Adatvédelem és információszabadság – 2011/2012. őszi félév

1. előadás - 2011.09.08.

0. Adminisztratív dolgok, tárgykövetelmény, etc.

1. Fogalmak

Adatvédelem: alapelvek + szabályok + eljárások + eszközök a személyes adatok gyűjtésének-feldolgozásának-felhasználásnak korlátozására, a szem. adatok védelmében (data protection)

→ *CSAK személyes adatra értelmezhető, az adatalanyokat védem*

Adatbiztonság (data security): jogosulatlan hozzáférés (módosulás, tönkremenetel) elleni védelem, bármilyen adatra értelmes, magát az adatot védem

Adatvédelemhez kell adatbiztonság, fordítva nem feltétlenül szükséges!

2. Személyes adat

információ → !! rögzített + struktúrált + kereshető !! → adat
adat → adott kontextusba helyezve újra információ

Példa 1
Szekus nézi a monitort → fejben rögzíti a képeket, tkp. adatot kezel („Mikor jött a csini titkárnő?”)
Igazoltatásnál jó memória esetén az adat visszakereshető akkor is, ha nem írja fel → adatot kezel!

Bármilyen adat akkor és csak akkor személyes, ha egy azonosított/azonosítható személlyel kapcsolatba hozható!!

Példa 2 – a személyesség relatív dolog
Leolvasok egy rendszámot → nekem nem mond semmit a tulaj személyéről
Rendőr is leolvassa → van eszköze az azonosításhoz, itt már személyes adatról van szó, a rendőr adatkezelő!

→ Ha nem tudom azonosítani a személyt, akkor az adat nem személyes, akármennyi is a rendelkezésemre áll belőle!

A különféle személyazonosító adatok (lehet ez akár egy gyakori név, de mindenféle jellemzők!) mind-mind személyes adatok, de sokszor az egyértelmű azonosításhoz több kell belőle!

A hangminta, íriszminta, ujjlenyomat, DNS-minta, de akár a téves adat is személyes adattá válik annak a kezében (és emiatt kellő körültekintéssel kell kezelni!), akinek az eszközei megvannak az egyén azonosításához, a kapcsolatba hozatalhoz.

(Egy szöveg fotója is személyes adat lehet, a formátum teljesen mindegy!)

Egy adat tartozhat több emberhez is, de van, ami tipikusan 2 emberre vonatkozik. (Egy-egy, egy-több, több-több kapcsolatok)

Tény és következtetés is lehet adat → a bank „beárazza” a hitelkérőt, innentől kezdve ez személyes adat lesz.

Extrém példa: anonim véleménynyilvánítás → a tanár ismerheti az írásunk jellegzetességeit, hiszen az pl. előző dolgozatokból visszakereshető → „rejtett információ”

Az adat ismeretében nem feltétlen tudunk kapcsolatba hozni egy személlyel (pl. DHCP-s IP-címek), azonban következtetéssel találhatunk olyan adatot, amely már egyértelmű és kapcsolatba hozható.

Egy-egy kis adatból nem feltétlenül hozható létre kapcsolat egy személlyel, azonban sok adat („cloud”) egy egyéni ujjlenyomatot/viselkedési mintázatot tud létrehozni, ami kiválóan kapcsolatba hozható egy személlyel. (Pl. Google, FaceBook, etc.)

2011.09.15. – BME Sportnap, elmaradt az előadás

2. előadás – 2011.09.22.

Adatkezelés: bármilyen, személyes adattal végzett művelet vagy műveletek csoportja
Nincs olyan művelet, ami nem adatkezelés, ha személyes adaton végzem!
(Csak személyes adatra van értelmezve!, „data processing”)

Pl. gyűjtés, felvétel, összekapcsolás, zárolás, tárolás, etc.

DE: fénykép-, hang vagy filmfelvétel készítése, DNS-minta és egyéb, azonosításra alkalmas fizikai jellemzők rögzítése, etc. is

Adattovábbítás: a személyes adatot meghatározott, harmadik fél számára hozzáférhetővé tétele
(Nem szükséges az adat átvitele, vagy a hozzáférés érvényesítése)

Nyilvánosságra hozatal: adattovábbítás mindenki számára (pl. blog írása)

Adatkezelő: az a természetes/jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, amely az adatok kezelésének célját és az adatkezeléssel kapcsolatos döntéseket meghozza és végrehajtja – VAGY: az általa megbízott végrehajtóval hajtatja végre.

Példa: Neptun-kódos dolgok esetén az adatkezelő a BME, és nem a KTH-s kisasszony

Adatfeldolgozás = kiszervezett (outsource) adatkezelés: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (módszer, eszköz, hely nem számít)

DE: nem szükséges tényleges feldolgozást végezni, bármely kiszervezett személyesadat-kezelési művelet adatfeldolgozás.

Példa: bérszámfejtés, számlaküldés, irattárolás, informatikai fejlesztés, call center, etc.
→ minden olyan tevékenység, amelynek során a tevékenységet végző személyes adatokhoz jogszerűen férhet hozzá, adatfeldolgozásnak minősül!

Adatfeldolgozó: az a természetes/jogi személy, vagy jogi személyiséggel nem rendelkező szervezet, amely az adatkezelő megbízásából a személyes adatok feldolgozását végzi.

Törvény: adatfeldolgozó nem alkalmazhat újabb adatfeldolgozót személyes adatok esetén!
(lánc-adatfeldolgozás tilalma)

DE #01: ha nem személyes adatot dolgoztat fel, akkor lehet további adatfeldolgozó!
(A személyes adatokhoz 1 adatkezelő és 1 adatfeldolgozó férhet hozzá!)

DE #02: ha minden adatfeldolgozóval külön szerződik az adatkezelő → köztük lehet személyes adatok forgalma

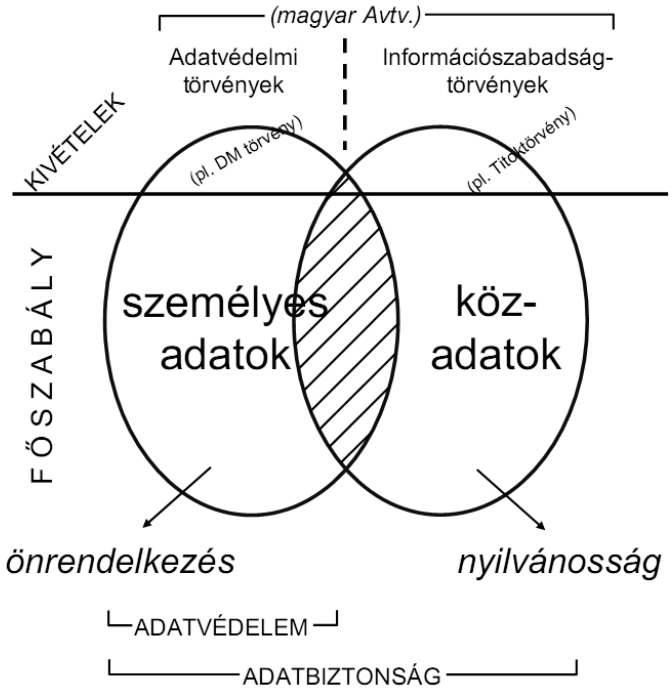
Adatkezelő: teljes felelősség

Adatfeldolgozó: korlátozott felelősség
→ érdemi, adatkezelést érintő döntést nem hozhat
→ személyes adatokat kizárólag az adatkezelő utasításai szerint dolgozhatja fel
→ saját célra nem végezhet feldolgozást
→ nem lehet érdekelt a feldolgozandó adatokat felhasználó üzleti dolgokban

Jogi folyamat lefolyása:
1. Adatfeldolgozó kárt okoz
→ 2. Adatalany pert indít, DE: az adatkezelő ellen
→→ 3. Adatkezelő kártéríti az adatalanyt
→→→ 4. Adatkezelő az adatfeldolgozóval elszámolja a költségeket

---

Alapmodellek

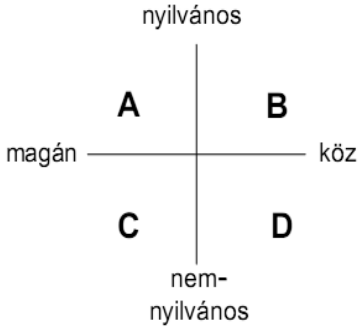


Személyes és közadatokra szétválasztás → minden terület lefedhető ezzel a kettővel, egy alapvető keretet határoznak meg. (Filozófiai és jogelméleti alapkoncepció, Székely-féle modell)

Személyes adat → főszabály: önrendelkezés, jog: információs önrendelkezés
Közadat → főszabály: nyilvánosság, jog: információszabadság

A kettő metszetében pl. köztisztviselő tevékenységével összefüggő személyes adatai vannak, ezekre a főszabály a nyilvánosság!

A fenti modell hiányossága: a nem állami szervezetek nem jeleníthetőek meg → az igazán jó modell 3 hosszúkás, ívelt idomból áll, melyek egy gyűrűt alkotnak, átfedésekkel



Heller-Rényi-modell: magán/köz és nyilvános/nem nyilvános alapján 4 kategória (ábra →)
Szociológiai-tömegkommunikációs alapkoncepció

Az adatok titkosítása többféle jog és érdek alapján történhet:
→ van, ami a főszabályt erősíti (pl. orvosi titok)
→ van, ami jelentős kivétel (pl. államtitok)

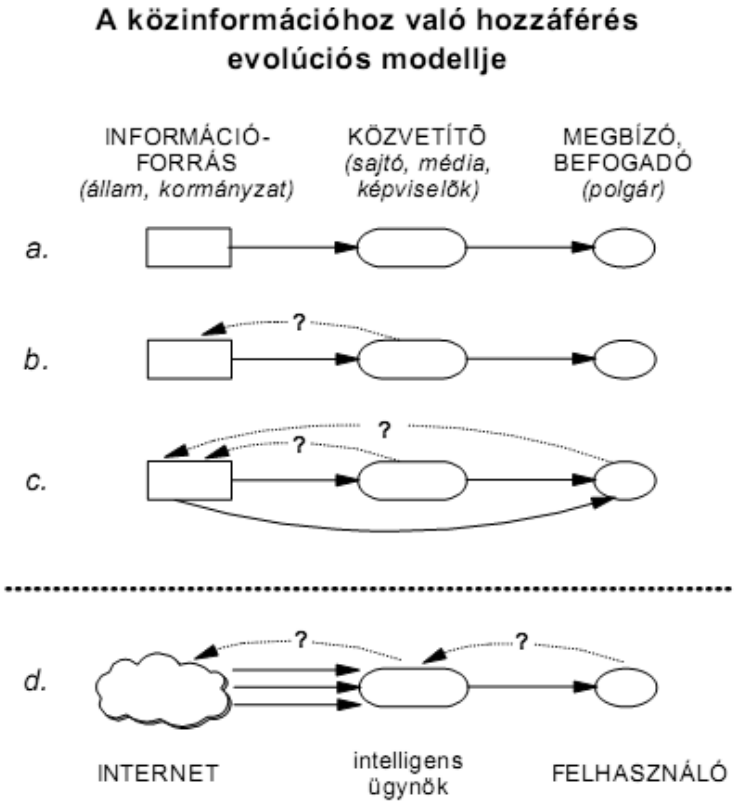
A fentiek alapján az ábrákon való elhelyezésük is különböző.

A különböző területeket más-más törvények, jogszabályok, etikai kódexek szabályozzák, *DE: az általános magán/közérdekű szétválasztás itt is érvényesítve van!*

A kategorizálás már jóval a gépi korszak előtt megjelent, azonban a gépi feldolgozás megjelenése erősen rásegített az elvek fontosságának kiemelésére!

A modern informatikai és távközlési technológiák sok problémát vetnek fel az információs szempontból gyengébb és erősebb fél között. Fő okok:
→ információs hatalom ellenőrző és befolyásoló hatása → személyes szféra határainak eltolódása
→ az információs hatalom, mint közinformációkat kezelő monopólium koncentrálódása

A közinformációhoz való hozzáférés modelljei



Kezdetben: király → nép **kvázi-közvetlen kommunikáció**, közvetítő esetleg egy-egy hivatalnok volt

A. eset: képviseleti demokrácia információs modellje
→ a polgárt képviselő sajtó/média a közvetítő a forrás és a befogadó között

B. eset: sajtószabadság modellje
→ a képviselő nem csak közvetít, de privilégiumai okán követelhet is információt

C. eset: információszabadság modellje
→ a befogadó (polgár) közvetlenül is hozzáférhet, ill. követelhet információt *(„direkt demokrácia")*

DE: az Internet térhódításával a befogadó komoly problémákkal szembesülhet
→ az információforrás nem egy személy/szerv lesz, hanem egy hatalmas adattömeg (virtuális forrás) lesz, amely mögött valahol valódi források állnak
→ minőségi: a szemét és az információ egyforma, a feltett anyagot senki nem ellenőrzi
→ mennyiségi: túl sok információ, minőségi gondokkal

Részleges megoldás: **intelligens ágens (ügynök) alkalmazása, mint közvetítő → D. ábra**
→ az ügynök egy személyre szóló tudásbázist tartalmaz, előszelektálja a kért információt
→ az ágens a felhasználók manipulálásának leghatékonyabb, alig kontrollálható eszköze is lehet!!

Az adatvédelem alapelvei

Nemzetközileg elfogadott, tételes alapelvek a főszabály (információs önrendelkezés) és kivételeinek érvényre juttatásához. Az előadáson kivonatosan vettük az OECD Irányelveit:

1. Az adatgyűjtés korlátozásának elve → személyes adat gyűjtése csak törvényes és tisztességes eszközzel, az adatalany tudtával és beleegyezésével.

2. Az adatminőség elve → az adatok az adatkezelés céljával összhangban legyenek pontosak, teljesek és aktualizáltak.

3. A célhozkötöttség elve → személyes adatot csak előre meghatározott célból, a cél eléréséhez szükséges mértékig és ideig lehet kezelni.

4. A korlátozott felhasználás elve → adatok felhasználása csak az alany engedélyével vagy törvényi felhatalmazással

5. A biztonság elve → az adott kor technikájának megfelelő, ésszerű intézkedésekkel védeni kell az adatokat a jogosulatlan hozzáférés (törlés, publikálás, sérülés, megsemmisülés) ellen

6. A nyíltság elve → az adatkezelés ténye, helye, célja, politikája, valamint az ezt végző személye nyilvános legyen

7. A személyes részvétel elve → az adatalany a rá vonatkozó adatokat megismerheti és ha helyénvaló, akkor módosíthatja, bővítheti vagy akár töröltetheti is azokat

8. A felelősség elve → az adatot kezelő a fenti elvek betartásáért felelős, az adatkezelés jogszerűségét igazolnia kell tudni

Az információszabadság alapelvei

Freedom of Information = FoI

A közadatok hozzáférését szabályozza.

1. Az információszabadsághoz mindenkinek joga van. → nem kell igazolni, milyen célból érdekel egy adat.

2. A nyilvánosság a főszabály, a titkosság a kivétel. → titkosítani csak szigorú indokok miatt, szűk körben lehet.

3. A jog az összes közintézményre kiterjed. → állami, önkormányzati szervek, DE: adófizetők pénzéből részesülő szervezetek + közfeladatot ellátó magánszervek is

4. Az információigénylés egyszerű, gyors és ingyenes legyen. → bárki képes legyen egy közadathoz hozzáférni komolyabb erőfeszítések nélkül, ingyen

5. A hivatalnok kötelessége, hogy segítse az adatigénylőt.

6. A visszautasítást indokolni kell. → a főszabálynak: nyilvánosság ellent mond a visszautasítás, így azt törvényi alapon, az igénylő számára minden részletében világos és érthető módon meg kell indokolni

7. A közérdek elsőbbséget élvez a titkossággal szemben. → ha a közérdek erősebb, mint az okozott kár, akkor a titkosítás semmisnek vehető (pl. környezet, egészség, emberi jog, korrupció esetei)

8. Mindenkinek joga van fellebbezni az elutasítás ellen.

9. A közintézmények aktívan tegyék közzé a lényegi információkat. → a lényeges dolgokat kérdés és kérés nélkül, up-to-date publikálják (akár off-, akár online), DE: ettől még kell válaszolniuk, ha bárkinek kérdése van

10. Független testület garantálja az információszabadság érvényesülését.
→ ombudsman/parlamenti biztos. Feladatkör: köztudat erősítése, visszautasítások és fellebbezések vizsgálata

Nemzeti és nemzetközi szabályozás

Adatvédelem következő szintje
OECD Irányelvei, Európa Tanács Adatvédelmi Egyezménye, Eu Adatvédelmi Direktíva

irányelv (guideline) → követése nem kötelező
direktíva (directive) → az ebben foglaltak követése a belső jogban kötelező

OECD irányelv + ET egyezmény: egyszerre készültek
→ OECD: határátlépő adatáramlás szükségessége és annak garanciái
→ ET: információs jogok biztosítása ebben az áramlásban
→ OECD követése ajánlott, ET viszont az egyezmény aláírása után kötelező

EU direktíva: adatkezelés azon közös, részletes szabályai, melyet a tagországoknak kötelező átemelniük a belső jogukba
→ a már meglévő törvényeket és gyakorlatokat át kellett szabni, szükség szerint
→ az új jogszabályok a tagfelvételre váró országokban is már eszerint készültek

ET egyezmény: azonos védelem, míg EU direktíva: csak megfelelő védelem
→ egyezményen és EU-n kívüli harmadik országba csak akkor küldhető korlátozás nélkül személyes adat, ha az a megkövetelt adatvédelmi szintet megüti (azonos, ekvivalens védelem)
→ megfelelő (adekvát) védelem eltérő környezetben, alternatív eszközökkel és módszerekkel is elképzelhető

→→ *egy nem-adekvát védelmi kategóriás országba irányuló személyes információáramlást korlázoni kell → a globális információáramlás korában ez komoly gazdasági és politikai kérdéseket vet fel*

Belső (nemzeti) jog: következő szintje az adatvédelemnek.
→ a magyar szabályozás korszerű, az európai hagyományakt követi
→ **közös törvény** szabályozza az adatvédelmet és az információszabadságot
Alkotmánytól a keretszerű Adatvédelmi törvényen át a szektoriális törvényekig, rendeletekig

A belső jog érvényesülését különféle ellenőri intézmények ellenőrizhetik.
→ testület (pl. francia CNIL)
→ egyszemélyes tisztség (brit I.C.)
→ parlament által választható / kormány által kinevezhető
→ hatósági, bírói vagy ombudsmani jogosítványok

Magyarország: adatvédelmi biztos (1995 óta), Parlament választja, ombudsmani jogosítvány
→ fő tevékenység: panaszok kivizsgálása, de ő is indíthat vizsgálatokat mind az állami, mind a magánszektorban
→ a vizsgálatok eredménye csak ajánlás, melyek elfogadottsága magas arányú

---

1. zárthelyi (2011.10.27.) anyaga