Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék

Székely Iván[*] – Vasvári György[**]

Adatvédelem és/vagy adatbiztonság?

(A HISEC 2003 konferencián tartott előadás kiegészített és módosított szövege)

Ajánlás 3.0

2004

[*] Dr. Székely Iván társadalmi informatikus, adatvédelmi szakértő. Az adatvédelem és az információszabadság multidiszciplináris területeinek nemzetközileg ismert kutatója, a Nyílt Társadalom Archívum főtanácsadója. Kandidátus; a Budapesti Műszaki Egyetem GTK Információ- és Tudásmenedzsment Tanszékének docense.

[**] Vasvári György aranydiplomás villamosmérnök. 1957 óta foglalkozik számítástechnikával, 1992 óta biztonsággal. Okleveles informatikai biztonsági menedzser (ISACA). Informatikai biztonsági szakértő (NJSZT). Tiszteleti egyetemi docens (BME) több mint tíz éves oktatói munka után. Neumann díjas.

Több mint tíz évvel az adatvédelmi törvény és nyolc évvel az adatvédelmi biztos intézményének megszületése után az „adatvédelem" és az „adatbiztonság" fogalmak tartalma még sokak számára félreértések forrása. Tisztázásuk, a helyes fogalomhasználat elterjesztése és következetes alkalmazása régi adóssága a szakmának, elsősorban a műszaki értelmiség körében.

A félreértés egyik fő forrása az, hogy egyesek adatvédelmen szó szerint „az adatok védelmét" értik, s nem veszik figyelembe, hogy e szó fogalmilag csak személyes adatok, illetve az érintett személyek (adatalanyok) esetében értelmezhető. Az a hasonló hangzású, a laikusok számára rokon képzeteket keltő szó, amivel összetévesztik: az adatbiztonság. Ennek a műszaki világban világosabb a jelentése, bár itt is vannak félreértések: sokan az adatbiztonságot a kriptográfiával vagy más részterületével azonosítják, s így leszűkítik a tartalmát.

Széles körben tapasztalható, hogy még ma is születnek tartalmilag értékes, de helytelen fogalomhasználatú kiadványok, folynak ilyen kurzusok, tanfolyamok. Mindez a félreértések továbbélését segíti elő. A tisztázás igényének különös aktualitást ad az, hogy az Adatvédelmi törvény 2004. január 1-én hatályba lépő – az EU szabályozásnak megfelelő – új rendelkezései szerint belső adatvédelmi (és nem adatbiztonsági) felelőst kell kinevezni számos adatkezelőnél, s a törvény a felelősök feladatait is előírja.

A HISEC konferenciák célul tűzték ki, hogy mind az adatvédelem, mind az adatbiztonság területével foglalkozó előadásokat tartalmazzanak. Ebben a tanulmányban az adatvédelem, illetve az adatbiztonság területének egy-egy szakértője arra tesz kísérletet, hogy röviden megfogalmazza/áttekintse saját szakterületének legfontosabb aspektusait, s hogy ezzel is hozzájáruljon e két fogalom tartalmának tisztázásához, a helyes fogalomhasználat elterjesztéséhez.

❖

1. Az adatvédelemről

1.1 Az adatvédelem fogalma

Legegyszerűbben úgy határozhatjuk meg az adatvédelmet, hogy az az, amiről az Adatvédelmi törvény[1] szól. Vagy mondhatjuk azt is: az, amivel az adatvédelmi biztos[2] foglalkozik. Esetleg: az, amivel 2004. január 1-től a belső adatvédelmi felelősöknek kell (kellene) foglalkozniuk. Ezek természetesen nem szakszerű definíciók, de alapfokon orientálják az érdeklődőt.

Közelebbről vizsgálva: az Adatvédelmi törvény címéből és tartalmából egyértelműen következik, hogy a *személyes adatok* védelmével foglalkozik, s az is, hogy nem az adatvédelem valamely részterületét szabályozza.[3]

A személyes adat meghatározását a törvény tartalmazza; eszerint személyes adat bármely meghatározott (azonosított vagy azonosítható) természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintett személlyel kapcsolatba hozható következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

Noha a törvény magára az adatvédelem fogalomra nem ad definíciót, a törvény tartalmából, az adatvédelmi biztos gyakorlatából, a nemzetközi normák szövegéből, a kiterjedt szakirodalomból és az adatkezelői gyakorlatból egyértelműen következik, hogy az adatvédelem (data protection, Datenschutz, protection des données) nemcsak jogszabályi vonatkozású, hanem belső szabályozási (pl. belső adatvédelmi szabályzat készítése és végrehajtása), szervezeti (pl. belső adatvédelmi felelős kinevezése és feladatai), informatikai (a számítógépes személyesadat-kezelési rendszer tervezése és működtetése) és gyakorlati adatkezelési aspektusokat is tartalmaz.

Egy komplex adatvédelmi (nem adatbiztonsági!) átvilágítás sem csupán a jogi és belső szabályozási dokumentumok vizsgálatára, az adatalanyok jogainak érvényesíthetőségére terjed ki, hanem az informatikai rendszer adatvédelmi szempontú elemzésére, a rendszer felépítésére és működésére vonatkozó javaslatok megfogalmazására is.

---

[1] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

[2] A három országgyűlési biztos egyike, az adatvédelem független ellenőre (lásd www.obh.hu). Jogosítványai 2004. januárjától erősödnek, bizonyos tekintetben hatósági jellegűekké válnak.

[3] A jogalkotó ezen túlmenően – kanadai mintát követve – ugyanebben a törvényben szabályozza egy másik alapjog, az információszabadság érvényesülését is, tehát közös adatvédelmi és információszabadság törvényről van szó.

Az adatvédelem tehát *a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.* (Az adatvédelem fogalmilag csak személyes adatok esetében értelmezhető. Másfelől, jogi személyeknek nincsenek személyes adataik, így sem az adatvédelem fogalomköre, sem az adatvédelmi törvény személyes adatok kezelésére vonatkozó rendelkezései – adatalanyként – nem vonatkoztatható rájuk.)

A műszaki értelmiség egy része – éppen a törvényi szabályozás miatt – a fentieket „jogi adatvédelem"-nek nevezi, azt éreztetve, hogy létezhet egy nem jogi, azaz „technikai" adatvédelem is. Talán a szakmai presztízs szempontjai is hozzájárulnak ahhoz a törekvéshez, hogy a törvény által kifejtett adatvédelmet valamely műszaki terület részterületének, speciális esetének próbálják tekinteni. E törekvés része az is, hogy egyes szakemberek azt állítják: az adatvédelem azt mondja meg, hogy *mit,* az adatbiztonság pedig azt, hogy *hogyan.* Ez azonban a legjobb esetben is csak féligazság. Ha ugyanis figyelembe vesszük, hogy az adatvédelmi ajánlások, törvények és belső szabályzatok megmondják azt is, hogy *hogyan* kell kezelni a személyes adatokat, az adatbiztonsági előírások pedig azt is, hogy *mit* kell a kritériumoknak megfelelően besorolni és kezelni; továbbá ha figyelembe vesszük azt is, hogy az adatvédelem csak személyes adatokra, az adatbiztonság pedig bármilyen adatra értelmezhető, tehát a tárgyuk sem azonos lefedésű – akkor a két fogalom ily módon történő párba állítása nem szerencsés.

Be kell látnunk mindazonáltal, hogy a számítástechnikusok, műszaki informatikusok jogosan panaszkodnak, mert az adatvédelmi előírások részletes lebontása az informatikai rendszer szintjéig nem történik meg, s a személyesadat-kezelési rendszerek tervezésénél és működtetésénél gyakran az adatvédelmi előírásokkal ellentétesen ható üzleti vagy igazgatási érdek dominál.

Ugyanakkor az adatbiztonságnak (az adatok jogosulatlan megismerése, megszerzése, továbbítása, módosulása és tönkremenetele elleni, illetve hitelességük, integritásuk, bizalmasságuk és rendelkezésre állásuk biztosítása érdekében tett intézkedéseknek) is van jogi és szabályozási vetülete, nemcsak műszaki és szervezési aspektusa; előírásai azonban részletesek, szabványosíthatók, a műszaki informatikusok számára jól értelmezhetők.

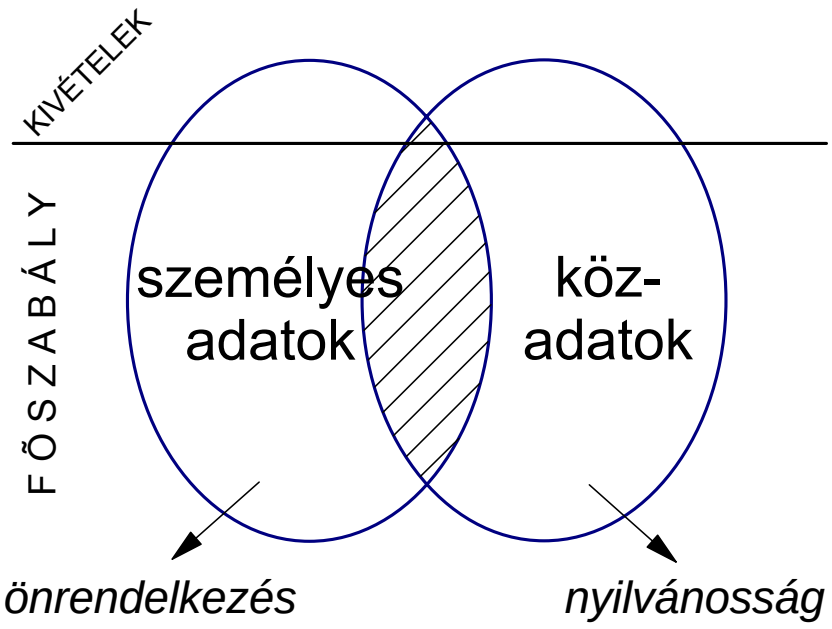
1.2 Adatvédelem és titokvédelem

Amíg az adatvédelem szó értelme első hallásra megtévesztő lehet (hasonlóan a vírusvédelemhez, a balesetvédelemhez vagy a munkavédelemhez, amelyek nyilvánvalóan nem a vírusok, a balesetek vagy a munka védelmét jelentik), addig a titokvédelem valóban valamilyen „titok" védelmét, megismerésének korlátozását jelenti.

Vajon a személyes adat titoknak tekinthető-e? Néhány kivételes esettől eltekintve[4] a személyes adat nem „titok”, hanem önrendelkezés tárgya: elvben (és a törvényi rendelkezések szerint is) alapvetően mindenki maga döntheti el, hogy személyes adataival mi történjék. Ez az alapvető jog természetesen korlátozható, de a korlátozásnak szigorú feltételei vannak.

A jogi és köznyelvben számos nevesített titokkategória ismeretes, például üzleti titok, államtitok, szolgálati titok, magántitok, ügyvédi titok, orvosi titok, banktitok, gyónási titok stb. E titokfajták egy részének védelme (pl. orvosi titok) ráerősít a személyes adatok védelmére, illetve az érintettek információs önrendelkezésére, más része (pl. államtitok) csak kivételesen vonatkoztatható személyes adatokra. Ha a „ráerősítő” titokvédelmi előírásokat tekintjük, akkor az orvosi titok védelme egybeesik a betegek személyes adatainak védelmével, hiszen csak természetes személy lehet páciens, azonban az üzleti titok, a banktitok, az adótitok stb. nemcsak természetes személyek adataira vonatkozik, mivel nemcsak lakossági ügyfelek vagy magánszemély adóalanyok szerepelnek az adatkezelők nyilvántartásaiban.

Az államtitok és a szolgálati titok fogalma felveti a személyes adatok ellenpárja, a *közadatok,* avagy *közérdekű adatok* kezelésének kérdéseit. A közérdekű adatok kezelésének főszabálya a nyilvánosság, a bárki számára való megismerhetőség. Az államtitok, a szolgálati titok – illetve „puha” rokonuk, a belső használatra készült, illetve döntés-előkészítéssel összefüggő, nem nyilvános adat – tehát nem a főszabályt erősíti, ellenkezőleg: annak jelentős kivételeit képezi.



1. ábra

[4] Például nemzetbiztonsági alkalmazottak személyes adatai *egyúttal* államtitkot is képezhetnek.

Az 1. ábrán az ún. Székely-féle modell látható, amelyben a mindkét alapvető adatkategóriára egy-egy főszabály vonatkozik: a személyes adatokra az önrendelkezés, a közadatokra a nyilvánosság. A vonal alatti területeken érvényesülnek a főszabályok, a vonal felett a kivételek; az államtitok például a közadatok nyilvánossága alóli kivételek mezőjébe tartozik. Az átfedő (satírozott) terület azon személyes adatokat tartalmazza – például a közfunkciót betöltő személyek e tevékenységével összefüggő személyes adatait –, amelyekre nem az önrendelkezés, hanem a nyilvánosság főszabálya vonatkozik.[5]

Említést kíván, hogy egyes államigazgatási titokvédelmi előélettel rendelkező, jelenleg az üzleti szférában tevékenykedő szakértők azt javasolják az üzleti szektor szervezeteinek is, hogy üzleti titoknak (banktitoknak, biztosítási titoknak stb.) minősülő adataik, valamint az adatvédelmi előírások hatálya alá eső lakossági ügyfél-adataik védelmére is alkalmazzák az állam-, illetve szolgálati titkok védelmének formális szervezési eljárásait és módszereit.

1.3 Az adatvédelem gyakorlati megvalósítása

Az adatvédelem (az információs önrendelkezés, avagy az információs *privacy*) biztosítására a szakirodalom általában négyféle elvi lehetőséget ír le: a jogi szabályozást (törvényeket, jogszabályokat, valamint azok megsértésének szankcionálását), az önszabályozást (elsősorban az üzleti szektor adatkezelőinek belső szabályzatait, etikai kódexeit), a fejlett adatvédelmi technológiák (a PET technológiák) alkalmazását, valamint az adatalanyok és az informatikusok oktatását.

A jogi szabályozás terén a legfontosabb forrás Magyarországon a keretjellegű Adatvédelmi törvény, amely az alapvető szabályokat tartalmazza, illetve az egyes tipikus adatkezelési területeket szabályozó szektorális vagy területspecifikus adatkezelési törvények[6], amelyek a speciális szabályokat, illetve az alapvető adatvédelmi szabályok alóli kivételeket, adatkezelési felhatalmazásokat tartalmazzák. Nemzetközi szinten pedig, csak a legismertebbeket említve, a magyar adatkezelők számára is követendő az Európa Tanács adatvédelmi egyezménye[7] és szektorális ajánlásai[8], valamint az Európai Unió adatvédelmi direktívája,[9] amely Magyarország

[5] A Székely-féle alapmodell kritikája, hogy nem jeleníthetők meg rajta a nem állami (üzleti, társadalmi) szervezetek adatkezelési viszonyai. Továbbfejlesztett változata nem három, egymást részben átfedő körből vagy ellipszisből áll, hanem három hosszúkás, ívelt idom – a három adatkör szimbóluma – gyűrűjéből, ahol a szomszédos idomok végei átfedik egymást.

[6] Például az 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, vagy az 1995. CXIX. törvény a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről.

[7] *Convention for the protection of individuals with regard to automatic processing of personal data.* Council of Europe, Strasbourg, 28 January, 1981. *European Treaty Series* No. 108.
Lásd még a kihirdetéséről szóló 1998. évi VI. törvényt.

[8] Megtalálhatók a www.coe.int portálon

[9] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official*

csatlakozása után formálisan is vonatkozni fog a magyar adatalanyokra és adatkezelőkre.[10] A törvényi rendelkezések végrehajtásának szakosított ellenőre az adatvédelmi biztos, a személyes adatokkal való visszaélés súlyosabb eseteit pedig a Büntető Törvénykönyv tartalmazza.

Az önszabályozás terén a legismertebb forma a belső adatvédelmi szabályzat, de több üzleti ágazat szakmai-érdekvédelmi szervezeteinek etikai kódexei is tartalmaznak adatvédelmi szabályokat.[11]

Az adatvédelmi elvek és rendelkezések megvalósításának technológiai szintjét képviselő PET (Privacy Enhancing Technologies) összefoglaló néven ismert változatos információs és kommunikációs technológiákat abból a célból fejlesztették ki, hogy ne csak az adatokat, hanem az adatok *alanyait* is védjék a visszaélések ellen. Burkert csoportosítása szerint[12] megkülönböztethetünk szubjektum-orientált, objektum-orientált, tranzakció-orientált és rendszer-orientált PET technológiákat. A rendeltetésszerűen használt PET eszközök és rendszerek mindig a *gyengébb felet* (jellemzően az adatalanyt) védik az információs túlhatalommal rendelkező erősebb féllel szemben. Ismertebb PET vonatkozású technológiák például a biometrikus rejtjelezés (bioscrypt), a Crowd, a Chaum-féle Mix-ek, az onion routing, az anonim remailer, a Platform for Privacy Preferences (P3P) stb.

A PET technológiák, alkalmazásuk során védik az informatikai erőforrások felhasználóinak identitását az anonimitás, a pszeudonimitás, az erőforrások használatának, illetve a felhasználók személyének külső szemlélő általi összeköthetetlensége (unlinkability), valamint a használat, illetve kommunikáció tényének megfigyelhetetlensége (unobservability) biztosításával. A „nem-felhasználó" adatalanyok identitását az anonimitás és a pszeudonimitás biztosításával védik, illetőleg általánosságban biztosítják a személyes adatok bizalmasságát és integritását. E kritériumok az *adatbiztonsági* szabványokban is megtalálhatók, ami felhívja a figyelmet arra, hogy hasonló kritériumok eltérő célt szolgálhatnak, eltérő jogszabályi rendelkezések végrehajtását célozhatják, ezért teljeskörű megítélésük és minősítésük csak az adatkezelési kontextus ismeretében végezhető el – vagyis annak ismeretében, hogy az adott kritérium teljesítése kinek az érdekében, milyen célból történik.

Journal of the European Communities No. L 281/31, 23.11.1995
(Magyarul: Az Európai Parlament és a Tanács 95/46/EC Irányelve az egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról. Adatvédelmi Biztos Irodája, Budapest 1995.)

[10] Magyarország, Svájc után második EU-n kívüli országként már 2000-ben hivatalosan megkapta az EU adatvédelmi normái szerinti ún. adekvát státust.

[11] Például a Magyar Áruküldők Egyesülete etikai kódexe, vagy a Magyarországi Tartalomszolgáltatók Egyesülete által alkotott Tartalomszolgáltatási Kódex.

[12] Herbert Burkert: Privacy-Enhancing Technologies: Typology, Critique, Vision.
In: Agre, P.E. – Rotenberg, M. (eds.): *Technology and Privacy: The New Landscape.*
MIT Press, 1997.

Ugyancsak eltérő célt szolgálhat egyes technológiák alkalmazása is: garantálható-e, hogy egy Crowd, vagy egy onion routing alkalmazás (mely utóbbit az amerikai hadsereg egyik ágazatában fejlesztették ki) valóban az adatalanyok védelmét szolgálja-e, vagy egy információs túlhatalommal rendelkező hatóságét vagy nyomozó szervét? Ez a kérdés még a bioscrypt alkalmazása esetében is feltehető. A válasz nyilvánvalóan az, hogy önmagában nem garantálható, mégis a PET technológiák *rendeltetésszerű* használata az informatikai alkalmazások szintjén lehetővé teszi az információs önrendelkezés technikai biztosítását, a gyengébb fél védelmét.

Az oktatás terén még sok a tennivaló. A Műegyetemen van ugyan a helyesen értelmezett adatvédelemről szóló kurzus, de téves elnevezésű adatbiztonsági tárgyak is vannak, s az Adatvédelmi törvény által előírt belső adatvédelmi felelősök képzésére olyan, félreértésen alapuló, adatbiztonsági tartalmú tanfolyamok hirdetései is napvilágot láttak a sajtóban, amelyek egyfelől megtévesztik a felkészülni kívánókat, másfelől nehéz helyzetbe hozzák szervezetüket az új rendelkezések hatályba lépésekor. Az adatalanyok oktatásáról pedig érdemben nem is beszélhetünk.

Hozzá kell tennünk, hogy az adatkezelők oktatása is fontos lenne az adatvédelem gyakorlati érvényesítése szempontjából, és nem feledkezhetünk meg – az informatikusok oktatásán túl –az információs rendszerek megfelelő, auditálható kialakításáról és működtetéséről, valamint az érintettek jogainak gyakorlati biztosításáról sem.

1.4 Adatbiztonság az adatvédelem szemszögéből

Létezhet-e adatvédelem adatbiztonság nélkül, és fordítva? – A válasz nem triviális, mert adatvédelem bizonyos fokú adatbiztonság nélkül valóban nem létezhet, ugyanis ha nincsenek olyan technikai eszközeink, amellyel kontrollálni tudjuk a személyes adatok hozzáférhetőségét, integritását, akkor nem is tudjuk megvédeni az adatok alanyait. Fordítva viszont lehetséges: lehet tökéletes adatbiztonság, adatvédelem nélkül – erre számos példát adnak a diktatórikus országok vagy a stratégiai munkahelyek makro- és mikroszintű adatkezelési rendszerei.

Az adatvédelem oldaláról tehát azt állíthatjuk, hogy az adatbiztonság szükséges feltétel, ugyanakkor az adatvédelmi felelős jellemzően nem műszaki feladatkör, és az adatvédelmi auditálás sem műszaki jellegű tevékenység.

❖ ❖ ❖

2. Az adatbiztonságról

2.1 Az adat általános fogalma, és a titokvédelem

Az *adat fogalma* a BS 7799 Brit informatikai szabvány szerint:

∗ Az adat tények, elképzelések, utasítások formalizált ábrázolása ismertetés, feldolgozás, illetve távközlés céljára.

Ez azt jelenti, hogy az adat bővebb fogalom a személyes adatnál.

Az adatok " biztonság érzékenységi" osztályozása előtt (vagy inkább egy magasabb szinten) van egy jogi, illetve funkcionális jellegű osztályozás is. Eszerint lehetnek egyfelől személyes adatok, másfelől közérdekű adatok; e két nagy osztályon belül lehetnek üzleti titkok, orvosi titkok, minősített adatok (azon belül államtitkok, szolgálati titkok), belső használatú és döntés előkészítő adatok stb. Az adatkezelőnek e kategóriák, és funkciók alapján kell meghatároznia a védelmi osztályt, illetve az adatnak a biztonság érzékenységét.

Tehát az információ rendszerekben például biztonság kritikus lehet nem csak a személyes adat, hanem általában az adatok (pl. üzleti adatok), és az egyéb ***informatikai erőforrások is****. Az erőforrások az adat, ember, technológia (hardware, netware, rendszer software), alkalmazás, kisegítő berendezések, helyiségek eszközök bármelyike.*

Az MSZ ISO/IEC 17799 INFORMÁCIÓTECHNIKA, Az informatikai biztonság menedzselésének rendje, tárgyú szabvány 5.2 pontja szerint: Az információkat (az információt adatként értelmezzük), adatokat osztályozni kell biztonság érzékenységük, fontosságuk, és a szükséges védelem szerint. Ebből következik, hogy a védelmi intézkedések erősségét ennek megfelelően kell meghatározni.

2.2 Az adatbiztonság fogalma

Az 1992. évi LXIII. Tv. Az Adatbiztonság című fejezetében a következőket mondja ki:

10. §. (1) *Az adatkezelő köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*

(2) *Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg a sérülés vagy megsemmisülés ellen*.

Ezt az adatok, bizalmasságának, sértetlenségének, és a rendelkezésre állásának szervezési (humán, jogi), és technikai (fizikai, logikai) védelmével lehet

megvalósítani, ugyanis a rendelet más megfogalmazása ennek, de egyértelműen erről van szó.

2.3 Az informatikai biztonság – titokvédelem

Az adat az informatikai erőforrások egyike. Az erőforrások védelmének, az informatikai biztonságnak azonosak a követelményei az adatbiztonságéval, éspedig az erőforrások bizalmasságának és/vagy sértetlenségének és/vagy rendelkezésre állásának védelme. Ezzel a titokvédelem is foglalkozik. Az adatbiztonságnál az adat tehát bővebb fogalom, mint az adatvédelem, amely csak a személyes adatokra vonatkozik. A személyes adatok tehát az informatikai erőforrások egyikének, az adatoknak részét képezik. A belük kapcsolatos önrendelkezési jog úgy valósítható meg, ha a titokvédelem részévé tesszük a személyes adatokat.

A bizalmasság azt jelenti, hogy valamit csak korlátozott számú kevesek ismerhetnek. A bizalmasság védelme a felfedés elleni védekezést jelenti.

A sértetlenség azt jelenti, hogy valami az eredeti állapotának megfelel, és a forrása is eredeti (hitelesség). A sértetlenség védelme a jogosulatlan változtatás elleni védelmet jelenti.

A rendelkezésre állás az erőforrások olyan állapota, amelyben eredeti rendeltetésének megfelelő szolgáltatásokat nyújtani tudja (működőképesség), meghatározott helyen és időben (elérhetőség). A rendelkezésre állás védelme az erőforrás (-ok) szolgáltatásai folyamatosságának védelmét jelenti.

Az MSZ ISO /IEC 17799 szabvány 7. pont azt írja: a biztonság kritikusság szerint a helyiségeket, és eszközöket arányos védelemmel kell védeni, azaz osztályozni kell őket is. A hatályos jogszabályok definiálnak üzleti titkot, titkos lehet egy technológia, egy eljárás, egy berendezés, egy helyiség is (ha a vállalatnak méltányolható érdeke fűződik hozzá). Ezért a Titokvédelem az informatikai erőforrások biztonsági osztályozásával foglalkozik, amelyből a védelmi követelmények a későbbiekben meghatározhatók.

A védelmi intézkedések lehetnek:

- Szervezési védelmi intézkedések
  - Biztonsági szervezet szabályozása
  - Humán védelem
  - Iratkezelés szabályozása (papír- és elektronikus alapú)
  - Biztonsági dokumentációk biztosítása
  - Kockázat áthárítás
- Technikai védelmi intézkedések
  - Fizikai, és logikai hozzáférés védelem

- Fizikai, és logikai rendelkezésre állás biztosítása
- Hálózatok védelme
- Információ rendszerek életciklusa alatti védelme.

2.4 Az osztályozás

*Az **adatok** osztályozására egy példa (gazdasági szervezeteknél):*

Védelmi osztály	Adatok
A. Titkos	Üzleti titkot képező adatok
B. Bizalmas	Személyes adatok
C. Belső használatra	Belső használatra szóló adatok
D. Nyilvános	Nyilvános adatok

Minősítést a jogszabályban meghatározott, elsősorban állami szervezetek, az osztályozást a gazdasági szervezetek végezhetnek.

Az alábbiakban bemutatunk egy példát a **hozzáférés védelem** erősségének az adatok osztályozását figyelembe vevő meghatározásáról.

A védelmi osztály	Védelmi osztályba sorolt adatok (pl.) Gazdasági szerv.	Védelmi intézkedés
A. Titkos	Üzleti titkot képező adatok	*Biometriai jelszó*
B. Bizalmas	Személyes adatok	*Egyszer használatos jelszó*
C. Belső használatra	Belső használatra szóló adatok	*Többször használatos jelszó*
D. Nyilvános	Nyilvános adatok	*Nincs védelem*

**A személyes adatok mint az előbbiekben szerepelt a természetes személy rendelkezése szerint kezelendők, tegyük hozzá titokként, vagy nem titokként. Ezt azonban csak úgy tudja az informatika biztosítani, hogy az adatokat, ezzel a*

személyes adatokat titokként kell kezelni, és a nem titokként kezelés, mint kivétel a természetes személy önrendelkezésével valósítható meg.

*A fizikai hozzáférés -védelemnél **a helyiségek** védelmét az osztályozás alapján legalább az egyes osztályokban a következőképpen kell például kialakítani:*

Védelmi Osztály	Belépés ellenőr-zés	Mozgás ellenőr-zés	Behato-lás vé-delem	Tűz-véde -lem	Légálla-pot vé-delem	EMC EMI véd.	Felü-gye-let
A. zárt	E	E	E	E	T	T	T
B. kiemelt	R	R	R	N	R	-	T
C. ellenőrzött	M	M	M	N	R	-	T
D. nyílt	É	M	-	N	-	-	É

A jelölések: E= erősített, É= élőerővel, M= minimális, N= normál, R= részleges, T= teljes.

Az **eszközök** védelmi osztályba sorolására példa az alábbi:

Védelmi osztály	Eszköz
A. Titkos	Rejtjelező gép, sw
B. Bizalmas	Licencelt gépek, Beléptető kártya
C. Nyilvános	Egyéb gépek

2.5 Az adatbiztonság helye a vállalati szervezetben

Az informatikai-, és ezen belül az adatbiztonságért felelős vezető a vezérigazgató közvetlen alárendeltségébe tartozó **biztonsági vezető** beosztottja, miként a vagyonbiztonsági vezető is (ha termelő, szolgáltató üzemről van szó, az üzembiztonsági vezető is). A biztonság egyik feltétele ugyanis az integrált biztonsági szervezet. Ugyanakkor annak a meghatározása, hogy a bővebben értelmezet adatok, és egyéb erőforrások mennyire biztonság érzékenyek a titokvédelem tárgya. A Titokvédelmi felelős pedig szintén a Vezérigazgató titkárságán kell dolgozzon, szintén elválasztva az adat, illetve informatikai biztonságtól.

3. Adatvédelem és/vagy adatbiztonság?

Az adatvédelem és az adatbiztonság tehát két külön álló feladat. Adatvédelem valamilyen fokú adatbiztonság nélkül a gyakorlatban nem valósítható meg, azonban fordítva lehetséges: tökéletes adatbiztonság (az adatkezelő – például a zsarnoki főnök – érdekében) nulla adatvédelemmel párosítva (senki és semmi sem védi az adatalanyt, mondjuk a beosztottat). A kérdésre a válasz, tehát az **és. Végül meg**

kell állapítanunk azt, hogy az adatbiztonság értelmezhető az informatikai biztonságban, úgy mint a többi erőforrás biztonsága is például: Technológiai biztonság, humán biztonság stb.). Tehát az adatbiztonság az informatikai biztonság egy része, és semmiképpen nem azonosítható vele, még kevésbé az adatvédelem.

3.1 Következtetések

- Az adatvédelmi és az informatikai biztonsági szervezetet a fentieknek megfelelően kell szétválasztani, és a felelősök helyét a szervezetben meghatározni (COBIT3 szerint ez a biztonság kritikus feladatok szétválasztása elvének alkalmazása).
- Az ADATVÉDELMI, ÉS ADATBIZTONSÁGI szabályzatokat, és a TITOKVÉDELMI UTASÍTÁST az adat, és titokvédelmi felelős készítik el, és tartja karban, a Vezérigazgató írja alá. Ezek nem részei az informatikai biztonsági szabályzatoknak, hanem a védelem erősségének követelményeit határozzák meg.

Melléklet

Néhány fontosabb jogszabály és szabvány

a) A személyes adatok kezelésével és védelmével kapcsolatos jogszabályok

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról

1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

1994. évi XXXIV. törvény a Rendőrségről, VII.–VIII. fejezet

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, 38–72. §, 3. sz. melléklet

2001. évi XL. törvény a hírközlésről, VIII. fejezet

1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

1978. évi IV. törvény a Büntető Törvénykönyvről, 177–178. §

b) Titokvédelemmel kapcsolatos jogszabályok

1995. évi LXV. törvény az államtitokról és a szolgálati titokról

43/1994.(III.29.) Korm. rend. a rejtjeltevékenységről

1978.évi IV. törvény a Büntető Törvénykönyvről (221–223., 274–278., 299–300., 303–306., 312–313. §)

c) Hatályos szabványok

Common Criteria for Information Technology Security Evaluation 2.1 (ISO 15408 1, 2, 3).

BS 7799 (brit szabvány).

MSZ ISO/IEC 15408 1, 2 , 3 Informatikai biztonsági szabvány.

MSZ ISO/IEC 17799 Informatikai biztonsági szabvány (A BS 7799-2: -2002 alapján)

COBIT3, Governance, Control and Audit for Information and Related Technology.
IT Governance Institute, 2000 July.