Adatvédelem és információszabadság

Hallgatói jegyzet

Összeállította

Ulicska Gergely

Lektorálta

Dr. Székely Iván

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
2019

Tartalomjegyzék

Előszó

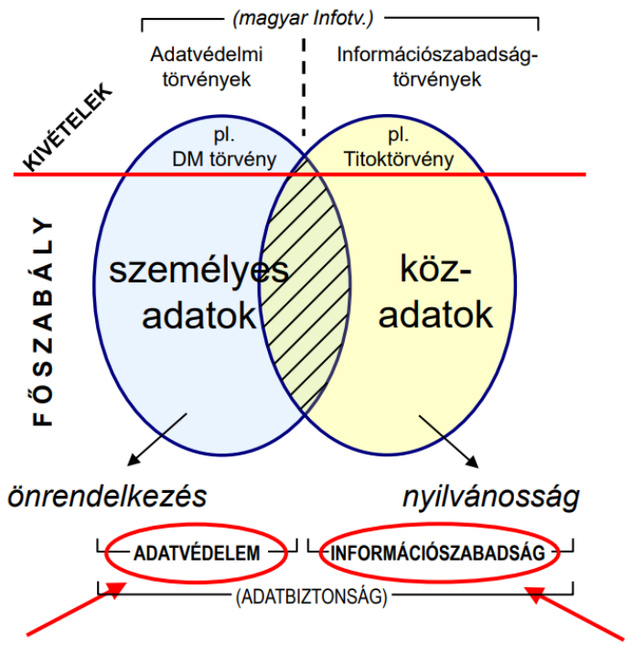
Ez a hallgatói jegyzet az Adatvédelem és információszabadság c. tárgy (VIETAK49) 2019. tavaszi kurzusa alapján készült, a tárgyalt témák ott elhangzott sorrendjét követve.

Sikeres felkészülést!

1. Alapmodellek

1.1. Székely-féle modell

Az adatokat ebben a tárgykörben két alapkategóriára, személyes adatokra és közadatokra osztjuk. Ezt mutatja be a Székely-féle modell, amelyben az alapkategóriákra egy-egy főszabály (a táblázatban) vonatkozik.



1. ábra. A Székely-féle modell
(Forrás: Dr. Székely Iván oktatási segédlete)

személyes adatok	önrendekezés
közadatok	nyilvánosság

1. táblázat. Alapkategóriákra vonatkozó főszabályok

A vörös vonal felett találhatóak a kivételek, melyekre a főszabályok nem érvényesek.[1] Az adatvédeledelem a személyes adatok kezelésére vonatkozik, az információszabadság a közadatok kezelésére. (Az adatbiztonság mindkét alapkategóriára értelmezhető.) A rájuk vonatkozó törvények a nevükből adódnak; tárgyunk egészét lefedő törvény a magyar Infotv.[2]
A legérdekesebb része az ábrának mégis a középső satírozott rész, mely a közadatok és a személyes adatok metszetét jelzi. Ez a terület olyan személyes adatokat ábrázol, melyek *közfeladatot ellátó*, avagy közszereplő természetes személyekhez tartoznak, így ezekre mégis a nyilvánosság főszabálya vonatkozik.

1.2. A közinformációhoz való hozzáférés evolúciós modellje

Az információszabadság területén létrejövő információáramlásnak három fő résztvevője van:

1. információforrás
2. közvetítő
3. megbízó, befogadó

Még az elején fontos kiemelnünk, hogy az állam (az adminisztráció) nem ekvivalens fogalom a kormányzattal (a politikával), az utóbbi az előbbinek csak egy része.

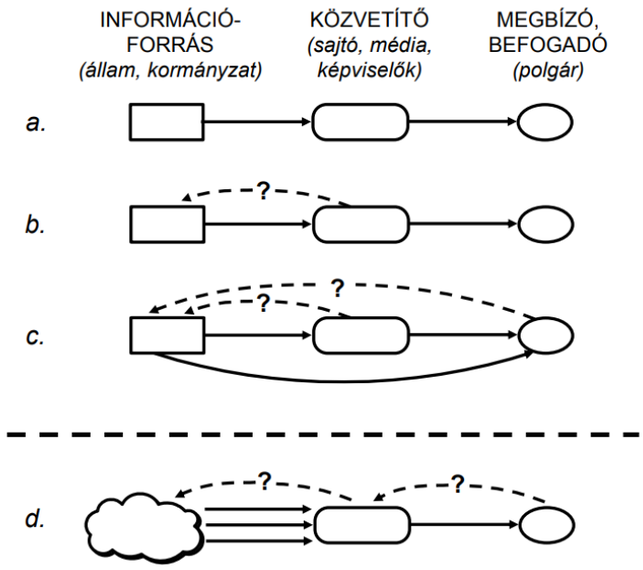
1.2.1. a) A képviseleti demokrácia modellje

Ennek a modellnek a legfontosabb eleme, hogy a közvetítők ott lehetnek a forrásnál (átvitt értelemben a polgárt képviselő sajtó) és eljuttathatják a közinformációkat a forrástól a befogadóig. Fontos még kiemelni, hogy ez nem magától értetődő sok helyen, még ma is vannak kivételek, de a közadatok esetében a főszabály továbbra is a nyilvánosság.[3]

1.2.2. b) A sajtószabadság modellje

A képviseleti demokráciához képest itt az a fejlődés vehető észre, hogy a közvetítő követelhet is információt a forrástól. Ennek a modellnek hátránya lehet, hogy a forrás élhet a nemválaszolás jogával, esetleg előre megbeszélt kérdések szerint is folyhat az interjú.

[1] DM: DirektMarketing, azaz 'közvetlen üzletszerzés'.
[2] Az információs önrendelkezésről és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), amely a korábbi törvény hatályon kívül helyezésével vált irányadóvá.
[3] Például a tárgyalóteremben a bírónak teljhatalma van, eltetetheti a jegyzeteket, a fényképezőgépet.



2. ábra. A közinformációhoz való hozzáférés evolúciós modellje
(Forrás: Dr. Székely Iván oktatási segédlete)

1.2.3. c) Az információszabadság modellje

A legfontosabb változás az előzőekhez képest, hogy itt a befogadó is követelhet és kaphat információt. Felmerülhet a kérdés, hogy ebben az esetben miért van szükség a közvetítőre. Ez esetben elég csak az internetre, mint információközvetítőre gondolni: nincs fönt minden; ami ott van, azt is valaki úgy tette fel, ahogyan: fontos különbséget tenni az érték és szemét között, ezt pedig csak több közvetítő, több értelmezés segítségével érhetjük el.

1.2.4. A d) modell[4]

Ebben a modellben megfigyelhető az internet létrejöttével együtt elterjedő *látszólagos dezintermediáció*[5]. Ez több problémát is magában hordoz, leginkább a már említett mennyiségi és minőségi problémákat, miszerint nem tudunk mit kezdeni a rendelkezésünkre álló hatalmas adathalmazzal, nem tudjuk eldönteni, mi valós, mi nem. Erre mutat megoldást a szemléltetett **intelligens ágens**, amely az internet és a felhasználó közé beékelődve, mint egy mesterséges intelligencia, redukálja a mennyiséget és szűri a káros információkat. Ez természetesen további kérdéseket hordoz magában, miszerint az alany változik, avagy az internet változtatja meg és hasonlóak. Összességében állíthatjuk, hogy a valóságnak csak egy szűrt képét láthatjuk; de magát a szűrőt nem.

[4] A szaggatott vonal jelzi, hogy itt a szereplők megváltoznak.
[5] Itt: a közvetítő kiiktatása.

2. Adatvédelemmel kapcsolatos fogalmak

2.1. Adatvédelem és adatbiztonság

Adatvédelem A **személyes adatok** gyűjtésének, feldolgozásának és felhasználásának **korlátozását**, az érintett személyek **védelmét** biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége; az önrendelkezés joga személyes adatok esetében. *(Fontos kiemelni, hogy adatvédelem csak a személyes adatok esetében értelmezhető, azaz a közadatok esetében nem!)*

Adatbiztonság Az adatok jogosulatlan megszerzése, módosulása és tönkremenetele elleni **műszaki és szervezési megoldások** rendszere. *(Azaz, az adatbiztonság a nem személyes adatok esetében is értelmezhető.)*

A két fogalmat a végtelenségig leegyszerűsítve mondhatjuk, hogy az adatvédelem az adatalanyokról, míg az adatbiztonság az adatokról szól, ahogy a táblázat is mutatja.

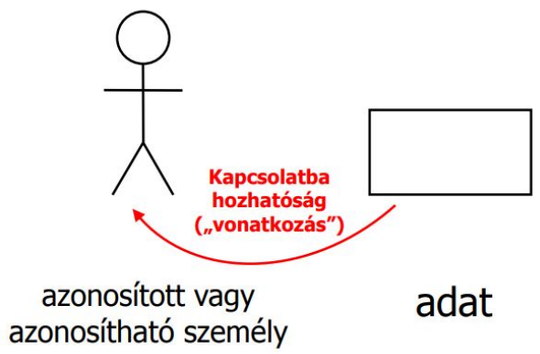
adatvédelem	adatalanyok
adatbiztonság	adatok

2. táblázat. Mi minek a védelme?

2.2. A személyes adat

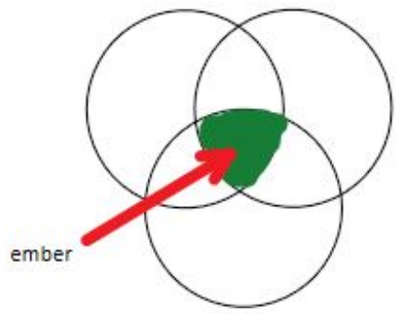
A személyes adat Azonosított vagy *azonosítható* természetes személyre („érintettre") vonatkozó bármely információ. (Például: tényadat, vélemény, következtetés, származtatott adat, téves adat, fénykép, hangfelvétel, video, ujjlenyomat, íriszkép, DNS minta, ...)

Azonosítható személy Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.



3. ábra. A személyes adat alapkritériuma a kapcsolatba hozhatóság
(Forrás: Dr. Székely Iván oktatási segédlete)

Ahogy a képen is látszik, a személyes adat attól lesz személyes adat, hogy az **kapcsolatba hozható** az adatalannyal. Ezt a azonosíthatóságot a fogalom már tisztázta, mi minden lehet, elég csak a személy nevére gondolni, ami sokszor egyértelműen be is tudja határolni az adatalanyt (esetleg egy felhasználónévre, ami nem ismétlődhet); azonban, nem csak egyféle dolog azonosíthatja a szóban forgó személyt: itt jön képbe az **anonimitási halmaz**[6].

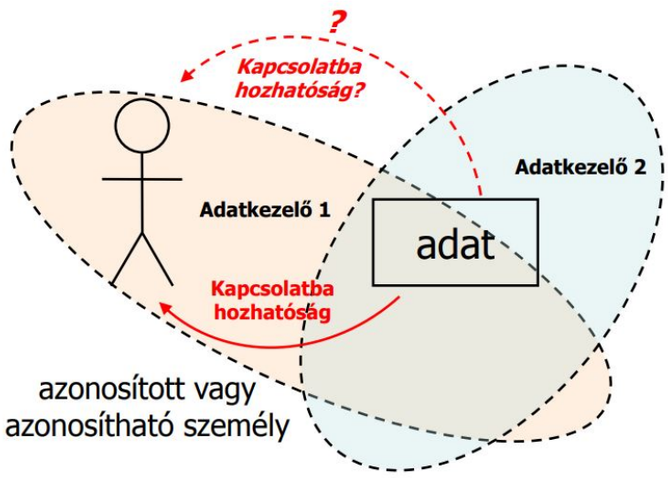


4. ábra. Anonimitási halmazok metszete
(Saját szerkesztés)

Ahogy a kép is mutatja, az anonimitási halmazok (például: neme, hajszíne, szemüveges-e?) metszetében található az alany. Minél több adatot tudunk így felsorakoztatni, annál pontosabban határolható be a személy, így úgymond egy „egyéni ujjlenyomat" alakul ki, melyet sokan ki is tudnak használni. (Nem is hinnénk, mennyire körbehatárolhatóak vagyunk, miközben a számítógépünket használjuk; a képernyőfelbontásunk, a színhasználatunk, a

[6] Olyan halmaz, amelyen belül az egyes alanyok között a rendelkezésre álló jellemzők alapján nem tudunk különbséget tenni.

ki- bekapcsolási időnk és az egyéb személyes beállításaink segítségével könnyen azonosíthatóak vagyunk.[7])
A téma további kérdéseket is felvet, például, mi a helyzet több adatkezelő esetében. Az *azonosított, vagy azonosítható személy* kapcsolatban áll a képen csak *Adatkezelő 1*-gyel jelzett szervezettel/személlyel, mely az adatainak a birtokában van, így a személyt kapcsolatba tudja hozni az adatokkal. Ellenben kérdés vetődhet fel, hogy mi történik, ha az adatokat egy *Adatkezelő 2*-vel jelzett másik szervezet/személy is megszerzi, aki nem tudja kapcsolatba hozni azokat az eredeti személlyel. Ugyanazok az adatok tehát *Adatkezelő 1* számára személyes adatoknak minősülnek, *Adatkezelő 2* számára nem személyes adatoknak.



5. ábra. Ugyanaz az adat lehet személyes és nem személyes két adatkezelőnél
(Forrás: Dr. Székely Iván oktatási segédlete)

2.3. Adatkezelés

Adatkezelés A személyes adatokkal végzett **bármely** művelet vagy a műveletek összessége. *(Nincs olyan, személyes adatokkal végzett művelet, amely nem minősül adatkezelésnek!)*; *„Így különösen"*[8] gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, **továbbítása, nyilvánosságra hozatala**, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, *„továbbá"* fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (*például* ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

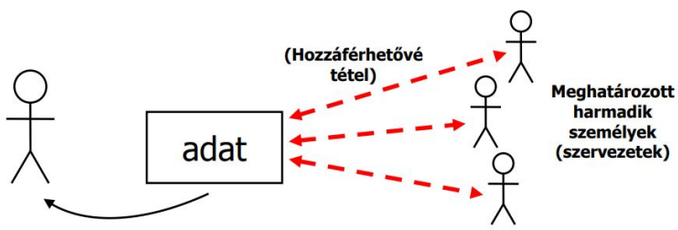
A definícióban előfordul az adattovábbítás és a nyilvánosságra hozatal kifejezés, ezért fontos megérteni a kettő között a különbséget:

Adattovábbítás Az az adatkezelési művelet, amelynek során a személyes adatot **meghatározott harmadik személy** számára hozzáférhetővé teszik. *(Nem szükséges az adat fizikai továbbítása vagy a hozzáférés érvényesítése: a hozzáférhetővé tétel már adattovábbításnak minősül.)*

Nyilvánosságra hozatal Az az adatkezelési művelet, amelynek során a személyes adatot **bárki** számára hozzáférhetővé teszik. *(Nem szükséges a hozzáférés érvényesítése: a hozzáférhetővé tétel már nyilvánosságra hozatalnak minősül.)*

adattovábbítás	meghatározott harmadik személy
nyilvánosságra hozatal	bárki

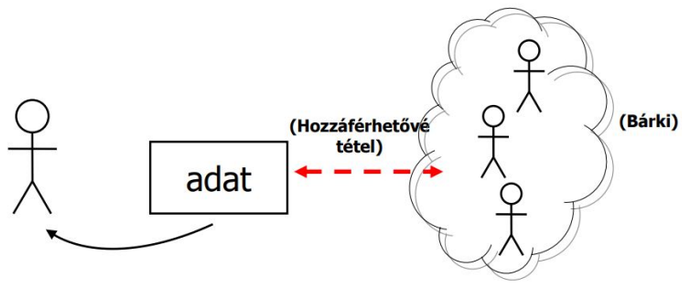
3. táblázat. Ki számára lesz hozzáférhető az adat?



6. ábra. Adattovábbítás
(Forrás: Dr. Székely Iván oktatási segédlete)

[7] Gondoljunk csak a TOR böngésző figyelmeztetésére, mikor kinagyítjuk az ablakot: ilyenkor szól, hogy ne tegyünk, ezzel is megnehezítve az utánunk kutatók dolgát, mivel így nehezebb kideríteni a képernyőfelbontásunkat.

[8] Ezek a szófordulatok a jogszabályokban („így különösen", „továbbá", „például", „nem teljes") mutatják, hogy nincs minden felsorolva, csak példákat hoznak, ezért is nagyon fontos megérteni a fogalomban a **bármilyen** szó lényegét.



7. ábra. Nyilvánosságra hozatal
(Forrás: Dr. Székely Iván oktatási segédlete)

2.4. Az adatkezelő és az adatfeldolgozó

Kezdjük is egy minket érintő példával! Ki a mi adatkezelőnk?
A tanulmányi előadó? Hisz ő ellenőrzi az iratainkat zh-nál. NEM
Esetleg a tanszék? Megkaphat minden adatot rólunk...? NEM
Talán maga a VIK? NEM
A mi adatkezelőnk a BME.

Adatkezelő Az a természetes vagy jogi személy, amely a személyes adatok kezelésének **céljait** és eszközeit (önállóan vagy másokkal együtt) **meghatározza**; az adatkezelésre vonatkozó döntéseket **végrehajtja** vagy az **általa megbízott adatfeldolgozóval végrehajtatja**.

Kiszervezett adatkezelés Az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége; azaz az adatokat nem szükséges „feldolgozni", bármely kiszervezett személyesadat-kezelési művelet adatfeldolgozásnak minősül!

(Például: bérszámfejtés, számlaküldés, megszemélyesítés (lettershop), kiszervezett call center, kiszervezett biztonsági szolgálat, irat- és adattárolás, irat- és adatmegsemmisítés, informatikai fejlesztés, üzemeltetés, karbantartás, ...)
Minden olyan kiszervezett tevékenység, amelynek ugyan nem fő célja személyes adatok kezelése, de amelynek során a tevékenységet végző jogszerűen hozzáférhet személyes adatokhoz, *e tekintetben* adatfeldolgozásnak minősül. Az előző játék apropóján megemlítendő, hogy az adatfeldolgozó egyes esetekben nem a BME, hanem a megbízás által megkeresett Bérszámfejtő Kft. Hogy ez szerencsés-e, az alábbi táblázat mutatja.

előnyök	hátrányok
olcsóság, hatékonyság, köztehermentesség	érzéskeny adatok kijuthatnak

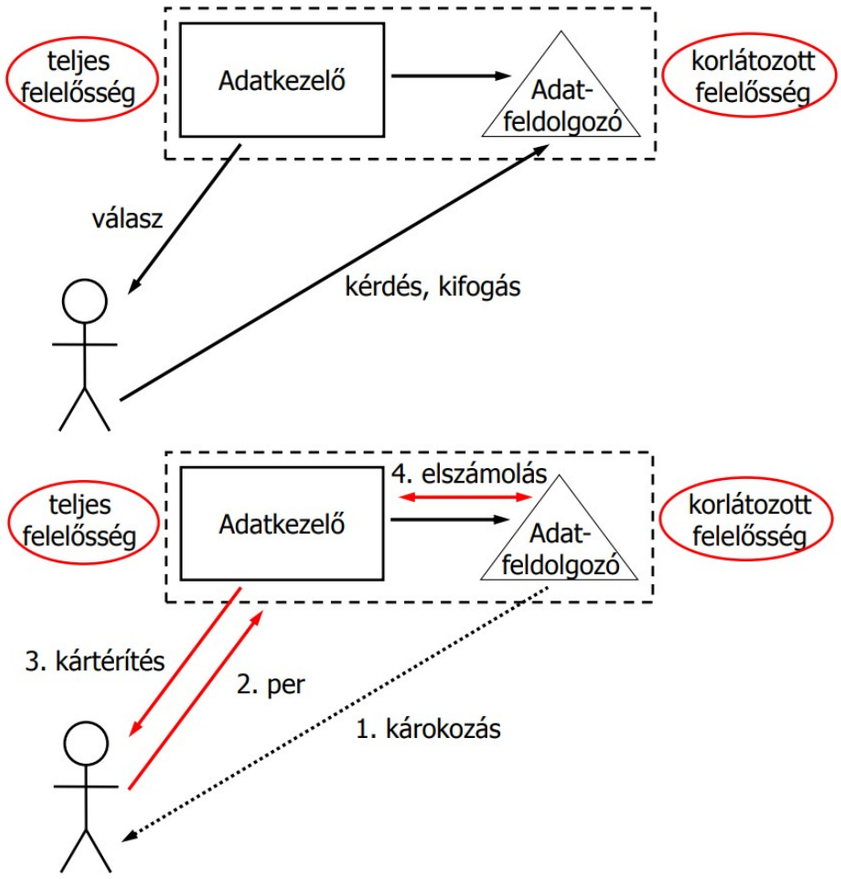
4. táblázat. A kiszervezés előnyei és hátrányai

Így, például, problémákhoz vezethet, hogy a Bérszámfejtő Kft-t nem *csak* a BME, hanem az ELTE, a Sóhivatal, stb. is megbízhatta, így érzékeny adatok is kikerülhetnek (persze, erre kevés az esély).
További példaként említhetjük a call center-eket, amelyeket több cég is alkalmazhat. Itt az alkalmazottat többféle üggyel is megkereshetik, többféle céggel kapcsolatban, így ha az esetleg összekapcsolná az adatokat, az bajt jelenthetne.
Problémát jelenthet a lánc-adatfeldolgozás is.[9]

Adatfeldolgozó Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az **adatkezelő megbízásából** vagy rendelkezése alapján személyes adatokat kezel.

De mi is történik, ha az előbb említett probléma adódik? Ezt az alábbi kép szemlélteti.

[9] Eljárás, melynek során a fő adatfeldolgozó, amellyel az adatkezelő tulajdonosa kapcsolatban áll, további cégeknek szervezi ki az alfeladatokat, így ezek a cégek is adatfeldolgozóvá válhatnak. A lánc-adatfeldolgozás tilalma formailag megszűnt 2012-ben, de 2018-tól az adatkezelőnek beleszólása van a további adatfeldolgozók igénybevételébe, így például ragaszkodhat hozzá, hogy csak a nem személyes adatok kerüljenek tovább, avagy mindegyik adatfeldolgozóval külön álljon kapcsolatban az adatkezelő.



8. ábra. Adatkezelő és -feldolgozó kapcsolata
(Forrás: Dr. Székely Iván oktatási segédlete)

1. Az adatfeldolgozó kárt okoz az adatalanynak (adatvédelmi incidens);
2. Mivel az adatalany csak a károkozás tényét észlelte, esetleg nem is tudott a kiszervezésről, az adatkezelőt perli be (mivel övé a teljes felelősség!);
3. Ha a pert megnyeri, az adatkezelő fizet;
4. Az adatkezelő és az adatfeldolgozóval egymás között elszámolnak.

Az adatfeldolgozó ezek mellett:

- az adatkezelést érintő érdemi döntést nem hozhat;
- a személyes adatokat kizárólag az adatkezelő írásbeli rendelkezései szerint dolgozhatja fel;
- az általa megismert személyes adatokra titoktartási kötelezettséget vállal;
- a műveletek befejezése után törli és/vagy visszaadja az adatokat az adatkezelőnek.

2.5. Személyi adat, különleges adat

A különleges adat fogalmának megértéséhez először a személyes adatok *részhalmazait* kell definiálnunk. A **személyi adat**ok legegyszerűbb megfogalmazásban *azok az adatok, amelyeket egy webes form-on megadunk* (például anyja neve, születési idő, lakcím, stb.).
A **különleges adatok**[10] pedig azok az adatok, amelyek az életünket legjobban befolyásolják. Az érzékenység mindig a kontextustól függ, ezért akár a személyi adatok is ide tartozhatnak, de a törvények külön is felsorolják a különleges személyes adatok körét, amelyek kezelésére szigorúbb szabályok vonatkoznak. Ilyenek többek között az egészségi állapot, a politikai nézet, a vallási hovatartozás, a szexuális orientáció, stb.[11]

2.6. Magyar-angol kisszótár a témához

adatvédelem	data protection
adatbiztonság	data security
adattovábbítás	data transfering
adatkezelő	data controller
kiszervezés	outsourcing
adatfeldolgozó	data processor
adatalany	data subject
különleges adat	special categories of data

[10] Más néven szenzitív (érzékeny) adatok.
[11] Ebben a témakörben érdemes lehet megismerni Cayla és i-Que babák történeteit az alábbi linken: `https://www.youtube.com/watch?v=lAOj0H5c6Yc`.

3. Az adatvédelem alapelvei

Ebben a fejezetben a **személyes adatok** kezelésének alapelveit mutatjuk be az OECD[12] irányelvei alapján.

3.1. Az adatgyűjtés korlátozásának elve

Fontos, hogy a személyes adatok gyűjtését korlátozni kell, így az alapelvnek megfelelően két szabályt kell eközben betartani:

1. törvényes és tisztességes eszközökkel;
2. ha lehet, az adatalany tudtával és beleegyezésével történjen.

Míg a törvényes eszközök teljesen érthetőek és behatárolhatóak (általában), addig a tisztességes módszer egy elég tág fogalom, ezért pontosítást igényel. Egy példával élve a marketing leveleken (ún. mailing során) három fontos dolgot is említeni illik: 1) *honnan* szerezték meg az adatokat, 2) *mire* akarják használni, 3) hogyan lehet *leiratkozni* a levelezőlistáról.

3.2. Az adatminőség elve

E szerint az elv szerint az adatoknak három fontos minőségi szempontnak kell megfelelniük:

1. pontos;
2. teljes;
3. aktuális.

Ezek a feltételek konjunktívak, vagyis egyidejűleg kell érvényesülniük. Példaként felhozható a lakcímkártya esete:

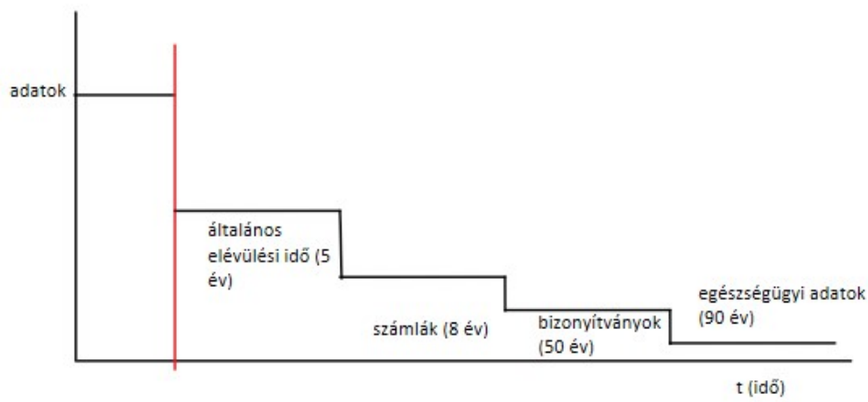
1. pontos legyen, azaz nem elég az utcát megadni, a házszámnak is rajta kell lennie;
2. teljes legyen, azaz minden adat szerepeljen rajta (név, város, utca, házszám, stb.);
3. aktuális legyen, azaz a költözés esetében azonnal új kártyát kell készíttetni.

3.3. A célhozkötöttség elve

A legfontosabb alapelv mind közül! Két fő része van:

1. előzetes célmeghatározás;
2. adatkezelés.
    - a célnak megfelelő *mértékben*;
    - a célnak megfelelő *ideig*.

E szerint az alapelv szerint az adatkezelés célját **előre** tudnia kell az adatalanynak. Így például, mikor betéti kártyát kapunk (amivel nem lehet túllépni a meghatározott pénzügyi keretet), sokkal kevesebb adatot kellene elkérnie a banknak, mint mikor hitelkártyáért folyamodunk (mivel itt van rizikója a banknak). Ebben a példában az adatok a bank biztonságát (biztonságérzetét) szolgálják, így ez is a cél.
Az alábbi képen látható, hogy milyen típusú adatokat meddig szabad őrizni a közvetlen cél megszűnése után, a célhozkötöttség figyelembevételével. (Azaz a tárolás tiltott dolog egy idő után!)



9. ábra. Adatmegőrzés az idő előrehaladtával
(Saját szerkesztés)

[12] Lásd a 6.1 fejezetben.

3.4. A korlátozott felhasználás elve

...egy ún. ökölszabály, mert könnyen megjegyezhető és mindig alkalmazható. Ez az elv kimondja, hogy az adatkezelés csak két esetben lehet jogszerű[13]:

- az **adatalany** hozzájárulásával;
- **törvény** rendelkezése alapján.

3.5. A biztonság elve

Az adatkezelési célnak és a technika mindenkori állásának megfelelő **ésszerű** biztonsági intézkedések megtétele, például: illetéktelen hozzáférés, módosítás, felhasználás, elvesztés, megsemmisülés ellen, stb.

3.6. A nyíltság elve

Az **adatkezelés**nek és az adatkezelési politikának nyilvánosnak kell lennie. Az adatok körének, kezelésük céljának, jogalapjának, az adatkezelő kilétének megismerhetőségét biztosítani kell.

korábban	központi Adatvédelmi Nyilvántartás
most	az adatkezelő felelőssége

5. táblázat. Ki biztosítja a megismerhetőséget?

3.7. A személyes részvétel elve

Ez az elv tartalmazza, hogy mi mindenhez van joga az adatalanynak:

- megtudni, hogy van-e róla adat;
- ha van, azokat megkapni;
- az elutasítás indokát megismerni és kifogásolni;
- az adatokat helyesbíteni vagy töröltetni.

Fontos, hogy az adatalany az adatokat *elfogadható időn belül, érthető formában, ingyen vagy méltányos díj ellenében*[14] kapja meg.
Az elutasításnál néha kérdéses lehet a pontos indok megnevezhetősége, például egy nyomozás esetében.
A helyesbítést pedig, természetesen, csak igazolt esetben lehet elvégezni[15]; megsemmisítésre példa a marketing hírlevelek már említett esete.

3.8. A felelősség elve

Kimondja, hogy az adatvédelmi alapelvek betartásáért az adatkezelő felelős, így egy példával élve a bíróságon a másik félnek kell bizonyítania, hogy *nem* történt meg, amit az adatalany állít (ún. bizonyítási teher).

[13] De lásd GDPR: szerződés teljesítése, adatkezelő kötelezettsége, adatkezelő vagy harmadik fél jogos érdeke is jogalap lehet; GDPR: Az általános adatvédelmi rendelet, hivatalosan *Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg)* (angol terminológiával: General Data Protection Regulation, röviden: GDPR) az Európai Unió rendelete, amely az EGT, azaz az *Európai Gazdasági Térség* területén tartózkodó természetes személyek személyes adatait védi és rendelkezik a tagállamok közötti szabad információáramlásról. A rendelet 2016. május 24-én lépett hatályba, és kétéves türelmi időszak után 2018. május 25-től kell alkalmazni.

[14] Nyomtatási költség, stb.

[15] „Nem lehet a kereset végéről egy nullát letörölni."

4. Információszabadsággal kapcsolatos fogalmak

4.1. Közinformáció, közadat

Az információs „közös jószágokat” háromféle csoportba sorolhatjuk:

1. szellemi közjavak;
2. digitális közjavak;
3. kreatív közjavak.

Míg a szellemi közjavakhoz sorolhatjuk például a Wikipédiát, addig digitális közjavaknak számítanak a nyílt forráskódú szoftverek (free softwares). A kreatív közjavak „Creative Commons” néven ismertek.

Jele	Neve	Hogyan kell eljárni vele?
(c)	copyright	a védett alkotás használatához engedélyt kell kérni, esetleg fizetni is kell
(cc)	Creative Commons[16]	nem kell engedély, se fizetés (de az alkotó feltételeit be kell tartani)

6. táblázat. Különbség a copyright és a Creative Commons között

Itt fontos megemlíteni az általános értelemben vett „közjó” („public goods”) fogalmát, amelybe az olyan, egymással nem versengő „jószágok” tartoznak, amelyek használatából senki sem zárható ki.[17]Ennek részhalmaza az „alkotó közjavak” köre, amelyek a szabad, demokratikus társadalmak olyan alapértékei, amelyek e társadalmak elidegeníthetetlen lényegét alkotják.[18]
Így eljutottunk az **információszabadság**ig, mint fogalomig: **a közinformációk nyilvánossága**; azaz kicsit hosszabban megfogalmazva: mindenkinek alapvető joga arra, hogy a közadatokat (közérdekű adatokat) megismerje és terjessze, és e jogát csak törvény korlátozhatja.

4.2. További fogalmak

Közérdekű adat A közfeladatot ellátó szerv vagy személy kezelésében lévő és a tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, **a személyes adat fogalma alá nem eső** adat.

Közérdekből nyilvános adat A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét **törvény** közérdekből elrendeli.[19]

Nemzeti adatvagyon A közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.

Közadat Az információs önrendelkezési jogról és az információszabadságról szóló törvényben[20] meghatározott közérdekű adat és közérdekből nyilvános adat[21].

4.3. A közérdekű adatok ára

Ebben a kérdésben két érv szokott összecsapni:
Első érv: Az adatokat kezelő szervezeteket mi, adófizetők tartjuk fenn, miért fizessünk még egyszer az adatért?
Második érv: Ha a polgárok kéréseit kell kiszolgálnunk, akkor ez elvonja az **erőforrás**ainkat a *köz* szolgálatától, tehát fizessen ezért a polgár!
Így adja magát a válasz, hogy *alapvetően* törekedjünk az ingyenességre, ezzel szemben, ha valamilyen költség felmerülne (például nyomtatás) azt fizesse az igénylő.

4.4. Tendenciák a hozzáférés korlátozására

Létezik a közszféra információinak további felhasználásáról szóló EU-s **irányelv**, melyet Magyarországon a „Közadat tv.”[22] garantál és kimondja, hogy „**ésszerű** nyereséghányad” felszámolható a közadatigénylés során. További korlátozó tendenciának számít, hogy a néhol egyre erősödő piaci szemléletű szabályozás sokszor szöges ellentétben áll az információs alapjoggal.

[16] Lásd az órán lejátszott videókat.
[17] Gondoljunk csak a levegőre, vagy akár a nemzetbiztonságra.
[18] Székely Iván: „Közadatok és nyilvános adatbázisok: a hozzáférés kérdései” *Educatio*, Vol. 24, 2015 ősz, 40–49. old.
[19] Például a korábbi politikai rendszer titkosügynökeinek adatai.
[20] A 2011. évi CXII. törvény, az Infotv.
[21] Azaz személyes, de nyilvános adatok egyik forrása.
[22] A közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény.

5. Az információszabadság alapelvei

A **közérdekű adatok** kezelésének alapelvei az Open Society Justice Initiative dokumentuma alapján[23]. (Bár ezek az alapelvek hosszabbnak tűnnek, előnyük, hogynem szorulnak bő magyarázatokra a magától értetődésük miatt.)

5.1. Az információszabadsághoz mindenkinek joga van

...állampolgárságtól, nemzetiségtől és foglalkozástól függetlenül. Emellett elengedhetetlenül fontos, hogy nem kell igazolni, hogy milyen célból szeretnénk az adatokhoz hozzájutni, továbbá nem kérni, hanem *igényelni* kell az adatot.

5.2. A nyilvánosság a főszabály, a titkosság a kivétel

Információt visszatartani csak nagyon szűk körű indokok alapján lehet; ezek törvényekben és nemzetközi normákban vannak meghatározva.

5.3. A jog az összes közintézményre kiterjed

...így az állami és önkormányzati szervekre, az adófizetők pénzéből részesülő szervezetekre és a közfeladatot ellátó magánszervezetekre[24] egyaránt, melyeknek így a működésük és a pénzügyeik is nyilvánosak.

5.4. Az információigénylés egyszerű, gyors és ingyenes legyen

Az igénylés eljárása egyszerű legyen, ha nem is ingyenes, minimális költségű (a már említett *ésszerűség* keretein belül), csak a legszükségesebb adatok megadásával, szóban[25] vagy írásban történjen.

5.5. A hivatalnok kötelessége, hogy segítse az adatigénylőt

Például, ha rossz helyen jelentkezik az adatigénylő, tegyék át az igénylését a megfelelő szervezethez.

5.6. A visszautasítást indokolni kell

...természetesen csak törvényi alapon, világos indoklással[26].

5.7. A közérdek elsőbbséget élvez a titkossággal szemben

A titkosítás felülbírálható, ha a közérdek erősebb, mint a titkok nyilvánosságra kerülésével okozott kár, különösen, ha a környezet, az egészség, az emberi jogok, vagy a korrupció szóbakerül[27].

5.8. Mindenkinek joga van fellebbezni az elutasítás ellen

(A nemválaszolás esetén is!) Ennek az eljárásnak gyorsnak és hatékonynak kell lennie.

5.9. A közintézmények aktívan tegyék közzé a lényegi információkat

Kérdés nélkül, aktuális információkat, világos formában, mindenki számára érthető nyelven. (Az elektronikus információszabadság-törvény[28] immáron kimondja, hogy kötelező minden közintézménynek egy weblapot üzemeltetnie a törvényben megnevezett információkkal, így próbálják elősegíteni és támogatni a további kérdéseket és ezzel az információszabadságot.)

5.10. Független testület garantálja az információszabadság érvényesülését

Míg eddig ezt az adatvédelmi (országgyűlési) biztos látta el, egy ideje a NAIH[29] felelős érte.

[23] `http://www.oas.org/dil/access_to_information_human_Policy_Recommendations_10_Principles_on_the_Right_to_Know.pdf`

[24] Könnyen megjegyezhetőek: minden olyan intézmény, melynek nevében a „köz" szó megtalálható (pl.: Közművek, Távközlés, stb. alapszolgáltatások.

[25] Pl.: telefonon.

[26] „A főnök azt mondta, hogy nem": ilyen nem történhet.

[27] Isd.: nagytétényi vegyi gyár és mérgező anyagok; Csernobil.

[28] 2005. évi XC. törvény az elektronikus információszabadságról. (Később beleolvadt az Infotv.-be)

[29] Nemzeti Adatvédelmi és Információszabadság Hatóság

6. Nemzetközi adatvédelmi szabályozás

6.1. OECD

Az **OECD**[30] a fejlett országok együttműködési szervezete. (The Organisation for Economic Co-operation and Development, azaz Gazdasági Együttműködési és Fejlesztési Szervezet.)
Fontos még a fejezet elején hangsúlyozni, hogy míg ebben a szervezetben ismertetett irányelvekhez (*guidelines*) alkalmazkodni nem kötelesek a résztvevő országok (inkább nevezhető eligazításnak, iránymutatásnak), addig az azonos fordítású, ámbár különböző jelentést hordozó *directive*-et kötelező követni.

guideline	eligazítás, lágyabb
directive	kötelező követni

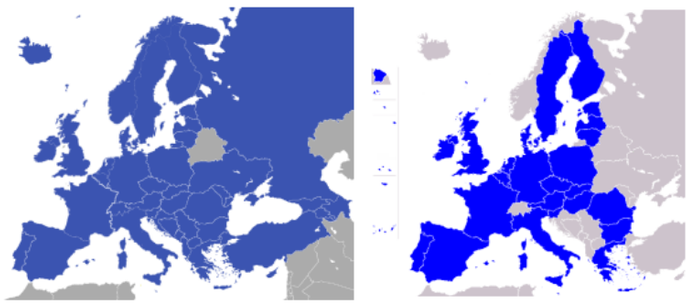
7. táblázat. Irányelvek közti különbség

6.2. Európa Tanács (Council of Europe) vs. Európai Unió (European Union)

	Council of Europe	**European Union**
Foglalkozási kör leegyszerűsítve	jogok és kultúra	pénz és politika
Tagországok [db]	**47**	**28**
Védelmi szint	**ekvivalens**[31]	**adekvát**[32]
Székhelye	Strasbourg	Brüsszel

8. táblázat. Council of Europe vs. European Union

Első ránézésre furcsának is nevezhetnénk a vastagon szedett látszólagos ellentmondást, miszerint egy kisebb létszámmal (28 tagországgal) rendelkező szervezet (melynek tagjai résztvevői a nagyobb létszámúnak is) védelme kevésbé szigorúbb, de ez egyszerűen magyarázható a külkereskedelemmel, mivel például az USA az adatvédelmi szintje nem azonos az európai szinttel, vagyis legfeljebb adekvát megítélést kaphat Európában[33].
Hangsúlyoznunk kell, hogy az EU Általános Adatvédelmi Rendelete (a GDPR) 2018 óta már egységesen vonatkozik minden uniós országra, és az Európa Tanács is modernizálta egyezményét, hogy alkalmazkodjon a GDPR követelményeihez – így a védelmi szint különbsége már csak történelmileg fontos.



6.3. Európai és amerikai modellek

	Európai modell	**Amerikai modell**
Szektor:	magánszektorra és közszektorra[1]	csak a közszektorra
Feldolgozás:	automatikus (gépi) és manuális (papír alapú) feldolgozásra	csak automatikus feldolgozásra[34]
Lefedés:	általános lefedésű	mozaikszerű
Ellenőr:	van	nincs

9. táblázat. Európai és amerikai modellek

Ellenőrző szerveknél említhetjük a Magyarországon eddig tevékenykedő adatvédelmi biztost, ami helyett immáron **NAIH** (Nemzeti Adatvédelem és Információszabadság Hatóság) van, míg Amerikában ilyen esetekre a bíróság van (ennek ellentmond a velejáró sok nehézség: költségek, odajárás, ...). A lefedés kiterjed minden szabályzásra is, elég csak a KRESZ szabályokat példaként felhoznunk: Európában a biztonsági övekről így írnak: „... mindenkinek kell használni, kivéve...", míg az amerikai modellnél példaként lehet említeni a videókölcsönzők esetét, mikor egy egy főbíróról kierült, hogy pornográf kazettákat kölcsönzött, így erre a speciális esetre egy speciális törvényt hoztak az ügyfelek adatainak védelmében (míg például az autókölcsönzők ügyfeleinek esetében nincs ilyen), ezért is nevezik ezt a modellt botrány-/konflikusorientált hozzáállásnak.

[30] Organisation for Economic Co-operation and Development, azaz a Gazdasági Együttműködési és Fejlesztési Szervezet, mely azzal a céllal jött létre, hogy segítse a tagállamok kormányait a lehető legjobb gazdasági és szociális politika kialakításában és fenntartásában.
[32] azonos
[32] megfelelő
[33] Megfelelő, azaz a fügefalevél példájával élve csak azt takarja, amit kell.
[34] Emiatt könnyű manipulálni az adatokkal, azzal a trükkel, hogy kinyomtatjuk, manipuláljuk (mivel csak automatikus feldolgozás esetén van korlátozás) és beszkenneljük

6.4. Külön egyezmények, további jogi dokumentumok

Külön egyezményeket is hoztak az EU-USA kapcsolat kiépítése érdekében, az egyik ilyen az ún. *Passenger Name Record (PNR)*, melynek keretében az amerikai hatóságok a ki-, be-, vagy átutazók neveit rögzítik; avagy a *Safe Harbor Principles* (mely helyett már a *Privacy Shield*[35] van érvényben), ami a „8 OECD alapelv egyszerűsített változata".
Ezen kívül léteznek további, tárgyunkban fontos szerepet betöltő európai jogi dokumentumok is, ilyen a *Távközlési adatvédelmi irányelv*, azaz az *„e-Privacy **Directive***[36], avagy a *Cookie **Directive***, mely bár nem külön irányelv, kimondja, hogy nem létezhet ún. láthatatlan követés és a követés maga legyen is kikapcsolható (így a már említett rendszerujjlenyomatunk nem lesz olyan pontos). Az *e-Privacy **Directive*** után várható az *e-Privacy **Regulation*** 2019-ben, melyet a tagországok **kötelesek lesznek betartani**. Ez a rendelet többek között a metaadatokról szól, például a telefonálásnál míg a „ki, kit, mikor hívott" adatok megőrizhetőek, a tartalom nem, viszont ennek hátulütője, hogy az alany profilja ebből is felépíthető; továbbá az adatmegőrzési idő is minimum 6 hónap, akkor is, ha sikertelen a hívás.

6.5. Esetjogi (bírósági) fejlemények

A Google Spain ítélet, mely 2014 májusában született, fordulópontot jelentett a témában: az eset egy Mario Costeja González nevű személlyel kezdődött, akinek kétes adatait a keresőóriáson keresztül „jó útra térése után" is el lehetett érni („az internet nem felejt")[37]. A pert megnyerte, azóta lehet az adatokat úgymond törölni (jobban mondva az **elérhetőségét korlátozni**) és további fejleményként számolható el, az adatvédelmi szabályok tekintetében nem az adatkezelő székhelye számít, hanem az érintett polgárok állampolgársága vagy tartózkodási helye[38].
A legutóbbi nagyobb fejlemény 2016 januárjában történt, mikor az Európai Emberi Jogok Bírósága a magyarországi TEK ellen hozott határozatot a bírósági felhatalmazás nélküli lehallgatási gyakorlatuk ellen, így ehhez most már független szerv felhatalmazása kell.[39]

6.6. GDPR[40] néhány fontosabb eleme

- Az EU-s polgárokra irányuló tevékenységekre vonatkozik, akkor is, ha a cég máshol van.
- A hozzájárulás visszavonható és nem érvényes, ha az adatkezelő erőfölényben van.
- Külön szabályok a gyermekek adatainak kezelésére (gondoljunk csak a sérülékenységükre és Cayla-ra).
- A törléshez való jog („az elfeledtetéshez való jog") (Right to erasure, 'right to be forgotten')
- Beépített adatvédelem, alapértelmezett adatvédelem (Data protection by design and by default):

by design	már a tervezésnél **eleve** legyen képes az adatvédelemre
by default	csak az elindításhoz szükséges és elégséges dolgok kellenek

10. táblázat. Data protection by...

- Az adatbiztonsági incidenseket jelenteni kell a hatóságnak és az érintett alanyoknak, így egy tömeges banki adatkezelési problémát többé nem lehet (az eddig alkalmazott módszer szerint) titkolni.
- A bírság felső határa 20.000.000 EUR (vagy az éves világpiaci forgalom 4%-a, ha ez magasabb), így a Google például 50 milliós bírságot kapott, míg Magyarországon a legnagyobb (NAIH által) kiszabott büntetés 1 millió forint volt.

[35] 2015 októberében érvénytelenítették a Safe Harbor Principles-t
[36] Directive on privacy and electronic communications
[37] `https://www.bbc.com/news/world-europe-27388289`
[38] A Google leányvállalatai az EU jog alá tartoznak.
[39] `https://civilhetes.net/kitiltottak-a-tek-et-a-haloszobakbol`
[40] Lásd a 13. lábjegyzetet.

7. Privátszférát erősítő technológiák (PET-ek) - Bevezetés

7.1. Definíciók

Alapjában véve kétféle definíciót érdemes elolvasnunk, hogy megértsük, mik is azok a **PET**-ek, azaz a Privátszférát erősítő technológiák[41].

Első definíció A PET olyan információs és kommunikációs technológiák gyűjtőfogalma, amelyek megerősítik az egyén magánéletének védelmét egy információs rendszerben azáltal, hogy **megakadályozzák** a személyes adatok szükségtelen vagy jogellenes felhasználását, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén **ellenőrzését** személyes adatai felett.[42]

Azaz ezek a technológiák a *célhozkötöttség elvét* próbálják érvényre juttatni.

Második definíció A PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs privacy-t a személyes adatok kezelésének kiiktatásával vagy **minimalizálásával** védi, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, **anélkül, hogy csökkentené az információs rendszer funkcionalitását**.[43]

Ez a definíció kicsit más irányból közelíti meg a tárgyat, az úgy nevezett „data minimization", azaz az adattakarékosság és az adatelkerülés oldaláról.
A definícióban a funkcionalitás vonatkozhat például egy internetes alkalmazás esetében a gyorsaságra (csak néhány másodperces türelmi idővel számolhatunk maximum).

7.2. Céljuk

Miután megismertük a PET-eket, fontos különbséget tennünk köztük és a biztonsági technológiák között, mivel ez a kettő nagyon hasonló, mégis különböznek. Míg a biztonsági technológiák a **menedzsmentet, a szervezetet** védik a támadások ellen [44], addig a PET-ek a **gyengébbik felet** (az adatalanyt) védik az erősebb, információs túlhatalommal rendelkező féllel szemben.
Így általános céljuknak nevezhetjük, hogy ne csak az adatokat, hanem az adatok **alanyait** is védjék a visszaélések ellen, emellett biztosítsák az adatalanyok információs önrendelkezését is (például egy weboldalon, ha igazolni kell, hogy az alany felnőtt, ne kelljen születési dátumát megadnia, csupán azt bizonyítania, hogy ő már a korhatáron túl van).

7.3. Csoportosítás

A PET-eket sokféle szempont szerint lehet csoportosítani, ezek közül most ötfélét fogunk megtekinteni:

1. A Burkert-féle csoportosítás[45]
   (a) szubjektum-orientált (pl. anonim kártyabirtokosok)
   (b) objektum-orientált (pl. anonim digitális pénz)
   (c) tranzakció-orientált (pl. rekordok automatikus törlése)
   (d) rendszer-orientált (a fenti elemek integrálása)
2. Melyik adatvédelmi alapelv érvényesülését segíti elő?
   Ilyen lehet például a már említett célhozkötöttség elve, de az adatminőség elve is jelentős szerephez szokott jutni.
3. Mi az alapja?
   (a) Technológia-alapú PET-ek (pl. hitelesítés azonosítás nélkül)
   Ezeknek a PET-eknek a magja általában a kriptográfia.
   (b) Humán interakció alapú PET-ek
      i. **P3P** (Platform for Privacy Preferences Project), melyet a World Wide Web Consortium (W3C) fejlesztett ki. Lényege, hogy a weblapok csak akkor teremthessenek kapcsolatot az adatalannyal, hogy ha megfelelnek az alany előzetes feltételeinek (ezt egy táblázatban lehet dokumentálni).
      ii. **OPS** (Open Profiling Standard), egy hasonló célú korai szabványjavaslat.
      iii. **TRUSTe**: egy trustmark (azaz bizalmi védjegy) típus, mint például a „Kiváló magyar élelmiszer".

(a) TRUSTe

(b) Kiváló magyar élelmiszer

10. ábra. Bizalmi védjegyek logói

[41] Angol terminológiával: Privacy Enhancing Technologies.
[42] Privacy Enhancing Technologies: White Paper for Decision-Makers. Ministry of the Interior and Kindom Relations, The Netherlands, 2004.
[43] G.W. van Blarkom, J.J. Borking and J.G.E. Olk: *Handbook of Privacy and Privacy-Enhancing Technologies*, PISA Consortium, 2003.
[44] Ezeket a szervezetek esetében legnagyobb százalékban belső mukatársak követik el; ők jelentik a legnagyobb veszélyt, mivel ők vannak jelszavak és egyéb bizalmas információk birtokában.
[45] Herbert Burkert: "A privátszférát erősítő technológiák: tipológia, kritika, vízió", *Információs Társadalom*, 2005. V. évf. 2. szám, `https://www.infonia.hu/digitalis_folyoirat/2005_2/200_2_herbert_burkert.pdf`

4. Megoldás módja szerint

   (a) egyedi problémák megoldását célzó technológiák (pl. webpoloska-detektor, anonim böngésző)
   Anonim böngészőnek számít például a TOR (The Onion Router), mely teljesen elfedi az alany kilétét, viszont ez csak a böngészésre ad megoldást, ezért egyedi.

   (b) rendszerszerű megoldást nyújtó technológiák (PRIME, Private Credentials)
   A PRIME-mal (Privacy and Identity Management for Europe) külön fejezetben foglalkozunk.

   (c) vizualizáló technológiák (pl. e-mail path visualizers, Mozilla Lightbeam)
   A Thunderbird nevű levelezőprogramnak volt egy kiegészítője, mely láthatóvá tette, hogy egy küldött, vagy kapott email milyen utat jár be és az útja során érintett országokban milyen az adatvédelmi szabályozás. A Lightbeam pedig valós időben megmutatja, hogy tudtunk nélkül milyen más weboldalak kapcsolódtak a böngészésünkbe, és hová adták tovább a kapcsolatot.

5. Titkosítás módja szerint

   (a) a tevékenység elrejtését célzó technológiák (szteganográfia)
   A szteganográfia egyfajta titkosítási ágazat, melynek célja, hogy az adatok *léte* se látszódjon.

   (b) az adatalany kilétét elfedő technológiák (TOR)

   (c) obfuszkációs[46] technológiák (AdNauseam, TrackMeNot)

7.4. PET tartalmú termékek, szolgáltatások

A teljesség igénye nélkül:

1. **nym-generátorok**[47]: ID-ból úgynevezett nym-et készítenek egyirányú adatátalakítással, így nem kötheőek össze az adatok

2. **remailer-ek**: nem csak a levelező feleket és a levelet, hanem a csatornát is védik

3. **RFID PET-ek**: rádiófrekvenciás azonosító rendszer, melyet beléptetőkártyáknál, vagy lopásgátlóknál használnak többek között; fontos tulajdonsága, hogy csak akkor sugároz, ha az alany hozzájárul, emellett van rajta egy ún. „kill" funkció is, melynek aktiválása után az eszköz használhatatlan lesz

4. **digitális pénzrendszerek**[48]: itt különösen fontos, hogy a kapcsolati lánc ne legyen felderíthető
   ...

7.5. Protokollok

Számos PET technológia anonimizáló protokollok alkalmazásán alapul.

1. **Mix-net**: bár a többféle protokoll is használatos, az esetek 95 százalékában mégis ezt használják. Működése a be- és kimenetek összekeverésén alapszik. A TOR hálózatnak is ez jelenti az alapját.

2. **DC-net**: a Dining Cryptographers'[49] nevű problémából jön a neve, melyről David Chaum írt tanulmányt[50]. A probléma lényege, hogy két kriptográfus elhívja közös barátjukat étterembe azzal a kikötéssel, hogy nem fizethet, viszont afelől, hogy a számla rendezve lett, a vendég szeretne tökéletesen (azaz 100 százalékos pontossággal) megbizonyosodni. A megoldást az ún. *feltétlen nyomonkövethetetlenségű* üzenetek nyújtják (lsd. 11. ábra).

11. ábra. Dining Cryptographers' Problem
(Forrás: Dr. Székely Iván oktatási segédlete)

3. p^5 (Peer-to-Peer Personal Privacy Protocol)

4. **Buses**

[46] Összezavaró, lásd Spartacus című film híres jelenete: „Én vagyok Spartacus"
[47] `http://acronymcreator.net/`
[48] Pl.: e-Cash, Bitcoin, stb.
[49] Lásd David Chaum: „The dining cryptographers problem: Unconditional sender and recipient untraceability", Journal of Cryptology, Vol.1, Issue 1, 1988, 65-75. old.
[50] `https://users.ece.cmu.edu/~adrian/731-sp04/readings/dcnets.html`

7.6. Nyelvek

Az adatkezelő szervezetén belül az egyes személyes adatok kezelésére vonatkozó szabályok egyszerűbb jelölésére és automatikus végrehajtására ún „jelölő” (markup) nyelveket fejlesztettek ki:

Nyelv	Tervező	Rövidítés eredete
XACML	OASIS	eXtensible Access Control Markup Language Standard
EPAL	IBM	Enterprise Privacy Authorization Language

11. táblázat. Nyelvek

7.7. Ellenérvek

Mint minden témában, természetesen itt is akadnak ellenérvek. Többek között sokan nincsenek megelégedve ezen termékek áraival, mivel meglehetősen sokba tudnak kerülni, így az átlagemberhez nem jutnak el. Emellett minden felhasználó potenciális bűnöző (gondoljunk csak a TOR hálózatra, vagy a Dark Web-re) és így a tökéletes (nyomok nélküli) bűntény is megvalósítható lenne. Harmadik (és egyesek szerint a legnyomósabb) érv, miszerint az adatvédelem rontja az üzletet.

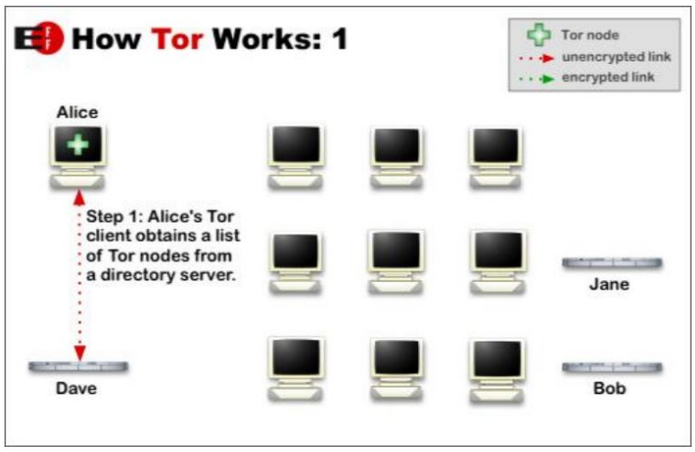
7.8. Érdekes linkek a témában

- **International PET portal and blog** (magyarul): `https://pet-portal.eu/start/`
- **Dining Cryptographers' Problem**: `https://users.ece.cmu.edu/~adrian/731-sp04/readings/dcnets.html`

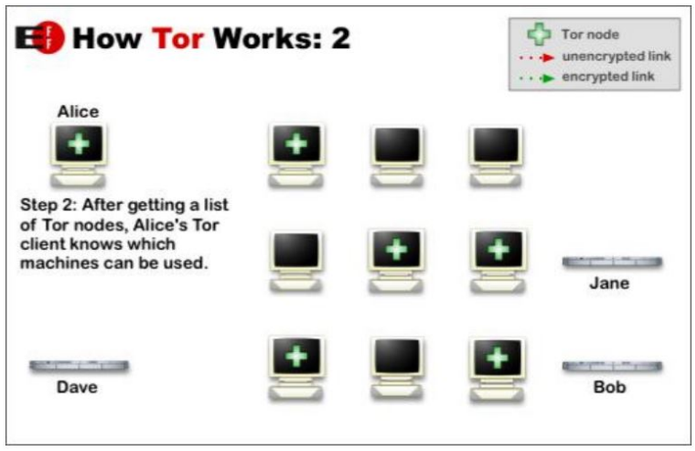
8. TOR

Ki ne hallott volna a teljesen anonim hálózatról, a The Onion Router-ről, mely azért jött létre, hogy az információk olyan országokban is szabadon áramolhassanak, ahol ez nem lenne lehetséges és amit nagy arányban mégis másra használnak? A TOR garantálja a névtelenségünket úgy, hogy a weboldalak ne tudják azonosítani a felhasználót és szinte semmilyen adatot se tudjanak róla (országa, stb.). A hálózat működési elve az útvonalak gyors és véletlenszerű váltogatásán alapszik, ezen felül az kommunikáció titkosítva és fregmentálva folyik. Felmerülhet a kérdés, hogy akkor miért nem ezt használja mindenki, erre a válasz a sávszélességben rejlik, mivel ez jelentősen alacsonyabb, tekintve, mennyi TOR csomóponton megy keresztül az adat, így meglehetősen lassú maga a kommunikáció is.

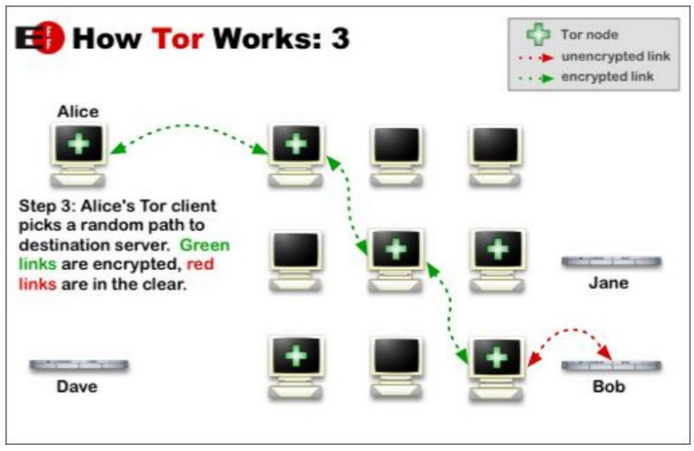
8.1. Hogyan is működik?[51]



12. ábra. Alice TOR kliense kikéri a használható, aktív TOR csomópontok listáját a címtárszerverről.

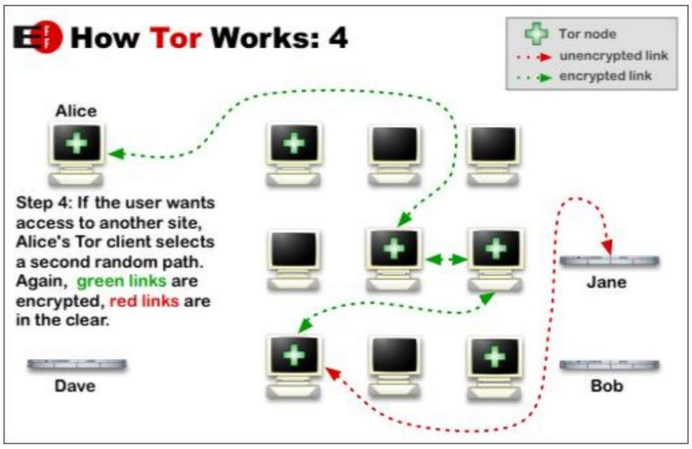


13. ábra. Miután megvan a listája, Alice TOR kliense tudja, melyik csomópontokat használhatja.



14. ábra. Alice TOR kliense választ egy véletlenszerű útvonalat a célszerverig. A zöld vonalak titkosítva vannak, a pirosak nem.

[51] Lásd például `https://2019.www.torproject.org/about/overview.html.en`



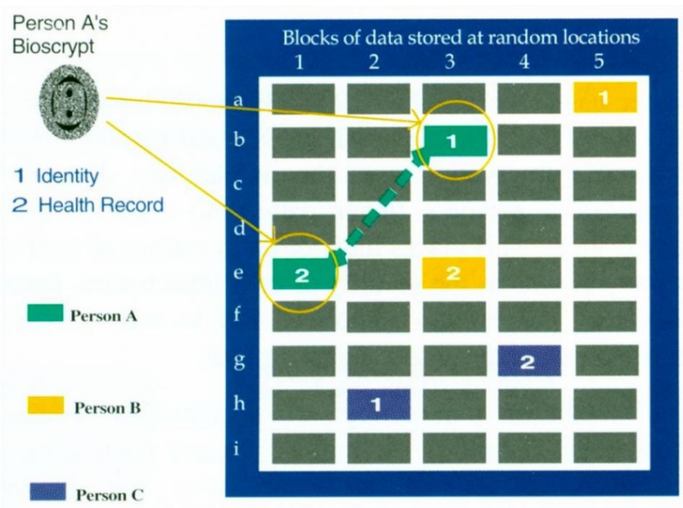
15. ábra. Ha a felhasználó egy másik oldalt szeretne elérni, Alice TOR kliense egy másik véletlenszerű utat választ. Megint: a zöld vonalak titkosítva vannak, a pirosak nem.

9. Bioscrypt

A bioscrypt (Biometric Encryption, biometrikus rejtjelezés) két fő alkotóelemből áll:

1. biometrikus elem (pl.: digitalizált ujjlenyomat);
2. nembiometrikus elem (pl.: kriptográfiai kulcs).

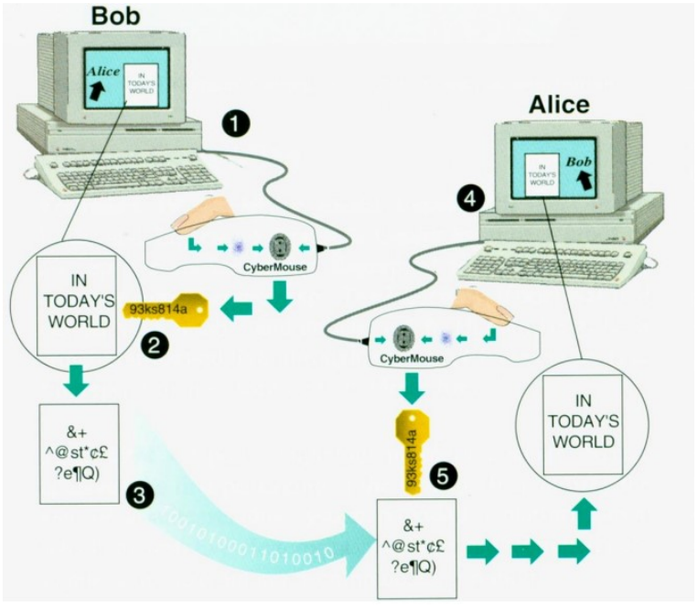
Ezt a kettőt a biometrikus rejtjelezés „olvasztja eggyé", így már csak mind a két elem használatával lehet visszafejteni a titkosított fájlokat, azaz az alanynak reprodukálnia kell a biometrikus adatot (például ujjlenyomatolvasó használatával). Alkalmazzák például anonim adatbázisok létrehozásánál, mely az alábbi módon szemléltethető:
A képen egy egészségügyi adatbázist láthatunk, melyben véletlenszerűen minden személyhez (itt zöld, sárga, kék)



16. ábra. Anonim adatbázis egészségügyi adatokkal
(Forrás: Mytec)

tartozik két blokk. Az egyik az alany identitását tartalmazza, a másik a róla készült egészségügyi (titkos) adatokat. Az egész adatbázis nyilvános, viszont csak a biometrikus elemmel lehet megtalálni, melyik identitáshoz melyik adat tartozik.
Felhasználási lehetőségei közé tartozik még az elektronikus kereskedelmi alkalmazás, így például a bankok esete. Az ügyfél megbízza a bankot, hogy fizessen a szolgáltatónak; ezt is bioscrypttel tudják megoldani, igazolni, hogy a megbízás ténylegesen valós, de minden résztvevő csak a rá tartozó adatokat láthassa.
A Bioscrypt gyakorlati alkalmazásához kifejlesztett eszköz az ún. „kiberegér"[52], melyben egy ujjlenyomatleolvasó kapott helyett, így nehézségek nélkül lehet titkosítani/dekódolni az üzeneteket.

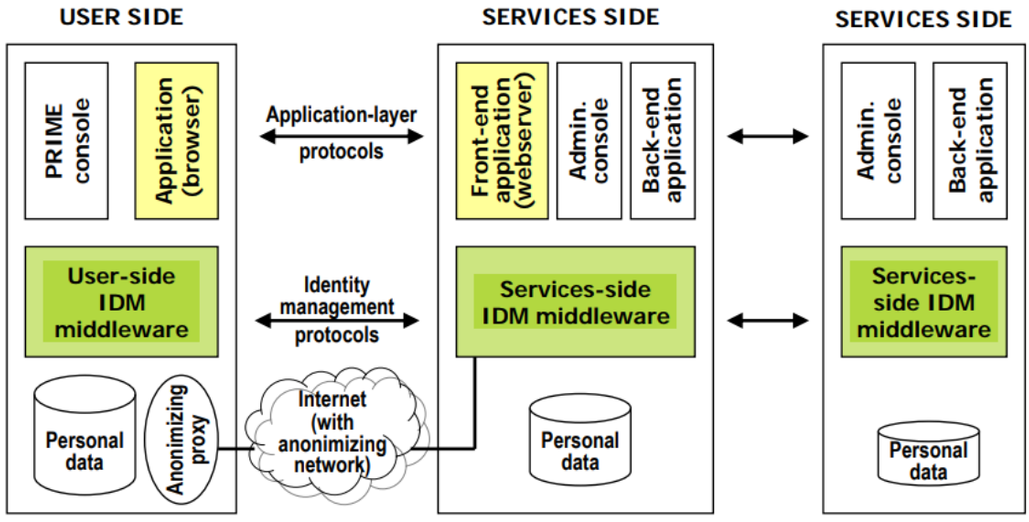
[52] Angol terminológiával cybermouse, melyben egy ujjlenyomatolvasó kapott helyet, így a jelszó beírása helyett egy egyszerű kattintással is tudjuk igazolni kilétünket.



17. ábra. Bioscrypt az internetes kommunikációban - a kiberegér
(Forrás: Mytec)

10. PRIME architektúra

A 2004-ben indult Privacy and Identity Management for Europe a legjelentősebb európai uniós projekt volt a témában. A PRIME egy rendszerszintű megoldás, egy middleware-szerű transzparens (alkalmazás- és platformfüggetlen) réteg, „melynek lényege, hogy a jogszabályi, szolgáltatói és/vagy felhasználói adatkezelési szabályokat a felszín alatt végrehajtsa. Gondoljunk csak bele, hogy mi történik, ha egy képet törlünk Facebook-ról, hol lesz még az elérhető, ki mentette le, a megosztásokkal mi a helyzet stb. A PRIME erre kínál megoldást, visszaköveti az eredeti kép útját és az bárhol is lenne, törli. További feladatai közé tartozik az identitásmenedzselés is például az üzleti életben, de akár a hatóságok felé is; ezt a feladatot a PRIME felhasználóközpontúvá szeretné tenni, azaz az adatalanyoknak kizárólagos jogot szeretne adni az adataik felhasználását illetőleg (természetesen a megfelelő jogi keretek között).



18. ábra. A PRIME architektúra felépítése; itt zöld színnel van jelölve a transzparens middleware rész.
(Forrás: Dr. Székely Iván oktatási segédlete)

További érdekességként érdemes megtekinteni a projekt folytatásának tekithető PrimeLife oldalát és kifejlesztett alkalmazásait: `http://primelife.ercim.eu/results/opensource/`

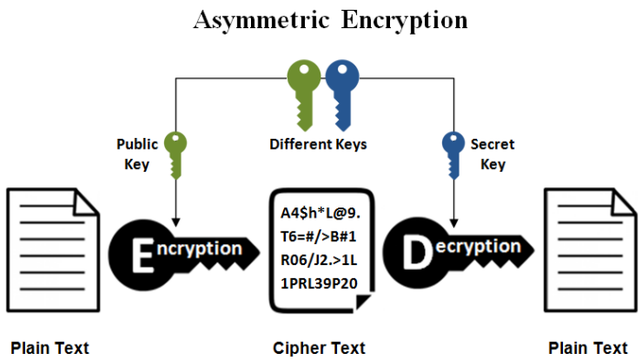
11. PET építőelemek

11.1. Kulcsok

A titkosítást mindig egy ún. kulccsal lehet kódolni, illetve feloldani. Ahogy már a Bioscrypt fejezet során is megismerhettük, ez lehet akár biometrikus adat, de a legáltalánosabb a jelszó. A kulcsoknak két fajtája létezik:

- szimmetrikus
- aszimmetrikus

Minden titkosítás során két kulcsot kell használnunk, egyet a titkosításhoz, egyet a feloldásához.
Ha a két kulcs ugyanaz, azt nevezzük szimmetrikus kulcsnak. Ez a megoldás a biztonságosabb a kettő közül; hátránya viszont, hogy a kulcsot el kell juttatni a címzetthez is és ezalatt nehéz garantálni a bizalmasságát és sértetlenségét.[53]
Az aszimmetrikus titkosítás[54] során szükség van egy **publikus kulcsra** és egy **privát kulcsra**, melyek segítségével titkosítani és dekódolni lehet az üzenetet/fájlt.[55]



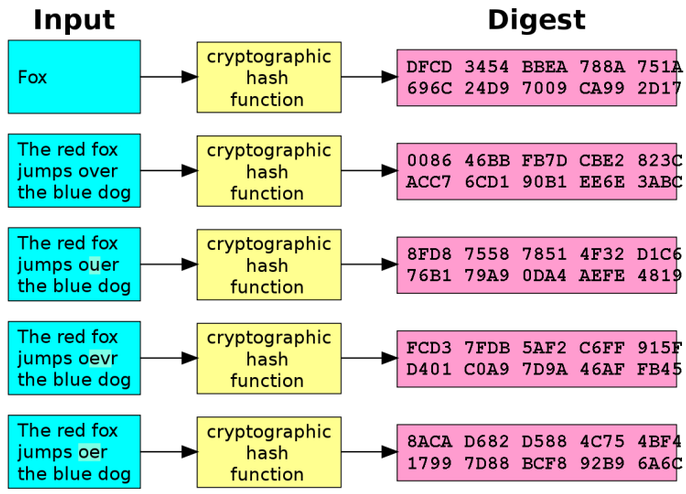
19. ábra. Az aszimmetrikus kulcsok példája
(Forrás: `https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences`)

11.2. Hash algoritmus

A hash algoritmus az egyirányú adatátalakítás legcélravezetőbb eszköze, mivel:

- nem visszafejthető;
- a bemenő adatból mindig ugyanaz a „zúzalék” (ábrán a Digest) keletkezik
- a kimenet fix hosszúságú.

Közeli példaként felhozható rá a NEPTUN kód, melyet minden hallgató nevéből egyesével alkotnak meg: egyik NEPTUN kód se fejthető vissza, az eljárás végén mindig ugyanaz és ugyanolyan hosszú lesz a kimenet; emellett *nem reprodukálható a hash képlet hiányában.*

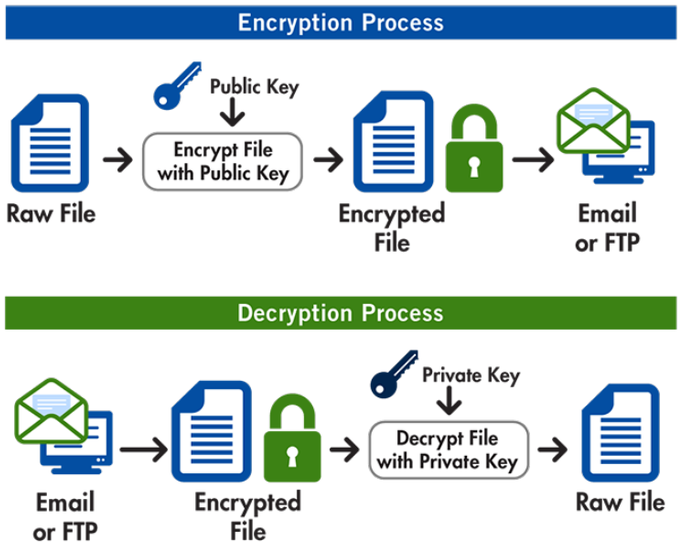


20. ábra. Hash algoritmus működése
(Forrás: `https://themoneymongers.com/bitcoin-hash/`)

[53] Erre jelent megoldást az ún. kétlakatos láda.
[54] Ezt nehezebb elképzelni, mivel a valóságban nincs olyan ajtó, amit más kulccsal zárunk és mással nyitunk.
[55] Legismertebb alkalmazott verziója az *RSA-kód*.

12. PGP titkosítás

A PGP titkosítás, azaz a a Pretty Good Privacy egy ingyenes, nyílt forráskódú számítógépes program. Legelső verzióját Philip Zimmermann alkotta meg. Akkor még főleg emailezés során volt használatos, mostanára már fájlokat, mappákat, merevlemezeket, stb. lehet vele titkosítani és hitelesíteni egyaránt.
Email tartalmának titkosítása során egy egyszer használatos szimmetrikus kulcsot használ, amit a küldő privát kulcsával titkosít, így azt a címzett a hozzá tartozó nyilvános kulccsal tudja dekódolni és így megkapni az *egyszer használatos* kulcsot az üzenet elolvasásához.



21. ábra. Egy email PGP-vel való titkosítása és feloldása
(Forrás: `https://www.freecodecamp.org/news/how-does-pretty-good-privacy-work-3f5f75ecea97/`)

Így ha illetéktelenek hozzá is jutnának az egyszer használatos kulcshoz, a többi levelet nem tudják ugyanúgy dekódolni és a korábbi kommunikációhoz se férnek hozzá.
A PGP emellett digitális aláírásokkal operál, hogy meg tudjuk állapítani, *ténylegesen* ki küldte a levelet.

13. Közérdekűadat-igénylést támogató rendszerek

13.1. KiMitTud

`https://kimittud.atlatszo.hu/`
Ahogy a linkből is kitűnik, a KiMitTud rendszerét az *átlátszó.hu* portál üzemelteti, mely egy tényfeltáró, oknyomozó hírportál. A KiMitTud azoknak nyújt segítő kezet, akiknek kérdésük van szervezetekhez/minisztériumokhoz és nem tudják, hogyan induljanak el.
Első lépésként egy űrlapot (sablont) kell kitölteni a kérdéssel és a címzettel (amit választhatunk is egy hosszú listából, vagy akár hozzá is adhatunk újat), de ami a legfontosabb, **az adatigénylő nevének is szerepelnie kell a levélen**, ami hátrányt jelenthet, mikor a válasszal együtt nyilvánosan megjelenik, mivel ez nem tartozik ez esetben a közérdekű adatok közé.
A rendszer ezután elküldi a levelet a címzettnek, amit addig ismételget, amíg választ nem kap rá (gondoljunk a nemválaszolás esetén fellépő jogainkra).
További lehetőségként még a korábbi leveleket és válaszokat is lehet keresni.

13.2. Fizettem.hu

`http://www.fizettem.hu/`
A *fizettem.hu* weboldalt, ahogy a KiMitTud-ot is, az *átlátszó.hu* üzemelteti (üzemeltette) és a kenőpénzzel, csúszópénzzel foglalkozik (emiatt nevezték sokan a **„korrupció leltárának”** is). Ahogy a képen is látszik, 3 kategóriába sorolja a bejelentéseket:

- fizettem,
- nem fizettem,
- nem fogadta(m) el.

22. ábra. A fizettem.hu bejelentéstípusai
(Forrás: `http://www.fizettem.hu/`

13.3. WhatDoTheyKnow és AskTheEU

`https://www.whatdotheyknow.com/`
`https://www.asktheeu.org/`
Ez a két honlap ugyanazzal a szoftverrel, az Alaveteli finn cég szabad hozzáférésű szoftverével üzemel, ahogyan a KiMitTud is. Angolul működnek, nonprofit szolgáltatások.
A WhatDoTheyKnow is egy ún. FOI[56] weboldal, melyet a mySociety, egy e-democracy project indított még 2008-ban.
Az AskTheEU nevéből adódóan az Európai Unió szervezeteinek adataihoz kínál hozzáférést.

[56] Freedom of Information

13.4. Data.gov

https://www.data.gov/
A Data.gov egy USA-beli ingyenes, 2009-ben indult kormányzati szolgáltatás, mely nem dokumentumokat, hanem **adatállományokat** tesz elérhetővé (köztük más külföldi nyílt adatforrásokat is), továbbá alkalmazásokat, fejlesztői eszközöket, statisztikákat, grafikonokat is. Technológiai hátterét vizsgálva fontos megemlíteni az ún. egységes metaadat-szabványt (Open Data Project[57]).

13.5. Érdekes linkek a témában

- **Átlátszó** https://atlatszo.hu/
- **KiMitTud** https://kimittud.atlatszo.hu/
- **MagyarLeaks** https://atlatszo.hu/magyarleaks/
- **Vastagbőr Blogging platform** https://vastagbor.atlatszo.hu/
- **Fizettem.hu** http://www.fizettem.hu/
- **WhatDoTheyKnow** https://www.whatdotheyknow.com/
- **AskTheEU** https://www.asktheeu.org/
- **Data.gov** https://www.data.gov/
- **Open Data Project** https://project-open-data.cio.gov/

[57] https://project-open-data.cio.gov/

14. Az egységes közadatkereső rendszer

14.1. Betekintés a törvényekbe

Az első elektronikus információszabadsággal foglalkozó törvény 2005-ben jelent meg Magyarországon[58], amit 2011-ben az új Infotv.[59] váltott fel. Ennek három fontos pillére van:

1. A bírósági határozatok nyilvánossága
2. A jogszabályok nyilvánossága
3. Az elektronikus közzététel kötelezettsége:
   Ez ugyancsak három elemből áll:
   - Közzétételi listák
     - általános
     - különös
     - egyedi
   - A közérdekű adatok központi elektronikus jegyzéke
   - **Egységes közadatkereső rendszer**

Ezeket fogjuk ebben a fejezetben áttekinteni.

14.2. A bírósági határozatok nyilvánossága

A Bírósági Határozatok Gyűjteménye megtalálható az interneten a `http://birosag.hu` webcímen.
Érdeklődés szintjén mindenképpen érdemes belenézni egy-két ilyen határozatba. Böngészésünk során láthatjuk, hogy itt a neveket (mivel ezek személyes adatok, bármit is követett el az adatalany) a történet szempontjából *visszakövethetően* titkosítják; a hatósági személyek nevét (mivel ezek a személyes és közadatok metszetébe tartoznak; emlékezzünk csak a Székely-féle modellre) nem törlik.
Pl.: *"[...] különleges személyes adatra elkövetett visszaélés személyes adattal vétsége (**Személy 2** erotikus fotóinak kihelyezése névvel, lakcímmel a világhálón), visszaélés személyes adattal vétsége (**Személy 1** sérelmére ... adatlapok létrehozása) [...] **dr. Megyes Géza s.k. - bíró**"*

14.3. A jogszabályok nyilvánossága

Maga a Magyar Jogszabálykereső a `https://magyarorszag.hu/`-n keresztül is elérhető, de a Nemzeti Jogszbálytárban (a `http://njt.hu/` címen) is lehet keresni.

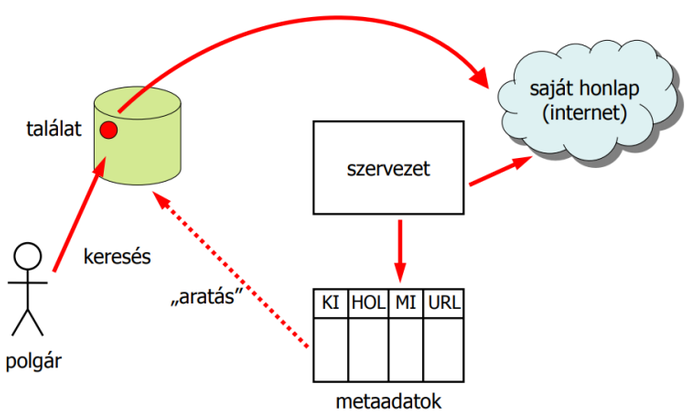
14.4. Egységes közadatkereső rendszer

Az egységes közadatkereső rendszer az ún. OAI-n, azaz az Open Archives Initiative-en alapszik, mely egy internetes tartalommegosztó szabvány és arra törekszik, hogy a résztvevő szervezetek egységes metaadat-sémákat használjanak és rendszereik interoperábilisak legyenek.

14.4.1. Működése

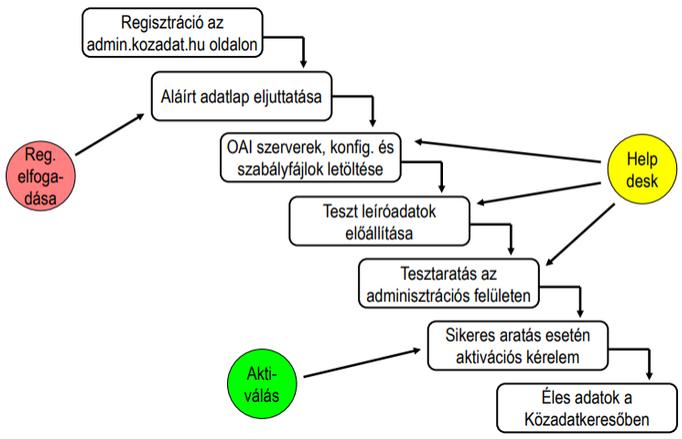
A rendszer működése egyszerű, három fő lépésből áll:

1. A szervezetek regisztrálnak egy közös oldalra (a 24. ábrán ez az admin.kozadat.hu).
2. Feltöltik metaadataikat egy előre megírt sablonba.
3. A rendszer úgymond „learatja” (harvesting[60]) az adatokat és berendezi egy közös adatbázisba, azaz *kereshetővé teszi* őket.



23. ábra. Az egységes közadatkereső működése
(Forrás: Dr. Székely Iván oktatási segédlete)

[58] 2005. évi XC. törvény az elektronikus információszabadságról.
[59] 2011. évi CXII. törvény az információs önrendelkezésről és az információszabadságról
[60] Metaadatok összegyűjtése elosztott rendszerben működő adattárakból egy közös metaadattárba.



24. ábra. Az adatszolgáltató szervezetek teendői
(Forrás: Dr. Székely Iván oktatási segédlete)

14.4.2. Résztvevők

Az OAI-en alapuló rendszereknek három fontos résztvevőjük van, amik nélkül nem működhetnének:

1. **Archive**
   Az információk tárháza, ahol a learatott metaadatokat meg lehet találni.
2. **Data Provider**
   Az Archive-ek üzemeltetői, akiktől az adatok származnak
3. **Service Provider**
   Akik az ún. OAI-PMH[61] protokollt használják, ez a szervezet végzi az „aratást” a Data Provider-ektől. (a képen a zöld hordó).

14.4.3. Céljaik

Open Archives Initiative többféle célt is szolgál:

- **webes** tartalommegosztás
- interoperábilis adat- és dokumentumtárak létrehozása és működtetése
- **metaadat-megosztás**
- publikálás
- archiválás
- **szabványosítás**

14.4.4. Általános keresők vs. Közadatkereső

	Általános keresők	Egységes közadatkereső
találatok	túl sok	csak a lényegi
a találatok relevanciája	kérdéses	eldönthető
megbízhatóság	kérdéses	megbízható
minőség	Best effort	Quality of Service

A magyar egységes közadatkereső használhatóságát lerontja a változó színvonalú feltöltési fegyelem a kötelezett szervezetek részéről.

14.5. Érdekes linkek a témában

- **Open Archives Initiative** `https://openarchives.org/`
- **Bírósági határozatok** `http://birosag.hu`
- **Jogszabályok** `http://njt.hu/`
- **Adatvédelemre és információszabadságra vonatkozó jogszabály (Infotv.)** `http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.362143`
- **Közadat.hu** `http://kozadat.hu`
- **Közadattár** `http://kozadattar.hu`

[61] Protocol for Metadata Harvesting; „aratási” protokoll a metaadatok szolgáltatók közötti megosztására.

15. Anonim remailer-ek

Eletronikus levelező szolgáltatások, melyek az anonimitást az üzenetek, a körülmények[62] és a felek titkosításával, elrejtésével érik el.

15.1. Alapkövetelmények

Hogy a felvezetőben megnevezett feltételeknek eleget tegyen, az alábbi alapkövetelményeknek kell megfelelnie az adott anonim remailer-nek.

1. A kommunikáló partnerek anonimitása
2. A partnerek közötti kapcsolat nyomonkövethetetlensége
3. Az üzenet tartalmának megfejthetetlensége
4. A remailer kompromittálhatatlansága

15.2. Fejlődés

Az anonim remailer-ek fejlődése leginkább egyfajta rabló-pandúr játékként írható le.
A fejlődést a támadások elleni védekezés indította el; az első a küldő és a címzett között elhelyezkedő remailer be- és kimeneteinek figyeltetése volt, melynek segítségével az üzenetek lecserélt fejlécét lehetett visszaállítani[63]. Ez ellen az üzenetek késleltetése („pufferolás") jelentett megoldást, mire válaszként a remaler-ek fölösleges üzenetekkel való elárasztását találták ki a támadók. Erre való megoldásként az üzenetek véletlenszerű továbbítása mozdította előre a remailer-ek fejlődését; de a támadók az üzenet-sokszorosítással álltak elő, mire a válasz magától értetődő volt, az azonos üzeneteket egyszerűen ki kellett szűrni a levéláramból[64]. Az útvonalfigyelés ellen a remailer-ek láncbafűzését ötlötték ki, melynek lényege, hogy minden remailer csak a sorban következő címét ismeri, a címzettét nem; ezt egy hagymahéjszerű titkosítással oldották meg, melynek során minden remailer csak a fölső „hagymahéjat szedi le" és olvassa ki belőle a következő remailer címét. Ennek hátránya volt, hogy az üzenetek mérete kiszámítható mértékben csökkent, így tökéletes támadásnak tűnt az üzenetek méretének figyelése, melyre a szabványos méret és formátum alkalmazása jelentette a megoldást[65].

Támadás	Védekezés
bemenet/kimenet figyelés	késleltetés
elárasztás	véletlenszerű továbbítás
üzenet-sokszorozás	azonons üzenetek kiszűrése
útvonalfigyelés	láncbafűzés
méretfigyelés	szabványos méret és formátum

12. táblázat. Az anonim remailer-ek fejlődése

15.3. Típusok

Fejlődési sorban:

1. **Pszeudonim remailer**: csak nevet cserél
2. **Type I: Cypherpunk**: aszimmetrikus[66] titkosítású
3. **Type II: Mixmaster**: többféle kódolású, fix méretű csomagok
4. **Type III: Mixminion**: összetett kulcskezelés, álforgalom, stb.

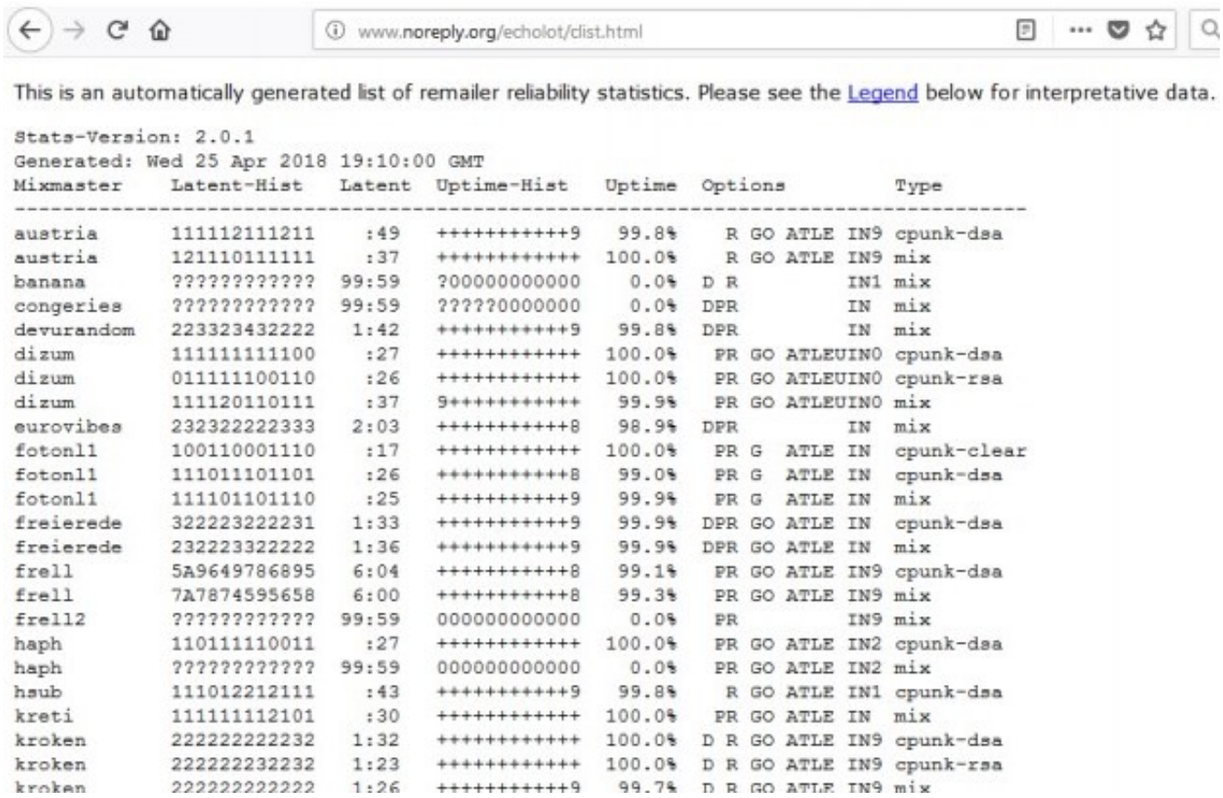
15.4. Működése

A remailer-ek használata egy külön programmal[67] történik, mely ingyenesen telepíthető (ellenkező esetben a fizetésnél az anonimitás lényegét vesztené).
Első lépésként az éppen aktuális remailer-ek listáját kell lekérni, mely a képen látható módon néz ki.
Az üzenetküldő lánc automatikusan épül fel ezek után, de fontos kiemelni, hogy az anonim remailer-ek nem a gyors üzenetküldést szolgálják - mindinkább a bizalmasat (gondoljunk csak a késleltetésre).

15.5. Érdekes linkek a témában

- **Remailer-ek listája** `http://www.kumpf.org/remailer-list.html`
- **EPIC, remailer tools** `https://epic.org/privacy/tools.html`
- **Mixmaster** `https://sourceforge.net/projects/mixmaster/files/`

[62] Leginkább a metaadatokként tárolt információkról van szó, mivel ezek egyszerűen használhatóak a deanonimizáláshoz.
[63] Ez a megoldás a kezdetleges, pszeudonim remailer-eknél volt alkalmazható.
[64] Ez később más üzenetküldő alkalmazásoknál is bevett szokás lett, mivel így a spam üzeneteket is szűrni lehet.
[65] A Mixmaster legfőbb jellemzője volt a szabványosítás.
[66] Azaz a titkosítás és a dekódolás nem ugyanazzal a felhasználói kulccsal történik.
[67] Chrome esetén például beépülő modullal is lehetséges.



www.noreply.org/echolot/clist.html

This is an automatically generated list of remailer reliability statistics. Please see the Legend below for interpretative data.

Stats-Version: 2.0.1
Generated: Wed 25 Apr 2018 19:10:00 GMT

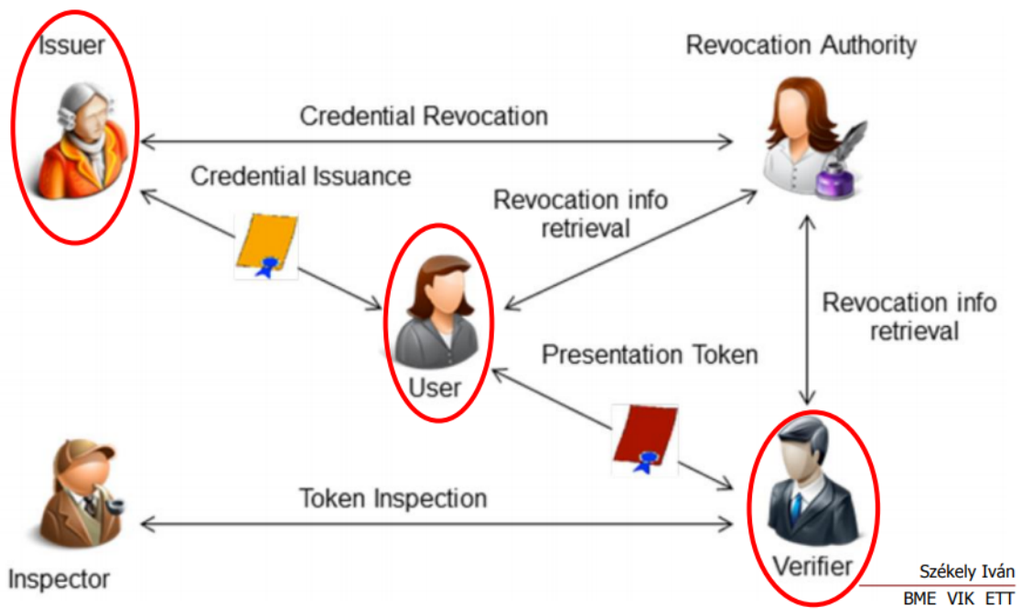
Mixmaster	Latent-Hist	Latent	Uptime-Hist	Uptime	Options	Type
austria	111112111211	:49	++++++++++9	99.8%	R GO ATLE IN9	cpunk-dsa
austria	121110111111	:37	++++++++++	100.0%	R GO ATLE IN9	mix
banana	????????????	99:59	?00000000000	0.0%	D R IN1	mix
congeries	????????????	99:59	?????0000000	0.0%	DPR IN	mix
devurandom	223323432222	1:42	++++++++++9	99.8%	DPR IN	mix
dizum	111111111100	:27	++++++++++	100.0%	PR GO ATLEUIN0	cpunk-dsa
dizum	011111100110	:26	++++++++++	100.0%	PR GO ATLEUIN0	cpunk-rsa
dizum	111120110111	:37	9++++++++++	99.9%	PR GO ATLEUIN0	mix
eurovibes	232322222333	2:03	++++++++++8	98.9%	DPR IN	mix
fotonl1	100110001110	:17	++++++++++	100.0%	PR G ATLE IN	cpunk-clear
fotonl1	111011101101	:26	++++++++++8	99.0%	PR G ATLE IN	cpunk-dsa
fotonl1	111101101110	:25	++++++++++9	99.9%	PR G ATLE IN	mix
freierede	322223222231	1:33	++++++++++9	99.9%	DPR GO ATLE IN	cpunk-dsa
freierede	232223322222	1:36	++++++++++9	99.9%	DPR GO ATLE IN	mix
frell	5A9649786895	6:04	++++++++++8	99.1%	PR GO ATLE IN9	cpunk-dsa
frell	7A7874595658	6:00	++++++++++8	99.3%	PR GO ATLE IN9	mix
frell2	????????????	99:59	000000000000	0.0%	PR IN9	mix
haph	110111110011	:27	++++++++++	100.0%	PR GO ATLE IN2	cpunk-dsa
haph	????????????	99:59	000000000000	0.0%	PR GO ATLE IN2	mix
hsub	111012212111	:43	++++++++++9	99.8%	R GO ATLE IN1	cpunk-dsa
kreti	111111112101	:30	++++++++++	100.0%	PR GO ATLE IN	mix
kroken	222222222232	1:32	++++++++++	100.0%	D R GO ATLE IN9	cpunk-dsa
kroken	222222232232	1:23	++++++++++	100.0%	D R GO ATLE IN9	cpunk-rsa
kroken	222222222222	1:26	++++++++++9	99.7%	D R GO ATLE IN9	mix

25. ábra. Az éppen aktuális anonim remalier-ek listája lekérdezés után
(Forrás: Dr. Székely Iván oktatási segédlete)

16. ABC szereplők[68]

Az ABC („Attribute-based credentials[69]") egyfajta private credential (személyes tanusítvány), melynek lényege, hogy az alanynak és a szolgáltatónak bizalma egymás iránt nem fontos, hogy meglegyen, mivel mindketten a többi szereplőben bíznak.

16.1. ABC4Trust szereplők

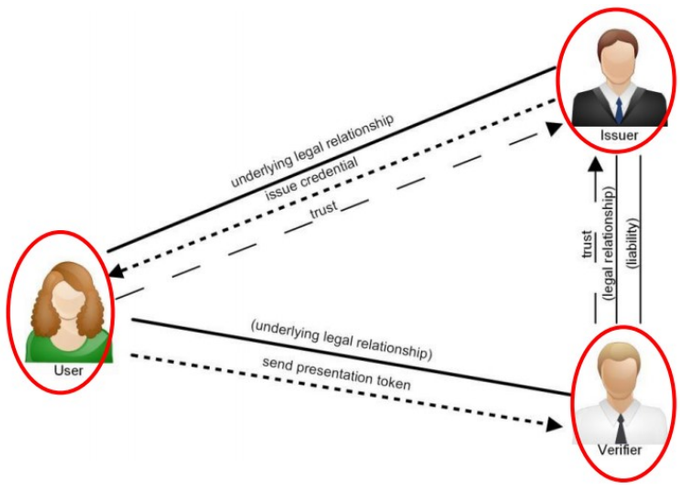


26. ábra. ABC4Trust szereplők
(Forrás: Dr. Székely Iván oktatási segédlete)

Az ABC-ben 5 személy/szervezet tölt be fontos szerepet, melyek a képen is láthatóak, mégis, a legfontosabb a középső piros körökben lévő három.
Ezen kívül az inspector-nak egyértelmű a feladata: felügyelni, hogy az adatokkal visszaélés ne történjen, míg a revocation authority gondoskodik arról, hogy abban az esetben, ha a tanúsítványok bizalmassága sérült, vagy visszaélés történt, azok érvényességét visszavonja.

[68] https://www.abc4trust.eu/
[69] Attribútum-alapú jogosítvány, **tanúsítvány**

16.2. ABC4Trust szereplők viszonyai

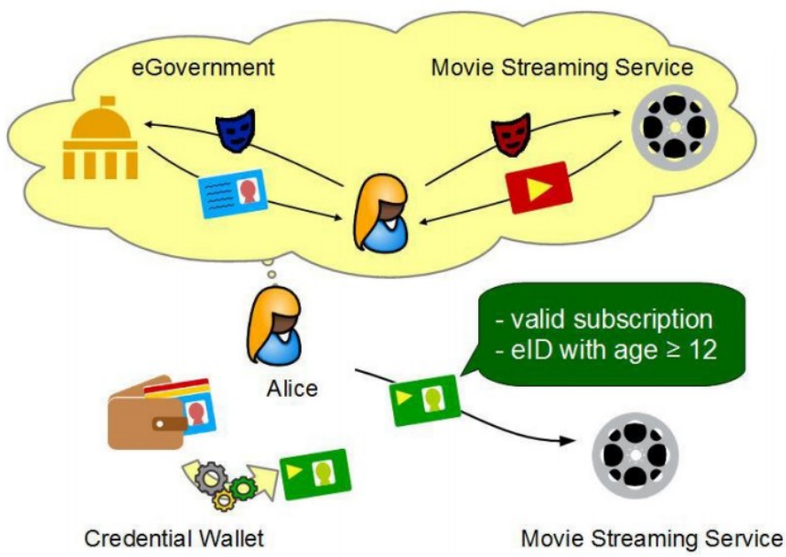


27. ábra. ABC4Trust szereplők viszonyai
(Forrás: Dr. Székely Iván oktatási segédlete)

A kép legfontosabb tanulsága, hogy a user és a verifier **nem bíznak egymásban**, csak a közös ismerősben, az issuer-ben (a hosszabban szaggatott vonal, a „trust" felirattal jelzi).

16.3. IBM Identity Mixer

Az IBM már hosszú ideje fejleszti az alábbi szolgáltatását, melynek lényege, hogy az alany (az ábrán Alice) adatait a megfelelő helyen és a megfelelő mértékben lehessen kezelni, mindezt annak az érdekében, hogy az alany válláról levegye az adatkezeléssel járó terheket. A képen látható módon a Movie Streaming Service-nek nem fontos tudnia Alice pontos születési dátumát (ellentétben az eGoverment-tel), így az Identity Mixer a Movie Streaming Service-nek csak azt adja meg, hogy Alice 12 évnél idősebb (szükséges mérték).



28. ábra. IBM Identity Mixer
(Forrás: https://www.youtube.com/watch?v=gKK1PxGu6Fo)

16.4. Angol-magyar kisszótár a témához

user	alany
verifier	szolgáltató
issuer	tanúsító hatóság
inspector	felügyelő hatóság
revocation authority	visszavonó hatóság

17. PET alkalmazások és alternatív szolgáltatások

17.1. Signal

Alkalmazás, mely leginkább chat-elésre, de hang- és videótovábbításra is alkalmas; társai közül ezt tartják a legbiztonságosabbnak, ami nem túl meglepő, hiszen ezt a protokollt használja a Facebook és a Whatsapp is (többek között). Mobilra és PC-re ugyanúgy telepíthető. Titkosítása SSL-el történik, mely csak a csatornát védi (így a felek láthatóak)[70], kulcsként „tűnékeny, illanó", azaz ephemeral kulcsot használ (akár a PGP titkosításnál) és 2FA[71]-t is alkalmaz.
`https://www.signal.org/`

17.2. ProtonMail

Alapjában véve egy fizetős üzenetküldő alkalmazás, aminek van ingyenes változata is. A cég központja Svájcban van és az alkalmazás PGP titkosítást használ. További előnyei közé sorolható, hogy a csatolmányokat is enkriptálja (ezzel szemben - furcsa megoldásként - a fejlécet nem, holott ebben a részben sok utalás szerepelhet az üzenet tartalmára).
`https://protonmail.com/`

17.3. Tutanota

Email alkalmazás, mely egyszerűen használható, ahogyan az eddigiek is (azaz nem kell semmiféle komolyabb informatikai háttértudás használatukhoz), német fejlesztésű és szimmetrikus/aszimmetrikus kulcsokat egyaránt használ. A titkosítás alapja itt az RSA; hátránya, hogy a 2FA-t nem támogatja és a már meglévő kontaktokat új eszközre nem lehet importálni.
`https://tutanota.com/hu/`

17.4. Posteo

Német fejlesztés, ahogyan a Tutanota is, különlegessége, hogy 100%-ban zöld energiát használ a működéséhez; 2FA-t támogatja, mobil applikációja azonban nincs.
`https://posteo.de/en`

17.5. Mailfence

Az előzőek kombinációja, hátrányai közé sorolható, hogy a frontend nincs titkosítva.
`https://mailfence.com/en/`

17.6. Jitsi

Videohívást tesz lehetővé, ahogyan a Skype, csak „jobb és biztonságosabb". Működése közben megfigyelhetjük, hogy egyedi, négy angol szóból összerakott (általában értelmetlen) kifejezést használ kulcsként, hogy a felek azzal találják meg egymást[72].
`https://jitsi.org/`

17.7. Veracrypt

A TrueCrypt utódja, fájlok, mappák, vagy akár egész meghajtók titkosítására használható.
`https://www.veracrypt.fr/en/Home.html`

17.8. Diaspora

Nevéhez hűen egy közösségi hálózat-építő program.
`https://diasporafoundation.org/`

17.9. Friendica

Facebook-alternatívaként használható közösségi alkalmazás.
`https://friendi.ca/`

17.10. Onion Pi

TOR hálózatot kiépítő mini router, mely a hagymahéjszerű titkosítást alkalmazza, és a Raspberry Pie bankkártya méretű mikroszámítógépre épül.
`https://learn.adafruit.com/onion-pi/overview`

17.11. Gotenna

Központ nélküli mobilhálózat; mobiltelefonokat összekötő hordozható eszközök, melyek nem központi szolgáltatón keresztül kommunikálnak, inkább hasonlatosak a walkie-talkie-khoz.
`https://gotenna.com/`

[70] Angol terminológiával: end-to-end encryption
[71] Two factor authentication; kétlépcsős azonosítás
[72] Példaképp: ObjectivePenguinsRepresentCuriously

17.12. Silent Phone

Régen Blackphone-nak nevezett, biztonságos mobiltelefon Phil Zimmermann-tól, aki a PGP titkosítást is megalkotta. A Silent Cirle-lel együtt, mely egy hozzá járó program, meglehetősen drágák, így nem terjedt el széles körben.
`https://www.silentcircle.com/`

17.13. Debian

Linux alapú biztonságos operációs rendszer.
`https://www.debian.org/`

17.14. Tails

Minimális erőforrásigényű (éppen ezért akár pendriveról is üzemelő) operációs rendszer, amely Linux-disztibúcióra épül.
`https://tails.boum.org/`

17.15. Etherpad

Irodai csomag, mellyel valós időben lehet együtt dolgozni, viszont nem anonimizál. Többek szerint a Google ezt az ötletet ellopta, míg mások szerint megvette.
`https://etherpad.org/`

17.16. Ethercalc

Csoportmunkára alkalmas Excel-alternatíva.
`https://ethercalc.org/_start`