleplező Snowden egy hős (http://hvg.hu/vilag/20130611_Assange_a_titkos_adatgyujtest_leleplezo_S) – 2015. július 30.
- Magyar Nemzet Online (2013. október 31.): Beismerte az NSA, hogy lehallgatták Merkelt (http://mno.hu/hirtvarchiv/beismerte-az-nsa-hogy-lehallgattak-merkelt-1192975) – 2015. július 30.
- Népszabadság Online (2014. augusztus 21.): Öt éve futhat magyar gépeken a mindent látó kémprogram (http://nol.hu/belfold/ot-eve-futhat-magyar-gepeken-a-mindent-lato-kemprogram-1481505) – 2015. július 30.
- Index.hu (2014. november 24.): Rejtélyes trójai kémkedett fél évtizedeken át (http://index.hu/tech/2014/11/24/rejtelyes_trojai_kemkedett_fel_evtizeden_at/) – 2015. július 30.
- Népszabadság Online (2015. január 23.): Komoly hibára bukkantak az Adobe Flash Playerben (http://mno.hu/digitalis/komoly-hibara-bukkantak-az-adobe-flash-playerben-1269211) – 2015. július 30.
- Mobilaréna (2015. június 17.): 600 millió Samsung telefon került veszélybe (http://mobilarena.hu/hir/600_millio_samsung_telefon_kerult_veszelybe.html) – 2015. július 30.
- GOV Cert Magyarország (2015. július 22.): A Google 43 sebezhetőséget javított a Chrome böngésző kapcsán. (http://tech.cert-hungary.hu/vulnerabilities/CH-12459) – 2015. július 30.

[1] Alvin Toffler: A harmadik hullám. Typotex Kft. Budapest, 2001.

Az emberiség „új korszaki hódításai” nem jöhettek volna létre a számítógépek hiányában. Fontos lépcső volt a fejlődésben az integrált áramkör (1958), majd a mikroprocesszor megjelenése (1971). A fejlődés hihetetlen dinamizmust mutatott, amelyekről Gordon Moore 1965-ben lejegyzett jóslata lassan ötven éve beigazolódik. „*Moore-törvénynek nevezzük azt a tapasztalati megfigyelést a technológiai fejlődésben, mely szerint az integrált áramkörök összetettsége – a legalacsonyabb árú ilyen komponenst figyelembe véve – körülbelül 18 hónaponként megduplázódik*.”[2] A jóslat eredetileg az integrált áramkörökre vonatkozott, de azóta az adattárolásban, a memória kapacitásban is hasonlóan fennmaradó fejlődési tendencia figyelhető meg. A technológiai fejlődés hova tovább elősegítette a „dipólusos világrend” felbomlását. Elegendő említeni a COCOM[3] lista, vagy a „csillagháborús törekvések” kulcsszavakat. Az informatikai technológiai fejlődés szempontjából a kutatás-fejlesztés gyorsasága mellett, lényegi tulajdonsága a fejlődésnek az eszközök előállítási- és működtetési költségeinek csökkentése, amely velejárója volt a méretcsökkentés igénye is. Ez vezetett a napjainkban is zajló miniatürizáláshoz és a funkcionális integráláshoz.

Schumpeter[4] innovációra vonatkozó megállapítására, amely szerint a kutatás-fejlesztésből kvázi monopolhelyzet következik, amely rövidtávon, az adott termék, vagy szolgáltatás „lemásolásáig” extraprofitot termel a gyártónak, egyértelműsíthető az a gyártói szándék, hogy termékeiket mindig új és újabb tulajdonságokkal vértezzék fel, ettől várva a piac kedvező fogadtatását.

Gondoljunk csak bele az elmúlt évtized „okos telefon” fejlesztéseibe, a telefonálástól idegen szolgáltatások integrálásába, a telefonban elhelyezett (számológép, naptár, zseblámpa, navigátor stb.) fényképezőképek felbontásának dinamikus növekedésére és itt állunk az „okos óra” térhódítása előtt, ami mind a miniatürizálás, mind a szolgáltatás integráció példája lehet.

A kutatás-fejlesztésből következő minőségromlás

A kutatás-fejlesztés és az ebből következő kvázi piaci monopolhelyzetű megjelenés óhatatlanul magában hordozza annak lehetőségét, hogy a gyártók a terméket korábban bocsássák piacra, mint hogy egy kiérlelt, minden komponensében kitesztelt, bevizsgált termék állna elő.

A kutatás-fejlesztés és a gyártás során az extraprofit szempontjából majdnem olyan fontos követelmény a gyorsaság, az első megjelenés, mint maga a fejlesztési ötlet és annak ipari szintű megvalósítása. Az extraprofit és a befektetett tőke vesztesége erősen függ az

[2] A Moore-törvény szócikk – Forrás: http://hu.wikipedia.org/wiki/Moore-t%C3%B6rv%C3%A9ny (Letöltés ideje: 2015. 07.30.)

[3] ”*A COCOM-lista egy, a keleti blokk országait sújtó, multilaterális kereskedelmi embargó volt. A lista az embargót koordináló 1947-ben alapított bizottság, a **Co**ordinating **Com**mittee for Multilateral Export Controls első két szavának rövidítéséből kapta nevét. A COCOM-lista egy csúcstechnológiai termékeket tartalmazó feketelista volt, melyeket nem volt szabad az embargó alatt álló országokba (KGST, Kína) exportálni, hogy azok így egyre inkább lemaradjanak a fegyverkezési versenyben. A COCOM-listát ezért a gazdasági hadviselés egyik formájának is lehet tekinteni*.” Forrás: http://hu.wikipedia.org/wiki/COCOM-lista (Letöltés ideje: 2015. 07.30.)

[4] Joseph Alois Schumpeter, Nobel-díjas osztrák közgazdász (1883. február 8. — 1950. január 8) az innováció természetének alapjairól szóló munkájában többek között kifejti, hogy a technológiai kutatás-fejlesztéssel termelt új javak rövidtávon monopolhelyzetet teremtenek, amely elméletet jól igazol az információ-technológiai verseny, az eszközalapú rendszerintegrációs törekvések (ld. mobiltelefónia)

ötlet és a piaci megjelenés között idő rövidségétől. Ebből azonban szükségszerűen következik, hogy a termék önmagában hordozhat (és hordoz) alapvető működési rendellenességeket, hibákat, a jövőben kihasználható biztonsági hiányosságokat. (Természetesen ugyanez a piaci versenyhez igazodó magatartás az asztali számítógépek, a szerverek operációs rendszereinek és az eszközök versenyében is megfigyelhető.) Ha elfogadjuk tényként, hogy az informatikai eszközök és szolgáltatások a fejlesztési versenyből következően önmagukban hordozzák a biztonsági kockázatot, akkor fontos az informatikai üzemeltetési és fenntartási tevékenységet tervszerűen, a kockázatokkal arányos módon szervezni úgy, hogy a kockázatok csökkenthetőek, az incidensek megelőzhetőek legyenek.

Az adatok tulajdonsága

Az informatikai rendszerben tárolt adatok minősége (tulajdonsága) alapján a jogszabályi környezet több féle adattípust különböztet meg (továbbiakban: adattípus). Ilyen adattípusok az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (továbbiakban: Infotv.) definiált:

- 3.§. 2. *személyes adat,*
- *különleges adat,*
- *bűnügyi személyes adat,*
- *közérdekű adat,*
- *közérdekből nyilvános adat.*

Ugyancsak adattípust definiál a minősített adat védelméről szóló 2009. évi CLV. törvény (továbbiakban: Mavtv.) a 3.§. 1. pontjában:

- *minősített adat*:
  a) *nemzeti minősített adat*
  b) *külföldi minősített adat*

Természetesen számos egyéb adattípust is definiálnak a jogszabályok, amelyeket az Informatikai Tárcaközi Bizottság annak idején (1996.) érzékeny[5] adatként definiált.Külön fontosnak tartom hangsúlyozni, amikor általánosságban adatkezelést definiálunk, hogy az informatikai rendszerben az adatkezelés nem értelmezhető kizárólag a felhasználói adatok körén, hiszen az informatikai rendszer működése önmagában is egy adatkezelő rendszer (hálózati továbbítás, megjelenítés, tevékenységnaplózás stb. „adatai").

Visszatérve az adattípusokra, jogszabályi definíciójuk nem öncélú, a jogszabályok az adatok körének és tartalmi tulajdonságainak meghatározása mellett eljárásrendeket, védelmi és biztonsági megoldásokat határoznak meg. Ebbe a körbe illik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) is, amely preambulumában rögzíti, hogy „*A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt - a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.*

[5] Érzékeny adat: érzékeny, de nem minősített adatok körébe tartoznak a jogszabályok által védendő adatok (személyes, illetve különleges adatok, az üzleti titkot, a banktitkot képező adatok, az orvosi, az ügyvédi és egyéb szakmai titkok, a posta és a távközlési törvény által védett adatok stb.) és az egyes szervezetek, intézmények illetékesei által, belső szabályozás alapján védendő adatok. (ITB 12. sz. 5.1 pont)

Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."

A biztonság megteremtésének egyik lépéseként megalkotja a felügyeleti tevékenységeket, a hatósági felügyeleti rendszert, illetve elrendeli az elektronikus információs rendszer biztonságáért felelős személy (továbbiakban: kiberbiztos) kijelölését vagy megbízását (11.§. (1) c) pont). Az adattípushoz tartozó „felelős személyt" (felügyeleti szerepkört) az Infotv. 24.§. (1) „ … *belső adatvédelmi felelőst kell kinevezni, vagy megbízni.*", és a Mavtv. is 23.§. (2) „*... a minősített adatot kezelő szerv vezetője által kinevezett biztonsági vezető ...*" kijelölni rendeli. A biztonsági vezető felügyelete mellett a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló

161/2010. (V.6.) Korm. rendelet (továbbiakban: Elektronikus r.) 11.§. (1) alapján „*Rejtjeltevékenységet folytató szerv vezetője rejtjelfelügyelőt jelöl ki vagy ...*" újabb az információbiztonsággal kapcsolatos felügyeleti szerepkört definiál a jogszabály abban az esetben, ha a minősített adat elektronikus úton is feldolgozásra kerül.

Szintén ebben a jogszabályban kerül definiálásra a „rejtjelző", a „rendszerbiztonsági felügyelő" és a „rendszeradminisztrátor" is.

Felügyeleti szerepkörök

Az egyes felügyeleti szerepköröket definiáló jogszabályok „szigetszerű" működést írnak le az egyes adattípusokra vonatkozó „elszigetelt" rendszerszemlélet alapján. Annak ellenére, hogy az informatikai rendszerben szinte sohasem fordul elő szeparált módon az egyes adattípusnak önállóan megfelelő informatikai alrendszer. Ebből következne, hogy szükséges a rendszer felügyeletének összehangolása is. Ez felveti az információbiztonsági szerepkörök jogszabályok közötti kohéziójának a megteremtési igényét.

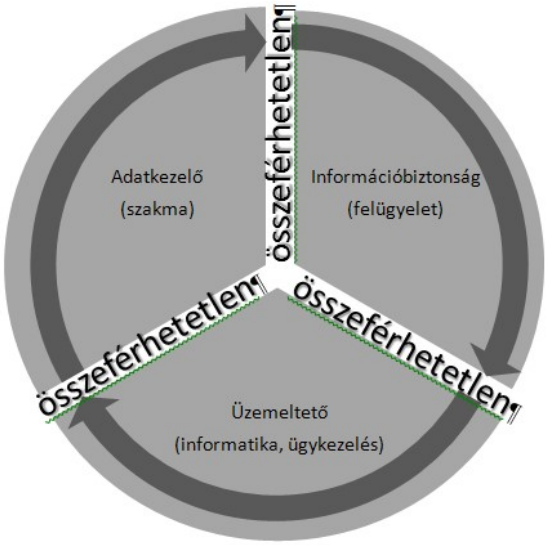
Áttanulmányozva az alapvető információbiztonsági jogszabályokat, valamint végrehajtási rendeleteiket az adat-, információvédelemmel kapcsolatos járulékos jogszabályokat, egyértelmű a jogszabályalkotó azon törekvése, hogy a közigazgatási szervek adatkezelését az adat tartalmától, minőségétől és megjelenési formájától függő módon, az adat minőségéhez – azaz az adattípushoz – rendelt védelmi megoldások érvényesítésével biztosítsa, a feldolgozás teljes szakaszában, az adatok komplex, kockázatokkal és kárértékkel arányos védelme mellett.

Összeférhetetlenség

A jogszabály kizárólag a belső adatvédelmi felelős esetében rögzíti (24.§. (1)), hogy „*... közvetlenül a szerv vezetőjének felügyelete alá tartozó… felelőst kell kinevezni…*", de a biztonsági vezető, illetve a kiberbiztos esetében ez kizárólag a szerv vezetőjének átruházott hatásköréből következtethető. Álláspontom szerint fentiek alapján alapvetően célszerűségi okok állíthatóak az információ védelmi tevékenység szerepköri összeférhetetlensége és alárendeltsége indokolására.

Az információbiztonság szempontjából ki kell alakítani a „fékek és ellensúlyok" rendszerét, amely egyik fontos pillére a szerepkörök és az összeférhetetlenségének

szabályozása. Célszerűség okán el kell különíteni az adatkezelői, az üzemeltetői és a felügyeleti szerepköröket.



1. számú ábra: információbiztonsági szerepkörök

A jogszabályok (Infotv., Mavtv., és a Ibtv. is) közös ismérve, hogy az adatot kezelő szerv vezetőjének felelősségét rögzítik, aki feladatkörében eljárva alakítja ki az adat védelmével kapcsolatos feltételeket, illetve nevezi ki az adat tulajdonsága szerint nevesített felügyeletet ellátó személyeket. Ezen túlmenően gondoskodni köteles, hogy belső normában meghatározásra kerüljenek a védelem tárgyai, módszerei, a védelemben résztvevők feladatai, felelősségük. A szerv vezetője, a felügyeleti szerepkörnek megfelelő végzettséggel, szakértelemmel és gyakorlattal rendelkező személyeket nevez ki a védelmi tevékenység megszervezésére és ellátására, illetve a szervezeti törvényből, az alap- és szaktevékenységeket meghatározó egyéb jogszabályokból következően a szervezeti és működési szabályzatban meghatározza az adatkezelők és az üzemeltetők feladatait, hatáskörét. Végső soron az adatkezelés szempontjából zárt és komplex rendszert alakít ki, a szerepkörök egyensúlyi helyzetének kialakításával.

Jogszabályi elégtelenség

A felügyeleti szerepkörök feladat és hatáskörét rögzítő jogszabályok közül kizárólag a belső adatvédelmi felelős esetében jelenik meg a szerv vezetőjének való közvetlen alárendeltség (Infotv. 24.§.(1)), a biztonsági vezető és a kiberbiztos esetében ez az átruházott hatáskörből közvetett módon származtatható.

A kiberbiztos megjelenéséig mind az adatvédelmi felelős, mind a biztonsági vezető a minősítés ténye mentén elkülönült feladatvégzést tudott megvalósítani (korábban disszonáns a minősített személyes adat kérdése), de a kiberbiztos szerepkör megjelenésével,

az egyértelmű kompetencia határok kijelölése további nehézségekkel terhelt lett. Az elektronikus információs rendszer biztonságáért felelős személy az elektronikus rendszerben kezelt adat tartalmi, minőségi tulajdonságától függetlenül felel a bizalmasság, hitelesség és rendelkezésre állás követelményeiért akkor is, ha az személyes adat, akkor is, ha az minősített adat.

Ahhoz, hogy értékelni lehessen a felügyeletet ellátók jogszabályban rögzített – vagy éppen hiányzó – működési elveit, nyolc alapvető kérdésre érdemes választ keresni a jogszabályban:

1. Jogszabály előírja-e a felügyeleti szerepkör létrehozását?
2. A működési feltételek kialakításáért a szerv vezetője felelős-e?
3. A felügyeleti szerepkört ellátó közvetlenül a szerv vezetőjének van-e alárendelve?
4. A felügyeleti szerepkört ellátó esetében vannak-e a képzettségre, végzettségre, tapasztalatra vonatkozó követelmények?
5. A jogszabály meghatároz-e összeférhetetlenségi elveket?
6. A jogszabály rögzíti-e a felügyeleti szerepkört ellátó feladatait?
7. A szerepkört ellátó személy vezető-e?
8. A szerepkört ellátót – ha nem vezető – megilleti-e hatáskörében az azonnali intézkedési jogosultság, vagy a kiadmányozási jog?

felügyeleti szerepkörök és jogi válaszok	1. Jogszabály előírja-e a felügyeleti szerepkör létrehozását?	2. A működési feltételek kialakításáért a szerv vezetője felelős-e?	3. A felügyeleti szerepkört ellátó közvetlenül a szerv vezetőjének van-e alárendelve?	4. A felügyeleti szerepkört ellátó esetében vannak-e a képzettségre, végzettségre, tapasztalatra vonatkozó követelmények?	5. A jogszabály meghatároz-e összeférhetetlenségi elveket?	6. A jogszabály rögzíti-e a felügyeleti szerepkört ellátó feladatait?	7. A szerepkört ellátó személy vezető-e?	8. A szerepkört ellátót – ha nem vezető – megilleti-e hatáskörében az azonnali intézkedési jogosultság, vagy a kiadmányozási jog?
2011. évi CXII. Infotv. (belső adatvédelmi felelős)	24.§. (1) "…belső adatvédelmi felelőst kell kinevezni vagy megbízni…"	nincsen jogi iránymutatás	24.§. (1) "…közvetlenül a szerv vezetőjének felügyelete alá…"	24.§. (1) "…jogi, közigazgatási, informatikai … felsőfokú végzettség …"	nincsen jogi iránymutatás	igen - 24.§. (2)	nincsen jogi iránymutatás	nincsen jogi iránymutatás
2009. évi CLV. Mavtv. (biztonsági vezető)	23.§. (2) "…szerv vezetője által kinevezett biztonsági vezető…"	23.§.(1) "A … védelmi feltételeinek kialakításáért … a szerv vezetője felelős…"	nincsen jogi iránymutatás	nincsen jogi iránymutatás	nincsen jogi iránymutatás	igen - 23.§. (és az Elektronikus r. 8.§.)	nincsen jogi iránymutatás	nincsen jogi iránymutatás
2013. évi L. ibtv. (elektronikus információs rendszer biztonságáért felelős személy - kiberbiztos)	11.§. (1) c) "…a szerv vezetője … felelős személyt nevez ki vagy biz meg …"	11.§. (1) "…szervezet vezetője köteles gondoskodni…"	nem, de 13.§. (1) "…közvetlenül adhat tájékoztatást, jelentést…"	13.§. (8) "…aki büntetlen előéletű, … szükséges felsőfokú végzettséggel és szakképzettség gel…", de mi ez?	azonos lehet a biztonsági vezetővel 11.§. c)	igen - 13.§.	nincsen jogi iránymutatás	nincsen jogi iránymutatás
161/2010. (V-6) Korm.r. (rejtjelfelügyelő)	7.§. (2) a) "…szerv vezetője kijelöli … a rejtjelfelügyelőt …"	6.§. (1) a) "… szerv vezetője … felelős a … feltételeinek kialakításáért …"	8.§. e) "… biztonsági vezető … irányítja a rejtjelfelügyelő … tevékenységét"	nincsen jogi iránymutatás	11.§. 10. és a 11.§. 15. pontokból következően nem lehet egy személy	igen - 12.§.	nincsen jogi iránymutatás	nincsen jogi iránymutatás
161/2010. (V.6.) Korm.r. (rendszerbiztonsági felügyelő)	7.§. (1) a) "…szerv vezetője kijelöli … a rejtjelfelügyelőt …"	6.§. (1) a) "… szerv vezetője … felelős a … feltételeinek kialakításáért …"	nincsen jogi iránymutatás	nincsen jogi iránymutatás	nincsen jogi iránymutatás	igen - 10.§.	nincsen jogi iránymutatás	nincsen jogi iránymutatás

2. számú ábra: felügyeleti szerepkörök

Az összesítésből látható, hogy a felügyeletet ellátók, a feladatuk és hatáskörük ellátásához nem rendelkeznek megfelelő hatáskörrel (kiadmányozási jogosultság), nincsen érdemi eszközük az azonnali intézkedést igénylő feladataik ellátásához (hierarchia szintjén nem közvetlen irányítás a szerv vezetője által – bürokratikus akadály).

Megállapítható az is, hogy a szervezeti működést alapvetően befolyásoló eszközök (kiadmányozás, azonnali intézkedési jogosultság, közvetlen irányítás és jelentés stb.), valamint az összeférhetetlenségi szabályok nagy többségében nem jelennek meg a jogszabályban, így a jogszabályban feladatként meghatározottak végrehajtása, a végrehajtás megkövetelése esetleges, a „bürokrácia útvesztőin" és a szervezet informatikai kultúrájának (információbiztonsági tudatosságának) mértékén keresztül jut, vagy nem juthat érvényre.

Problémát okozhat még, hogy az egyes felügyeleti szerepkörök, mivel nem szükségszerű a szerv vezetőjének való közvetlen alárendeltség, a szervezeti hierarchia különböző szintjein, és más-más irányítás alatt dolgoznak. Ennek következményeként nehéz (ha nem lehetetlen) összehangolni az adatvédelmi és a minősített adatvédelmi szabályozást az IBSZ-el, és még nehezebb koherens belső normatív környezetet kialakítani.

A diszharmónia felszámolása, a szerepkörök közötti illetékességi és hatásköri átfedések kiküszöbölése, a szerepkörök közötti egyensúlyi helyzet kialakítása érdekében célszerű a szerepköröket közös irányítás alá vonni. Figyelemmel az adatkezelőtől és az üzemeltetőtől elkülönített szerepkörökre, illetve az első számú vezető átruházott hatáskörére, illetve a végrehajtó és vezető-irányító szerepkörök elválasztására, célszerű a „volumen elvből" következően akár „információbiztonsági" szervezetet létrehozni, amelyik közvetlen vezetői alárendeltségben működik, így megteremtve valamennyi felügyeleti szerepkör megfelelő működési szabadságát, kompetenciáját. Az Infotv. előírásainak megfelelően a szervet az adatvédelmi felelős vezet(het)i.

Végkövetkeztetések

Az információbiztonsági szerepkörök áttekintése abból a célból történt, hogy értékeljem az egyes felügyeleti szerepkörök jogszabályi környezetét. Bemutassam az adatvédelem, minősített adatvédelem és az elektronikus információs rendszerek biztonságára vonatkozó „szigetszerű" szabályozást, a felügyeleti szerepkörök elégtelen jogszabályi direktíváját abból a szempontból is, hogy egy működő informatikai rendszerbe illesztett módon, a szervezeti bürokráciában megfelelő hatékonysággal, képesek-e tevékenységüket ellátni.

Megállapítottam, hogy a jogszabályok nem értékelik az egyes felügyeleti szerepkörökhöz való viszonyt. Nem állapítanak meg összeférhetetlenségi szabályokat – összeegyeztethetőeket sem. Nem adnak támpontot sem a vezetés-irányítás rendszerében való hely és szerep kérdésében, és nem biztosítanak a feladatkörhöz tartozóan hatásköri felhatalmazásokat sem, amellyel álláspontom szerint a döntési szabadságot és képességet veszélyeztetik (kiadmányozás, azonnali intézkedési jogosultság).

Az tapasztaltam, hogy a felügyeleti tevékenységet meghatározó jogszabályok a „szigetszerű" működési modell mellett az ideál tipikus működéshez készültek, azaz nem vették figyelembe, hogy a szervezet, milyen apparátussal, milyen méretben és milyen diszlokáció mellett lát el feladatokat, így azonos felügyeletet kell létrehoznia a 36 ezer fős Rendőrségnek és a 10 fős önkormányzatnak is.

Az Ibtv. esetében hiányosságként állapítottam meg, hogy a jogszabály bár „elektronikus információs rendszer" szóhasználattal él, de ezen első sorban számítástechnikai hálózati rendszereket ért, nem értékeli a vezetékes, vagy vezeték nélküli távközlési rendszereket (rádió, távbeszélő stb.).

Általánosságban megállapítható, hogy az informatikai rendszerekre vonatkozó jogszabályok nélkülözik az egységes informatikai terminológiát, nem üzemeltetési és

fenntartási szemléletű megközelítéssel határozzák meg az adatkezelő és az üzemeltető tevékenységét felügyelő információbiztonsági szerepköröket. Sok esetben a jogszabály hibás terminológiai kifejezése akadálya a helyes szaknyelvi megközelítésnek (lásd: adatvédelem), így szükséges az informatikai jogszabályok tételes felülvizsgálata és terminológiai megfeleltetése.

Általánosságban megállapítottam, hogy célszerű az egyes felügyeleti szerepköröket közös irányítás alá vonni a helyettesíthetőség és a hatékonyság érdekében. Szükségesnek látszik a cselekvőképesség és kompetencia megteremtése érdekében a felügyeleti szerepkörben dolgozók kiadmányozási és azonnali intézkedési jogosultsággal való ellátása már a jogszabályban biztosított módon, ahogyan szükséges az elvárt szakirányú végzettség, képzettség és tapasztalat meghatározása is.

Meggyőződésem, hogy a szervezeti működésben tovább erősödnek az informatikai megoldások, így a kibertér védelme, az egyes információbiztonsági szerepkörök egymást segítő tevékenysége nélkülözhetetlen a szervezet kockázatokkal arányos védelmi megoldásainak kialakításához.