Bevezetés - A jog szerepe az információs társadalomban

Dr. Mezei Kitti
Üzleti Jog Tanszék

TELJESÍTÉSI FELTÉTELEK

Az aláírás feltétele a foglalkozások 70%-án való részvétel. A jelenlétet jelenléti ívvel ellenőrizzük.

A félévközi jegy megszerzésének feltételei: Mindkét zárthelyin külön-külön el kell érni az összpontszám legalább 40 %-át.

ZH időpontok:

2024. október 14. 18.00

2024. december 02. 18.00

2024. december 09. 18.00 (pót zh)

A kurzushoz tartoznak önellenőrző kérdések, amelyeket a félév során kitölthetnek a hallgatók, ezek kitöltése a szorgalmi feladat. Pont akkor szerezhető, ha a teszten 5-ből legalább 4 tesztkérdésre hibátlan választ adott a hallgató. Az első órához nem lesz feltöltve, de a többihez igen.

Kurzus koordinátor: Grad-Gyenge Anikó tanszékvezető (grad-gyenge.aniko@gtk.bme.hu)

Hét	Előadások témái	Dátum
1.	Bevezetés, a jog jelentősége az információs társadalomban	2024.09.03.
2.	Az alapjogok védelme az információs társadalomban	2024.09.10.
3.	Sportnap (nincs előadás)	2024.09.17.
4.	Hírközlési jog	2024.09.24.
5.	Schönherz kupa (nincs előadás)	2024.10.01.
6.	Üzleti működés formái	2024.10.08.
7.	Szellemi tulajdonjogok (szerzői jog)	2024.10.15.
8.	Szellemi tulajdonjog (iparjogvédelem)	2024.10.22.
9.	Elektronikus kereskedelem	2024.10.29.
10.	Szerződések joga I.	2024.11.05.
11.	Szerződések joga II.	2024.11.12.
12.	Munkajog	2024.11.19.
13.	Adatvédelem	2024.11.26.
14.	Start up születik – szoftverfejlesztés és szerződések	2024.12.03.
Pót		2024.12.10.

INFORMÁCIÓS TÁRSADALOM

Az „információs társadalom” olyan társadalomra utal, amelyben az információ létrehozása, terjesztése, használata és manipulálása jelentős gazdasági, politikai és kulturális tevékenység.

Az ilyen típusú társadalomban az információs és kommunikációs technológiák (IKT-k) központi szerepet játszanak a társadalmi, gazdasági és politikai élet szervezésében.

Az információs társadalom fő jellemzői a következők:
Az IKT-k mindent átható használata
Az információ mint kulcsfontosságú erőforrás
Hálózati társadalom
Globalizáció
Kulturális és társadalmi változások

Az információ olyan feldolgozott, rendszerezett és kontextusba helyezett adatokra utal, amelyek felhasználhatók tudás létrehozására, döntések meghozatalára és tevékenységek irányítására.

INFORMÁCIÓS TÁRSADALOM

- **Az információhoz való széleskörű hozzáférés**
  internet, online platformok, okoseszközök
- **Tudásalapú gazdaság**
  digitális szolgáltatások és piacok térnyerése
- **Technológiai infrastruktúra**
- **Digitális kompetencia**
  például AI literacy
- **Információcsere és együttműködés**

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

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

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

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

Long tail

A „long tail” a tömegtermékekről a hiánypótló termékek szélesebb választéka felé történő elmozdulást jelenti, amelyet a speciális érdeklődési körökre és igényekre szabott digitális platformok tesznek lehetővé. Az e-kereskedelemben szinte korlátlat árubőséggel lehet találkozni (például digitális piacterek, app stores, streaming-szolgálgatások stb.).

Szabályozási kihívások:

- **Piaci méltányosság**: Annak biztosítása, hogy a kisebb, hiánypótló termékeket előállítók méltányos hozzáféréssel rendelkezzenek a digitális platformokhoz, és ne kerüljenek hátrányba a nagyobb versenytársakkal szemben.
- **Tartalommoderálás**: A tartalom és a termékek széles körének szabályozása, beleértve az illegális, hamisított vagy káros áruk értékesítésének megakadályozását, különös tekintettel az online térre.
- **Szellemi tulajdon**: A szellemi tulajdonjogok védelme, amikor a hiánypótló termékek gyakran a meglévő tartalmak újbóli összeállításával vagy újra felhasználásával járnak.

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

Figyelemgazdaság

A megnövekedett tartalom- és információmennyiségnek köszönhetően a figyelemből hiány alakul ki. A figyelemgazdaságban a vállalkozások versengenek a felhasználók figyelméért, gyakran reklámok vagy adatgyűjtés révén pénzzé téve azt.

Szabályozási kihívások:

- **Adatvédelem**: Annak biztosítása, hogy a figyelemalapú modellek révén gyűjtött személyes adatokat az adatvédelmi jogszabályoknak, például a GDPR-nak megfelelően kezeljék.
- **Mentális egészség**: A figyelemvezérelt online platformok mentális egészségre gyakorolt hatásával kapcsolatos aggodalmak kezelése, különösen a függőséget okozó viselkedés és a veszélyeztetett népességcsoportok kitettségének tekintetében (például gyermekek és idősek).
- **Átláthatóság és manipuláció**: A felhasználói viselkedést manipuláló algoritmusok használatának szabályozása, az átláthatóság biztosítása a tartalom ajánlása vagy megjelenítése tekintetében.

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.

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

Crowdsourcing

Ezek a modellek az egyének kollektív hozzájárulására támaszkodnak a termékek fejlesztése, a szolgáltatások tesztelése vagy a kezdeményezések finanszírozása érdekében.

Szabályozási kihívások:

- **Munkajog**: A crowdsourcingban vagy tömegtesztelésben részt vevő egyének jogainak és méltányos díjazásának védelme, akik nem feltétlenül rendelkeznek hagyományos munkavédelemmel.
- **Fogyasztóvédelem**: A crowdfunding platformok átláthatóságának és elszámoltathatóságának biztosítása a befektetők és a hozzájárulók védelme érdekében a csalással szemben.
- **Szellemi tulajdon**: A crowdsourcing révén létrehozott ötletekhez, termékekhez vagy tartalmakhoz kapcsolódó tulajdonjog és jogok tisztázása.

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

Freemium

A freemium modell az alapszolgáltatásokat ingyenesen kínálja, míg a prémium funkciókért díjat számít fel, és a bevételek generálása érdekében a feláras értékesítésre támaszkodik.

Szabályozási kihívások:

- **Fogyasztóvédelem**: Annak biztosítása, hogy a fogyasztókat ne tévesszék meg az ingyenes szolgáltatások költségeivel vagy korlátaival kapcsolatban, és hogy a feláras értékesítési gyakorlat átlátható legyen.

- **Verseny**: Annak ellenőrzése, hogy a freemium modellek nem teremtenek-e tisztességtelen versenyt, különösen ha a nagy platformok piaci erejüket kihasználva olyan ingyenes szolgáltatásokat kínálnak, amelyeket a kisebb versenytársak nem engedhetnek meg maguknak.

- **Adatvédelem**: Azoknak a kérdéseknek a kezelése, amikor az ingyenes szolgáltatások „ára” a felhasználói adatok gyűjtése és pénzzé tétele, az adatvédelmi szabályoknak való megfelelés biztosítása.

A SHARING ECONOMY

- **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), TaskRabbit.
- Számos szabályozási kérdést vet fel.

AKTUÁLIS GAZDASÁGI JELENSÉGEK ÉS TRENDEK

Sharing economy

Szabályozási kihívások:

- **Munkajog és munkavállalói védelem**: A tisztességes munkaügyi gyakorlatok biztosítása a platformgazdaságban (gig-gazdaságban) dolgozók számára, akik nem feltétlenül rendelkeznek a hagyományos munkaviszonyban dolgozók védelmével és előnyeivel.

- **Fogyasztói biztonság és felelősség**: A megosztott szolgáltatásokra vonatkozó biztonsági előírások és felelősségi kérdések szabályozása, biztosítva a fogyasztók védelmét, amikor magánszemélyek, nem pedig vállalkozások által nyújtott szolgáltatásokat vesznek igénybe.

- **Adózás és megfelelés**: A megosztáson alapuló gazdaságban keletkező jövedelmek adóztatásával kapcsolatos kihívások kezelése, amelyeket nehéz nyomon követni és betartatni, különösen a különböző joghatóságok között.

- **Helyi szabályozás**: A megosztáson alapuló gazdasági szolgáltatások és a helyi szabályozások, például az helyi jogszabályok, a szállodai előírások vagy a taxiengedélyek közötti konfliktusok kezelése.

SHARING ECONOMY BUSINESS MODEL

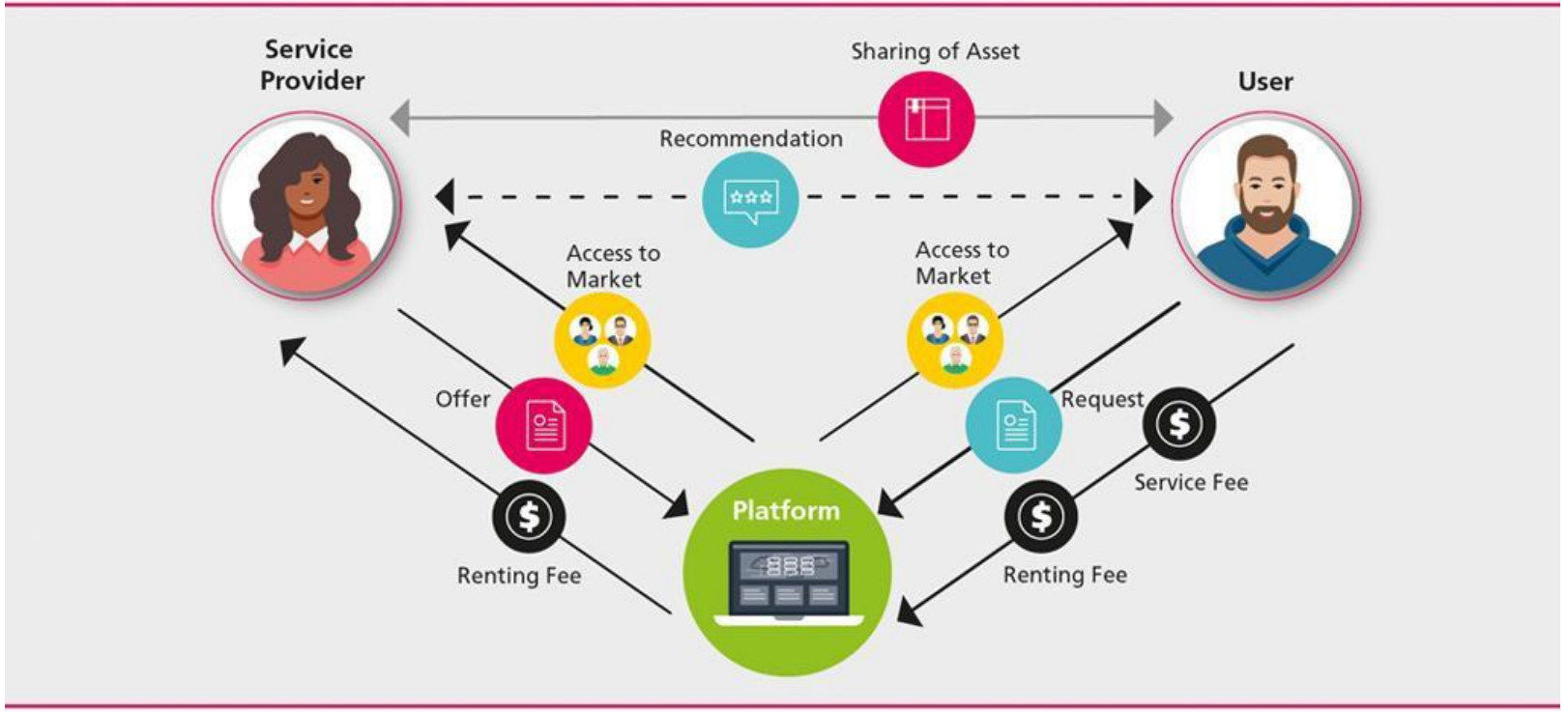


Figure 1: The Sharing Economy business model; **Source:** Business Model Toolbox

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 JOG ÉS A TECHNOLÓGIA KAPCSOLATA

Technológia vs. jog

Szabályozói foglyul ejtettség: a szabályozás előnyeit nem a köz, hanem a szabályozott élvezi, aki megpróbálja a szabályozót a saját érdekei mentén befolyásolni (például digitális piacok terén, Meta és társai).

Kihívások:

- A technológia felforgatja az addigi gazdasági, társadalmi viszonyokat,
- a technológiának valamilyen olyan jellemzője van, amely kihívást jelent a jogi szabályozás szempontjából (például feketedoboz hatás, pszeudoanonimitás stb.).
- Kockázatok megfelelő felmérése és kezelése
- Ex ante vs. ex post szabályozás

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 jogok védelmét	**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 a technológia szabályozás terén.

Például az EU DSA (digitális szolgáltatásokról szóló rendelete) szerint minél nagyobb egy online platform, annál nagyobb a hatása, és ennélfogva nagyobb kockázatot jelent a felhasználókra és a társadalomra nézve.

Az EU mesterséges intelligencia rendelete különböző kockázati szintekbe sorolja az MI felhasználási eseteket.

Emberi jogi hatásvizsgálat és adatvédelmi hatásvizsgálatok lefolytatása mint kockázatfelmérési eszköz (impact assessments).

SZABÁLYOZÁSI KIHÍVÁSOK

„By design” megközelítés (ethics by design, regulation by design, security by design)

A jogalkotók arra kötelezik a fejlesztőket, hogy biztosítsák, hogy a rendszer tervezése megfeleljen a konkrét jogi követelményeknek. A fejlesztők viszont úgy tesznek eleget ennek a követelménynek, hogy a jogi követelményeket műszaki követelményekké alakítják át, amelyek a „regulation by design” tartalmát beágyazzák a digitális rendszer kódjába.

- **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

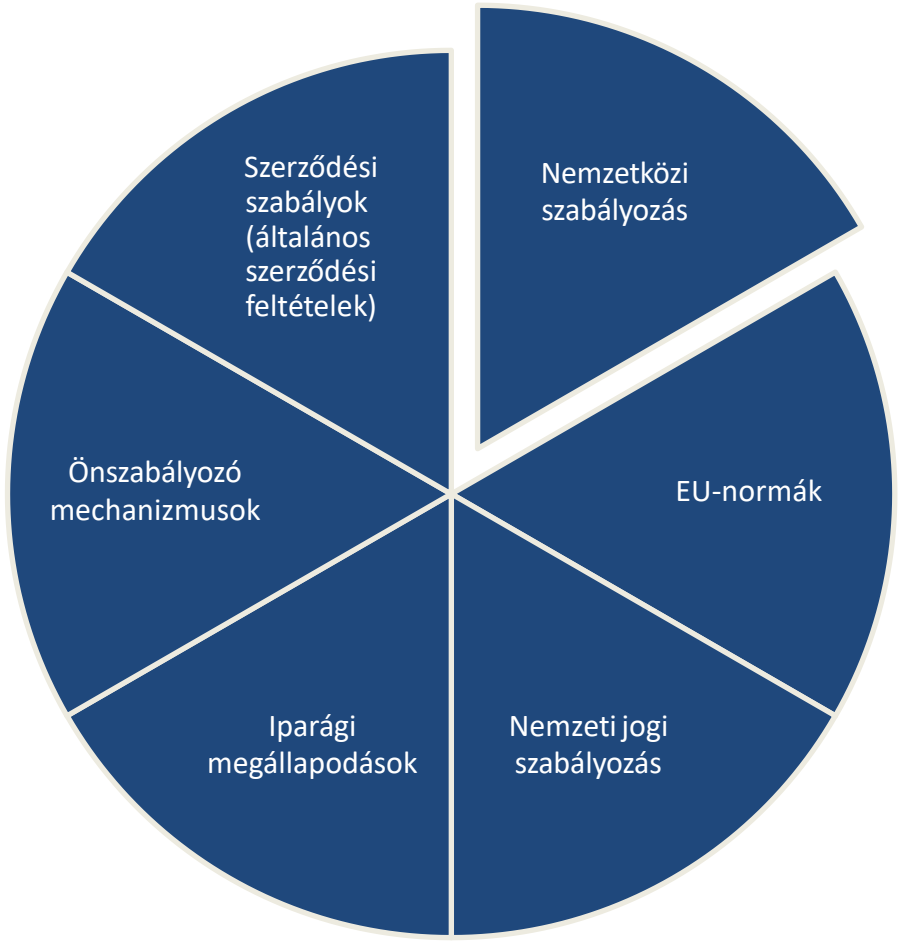
Társszabályozás

- 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.

Mesterséges intelligencia

KOCKÁZATALAPÚ MEGKÖZELÍTÉS
A MESTERSÉGES INTELLIGENCIA RENDELET TÜKRÉBEN

- Elfogadhatatlan kockázat (tiltott kategória)
- Nagy kockázat
- Mérsékelt kockázat
- Minimális vagy nincs kockázat

TILTOTT MI-GYAKORLATOK

- a hatóságok által végzett, mesterséges intelligencián alapuló, általános célú társadalmi pontozást (lásd Kína)
- a „valós idejű” és a „post” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken történő, bűnüldözési célú használata szintén tilos, utóbbi eltekintve bizonyos korlátozott kivételektől
- öntudatlanul, szubliminális technikák alkalmazásával nagymértékben manipulálni a személyeket, vagy kihasználni bizonyos veszélyeztetett csoportok sebezhetőségét
- további tilalmak közé kerültek az olyan mesterséges intelligencia-rendszerek, amelyek biometrikus adatokat használnak az egyének kategorizálására, bűncselekmények előrejelzésére, arcképek lekérdezésére az internetről és CCTV felvételekről arcfelismerő adatbázis készítéséhez, bizonyos kontextusokban az egyének érzelmeinek meghatározására (a bűnüldözésben, a határigazgatásban, a munkahelyeken és az oktatási intézményekben).

NAGY KOCKÁZATÚ MI

- A mesterséges intelligencia rendszer nagy kockázatúnak minősül:

- ha vagy egy már szigorúan szabályozott termékcsoport biztonsági eleme (a II. mellékletben felsorolt termékek, a játékoktól a kézműves termékeken át az orvostechnikai eszközökig),
- vagy mert olyan területen használják, ahol az egészségben és a biztonságban, környezetben okozott kár vagy az alapvető jogokat érő kedvezőtlen hatás tekintetében olyan *jelentős kockázattal* járnak, (ezeket a III. melléklet kifejezetten felsorolja, DE!), kivéve, ha a rendszer kimenete a meghozandó intézkedés vagy döntés tekintetében *„pusztán kiegészítő jellegű”.*

NAGY KOCKÁZATÚ MI

- A nagy kockázati besorolás alól mentesülnek:
- a szűk körű eljárási feladatok,
- a korábban elvégzett emberi tevékenységek eredményeinek javítása,
- a döntések vagy kiugró értékelések felderítése az emberi értékelések helyettesítése nélkül,
- valamint azok az esetek, amelyekben a rendszer célja a döntéshozatali minták vagy eltérések felderítése, nem pedig a korábbi emberi értékelések megfelelő felülvizsgálat nélküli helyettesítése vagy befolyásolása.
- Azonban bármely mesterséges intelligencia rendszer automatikusan nagy kockázatúnak minősül, ha a mesterséges intelligencia rendszer végzi az egyének profilalkotását.

MEGFELELŐSÉGÉRTÉKELÉS KÖVETELMÉNYRENDSZERE

- A nagy kockázatú mesterséges intelligenciával szemben támasztott követelmények a következők (Bizottság vezeti az adatbázist a nagy kockázatú MI-rendszer szolgáltatóiról):
- mindig kockázatértékelési rendszerekkel együtt kell működtetni
- megfelelő adatmenedzsment (data governance) rendszerekkel együtt kell működtetni. A tanító, validáló és tesztelő adatoknak (beleértve a címkéket is) relevánsnak, reprezentatívnak, hibák szempontjából megfelelően ellenőrizettnek, teljesnek kell lenniük
- részletes dokumentációt kell csatolni
- az eseményeket naplózó rendszereket kell társítani
- átláthatóan kell működniük
- mindig meg kell maradnia az emberi felügyeletnek és beavatkozási lehetőségnek
- meg kell felelnie a pontosság, a robosztusság és a kiberbiztonság követelményeinek
- emberi jogi hatásvizsgálatok lefolytatása.

MÉRSÉKELT KOCKÁZATÚ MI-RENDSZER

- Az egyéb, nem magas kockázatú, korlátozott mesterséges intelligenciával rendelkező rendszerek csak bizonyos különleges esetekben tartoznak az átláthatósági kötelezettségek hatálya alá.
- Például a felhasználók tájékoztatását, amikor chatrobottal lépnek kapcsolatba, vagy amikor egy mesterséges intelligenciával működő rendszer deepfake tartalmat gyárt, valamint bizonyos érzelemfelismerő és biometrikus kategorizáló rendszereket hoz létre.
- Egyéb kockázati szintbe be nem sorolt esetekben a rendelet a magatartási kódexek elfogadását támogatja, az önszabályozási mechanizmusok bevezetését (például fordításra, spam szűrésre használt MI esetén stb.).

ONLINE PLATFORMOK

- A kereskedelem területén a 2000-es évek elején kezdett elterjedni az eBay, de még különlegesnek számított az online vásárlás.
- A közösségi média szolgáltatók közül példaként említhető a Facebook, amely 2004-ben indult el, kezdetben leginkább a fiatalabb korosztály szabadidős tevékenységéhez kapcsolódott.
- A 2010-es évektől kezdve vált jelentőssé a platformok felfutása, váltak a mindennapi életünk részévé.
- Meghatározó információforrássá váltak, hirdetési felület, új foglalkozások, események befolyásolói (például választások).

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.**

Digitális szolgáltatásokról szóló rendelet (DSA)

Online biztonság növelése: felhasználók védelme az illegális tartalmaktól, áruktól és szolgáltatásokból (azonnali eltávolítási kötelezettség – felelősség)

Átláthatóság növelése: működésük kapcsán, moderálási tevékenység módja, hirdetések, felhasználói adatfelhasználás stb.

Tiszta verseny: tiszteséges verseny a digitális piacokon (erőfölénnyel visszaélés tilalma)

Platformok elszámoltathatósága: Például az óriásplatformoknak értékelniük és csökkenteniük kell a rendszerszintű kockázatokat, például a dezinformáció terjedését vagy a mentális egészségre gyakorolt hatást, és független ellenőrzéseknek kell alávetniük magukat.

ONLINE ÓRIÁSPLATFORM SZOLGÁLTATÓK

Az online óriásplatformok és keresőmotorok azok, amelyeknek több mint 45 millió felhasználója van az EU-ban.

1. Alibaba AliExpress
2. Amazon Store
3. Apple AppStore
4. Booking.com
5. Facebook
6. Google Play
7. Google Maps
8. Google Shopping
9. Instagram
10. LinkedIn
11. Pinterest
12. Snapchat
13. TikTok
14. Twitter
15. Wikipedia
16. YouTube
17. Zalando
18. Pornhub
19. Stripchat
20. Xvideos
21. XNXX

\+ keresőmotorok: Google Search és Bing

Digitális piacokról szóló rendelet (DMA)

A kapuőrök kijelölése: ezek jellemzően olyan nagy technológiai vállalatok, amelyek jelentős hatással vannak a digitális ökoszisztémára, és képesek kapuőrként fellépni a vállalkozások és a fogyasztók között (például app stores, online platform szolgáltatók, keresőmotorok stb.).

A tisztességtelen gyakorlatok tilalma: saját termékek vagy szolgáltatások előnyben részesítése a versenytársakkal szemben (például saját termékeik előnyben részesítése vagy a vállalkozásuk egyik részterületéről gyűjtött adatok felhasználása arra, hogy tisztességtelen előnyre tegyenek szert egy másik területen.

Kötelezettségek: például lehetővé kell tenniük a felhasználók számára az előre telepített alkalmazások eltávolítását, biztosítaniuk kell az interoperabilitást harmadik fél szolgáltatásaival, és tisztességes hozzáférést kell biztosítaniuk a platformjukhoz más vállalkozások számára.

Végrehajtás és szankciók: piaci vizsgálatok lefolytatása az Európai Bizottság által

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).

A technológiai fejlődés hatása a büntetőjogra

- Az új technológiák elterjedése (pl. internet, mobilinformatikai, IoT eszközök használata) lehetőséget teremt a bűnözés eddig ismeretlen formái számára (pl. kiberbűnözés).
- Új típusú bűncselekmények megjelenése (hackertámadások, adatmanipulációk), illetve a hagyományos bűncselekmények is könnyebben elkövethetők ezek segítségével (pl. csalás, zsarolás stb.).
- A technológiai környezet egyrészt a már létező társadalmi értékek új szféráját, másrészt egészen új a büntetőjog által védett értékeket hozott létre.

A technológiai fejlődés hatása a büntetőjogra

- Kiterjedt online jelenlét, tömeges informatikai támadások megjelenése
- Az internet globálig jellege lehetőséget teremt a határon átívelő bűnözésnek
- Kommunikációs csatornát, illetve platformot biztosít
- Profit-orientált, szolgáltatás alapú üzleti modellé vált a kiberbűnözés (Darknet fórumok)
- Titkosítást és anonimitást biztosító technológiák (kriptovaluták, TOR)
- Magas látencia jellemzi a kiberbűncselekményeket
- Könnyedén végrehajtható adat-, programmanipuláció, automatizált műveletek

A kiberbűnözés (cybercrime) fogalma

- Gyűjtőfogalom
- ún. tisztán informatikai bűncselekmények (pl. számítógépes vírusok, hacking)

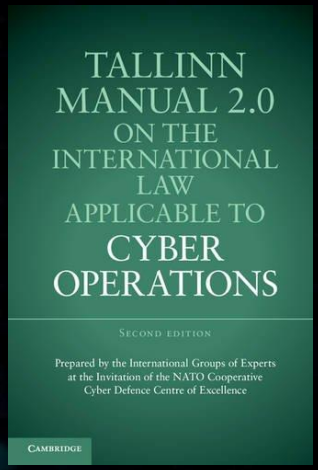
- az információs rendszer és a számítógépes adat az elkövetés tárgya

- hagyományos bűncselekmények az információs rendszerek felhasználásával elkövetve (pl. csalás, zsarolás, zaklatás)

- az információs rendszer az elkövetés eszköze

A támadások mögött húzódó motiváció a kibertérben

- Anyagi haszonszerzés (zsarolás)
- Károkozási célzat (DDoS-támadás, malware)
- Politikai, ideológiai indíttattás
  (amerikai elnökválasztás, hacktivism)
- Szexuális indíttatás (gyermekpornográfia)
- Kiberháború, kiberhadviselés
  (észt-orosz konfliktus, orosz-grúz háború, Stuxnet)
- Kiberterrorizmus



Információs rendszer vagy adat megsértése

- A következő szándékos elkövetési magatartásokkal követhető el:

➢ jogosulatlan belépéssel vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent maradással (ún. hacking),

➢ az információs rendszer működésének jogosulatlan vagy jogosultsága kereteit megsértő akadályozása (pl. DDoS-támadás indítása),

➢ az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz (pl. rosszindulatú programmal megfertőzi a rendszert, mint ilyen volt az elmúlt években a zsarolóvírus, ami az adatokat titkosította, ezáltal hozzáférhetetlenné tette, vagy a jogosulatlan belépést további adatmanipuláció is követi).

A jogosulatlan belépés, avagy a hacking

- Az információs rendszer vagy adat megsértése

➢ Btk. 423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

- Hacking-jellegű magatartások mögött húzódó motiváció: adatmanipuláció, jogtalan haszonszerzés és károkozási szándék, wardriving esete. További büntetendő magatartásokat segíthet elő.
- Elkövetői kör: „kívülálló” vagy „bennfentes” személy.
- Hazai szabályozás megköveteli a technikai intézkedés megsértését vagy kijátszását.
- Nem célzatos bűncselekmény, csak szándékosan követhető el.

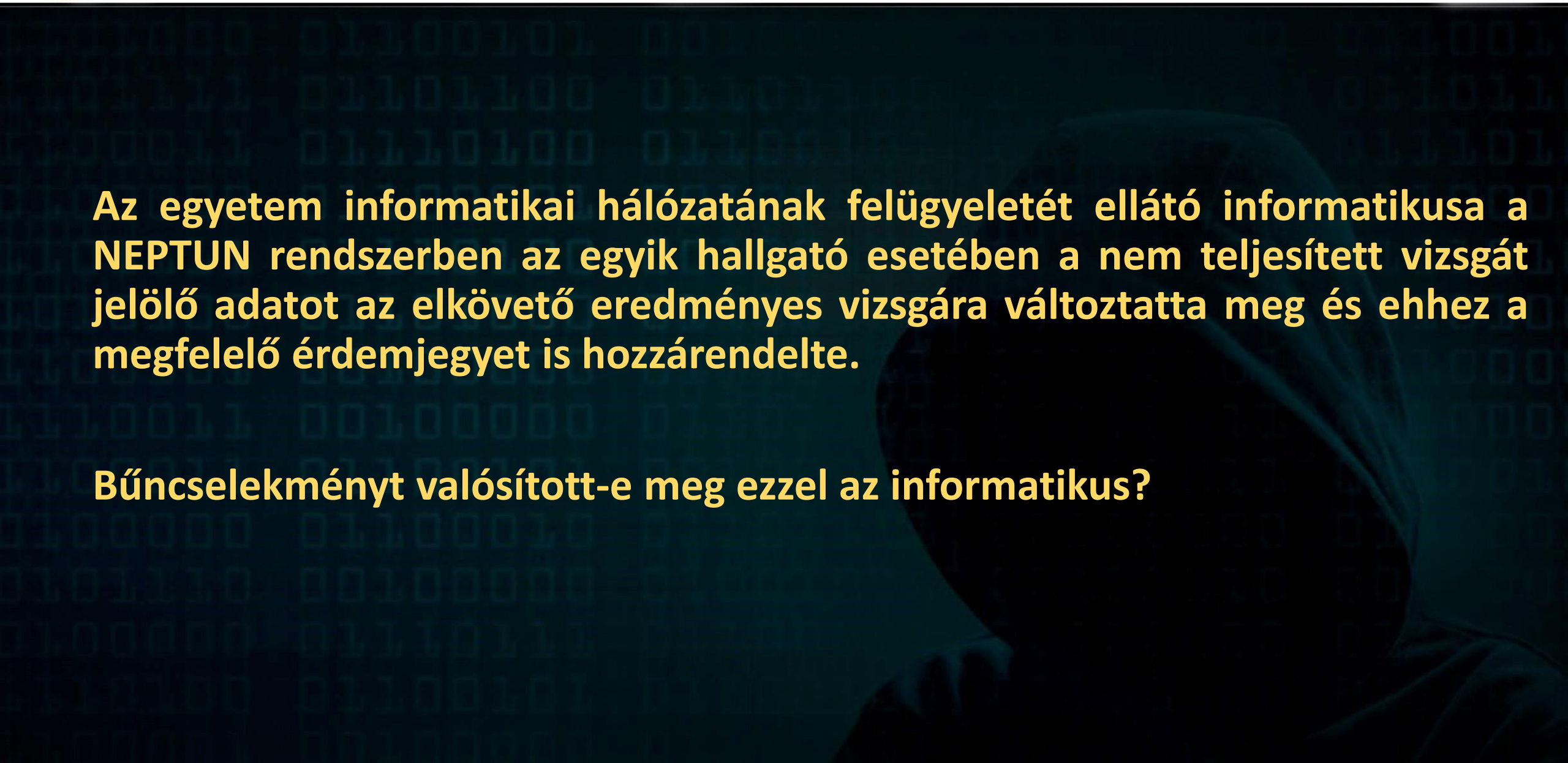
A jogosulatlan belépés, avagy a hacking

- BH 2017.12.392

➢ A büntetőjog alapelveivel összhangban a jogosultság keretein való túllépés is akkor minősül bűncselekménynek, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik (pl. más jelszavának a felhasználásával), ugyanis pusztán e jogosultság kereteinek túllépése nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván. Ennek hiányában a magatartás társadalomra veszélyessége csekély.

- Fekete, szürke vagy fehér kalapos hacker

➢ Etikus hacking kérdése: jogosultság hiányában nem beszélhetünk etikus magatartásról, azonban kérdés, hogy büntetőjogilag felelni kell-e (társadalomra veszélyesség vizsgálata, közérdekű bejelentés) – lásd Telekom és BKK-ügy



Az egyetem informatikai hálózatának felügyeletét ellátó informatikusa a NEPTUN rendszerben az egyik hallgató esetében a nem teljesített vizsgát jelölő adatot az elkövető eredményes vizsgára változtatta meg és ehhez a megfelelő érdemjegyet is hozzárendelte.

Bűncselekményt valósított-e meg ezzel az informatikus?

KIBERBIZTONSÁG

NIS irányelv – NIS 2 irányelv

- Információbiztonság
- Alapvető szolgáltatásokat nyújtó szereplők: A NIS2 irányelv sokkal nagyobb léptékben működik, mint elődje. Az élelmiszergyártástól és vízellátástól kezdve, a postai szolgáltatásokon át, a repüléstechnológiáig, a korábban még alulszabályozott szervezeteknek mostantól meg kell felelniük a NIS2-nek.
- 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, kiberbiztonsági incidencek kezelése.
- Adatvédelmi és Információbiztonsági Szabályzat
- Üzletfolytonossági terv

KIBERBIZTONSÁG

A 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és felügyeletről

A szervezeteknek gondoskodniuk kell az elektronikus információs rendszereik és azok fizikai környezetének a biztonságáról, a kiberfenyegetések által okozható károk mértékével arányos módon.

Ez magában kell, hogy foglalja az adatok, valamint az elektronikus információs rendszerek révén elérhető szolgáltatások bizalmasságát, sértetlenségét és rendelkezésre állását.

Kétévente kötelező kiberbiztonsági auditot végezni, amelyet a kiberbiztonsági követelményeknek való megfelelésről a tevékenység végzésére jogosult, független auditor folytathat le.

A felügyeletét a 2021-ben létrehozott **Szabályozott Tevékenységek Felügyeleti Hatósága** (SZFTH) látja el.

Kiemelten kockázatos ágazatok:

- Energetika (Villamos energia, Távfűtés és hűtés, Kőolaj, Földgáz, Hidrogén)
- Közlekedés (Légi közlekedés, Vasúti közlekedés, Közúti közlekedés, Vízi közlekedés, Tömegközlekedés)
- Egészségügy
- Ivóvíz, szennyvíz (Vízközmű szolgáltatás)
- Hírközlési szolgáltatás
- Digitális infrastruktúra
- Kihelyezett IKT (információs és kommunikációs technológia) szolgáltatások
- Űralapú szolgáltatás

Kockázatos ágazatok:

- Postai és futárszolgálatok
- Élelmiszer előállítása, feldolgozása és forgalmazása
- Hulladékgazdálkodás
- Vegyszerek előállítása és forgalmazása
- Gyártás (Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása, Számítógép, elektronikai, optikai termék gyártása, Villamos berendezések gyártása, Máshova nem sorolt gépek és berendezések gyártása, Gépjárművek, pótkocsik és félpótkocsik gyártása, Egyéb szállítóeszközök gyártása, Cement-, gipsz-, mészgyártás)
- Digitális szolgáltatók

KIBERRELIZIENCIÁRÓL SZÓLÓ RENDELET

Az EU döntött arról, hogy a kiberbiztonságot minden digitális elemmel rendelkező termék esetében kötelezővé teszi.

A jogszabály céljait a következő fő irányelvek révén lehet elérni:

- **fokozott biztonság:** mindenekelőtt a fejlesztőknek és a gyártóknak kell gondoskodniuk arról, hogy az EU piacain forgalomba hozott összes csatlakoztatott eszköz (IoT-eszköz) általánosságban biztonságosabb legyen (sebezhetőséget nem tartalmazhatnak stb.).
- **életciklus-menedzsment:** a második cél annak biztosítása, hogy a gyártók felelősek maradjanak eszközeik kiberbiztonságáért (még azután is, hogy azok elhagyják a gyár kapuit), hogy a biztonsági kérdéseket a termék teljes életciklusa során kezeljék.
- **tájékozott vásárlók:** végül a fogyasztókat megfelelően tájékoztatni kell az általuk megvásárolt és használt eszközök kiberbiztonsági szempontjairól.

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

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