

# ADATVÉDELLEN ÉS INFOSZABADSÁG

GZEKELY NAN, doans, ITN tanzsek (Információ és Tudásmenedzsment)  
Jönök Marianna (tanulmányi előadó) ST.1em.(18-32) tio@itm.bme.hu  
www.itm.bme.hu → Regisztráció  
http://lists.sch.bme.hu/wvs/info/adatvedelem

társadalmi informatikus ü

V: írásbeli vizsga, 3 alkalom

TK: jegyzet, szövegyűjtemény

www.hte.hu/onlinekonyv.html → 1.8 fejezet (definíció)

www.dh.hu → adatvédelmi biztos (eset, történet)

PRIME (www.prime-project.eu)

ADATVÉDELLEN: a személyes adatok gyűjtésének, feldolgozásának és felhasználásának | korlátozottsát, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek | összessége

↓  
lényeg!!!

↓  
jog

data protection, ... ≠ ADATBIZTONSÁG (data security)

SZENÉLYES ADAT: minden olyan rögzített, visszakereshető ismeret, ami egy adott személlyel kapcsolatba hozható

↳ ≠ személyi adat

x kelljen y-ről hogy...  
mindigük adata

- adat
- nyomon követhetőség
- vélemény
- teljes adat is!
- csoportra vonatkozó adat (a csoport minden tagjára)

parkoló autók rendszámának felírása → en: NEM személyes

→ rándór: SZENÉLYES

tehát függ az adat kezelőjétől is az adat milyensége,

↳ halottnak nincs személyes adata, DE van hozzáférési jog → az adatai a hozzáférőzők személyes adatai lehetnek

↳ jogi személynek jogi személyiséggel nem rendelkező társaságok NINCS személyes adata

## AZ ENBEREK NEM SZABADFORGALMÚ JAVAK!

It emberek személyisége, adatai sem szabadforgalmú javak. It adatvédelem fogalmilag csak személyes adatok esetében értelmezhető.

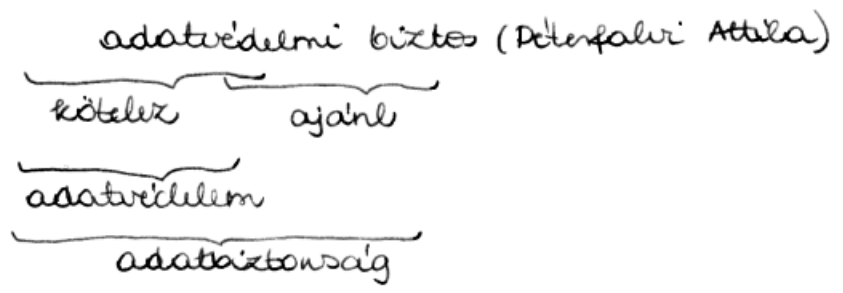
It adatbiztonság egyaránt értelmezhető magán- és nem magán-személy esetében.

It adatvédelem az ADATALANYOK védelme; az adatbiztonság pedig az adatok védelme.



3 kivétel pl. Kilon, törvényi szabályozás APEH, rendőrség, Spam, államtitok  
 } főszabály  
 ↓  
 Mindig a kivételnek kell magyarázkodnia!

Elvileg mindenkinek maga dönt a személyes adatai sorsáról.



Információszabadság  
 - a közadatok bárki számára, bármikor elérhetőek

- olyan személyes adat, amire a nyilvánosság vonatkozik
- személyes-ÉS közadat NINCS!
- közfeladat ellátó, közszereplő munkájával kapcsolatos adata  
 ↳ minél "magasabb rangú" egy ember, annál szűkebb a személyes szférája

2006.09.20

az ember életét döntő részben a számítógépes rendszerben róla tárolt adatok határozzák meg.

- Újraalkítás lehetőségei:
- information replica
  - digital persona

↳ digitális személyiségünk alapján döntenek automatizmusok  
 ↳ van erre tilalom is, tehát kötelező lehetőséget biztosítani személyes beavatkozásra is, és meg kell indokolni a döntést (automatizmus)

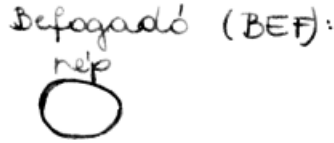
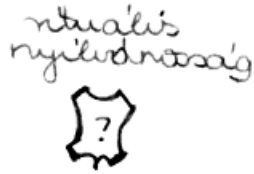
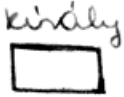


az életet különösképpen meghatározó adatok; szigorúbb védelem alá tartoznak; kizárólag IRÁSBAN lehet rendelkezni róla!

digital persona } így együtt  
 + "örök" megőrzés } ez nagyon VESZÉLYES!

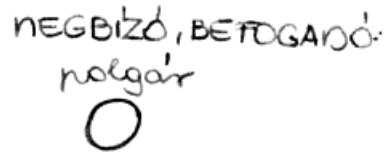
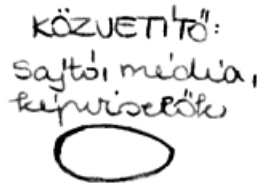
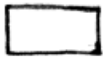
pmisz: igazságszolgáltatás + büntetőeljárás nyilvános  
 munkahelyi drogteszt: hozzájárulás után - tövényi alapon

Információforrás (IF):

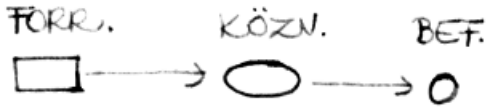


- semmit nem lehet tudni

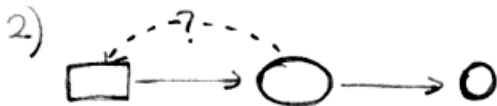
IF: állam, kormányzat



1) A KÖZINTORNACIÓHOZ VALÓ HOZZAFÉRÉS EVOLÚCIÓS MODELLEI

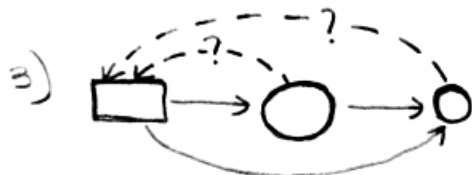


képviselői rendszer információs modellje



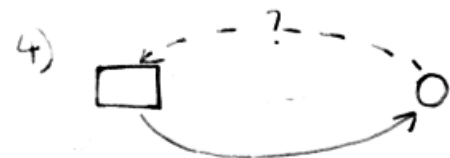
közvetítő információt közvetít és a kapott információkat megosztja a befogadóval

SAJTÓSZABADSÁG (sajtónak és képviselőnek joga van bármit megkérdezni)



mindenkinek közvetlenül van joga kérdésekhez és válaszokhoz

INTORNACIÓSZABADSÁG



DEZINTERMEDIÁCIÓ

nem kellnek közvetítők

- DE minőségi és mennyiségi problémák  
 - ez csak illúzió



INTERNET

↳ intelligens ágens: program, n.i., ami a felhasználó helyett elvégzi a keresést

- ez a kárhoat

- de nagyon manipulatív!

Judáshoz való jog - napja 09.28

↳ információszabadság nemzetközi napja

az adatvédelem alapelvei (OECD irányelvek csoportosításában)

- 1995 óta van adatvédelmi biztos No-n: Najtekny László
- 30% - adatvédelem ; 10% - információszabadság
- ↳ egyetemi ; ↳ közösségi

1) az adatgyűjtés korlátozásának elve  
 - a személyes adatok gyűjtését korlátozni kell (nem szabadforgalmú)  
 - az adatok megszerzése:  
 ↳ törvényes és tisztességes eszközökkel  
 ↳ ha lehet, az adatbirtokos tudtával és beleegyezésével (önrendelkezés)

2) az adatminőség elve  
 - pontos  
 - teljes  
 - aktuális  
 ↳ a célhoz összhangban, a célnak megfelelő mértékben

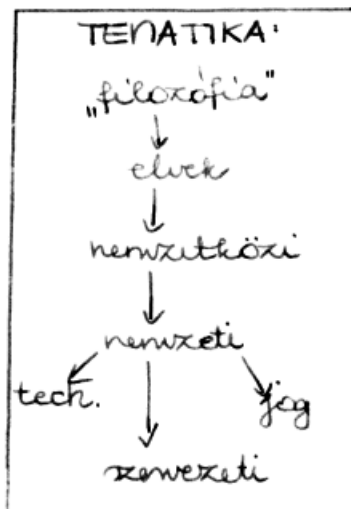
3) célhoz kötöttség elve (szaklatos pont!)  
 - előzetes célmeghatározás (nem szabad másra használni, kiszélesíteni)  
 - adatkizűlés → a célnak megfelelő mértékben (felülregezen ott adat)  
 ↳ a célnak megfelelő ideig (pl. bankváltás esetén + elváltási időket meghosszabbították)

4) korlátozott felhasználás ("ököl szabály")  
 - az adatkizűlés csak 2 esetben engedélyezett  
 ↳ adatbirtokos hozzájárulásával  
 ↳ törvény rendelkezése alapján (rendelék, utasítás, ajánlás alapján NEM)

opt in : önrendelkezés  
 opt out : hallgatélagos beleegyezés

5) a biztonság elve:  
 - az adatkizűlési célnak és a technika mindenkori állásának megfelelő észszerű biztonsági intézkedések megtételére  
 pl. illetéktelen hozzáférés, módosítás, felhasználás elvezetés  
 megsemmisítés ellen

6) a nyíltság elve  
 - az adatkizűlés és az adatkizűlési politika nyilvános  
 - az adatok körének, kizűlésük céljának, jogalapjának, az adatkizűlés kizűléseket megismerhetőségét biztosítani kell  
 ↳ Adatvédelmi Nyilatkozat (pl. kívül csak a saját dolgozó adatait kizűli) (pl. titkosszolgálatok :)



7) a személyes részvétel elve (beteleltetés - helysbítés - törlés)

- az adatalalanynak joga van

- megtudni, hogy van-e iza adat
- ha van, azokat kapni (elfogadható időn belül, érthető formában, ingyen vagy méltányos díj ellenében)
- az elutasítás indokait megismerni és kifogásolni
- az adatokat helysbíteletni vagy törléletni

adattámasztva

ha hozzájárulás alapján került be

penzmosás elleni törvény esetén ha a bank kedvel

AZ ÖV ESETÉBEN JOGELLENEZ ADATKEZELES NEM TÖRTÉNT ☺

8) a felelősség elve

- az adatvédelmi alapelvek betartásáért az adatkezelő felelős

- ↳ adatkezelőnek kell bizonyítania, hogy nem történt visszaadás (és NEM az adatalalany, hogy történt)

2006.10.04.

ADATKEZELES: az alkalmazotti eljárásról függetlenül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hozzáférése (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése.

Adatkezelésnek számít az adatok módosztatása és további felhasználásuk megokozódása is.

ADATFELDOLGOZÁS: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

pl.-bérzámfejlesztés (outsourcing)

- banki szervezetek számlázás, egyenleg-postázás (os.)
- lettershop (átadott címjegyzék alapján postázás direkt-marketing ajánlatokért)
- bértárolás (ha személyes adatokról van szó)
- informatikai rendszerek kezelési, karbantartója (ha ezt "éles"-ügyleti adatokat  
↳ fizetés, tervezés bizt-adatokkal)

ADATKEZELŐ (nem operátor)

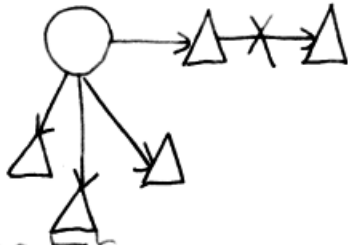
- teljes felelősség

- az adatkezelés céljának a meghatározása
- döntések meghozdása
- döntések végrehajtása
- adatfeldolgozói megpízás adása
- ↳ felelősség a megpízás jogszemléseéért

## ADATFELDOLGOZÓ:

- korlátozott felelősség
  - a megbízás végrehajtásáért
  - az adatok feldolgozásáért
  - megváltoztatásáért
  - törléséért
  - továbbításáért és nyilvánosságra hozataláért

Személyes adatok esetén tárhelyezés tilos!



○ adatkezelő  
Δ adatfeldolgozó

## ADATTOVÁBBÍTÁS

- az az aktus, amikor egy személyes adatot meghatározott 3. személy(ek) számára elérhetővé tesz
- nem fizikai továbbítás
- pl. jelző megadás, otthagyni a "naplót"

## NYILVÁNOSSÁGRA HOZATAL

- bárki számára hozzáférhetővé teszi
- pl. kiplakáttól személyes adatot

## AZ INFORMÁCIÓSZABADSÁG ALAPELVEI

(az Open Society Justice Initiative csoportosításában)

- 1.) az információszabadsághoz mindenkinek joga van
  - állampolgárságtól, nemzetiségtől és foglalkozástól függetlenül
  - nem kell indokolni, hogy milyen célból

2005 óta mindent kérés nélkül ki kell vonni az internetre;  
kérés → igénylés (mert joga van hozzá)

- 2.) a nyilvánosság a főszabály, a titkosság a kivétel
  - információszabadság csak szűk körű indokok alapján
  - törvényekben és nemzetközi normákban meghatározva

- 3.) a jog az összes közintézményre kiterjed
  - állami és önkormányzati szervek
  - adófizető pénzügyi "szerszám" szervezetek } és azt mire költi
  - közfeladatok ellátó magán-szervezetek (pl. ÁPV Rt.)

- 4.) az információigénylés egyszerű, gyors és ingyenes legyen
  - csak a legszükségesebb adatok megadásával
  - szóban vagy írásban
  - legfeljebb a reprodukációs költség számolható fel

- 5.) a hivatalnok kötelessége, hogy segítse az adatigénylőt
  - ha rossz helyen jelentkezik, tegye át az igénylőt a megfelelő szervezethez

6.) a vérszavastást indokolni kell  
- csak törvényi alapon  
- világos indoklással

7.) a közérdek elsőbbségét élvez a titkossággal szemben  
- ha a közérdek erősebb, mint az érintett érdeke  
- különösen: környezet, egészség, emberi jogok, korrupció

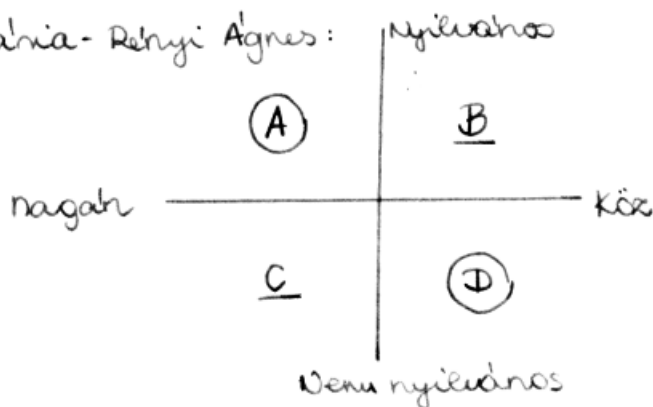
8.) mindenkinek joga van fellebbezni az elutasítás ellen  
- azonnali és hatékony eljárás  
- fellebbezés a nem-válaszadás ellen is

9.) a közintézmények aktívan tegyék közzé a helyi információkat  
- kérdés nélkül is  
- aktuális információk; világos formában; érthető nyelven;  
(lehetett volna dinamikus közzététel is ...)

10.) független testület garantálja az információszabadság érvényesülését  
- ombudsman (-person) vagy parlamenti biztos  
- kivizsgálja a vérszavastásokat  
- erősíti a köztudatot

2006.10.11.

Heller Nánia - Rényi Ágnes:



O természetes  
- kizárjuk, magánizandó

## PRIVACY

Habeas Corpus (Have Your Corpus)

- az ember egy modern polgári világban maga rendelkezik a testével

Habeas Data

- rendelkez az adatait felett

1) Magánélet és a "köz" közötti határfalat először rombolta le a telefon feltalálása.

Onnan az új technológiához lassan alkalmazkodott a jogalkotás.

pl. Amerikában a precedencia-jog van: a magánélet határait a telegrafal jelenti; hova teszük a kihallgatószerzőket című történet 1960-as évek végéig

Warren - Brandeis (1890): The Right to Privacy

- kívánhatatlan, hogy a modern kutyák beférjenek a magánéletünkbe

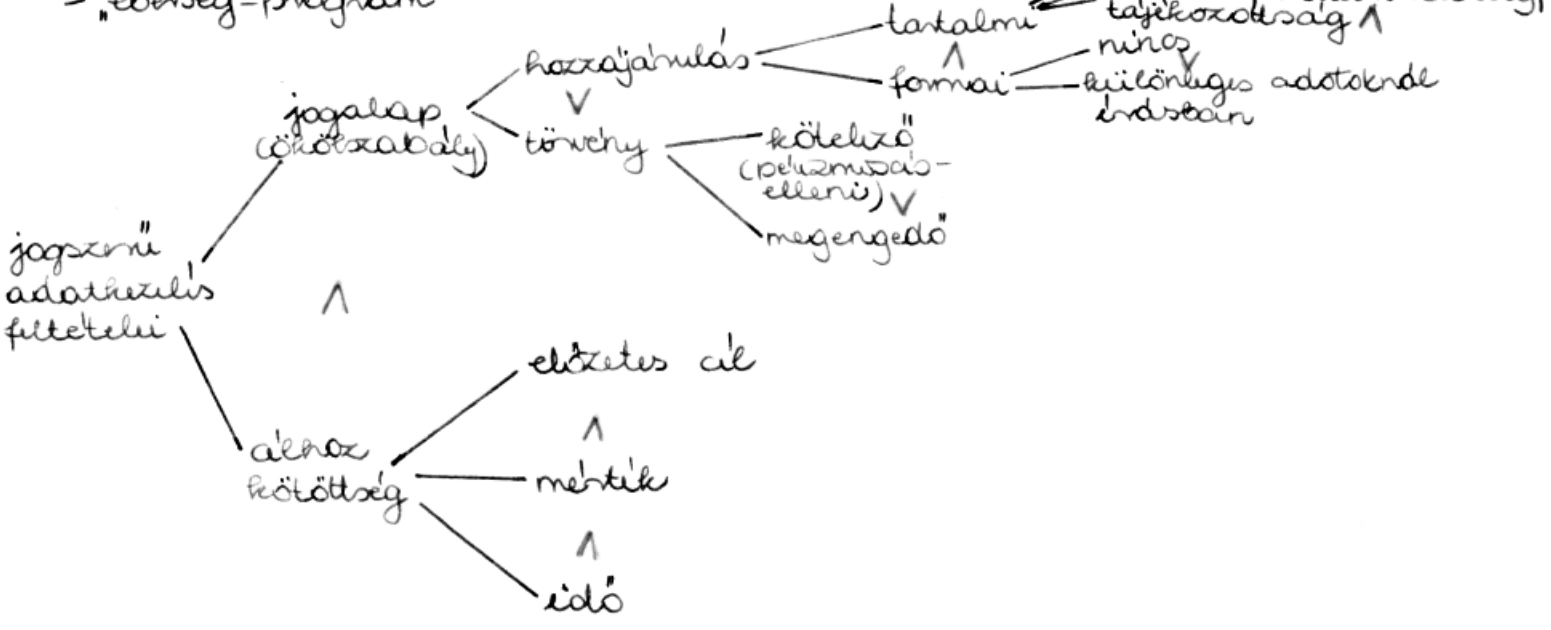
+ telefónia adta létösségek

2) számítógépesítés: felszabadult gépkapacitás felhasználása a lakosság gyűjtött adatainak feldolgozására

- 3) Internet:
- információszexis és -feldolgozás összefonódik
  - mostanság titkosít
  - dinamikus arazás (profil felépítése, és ajánlat alapján)
  - CRM (Customer Relation, Management)
    - nyújtott szolgáltatás ügyfélentik alapján

4) 09.18.

- tiltott biztonsági szabályozások törvényesség, mégé bírva
- "éberség-program"



önkényesség: fenyegetés, kényszer eseten nincs, plusz jutlatásnál igen  
 tájékoztató: olyan nincs, hogy a "hallgató bejegyzés" kattintás nem bejegyzés → nagy piros és zöld gombok  
 tájékoztató: interneten nem biztosítható → tájékoztató ablak ok-zása nélkül nem lehet továbblépni

BKV ellenőr: előszabály kööttség / jogalap - nincs hozzájárulás

nendőrké elkéri a személyi igazolványt, de az ellenőrnök nem adhatja oda; BKV 8napon belül kérheti az adatokat és ekkor a nendőrség átadja

2006.10.18.

Nemzetközi adatvédelmi szabályozás

- OECD: Data Protection Guidelines
- Council of Europe: Data Protection Convention
- European Union: Data Protection Directive



OECD: csak guideline, könnyen tiljítható

Európa Tanács: összeindpai szervezet (Fehérorország nélkül)  
foglalkozik foglalkozik (+kultúra)  
Strasbourg-ban van a központja

Európai Unió: 25 tag  
penzile, politikával foglalkozik  
Brüsszel a központja  
(tanácsadóak központja viszont Strasbourgban)

egyezmény: aláírta és ratifikálta  
olyan mint egy nemzetközi szerződés; kötelező betartani  
(mint egy magyar törvény, de a magyar törvények is  
elégendők minden problémára)

direktíva (irányelv): kötelező hatályú  
ha hoznak egy törvényt Brüsszelben, akkor  
azt 3 év után implementálni kell  
de mi már belépésünk előtt megfektünk a  
feltevéseknek

Európa Tanács: ekvivalens védelmi szint (azonos)

Európai Unió: adekvát védelmi szint (megfelelő)

De mi legyen a személyes adatokkal a 3. országban? (pl. USA, Korea, Japán)

### ADATVÉDELMI SZABÁLYOZÁS

szektor	EU modell magán + köz (D+Kft...) (állam...)	Amerikai modell köz
feldolgozás	automatikus (szg.) + manuális (papír)	automatikus
lifedés	általános (enyő- zés; radióadás)	mozaiszerű (konfliktus- orientált)
ellenőr	van	nincs

az amerikai modell nem felel meg az európai modellnek,  
egy korlátozásokkal kellene bevezetni Amerikával szemben.

DE Amerika túl erős, így csak egy alapelv gyűjtemény  
van: Safety Harbour Principles

↳ önkéntes lista, amire fel lehet jelentkezni; az itt  
jelentkező cégeket fogadja el az EU adekvát  
biztonsági szintűként

↳ de nincs ellenőrzés, nincsenek szabályok, kötelezettség

↳ 2000-ben No. is megkapta elők között

- 1) Európai Unió tag-e
- 2) Európai konveniót aláírta-e
- 3) adekvát státusszal (pl. Kanada)
- 4) szerződés aláírása (külön adatvédelmi szerződés v. melléklet)

↳ mintaszerződés letölthető Internetről  
↳ alapvető érdek! a megköltés

TASZ (Társaság a Szabadsáigjogokért)

- jogsegélyszervezet (beteg, információszabadság-jogok)

www.tasz.hu

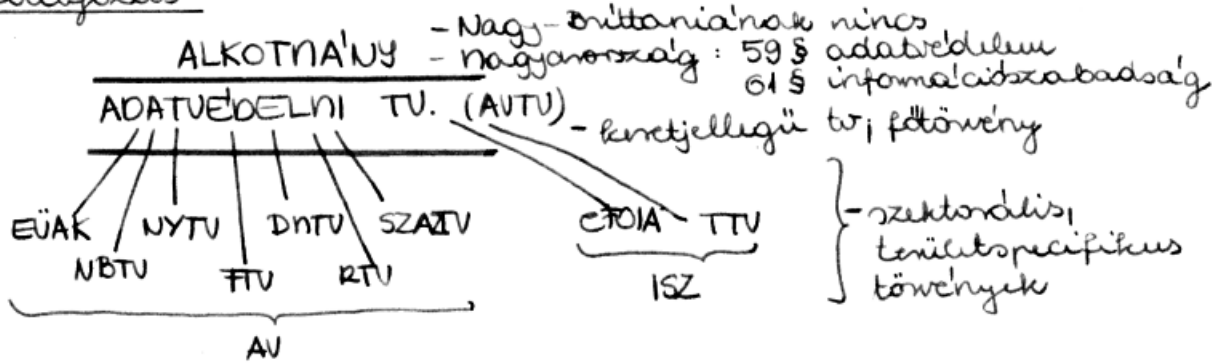
Svédországban 1766-ban írták információs szabadságról törvényt; minden információ szabad, így a titkos Uniós adatokhoz is hozzájuthatnak.

- tilos nyomozni a magánvéleményt nyilatkozókat után; ez már bühöselekmény

- whistleblowers (közérdekű bejelentő): aki olyan közérdekű, de titkos adatot hoz nyilvánosságra, amit egyébként nem lenne szabad

2006.10.25.

Nemzeti szabályozás:



AV

EÜAK → egészségügyi adatok védelme, 1997  
↳ főleg kivételket tartalmaz (pl. járvány esetén nem rendelkezem az adataim felett; anonym-AIDS szűrés)  
↳ először csak negatív esetben anonym; most már minden esetben kérhető

NYTV → (népszerűségi) nyilvántartási törvény, 1992

DNTV → Direkt Marketing törvény, 1995

SZAVT → Szakazonosító törvény, 1996  
↳ személyi igazolvány, TAJ-szám, adószám használatának szabályozása  
↳ kiegészítő törvény: SALÁTA-törvény  
↳ kapcsolat az azonosítók között - adószám APEH, UROP  
- TAJ TB, EÜ  
- személy. BN, Közp. Nyilv. Földhivatal  
↳ a 3 adatot elkülönítve kell kezelni (kezelni); ez valószínűleg meg a átkötöttséget

FTU → Felsőoktatási törvény 2. melléklete

RTV → Rendőrségi törvény  
↳ mikor igazoltatható

NBTV → Nemzetbiztonsági tv.  
↳ kihallgatás milyen engedélyekkel, feltétellel

ISZ

eFOIA → electronic freedom of information act (elektronikus információs szabadság törvénye)

TTV → titoktörvény  
↳ csak kivételket tartalmaz

RENDELETEK - öndöntő adatkezelés nem rendelhető el,  
DE például nyilvántartási törvények  
lehet (van) végrehajtási rendelete

BELSO SZABALYOK - szervezetre vonatkozó kötelező "belső"  
szabályok  
- adott szervezet, vagy iparág állítja  
elő

igazságtudati      egyedi

↓ hierarchia fentről lefelé, de az adatkezelők teljesen pont  
fordítva alkalmazzák

Alkotmánybíróság (AB) feladata, hogy vizsgálja, hogy az alkotmány  
és a törvények ellentmondás-e egymásnak

alapk: alkotmányos jogok  
más Alkotmánybíróság

főszabály: kombinált adatvédelmi és információszabadság törvény

kiegészítők: a) szektorális adatvédelmi törvények  
b) Titoktörvény

független ellenőr: országgyűlési biztós

szankciók: Btk.

## ADATVÉDELMI TÖRVÉNY

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

### a) ADATVÉDELMI

- tág definíciók (1999: adatfeldolgozó, adatfeldolgozás),
- adatkezelés alapfeltevése: törvény vagy hozzájárulás
- lefedés: köz és magánsector  
automatizált és manuális nyilvántartások
- adatvédelmi alapelvek
- az érintett személy jogai
- bírósági jogorvoslat, kártérítés  
↳ nem-vagyoni kár  
(ombudsman ↔ bíróság)

### b) INFORMÁCIÓSZABADSÁG

- közfunkción alapul (tulajdonos mindegy, lényeg hogy az  
adat a KÖZZEL kapcsolatos)
- pozitív és negatív információszabadság (nemcsak kérdésre  
kell válaszolni, hanem önkéntesen is adatot  
szolgáltatni)
- adatok + dokumentumok  
↓  
lényeg                      ↓  
közérdekű adatokat tartalmazó dokumen-  
tumokat is ki kell adni, megfelelő  
faxonitás után

- korlátozás: törvény + felsorolt érdekek
- puha titok: belső vagy döntéshozzáértő dokumentumok  
(„belső használatra” nevé gumipecsét)
- határidő: 15 nap DE elutasítás esetén 8 nap
- elutasított kérelmek: jelentés az adatvédelmi biztósának
- bírósági jogorvoslat (kártérítés nem kérhető)

### c) ADATVÉDELMI BIZTOS

- ellenőrzi az adatvédelem és információszabadság érvényesülését (az állami és magánsektorban egyaránt)
- egyedi panaszokat kivizsgál
- hivatalból indít vizsgálatot

### TITOKTÖRVÉNY

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

TITOKFAJTÁK - államtitok  
- szolgálati titok

Vato-ban 4 szintű minősítés: COSMIC, TOP SECRET, SECRET, CONFIDENTIAL

Államtitoknak nyilvánítás (=minősítés) feltételei:

- csak meghatározott személy és eljárás
- valamelyik titokkörbe tartozzon (149 titokkör + 20 kiegészítésként)
- formai követelmények ("Szigorlatos titok!" pecsét alul-felül)
- sértse az állam fennsúlyát érdekét

együttműködés

↓  
TÜK - Titkos ügykezelés vonatkozású utasítás

időtartam: titokkörönként eltérő maximum (leghosszabb: 30 év)

rendszeres felülvizsgálat (minimum 3 évenként)

széles körű kiadási lehetősége

tömeges visszaminősítés: 1980 előtti (titkos) dokumentumokra 1 éves határidő volt

ellenőrzés: - szakmai: Belügyminisztérium  
- tartalmi: adatvédelmi biztos

bírdát

(NSA - National Security Archives: különböző államokból kérik ki titkos adatokat, a széles körű kiadási lehetőséggel. Mindenképp különböző adatokat törölnék ki, így előállítható a teljes titkos dokumentum.)

2006.11.08.

AL ROBERTS:  
www.obh.hu

### A PET TECHNOLOGIAK (Privacy Enhancing Technologies)

A rendeltetésük szerint használt PET eszközök is rendszerük mindig a gyengébb felül - jellemzően az adatbázist - védik az információk tárhatalommal rendelkező erősebb féllel szemben.

kivéve pl: FBI, CIA

- nemcsak bármilyen adatot védjenek, hanem az adatbázisokat is

# A. Burkert-féle usportoztatás

- a) szubjektum-orientált (pl. anonim kártyabirtokosok)
- b) objektum-orientált → az anonimitást az eszköz biztosítja (pl. anonim digitális pénz)
- c) tranzakció-orientált → ne lehessen profilokat felépíteni a "szálak" feltételeivel (pl. rekordok automatikus törlése)
- d) rendszer-orientált (a fenti elemek integrációja)

B. a) a meglévő rendszerek biztonságát növelő technológiák (adattisztaság személyközi kommunikációban)

- b) új adattárolási és -hozzáférési technológiák (CNW, Demoprint)
  - csak akkor lehet írni-olvasni, mikor a megfelelő ujj(kenyomat) társítva van hozzá



- Magyar példány
- csak az írás-olvasást kezeli, de a kinyert adatot nem felelteti ki

c) tranzakció alapú technológiák (Bioscript, E-cash, CAFE)

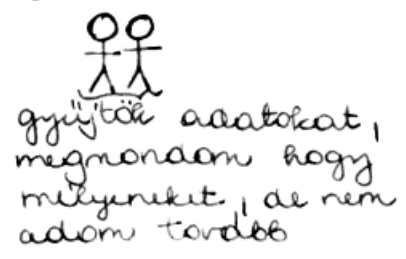
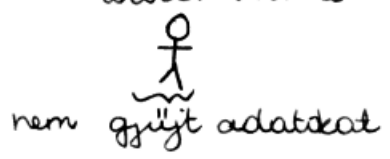
C. Néhány adatvédelmi alapvető elvhez illeszkedő segítség?

- D. a) technológia-alapú PET-ek (hitelesítés azonosítás nélkül) → blind-signature-alapú rendszerek (nagyon megbízható)
- b) humán-interakció alapú PET-ek (P3P, OPS, TRUSTE)

## PET, mint "önszabályozás"

- TRUSTE
- P3P (Platform for Privacy Preferences) → W3C alkotta meg; az áramló személyes adatok szabályozása "alkuszimilér"
- OPS (Open Profiling Standard)
  - ↓
  - a profilokat a felhasználó saját gépén tárolja

TRUSTE - trustmark (internetes bizalmas védjegy)  
 - személyes adatok védelmét garantálja  
[www.truste.org](http://www.truste.org) (www.tbonline)



# BIOSCRIPT

- ujjlenyomat → lenyom → bioscript egészenírtve
- biometrikus + nem biometrikus adat szükséges

↓  
ujjlenyomat lenyomra;  
tíjes képet rögzítők

↓  
PIN-kód, kulcs, pinter

a 2 adat összekutyulása

- megoldás: ujjlenyomat leírása; a rendszer kikutyulja az az adatokat és kiegészíti a nem biometrikus adat

→ anonim adatok: itt kell a POINTER!  
(egyébkel statisztikákat lehet készíteni az adatokból, de a pointer nélkül nem lehet személyhez kötni)

→ 2 személy ujjlenyomata nyitja a kulcsot ... Interneten

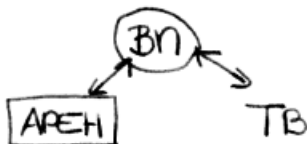
→ CYBER-NOUSE (egyetke épített ujjlenyomatlvasó ... emberi lustaság miatt)

→ elektronikus kereskedelem

kereskedő nem tudja olvasni a rendeléshez mellékelt bioscriptet; azt továbbítja a banknak és azt egy mesterséges intelligenciával lehet nyitni  
bank nem tudja, hogy mit rendeltem

## KAPCSOLATI KÓD:

pe. közzéad az adóhatóság és BN közötti kapcsolatban olyan azonosító, amely egy adatalányt azonosít (egyértelműen) 2 adatkészlet közötti kapcsolatban



nem a szokványos azonosítón tartanak nyilván a kapcsolatban, hanem a kapcsolati kódon

## INTRA-ORGANIZATION CONNECTING CODE

azonosító ← "idegen kulcs" → személyes adat

szervizben belüli azonosító kódok más-és-más személyes adatokhoz nyújtanak hozzáférést, akár az adatalánytól függetlenül is

	állandó	változó
természetes	anya neve születési hely	név
mesterséges	személyszám	nyitunkód ügyfélszám
biometrikus	ujjlenyomat hangminta DNS	arcnyomtat

2006.11.22.

TOR.PARK  
www.tornify.com } anonim böngészés  
Onion Routing

### CROWDS (HOROS)

- anonim böngészés
- közös erőfőnyés sk segítségével csoportos anonimitást biztosít
- külön infrastruktúra nem kell hozzá (a csoporton belüli gépek bekapcsolva vannak)

### ONION ROUTING

- felépülnek és lebomlanak utak véletlenszerűen
- kívülre nem lehet az egyedüket megfigyelni
- "halraj + kukac"

- 1.) A leendő a hálózatban működő gépek listáját
- 2.) véletlenszerűen felépült titkosított útvonalon üzenetet küld B-nek, aki egy végponthoz van csatlakozva
- 3.) a csomópontok nem ismerik a rajtuk átmenő forgalmat (legfeljebb elnyelheti)

### PRIME

- identitásmenedzselő és magánélet-védő megaprojekt
  - Európai Unió + Svájc + vállalatok közös vállalkozása (tevé)
  - al egy technológiától független réteg beépítése a kommunikációs csatornába (middleware)
  - követi a törvényi szabályozásokat és saját beállításokat
- www.prime-project.eu / whitepaper
- role-based privacy

### PET KRITÉRIUMOK

- anonimitás (név nélküli tranzakciók)
- pseudonimitás (nick névhez kapcsolódó személyiségek)
- megfigyelhetetlenség (observability - ne látszódjon, hogy erőfőnyést használ)
- összeköthetlenség (onlinkability - látszódjon, hogy ki melyiket használja)

→ de kiknek érdekében??

### PET tartalmú témák, szolgáltatások

- anonim böngészők,
- nym generátorok (nym - fedőnév, álnev)
- remailerok
- cookie-irtók
- spyware-irtók (kinprogramokat helyez el a távoli gép a gépiünkön)
- adat- és hangrögzítők → PGP
- web bug irtók (láthatatlan 1x1 px-es képt; 3. fél megfigyeli a szolgáltatást)
- profilgátlók → P3P és közöttek lelt csatornákat)
- bizalmi védjegyek → TrustE
- digitális penzrendszer
- bioscrypt
- spam-, webkldm-szűrők

www.bugnois.com

## Anonim e-mailer

- követelmények:
- a kommunikáló partnerek anonimitása
  - a kommunikáló partnerek közötti kapcsolatot nyomonkövethetetlensége
  - az üzenet tartalmának megfigyelhetetlensége
  - a e-mailer kompromittálhatatlansága

fejlesztés: kiselletetés hozzáadása + véletlen kiselletetés a szemet üzenetek kioldására + üzenetsziszorítás elleni üzenetfelismerés, és csak let fogad el + e-mailernek láncba felzése a láthatatlanságért + szabványos méret + formátum az üzenetanalízis ellen (méretfigyelés)

- típusok:
- egyzemi anonim levelezés
  - pseudonim levelezés
  - cypherpunk (1.) → folyamatosan csökken az üzenet mérete, ahogy eldobja a felhasznált "parancsokat"
  - mixmaster (2.)

padding után szabványos méretre bontás,  
aszimmetrikus (RSA) és szimmetrikus (3DES) titkosítás

cél: üzenet titkosítása  
"bekabaldós-joga" (pl. közszféra kintizálása, diszkrét)

2006. 12. 06.

1995. Direkt Marketing tv. (CXIX. tv.)

Nagytudományi Akadémia Egyesülete (régibben Kamara)

↳ kibővítték törvényi szabályozást: kutatás ...

- Tudományos kutató (zoosológia)
- Közvélemény- és piacutató (fogászati szokások, vélemények)
- Direkt Marketing ← X

↓  
személyes adatokat használ!

↓  
statisztikai adatokkal számolnak,  
(személyes adatokkal kezdenek dolgozni, amit utána törölnek)

DN-lista Zhelyől szerezhető be legalisan

0. bármilyen módon a telefonokban lévő, adatok

1. BN központi lakam- és név-nyilvántartás  
innen lehet venni (igazából csak térelni) adatokat,  
HA nincsen tiltva (demónyirodában kizárható ingyenes nyomtatvány segítségével)

2. nyilvántartás regiszterből feltűve HA a szerkesztő előre szölt és nem tiltakozott

3. "Kaszonló a Kaszonlótól": a fentebb említett szektorok tagjai a szektoron belül adatokat cserélhetnek, HA előre szölt és nem tiltakozott

De egymás között nem cserélhetnek adatokat, különösképpen közvéleménykutató, piacutató → DN

opt-in: csak akkor cserélkedhet, ha megengedte

opt-out: addig cserélkedhet, amíg meg nem tiltják

mailing - reklámüzenet, levél

prospect - leadó ügyfél

personalizálás - levél megszélyesítés



## Marketing kötelező tartozékai:

- honnan szerezte az adatot
- mine használják az adatot
- hogyan tiltakozhat (opt-out lehetősége)

Tiltakozás = töröljük át a címlistánál, de ilyen nincs: tilos törölni a listából, helyett van a tilalmi-lista (Robinson-lista), azaz, hogy újból ne kerülhessen fel a listára

Nagy kampányok előtt mindig új címetek vesznek a mobilitás miatt (születés, halálozás, elköltözés, házasság, ...).

A Robinson-listát tilos átadni.

Több vállalat állíthat fel közös Robinson-listát is, tehát saját<sup>ot</sup> is is fent kell tartani. Egyelőre nincsen ilyen nagy közös aig.

- Allow lista, hogy mikor indulnak kampányok.
- Deduplikálás: csak úgy lehet biztosan új adatokat kérni, hogy az államnak átadja az összes adatot, majd az allow elválogatja és megkapják az új adatokat
- Segmentálás: adatok elválogatása különböző szempontok alapján (kor, nem, lakóhely, ...).  
A különböző szektorok más-más mennyiségű szempontot kérhetnek. Szegmens tagjai is egymás között az adatalányok tulajdonosi alapján (mennyire lelkes vásárló, ...).

Nem postai marketingre opt-in szabály (nem opt-out)

- elektronikus kereskedelemre vonatkozó törvény
- előzetes beleegyezés szükséges