ÜZLETI JOG
Bevezetés - A jog szerepe az információs társadalomban

Dr. Mezei Kitti
Üzleti Jog Tanszék

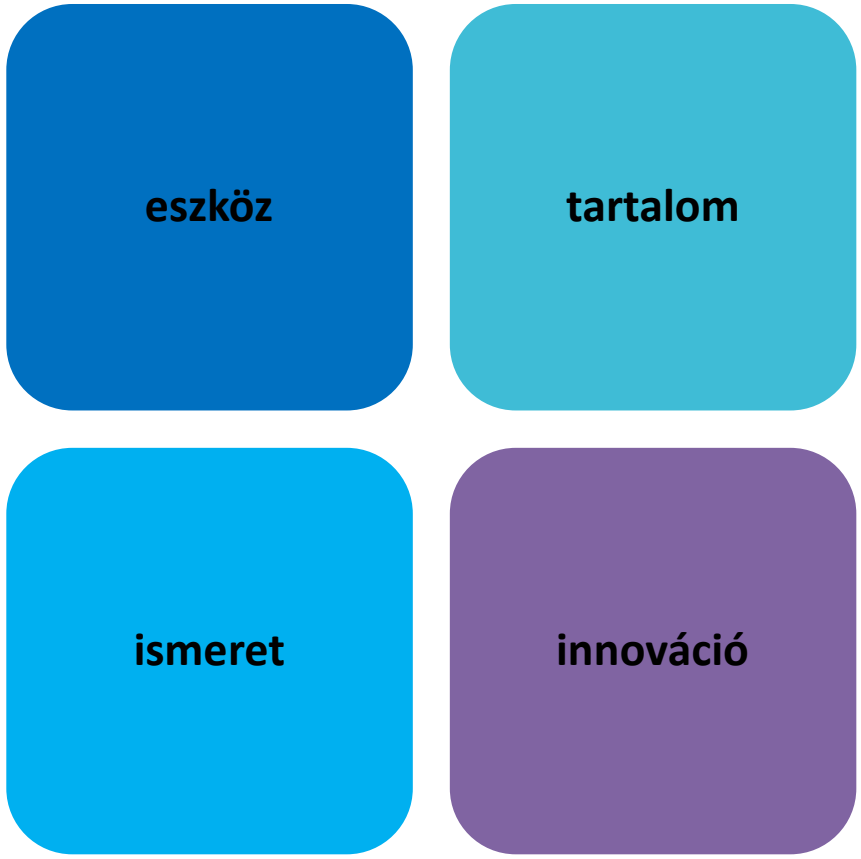
	Előadások témái	Előadó	Dátum
1.	Bevezetés, a jog jelentősége a társadalomban, az információs társadalomban	Mezei Kitti	2021.09.07.
2.	Az alapjogok védelme az információs társadalomban	Nagy Krisztina	2021.09.14.
3.	Hírközlési jog	Nagy Krisztina	2021.09.21.
4.	Elektronikus kereskedelem	Nagy Krisztina	2021.09.28.
5.	Szellemi tulajdonjogok (szerzői jog)	Grad-Gyenge Anikó	2021.10.05.
6.	Szellemi tulajdonjog (iparjogvédelem)	Grad-Gyenge Anikó	2021.10.12.
7.	Szerződéstípusok és funkcióik	Mezei Kitti	2021.10.19.
8.	Munkajog	Schubauer Petra	2021.10.26.
9.	Adatvédelem	Schubauer Petra	2021.11.02.
10.	Társaságok	Grad-Gyenge Anikó	2021.11.09.
11.	TDK	-	2021.11.16.
12.	Start up születik - alapítás, működtetés	Grad-Gyenge Anikó - Baksay-Nagy György	2021.11.23.
13.	Start up születik – szoftverfejlesztés és szerződések	Grad-Gyenge Anikó - Dudás Ágnes	2021.11.30.
14.	Konzultáció		2021.12.07.

I. ZH	2021.10.18	18.00-20.00
II. ZH	2021.12.06	18.00-20.00
Pót	2021.12.13	

INFORMÁCIÓS TÁRSADALOM

- **Az infokommunikációs technológiák** (IKT) már nem minősülnek külön ágazatnak, hanem **a modern, innovatív gazdasági rendszerek alapját képezik.**
- Az információs társadalom ideológiákkal telített fogalomrendszer, alapját az infokommunikációs technológia képezi.
- A fogalom mögött technológiai és társadalmi összetevők egyaránt vannak.
- **Az innováció** mint a gazdaság motorja különösen fontos tényező az információs társadalom megvalósításában (K+F tevékenység).

INFORMÁCIÓS TÁRSADALOM TECHNOLÓGIAI TÉNYEZŐI



E-GAZDASÁG

- A **hálózatiság** és a **globalizáció** révén teljesen új gazdaságról beszélhetünk.
- A hagyományos vállalatok és a teljes gazdaság működése is átalakult.
- **E-gazdaság:** a gazdaságnak ezt az internethez, elektronikus hálózatokhoz köthető része (elnevezés eredete: IBM – 90-es évek).
- Az e-gazdaság fogalma tágabb, mint az **e-kereskedelem**.

AZ E-GAZDASÁG SZEREPLŐI

A legfontosabb viszonyok meghatározásához három betűvel szokták rövidíteni a főbb szereplőket:

A mint Administration: államigazgatási szereplők,

B mint Business: üzleti vállalkozások,

C mint Consumer vagy Customer: fogyasztók, hétköznapi vásárlók.

AZ E-GAZDASÁG SZEREPLŐI

A2B (államigazgatástól – üzleti szereplőnek)

B2A (üzleti szereplőtől – államigazgatásnak)

B2B (üzleti szereplőtől – üzleti szereplőnek)

B2C (üzleti szereplőtől – fogyasztónak)

C2C (fogyasztótól – fogyasztónak)

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

Ezek a teljesség igénye nélkül megmutatják, hogy hogyan változik meg:

- a kínálat **(long tail)**,
- az információs termékek kezelése **(figyelemgazdaság)**,
- a kiszervezés, tesztelés vagy finanszírozás **(crowdsourcing, crowdtesting, crowdfounding)**,
- az árazás **(freemium)**
- és egyes termékek vagy szolgáltatások használata **(sharing economy)**.

LONG TAIL ÉS FIGYELEMGAZDASÁG

Long tail

- **Az e-kereskedelemben szinte korlátlan árubőséggel lehet találkozni.**
- A kínálat gyakorlatilag korlátlan a digitalizálható termékeknél.
- Lásd zenei streaming oldalak (Spotify vagy Apple Music).

Figyelemgazdaság

- **A megnövekedett tartalom- és információmennyiségnek köszönhetően a figyelemből hiány alakul ki.**
- Információmenedzsment-fogalom.

CROWDSOURCING

- Crowdsourcingnek több altípusa van:
- **Crowdtesting** (a hazai Testflight),
- **Crowdfunding** (Kickstarter).

- **Gazdasági jelentősége:** a segítségével „ingyen” munkaerőhöz, tömeges szakértelemhez és olyan más erőforrásokhoz (például tőkéhez, számítási kapacitáshoz stb.) juthatnak hozzá a vállalkozások.

AZ INGYENESSÉG ÉS A FREEMIUM MODELL ÉS A SHARING ECONOMY

- **Ingyenesség mint új radikális árképzés.**
- **Új üzleti modell: freemium.**

- **Sharing economy:** olyan gazdasági és társadalmi aktivitás áll, amely online tranzakciókon alapul, és segítségével megosztják az emberek saját vagy mások javait, szolgáltatásait.
- Lásd autómegosztás (Uber) vagy lakásmegosztás (Airbnb).
- Számos szabályozási kérdést vet fel.

SHARING ECONOMY BUSINESS MODEL

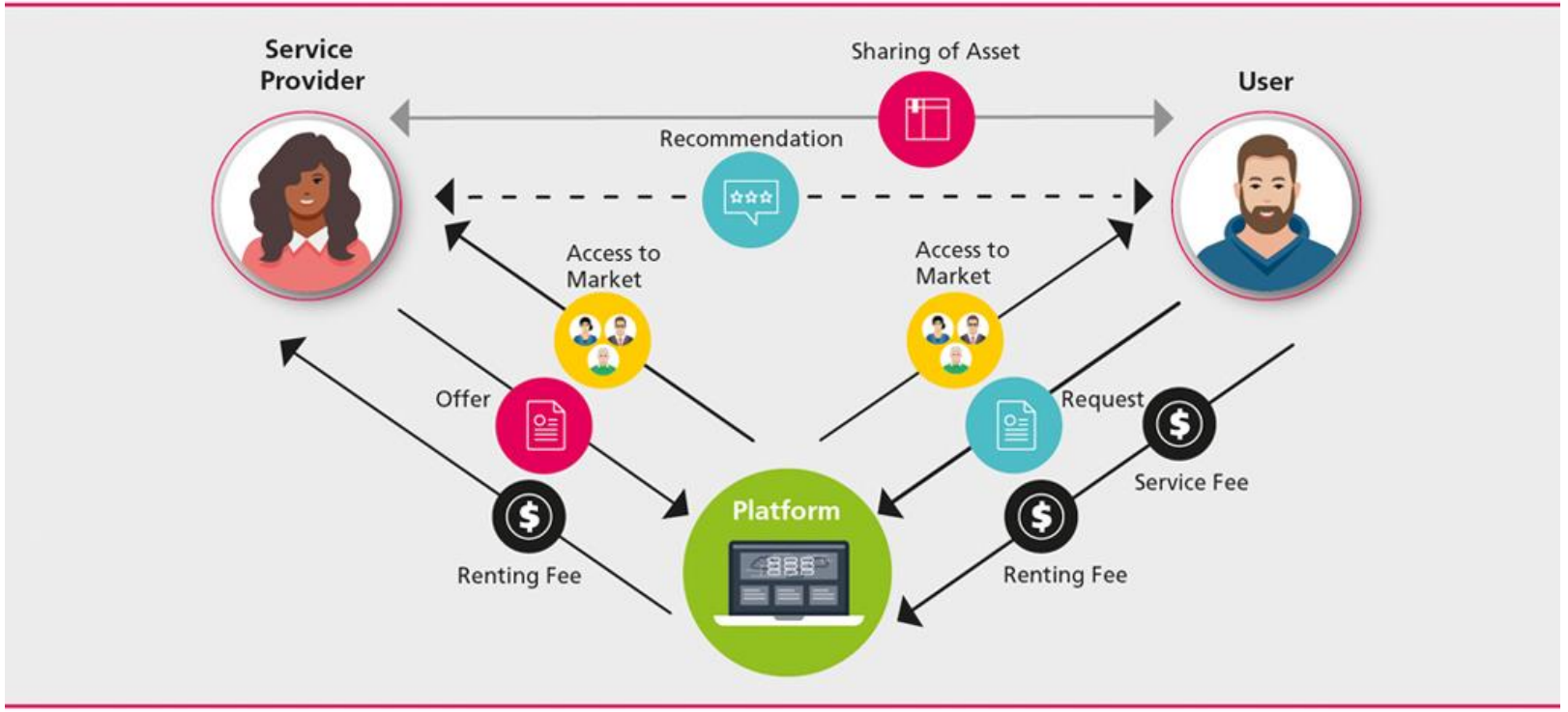
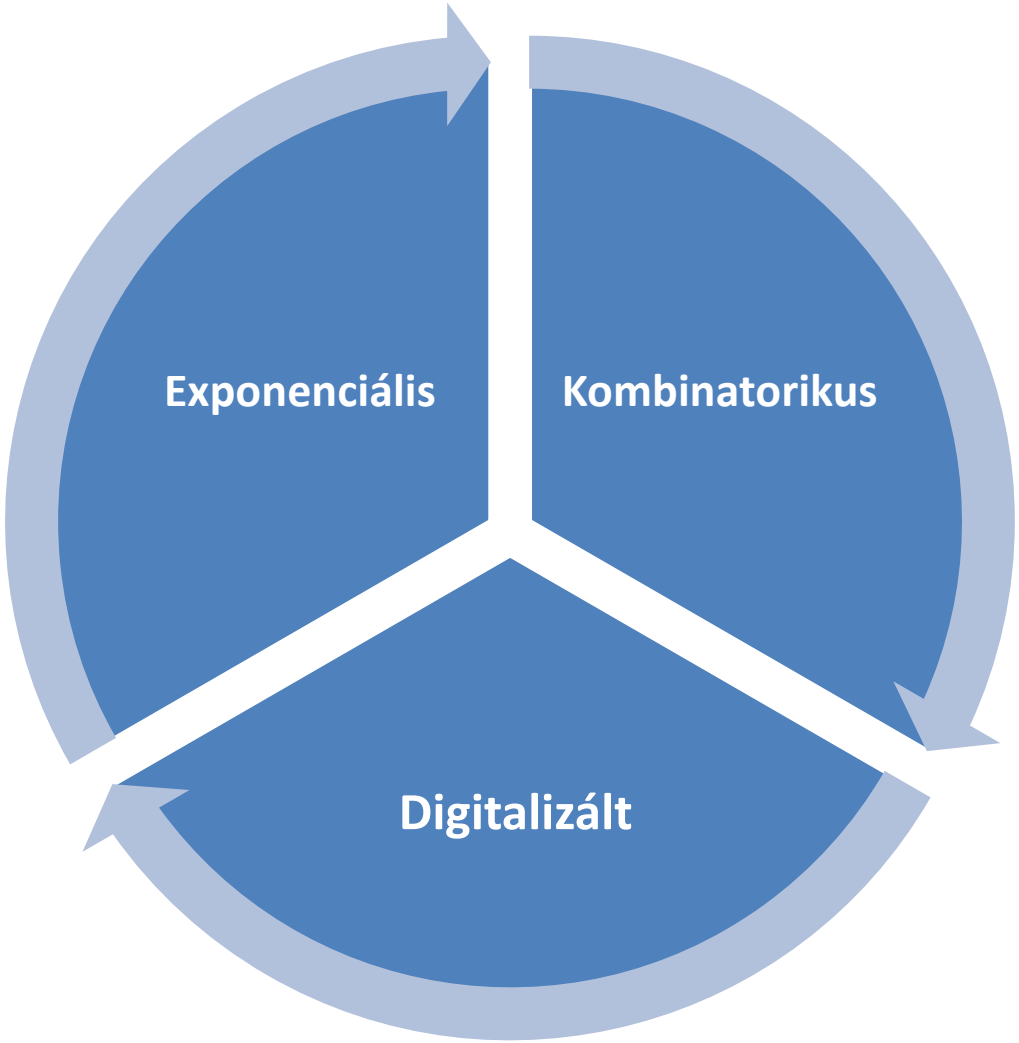


Figure 1: The Sharing Economy business model; **Source:** Business Model Toolbox

TECHNOLÓGIAI FEJLŐDÉS JELLEMZŐI



GAZDASÁGI KIHÍVÁSOK

- **A „győztes mindent visz piacok” kialakulása.**
- Az internet használata kiszélesíti a földrajzi értelemben behatárolt piacokat, sokkal több piaci szereplőt hozva ezáltal versengő pozícióba.
- **A digitális termékek terjesztése szinte költségmentes**, így az ilyen cégek mindenhol ott tudnak lenni.

- A hagyományos iparági versenyen túl a hálózati gazdaságban minden vállalat számára legalább két másik reláció is kiemelkedő fontosságú:
  - **a pénzintézetek és**
  - **a gazdasági szabályozás (kormányzat, jogrendszer).**

A JOG ÉS A TECHNOLÓGIA KAPCSOLATA

- **Technológia (haladás) vs. Jog**
- **Kreatív rombolás – romboló technológiák (disruptive technologies)**
- **Szabályozói foglyul ejtettség**

A szabályozási szempontból a technológia két aspektusával kell foglalkoznunk:

- **A technológia felforgatja az addigi gazdasági, társadalmi viszonyokat,**
- **a technológiának valamilyen addig nem ismert és jövőre nézve is nehezen megragadható jellemzője van.**

SZABÁLYOZÁSI KIHÍVÁSOK

Az ismeret hiánya a technológia szabályozásának legfőbb kihívása (pl. a technológia társadalmi elutasítottsága).

Az új technológiák a joggal szemben kettős elvárást támasztanak:

biztosítani kell az emberi szabadságjogokat	**a jog ne korlátozza a technológiai fejlődést**

A jog szabályainak megerősítésére, a jogalkotási folyamat újragondolására lehet szükség.

SZABÁLYOZÁSI KIHÍVÁSOK

Kockázatalapú megközelítéssel lehet megfelelő jogi választ adni.

Az új technológia blokkolható addig, amíg nem bizonyosodik be róla, hogy biztonságos.

A technológia nem csak a jogi szabályozás célterülete, de eszköze is lehet, például parancsként beépülhet a technológiába:

- **Mesterséges intelligencia rendszerek**
- **Beépített adatvédelem elve (privacy by design)**
- **Algoritmikus kereskedési rendszerek**

SZABÁLYOZÁSI SZINTEK

Jog

- jogszabályok, bírósági és hatósági döntések
- „informatikai jog”, „infokommunikációs jog”

Önszabályozás

- szakmai és iparági önszabályozás
- szabványosítás, domain, tartalomszabályozás

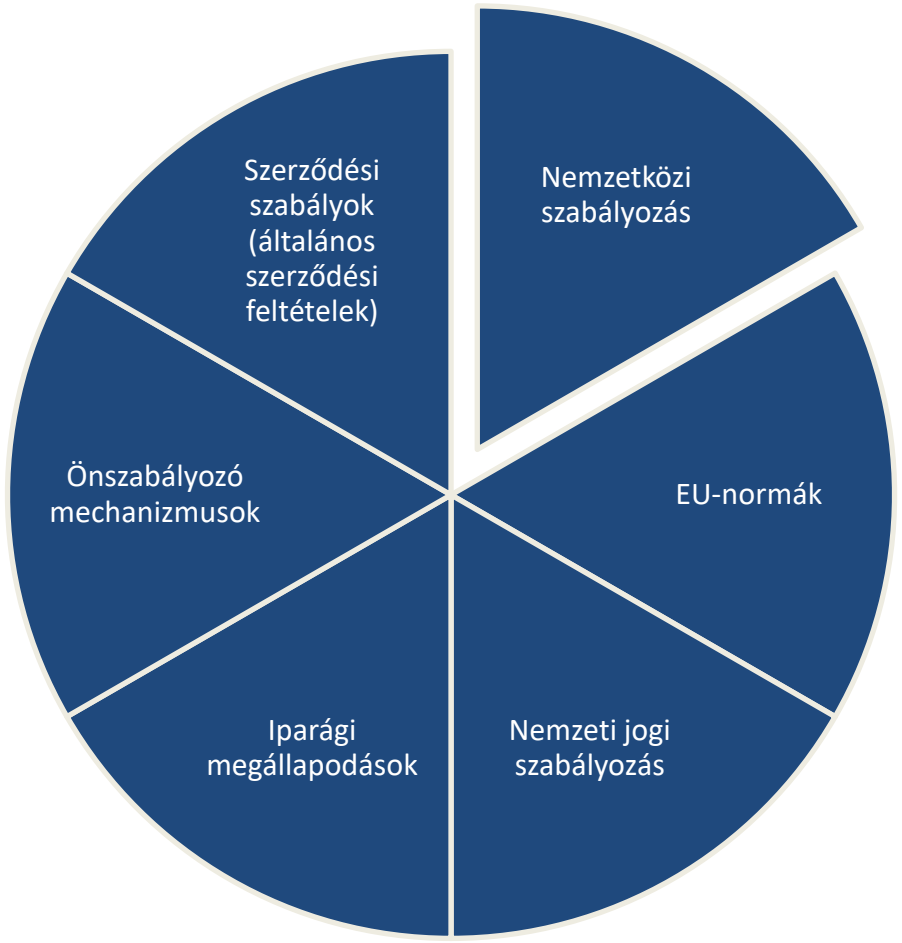
Társszabályozás

- a hatósági jogalkalmazás és az önszabályozás összekapcsolása
- tartalomszabályozás

„Kód”

- hálózati architektúra
- tartalomszűrés, hálózatsemlegesség

SZABÁLYOZÁSI SZINTEK



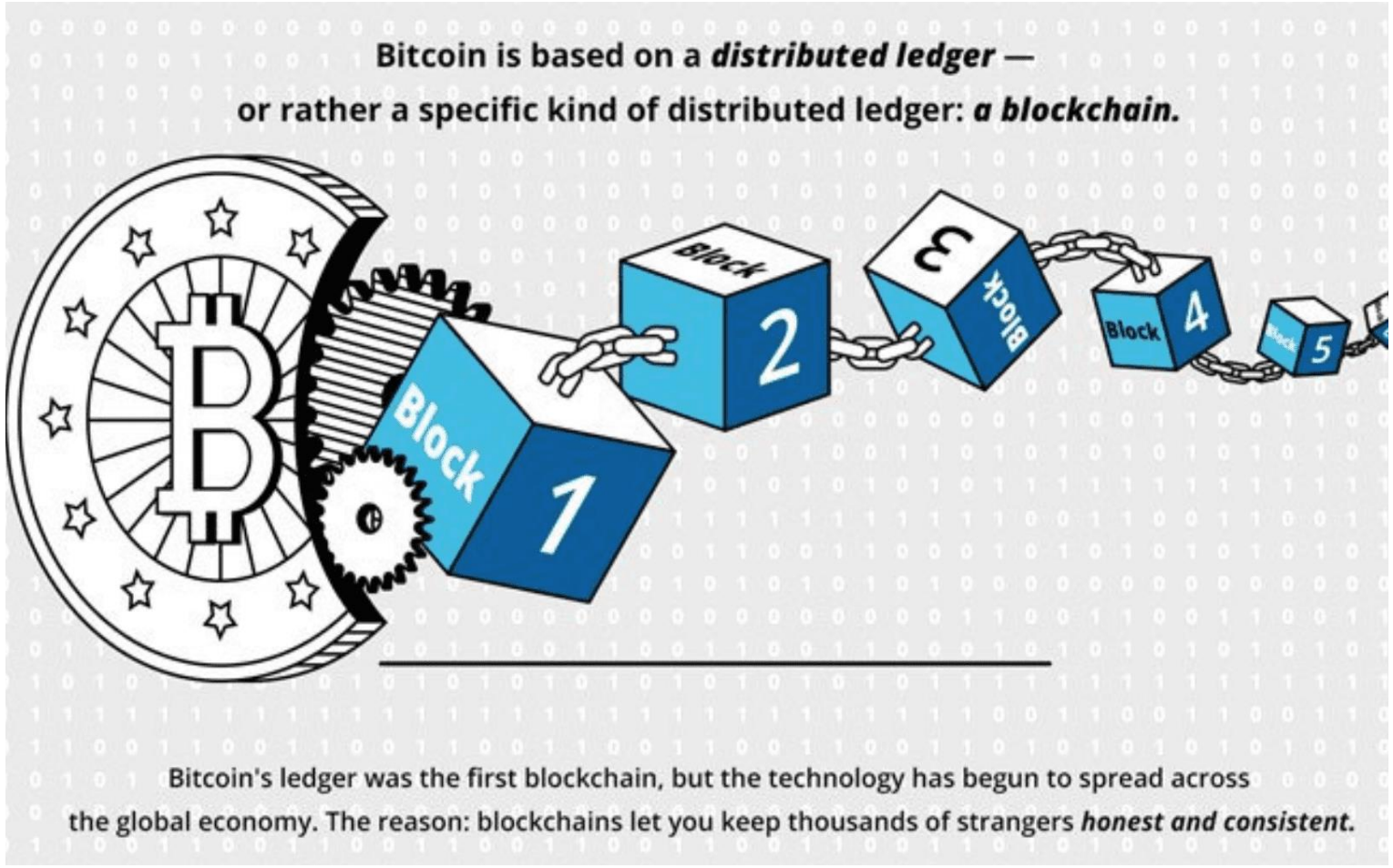
SZABÁLYOZÁSI SZINTEK

Az információs társadalom szűkebb jogrendszerébe a következő jogterületek tartoznak:

- **a magánjogon belül:** az elektronikus kereskedelem joga, a versenyjog, a digitális aláírás kérdése, a szerzői jog és iparjogvédelem.
- **közjogi területen:** az elektronikus kormányzás és a közigazgatási eljárással kapcsolatos kérdések.
- **vegyes szakjogként:** információs jogok, melyekbe az adatvédelmi jog és az információs szabadságjogok tartoznak, a médiajog.
- **büntetőjogi kérdések:** információs rendszerek elleni bűncselekmények, tartalombűncselekmények.

ÚJ KIHÍVÁS: INTERNET OF THINGS

ÚJ KIHÍVÁS: BLOCKCHAIN



BLOCKCHAIN

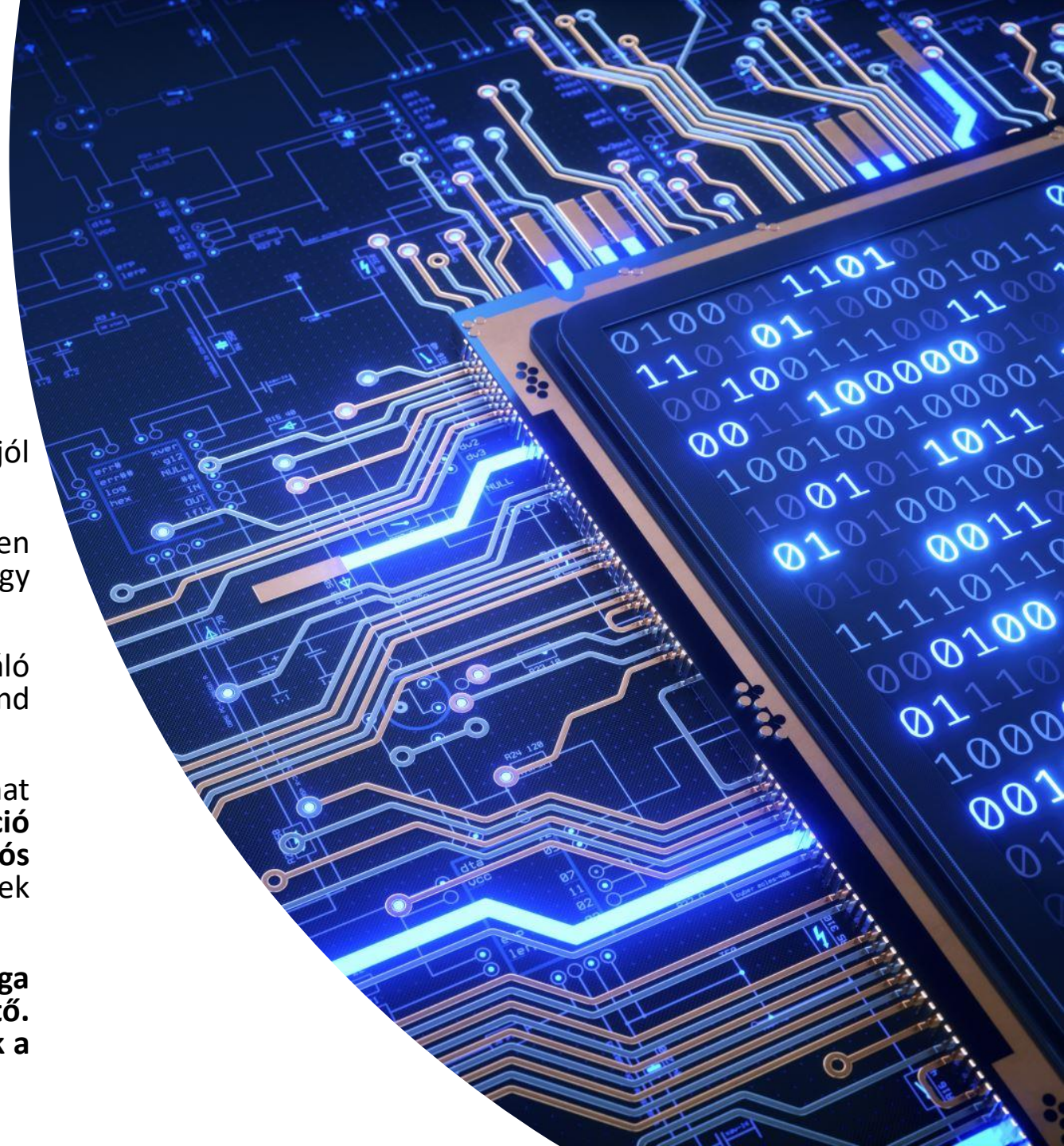
A blockchain jelentősége a technológia fő jellemzői mentén jól kirajzolódik:

- A megosztott főkönyvi rendszernek köszönhetően a blockchainben lévő tranzakciós adatok **visszamenőlegesen megmásíthatatlanok**, így alkalmazása adatbiztonsági szempontból kedvező.

- A decentralizált blockchain-adatbázisról minden felhasználó rendelkezik egy másolattal, így a rendszer mind az informatikai, mind a fizikai támadásokkal szemben **sokkálló.**

- A szereplők közti közvetlen és automatizált jóváhagyási folyamat jelentős egyszerűsítést és megtakarítást eredményezhet: **a tranzakció a korábbi átfutási idő töredéke alatt megtörténhet, a tranzakciós költségek pedig mérsékelhetőek** a közvetítő szerepének csökkentésével.

- A blockchain sajátosságai miatt **a felhasználók személyazonossága szinte nem, vagy csak komoly erőfeszítések árán visszakövethető. egyszerűsödhet az információmegosztás, valamint csökkenthetőek a rendszerintegrációs költségek is.**



Mesterséges intelligencia

MESTERSÉGES INTELLIGENCIA KÓDEXTERVEZET

A tervezet négy MI kategóriát állít fel. Az első kategória **a tiltott MI-k kategóriája**. Ezek az alábbiak:
•tudatalatti manipulálásra képes MI-k;
•bizonyos sérülékenységeket (például fogyatékosságot) kihasználó MI-k;
•társadalmi pontozást megvalósító MI-k;
•arcfelismerést közterületen végző MI-k.

•Ez utóbbi lista nyolc területen kéttucatnyi konkrét alkalmazást sorol fel, olyanokat, mint például *a természetes személyek biometrikus azonosítását, kritikus infrastruktúrák* (közlekedés, gáz, víz-, villanyellátás) *vezérlését végző MI-k*, és *még néhány*, különösen az amerikai szakirodalomból ismert területeken „tevékenykedő" MI (így a munkaerő felvétel, egyetemi felvétel, hitelbírálat és a bírói munkához adott tanácsok területén működő alkalmazások).

MESTERSÉGES INTELLIGENCIA KÓDEXTERVEZET

A tervezet hét, az MI-hez kötődő etikai kódexekből már jól ismert előírást vagy elvet igyekszik aprópénzre váltani a magas kockázatú MI-k esetén. Ezek a következők:

1) A magas kockázatú MI-ket mindig kockázatértékelési rendszerekkel együtt kell működtetni.

2) A magas kockázatú MI-ket megfelelő adatmenedzsment (data governance) rendszerekkel együtt kell működtetni. A tanító, validáló és tesztelő adatoknak „tisztának” kell lenni.

3) A magas kockázatú MI-khez részletes dokumentációt kell csatolni.

4) A magas kockázatú MI-khez az eseményeket naplózó rendszereket kell társítani.

5) A magas kockázatú MI-knek átláthatóan kell működniük.

6) A magas kockázatú MI-k felett mindig meg kell maradnia az emberi felügyeletnek és beavatkozási lehetőségnek.

7) A magas kockázatú MI-knek meg kell felelnie a pontosság, a robosztusság és a kiberbiztonság követelményeinek.


Image hosted by WittySparks | Image source FreePik
BANK


FINTECH
$ € £ ¥

FINTECH FŐBB IRÁNYAI

A technológiai újítások többsége a pénzügyi tranzakciókat érinti.

- Például gondoljunk a különböző mobilfizetési alkalmazásokra vagy az okoskészülékek érintéses adatátvitelére (NFC).

- **A hitelezési szolgáltatás pénzügyi intézmények nélkül is elérhetővé vált.**
  - Az új szereplők sokszor csak közvetítőként lépnek fel, indirekt módon hitelezve, így a banki szabályozások alól mentesülnek.
  - Az új üzleti modellek közül kiemelkedik az online piactér alapú hitelezés (alacsonyabb működési költség, banki kamatoknál alacsonyabban lehet hitelhez jutni, befektetők is magasabb hozamot érhetnek el).

- **A FinTech megoldások megkönnyítik a magánszemélyek pénzügyeinek követését és kezelését.**
  - A bankok a folyószámlakezelő rendszer adatbázisához hozzáférést kötelesek biztosítani nyílt szabványokon alapuló ún. API-kon keresztül engedéllyel rendelkező harmadik feles szolgáltatóknak.

- **A technológiai fejlődés a határon átnyúló szolgáltatásokat is átalakítja.**

- **A biztosítási értéklánc egészére vagy egyes elemeire is kiterjedhetnek az InsurTech újítások.**
  - A nemzetközi tapasztalatok alapján az InsurTech fontos szerepet játszik a FinTech megoldásokon belül.

BIG DATA

- **A big data kifejezés óriási mennyiségű, nem homogén módon strukturált adatok feldolgozására utal.**
- **A kezdetektől fogva magánszféra-védelmi kritikák és aggályok kísérték.**
- **A technológiai fejlődés nyomában elkerülhetetlenül a privacy zsugorodása jár.**

ADATALAPÚ GAZDASÁG

- **A személyes adatok a digitális gazdaság új nyersanyagai.**
- Az „ingyenes” online szolgáltatásnak van „igénybevételi díja”.
- A web2.0-nek köszönhető, hogy **a felhasználók nemcsak passzív alanyai, fogyasztói, hanem aktív részesei a netes tartalom alakításának.**
- A platformnak az lesz az érdeke, hogy a felhasználók figyelmének minél nagyobb szeletét ő kösse le.

A PLATFORM ALAPÚ GAZDASÁG JOGI VONATKOZÁSAI

Az online platformok különféle formában és méretben léteznek;

- lefedik az online piacokat, keresőket,
- a közösségi médiát,
- alkalmazásokat forgalmazó platformokat,
- távközlési szolgáltatásokat,
- fizetési rendszereket (FinTech)
- és a közösségi gazdaság platformjait.

A PLATFORM ALAPÚ GAZDASÁG JOGI VONATKOZÁSAI

A platformok növekvő szerepe és ereje szabályozási oldalról az alábbi problémákat veti fel:

- **Igyekeznek kihasználni szűk keresztmetszet pozíciójukat profitmaximalizálásra** (lásd területalapú korlátozások),
- **Megváltoztatják a társadalmi viszonyokat** (lásd fake news, szűrőbuborék) **vagy a létező piacokra gyakorolnak felforgató hatást** (lásd sharing economy),
- **Állam az államban,**
- **Súlyosan érintik az adatok védelmének kérdését.**

AZ ÚJ TECHNOLÓGIÁK ÁRNYOLDALA

Az új technológiák felhasználhatók bűncselekmények elkövetéséhez.

Új potenciális kockázatokat hordoznak magukban (lásd MI-rendszerek, önvezető járművek), amelyek a klasszikus jogi felelősségi rendszerek újragondolását igényelhetik.

A hálózati összekapcsoltság beépül a termékekbe és a szolgáltatásokba, ami (kiber)biztonsági fenyegetésekhez vezethet (lásd NIS irányelv – a kiberbiztonság felértékelődött szerepe).

A kiberbűnözés jelenti napjaink egyik legnagyobb kihívását (lásd hacking, phishing, malware, ransomware).

Megjelenik **a digitális fekezegazdaság** is (Darknet fórumok – Criminal2Criminal, magasfokú anonimitás, kriptovaluták használata).

KIBERBŰNÖZÉS
BUSINESS EMAIL COMPROMISE

Az „A” Kft. „B” üzleti partnere képviselőjének nevében elektronikus levelet kapott, amelyben kérték a vállalkozás pénzügyi ügyintézőjét, hogy a felek között fennálló beszállítói szerződés alapján esedékes számlák ellenértékét a megszokottól eltérő bankszámlaszámra utalják, mivel a cég folyamatban lévő auditálása miatt a számla kezelése bizonytalanná vált.

Az ügyintéző a kérésnek megfelelően tíz utalást indított a megadott számlaszámra közel 2,2 millió dollár értékben. Időközben kiderült, hogy az üzleti partner levelezési rendszerét feltörték és az elkövetők onnan szerezték meg a szükséges adatokat, és a cég bankszámlája helyett, sajátot adtak meg, amelyre az utalásokat az ügyintéző teljesítette.

KIBERBŰNÖZÉS
SIM SWAPPING

A sértettek egy 34 millió forintért kínált 50 négyzetméteres lakás hirdetésére jelentkeztek. Telefonon azt a tájékoztatást kapták egy férfitól, hogy a külföldön élő unokatestvére haza akar települni családjával, és sürgősen pénzre van szüksége, ezért is kedvezményes az ár. Utalt arra is, hogy a rokon hamarosan több más érdeklődőnek is megmutatja a lakást, amelyről mindössze egy fotót töltöttek fel a hirdetési oldalra, a férfi azonban további képeket és videót is ígért emailben. A sértett azt kérte, hogy egy nagy méretű fájlok küldésére alkalmas szolgáltatáson keresztül kaphassa meg a képeket, a hirdető mást ajánlott. Azt mondta, informatikus a szakmája, és egy általa ajánlott ingyenes szoftver segítségével gyorsan át tud küldeni mindent. Azonban nem sejtette, hogy a programmal visszaélést is elkövethetnek a számítógépén. A telepített program távoli asztalkapcsolatot létesít a számítógépek között. Így lehetőség nyílt arra, hogy a számítógépéhez hozzáférjenek, és nem volt más dolguk az adatok megszerzéséhez, mint megvárni, hogy a sértett belépjen az internetbank-fiókjába.

Csakhogy ez önmagában még nem elég a sikeres bűncselekményhez. Mivel az internetbankok rendszerébe csak kétlépcsős azonosítás után lehet belépni, az elkövetőknek szükségük volt azokra a kódokra is, amiket a számlatulajdonos a belépéskor, és minden tranzakció elvégzése előtt SMS-ben kap meg. Vagyis a belépéshez a sértett telefonja feletti rendelkezést is meg kellett szerezniük.

A Telenor – hosszú vizsgálat után – azt közölte, hogy egy ismeretlen személy az egyik üzletükben kezdeményezte a sértett házaspár cégének előfizetéséhez tartozó SIM-kártyák cseréjét. Arra hivatkozott, hogy ellopták azokat, ezzel együtt kérte az eredeti kártyák letiltását. Ekkor némult el a sértettek telefonja. Az ügyintézéshez a hamisított meghatalmazás mellett a sértettek cégének hamis aláírási címpéldányát mutatta be az ismeretlen.

Ezt követően a sértettek pénzét (30 millió forintot) az internet bank hozzáférését követően több részletben, többszöri átutalás után bitcoinra váltották.

KIBERBIZTONSÁG

NIS irányelv

- Információbiztonság
- Alapvető szolgáltatásokat nyújtó szereplők
- Digitális szolgáltatók (online piacterek, keresőszolgáltatások, felhőalapú számítástechnikai megoldások)
- Megfelelő és arányos műszaki és szervezési intézkedéseket kell tenniük a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében
- Nemzeti Kibervédelmi Intézet látja el az eseménykezelési feladatot
- Adatvédelmi és Információbiztonsági Szabályzat
- Üzletfolytonossági terv

KIBERBIZTONSÁG

E téren fontos hazai jogszabályok a következők:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról; az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok,
- valamint az információbiztonsági felügyelő feladat- és hatásköréről,
- a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet;
- az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet;
- az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet.

KIBERBIZTONSÁG

Adatvédelmi incidens: „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.”

Az adatvédelmi incidenst haladéktalanul, de legfeljebb az észlelését követő 72 órán belül kell bejelenteni az illetékes felügyeleti hatóságnak (Magyarországon ilyen ügyekben a NAIH jár el).

A GDPR egyik legjelentősebb újítása az **egységes adatvédelmi bírság** bevezetése minden tagállamban, amelynek mértéke mindenhol azonos, és jelentősen magasabb a korábbi bírságösszegeknél.

KIBERBIZTONSÁG

Az ügyfelek által látogatott honlapok üzemeltetőinek a fokozott biztonsági intézkedések betartása kiemelten fontos.

A NAIH erről elvi éllel a következőket határozta meg: „Az interneten nyilvánosan elérhető és (adott esetben nagyszámú) ügyfelek által is látogatható weboldalak kapcsán az esetleges sérülékenységekre való felkészültség fokozottan elvárható a fenntartók részéről. Ez a tudomány és technológia állása és a megvalósítás költségei szempontjából nem okozhatna az Ügyfélnek sem jelen esetben különösebb gondot, figyelemmel a piacon elfoglalt pozíciójára is. A weboldal és minden más interneten elérhető rendszer rendszeres sérülékenységvizsgálatának előírásáról az Ügyfél is intézkedett az incidens után, elismerve ennek szükségességét.”

(NAIH/2020/1160/10.).

Önmagában nem elégséges, ha az adatkezelő vagy adatfeldolgozó mindenre kiterjedő szabályzattal rendelkezik, ha a benne foglalt elvek és előírások a gyakorlatban nem valósulnak meg.

KÖSZÖNÖM SZÉPEN A FIGYELMET!

mezei.kitti@gtk.bme.hu