



Dr. Kollár Csaba PhD

A mesterséges intelligencia Kínában

a Társadalmi Kredit Rendszerének (nem csak) információbiztonsági kihívásai

A mesterséges intelligencia alkalmazásának hatása az alapjogokra

tudományos konferencia

2020. február 27.

Nemzeti Közsolgálati Egyetem Oktatási Épület

Budapest

BEMUTATKOZÁS



A MESTERSÉGES INTELLIGENCIA

társadalmi vetületei
gazdasági hatásai

**információbiztonság
humán aspektusa**

**biztonságtudatosság
fejlesztése**

intelligens városok

**ember-robot interakció
emberi oldala**

kibernetika reneszánsza

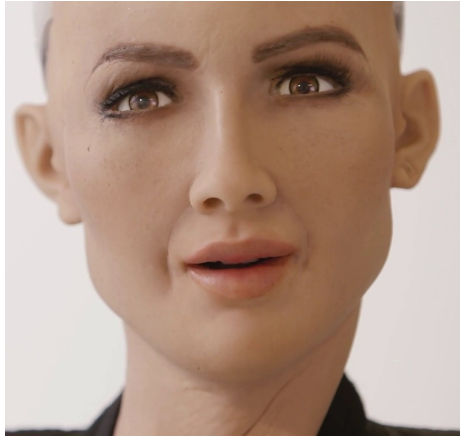
- 
1. Miért aktuális most beszélni a mesterséges intelligenciáról?
 2. Melyek a mesterséges intelligenciához kapcsolódó fontosabb technológiák és megoldások?
 3. Melyek a mesterséges intelligencia léptékei?
 4. Mit jelent, s hogyan valósítható meg a mesterséges intelligencia segítségével a társadalom tagjainak értékelése/minősítése?

AMIKOR ÉN MÉG KISSRÁC VOLTAM...

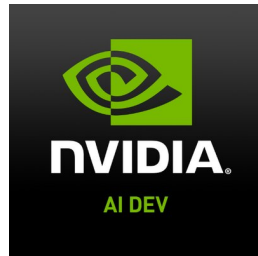


GONDOLATOK A MESTERSÉGES INTELLIGENCIÁRÓL

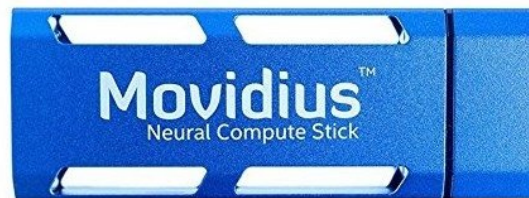
NÉHÁNY PÉLDA A MESTERSÉGES INTELLIGENCIÁRA



Sophia



Anki Cozmo

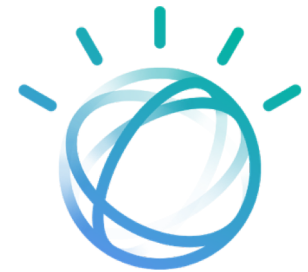


echo dot

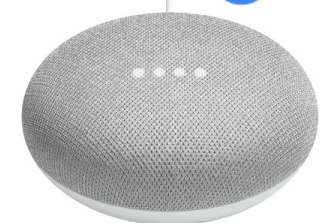
Add Alexa to any room



Deep Blue



Watson



A MESTERSÉGES INTELLIGENCIA LÉPTÉKEI

- Testen viselhető okoseszközök (óra, cipő, póló, külső „csontváz”)
- Testben levő okoseszközök (implantátumok, egészségügyi monitoring)
- Hordozható okoseszközök (telefon, tablet)
- Intelligens (önvezető) autók, járművek
- Intelligens épületek/létesítmények (domotika)
- Intelligens szervezetek/vállalatok
- Intelligens település/város
- **Intelligens ország/társadalom**
- Intelligens Föld

MESTERSÉGES INTELLIGENCIA – MIÉRT MOST?

Adatok

Rengeteg adat áll rendelkezésre, ezek mennyisége folyamatosan növekszik

Számítási kapacitás

Olyan számítások is elvégezhetők belátható időn belül, amire tíz évvel ezelőtt még a szuperszámítógépek sem voltak képesek

Algoritmusok

Az AI-t támogató tanulóalgoritmusok, statisztika és valószínűségszámítás, regressziós modellek, klasszifikáció, klaszterizáció, lágyszámítási módszerek megjelenése a gyakorlati, összetett, komplex, bonyolult problémák megoldásában

Szinergia

Technológiák fejlődése és összekapcsolódása

AZ MI FONTOSABB TUDOMÁNYTERÜLETI KAPCSOLATAI

**Biztonság-
tudomány**

**Számítás-
tudomány**

**Kommunikáció- és
nyelvtudomány**

**Biológia és
orvostudomány**

**Pszichológia és
pedagógia**

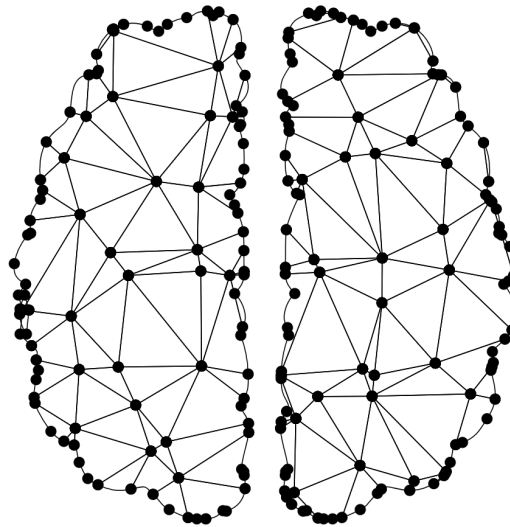
Idegtudomány

Szociológia

**Műszaki
tudományok**

Matematika

Filozófia és jog



MESTERSÉGES INTELLIGENCIA MÉRFÖLDKÖVEI

1. az emberek és aktivitásaik észlelése
2. a verbális kifejezések generálása (beszéd), illetve a beszéd megértése
3. nonverbális kifejezések generálása, illetve a nonverbális jelzések megértése
4. az érzelmi állapotok modellezése, kifejezése és megértése
5. a szándékos cselekvések felismerése és közvetítése
6. együttműködés az emberekkel
7. navigálás (fizikai helyzetfelismerés) az emberek környékén és környezetében
8. társadalmi kontextusban tanulni az emberektől

A GÉP AUTONÓMIÁJA – A SZÁMÍTÓGÉP...

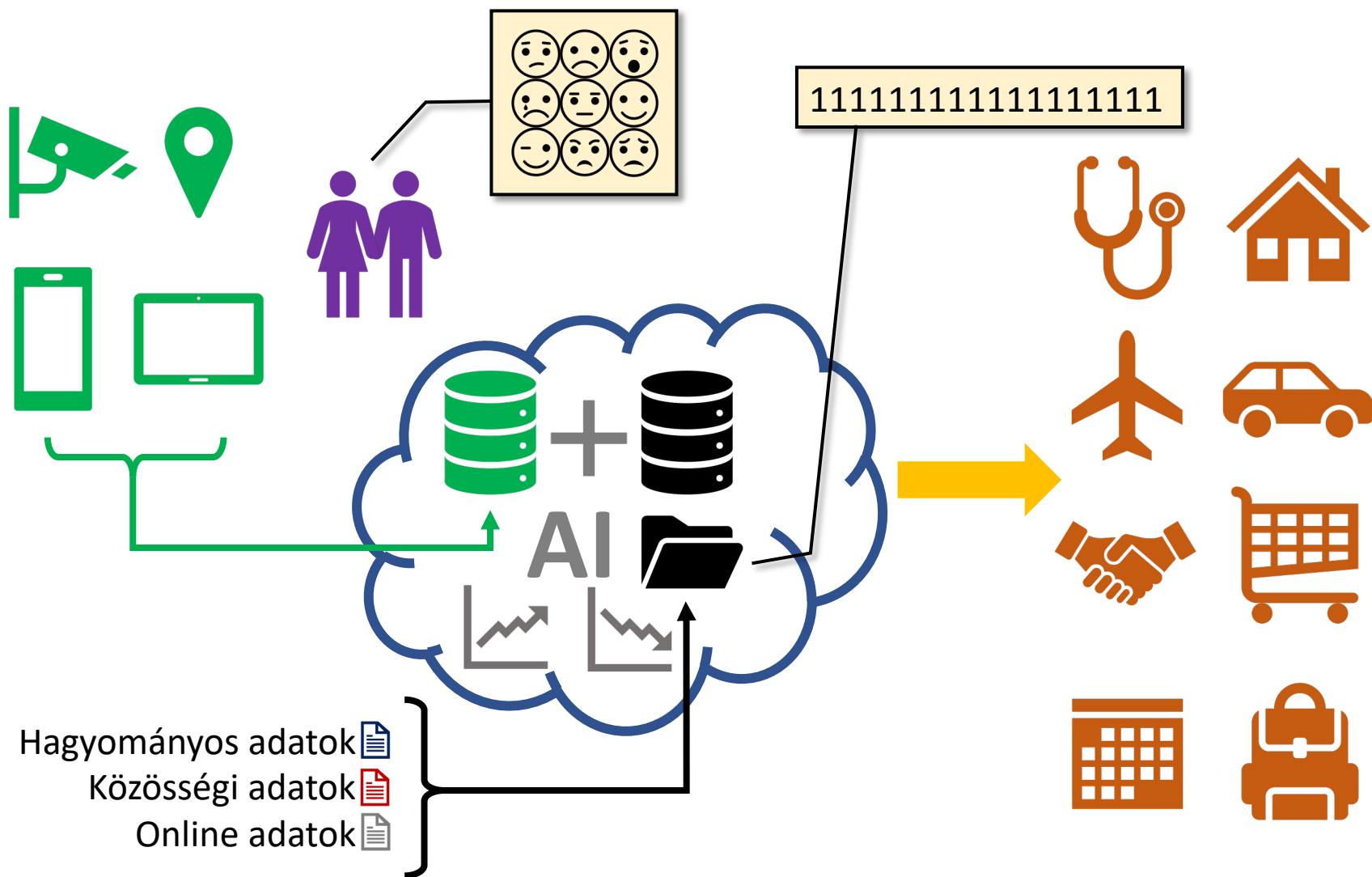
1. Nem nyújt semmilyen segítséget, mindent az ember csinál.
2. Teljes körű cselekvési alternatívákat kínál.
3. Leszűkíti a cselekvést néhány választási lehetőségre.
4. Egyetlen tevékenységet/műveletet végez.
5. Végrehajtja a műveletet, ha az ember jóváhagyja azt.
6. Mielőtt a műveletet végrehajtaná, lehetőséget ad az embernek, hogy azt megvétózza.
7. Automatikusan hajtja végre a műveletet, de erről feltétlenül tájékoztatja az embert.
8. A művelet automatikus végrehajtás után csak akkor tájékoztatja az embert, ha az kéri.
9. A művelet automatikus végrehajtása után csak akkor tájékoztatja az embert, ha ilyen döntést hoz.
10. Maga dönt el mindent, automatikusan működik, figyelmen kívül hagyva az embert.

A TÁRSADALMI KREDIT RENDSZERE

ALAPADATOK A TÁRSADALMI KREDIT RENDSZERÉRŐL

- Hivatalos bejelentés: 2014
- Bevezetés: 2020
- Polgárok száma: 1,3 milliárd fő
- Technológiák összekapcsolása
- Adatbázisok összekapcsolása
- Azonosítás: személyi igazolvány (azonosítószám) alapján
- Érintettség: egyének, vállalatok, intézmények
- Területek: politika, üzleti élet, társadalom, igazságszolgáltatás
- Fókuszterületek:
 - őszinteség a kormányzati ügyekben
 - üzleti becsületesség
 - társadalmi becsületesség
 - igazságügyi hitelesség
- Következmények:
 - jutalmak
 - büntetések

A TÁRSADALMI KREDIT RENDSZERÉNEK ALAPÁBRÁJA



ADATOK, BEMENETEK

 Jövedelemadó

 Kölcsön
visszafizetése

 Hitelkártya
számla

 Rezsiszámlák

 Perköltség
megfizetése

 Közlekedési szabályok
betartása

 Családtervezési
korlátok betartása

 Fizetés a
tömegközlekedésért

 Becsületesség

 Önkéntesség

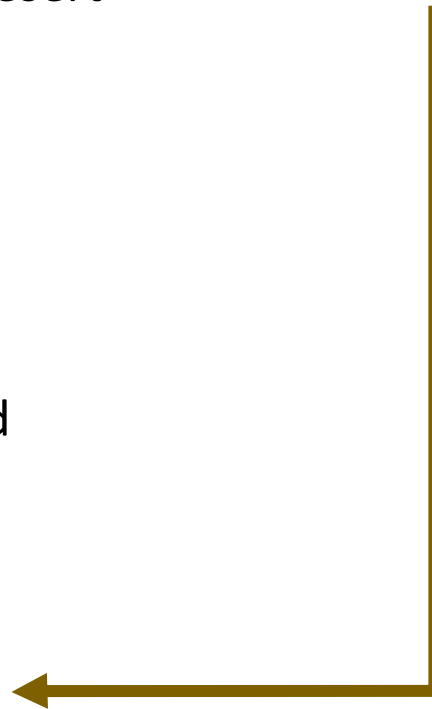
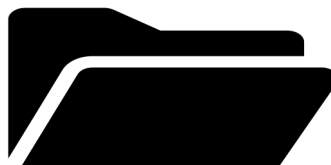
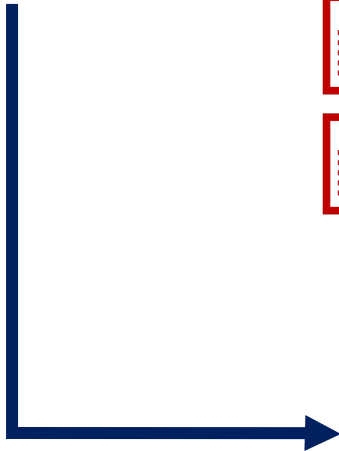
 Jó szülő

 Bűnözési rekord

 Kapcsolat a többi
internet-felhasználóval

 Online közzétett hírek
megbízhatósága

 Vásárlási szokások



JÓGYEREK VS. ROSSZGYEREK



DIFFERENCIÁLT ELBÍRÁLÁS

- Egészségügyi ellátás
- Várólista helyezés
- Utazás (lehetősége, VIP)
- Munkakeresés
- Vállalkozás indítása
- Lakásbérlés
- Ingó- és ingatlanvásárlás
- Hitelfelvétel, hitelképesség
- Gyerek tanulása/továbbtanulása
- Kedvezményes lehetőségek

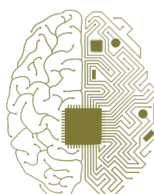
A TKR INFORMATIKAI HÁTTERE

KAPCSOLÓDÓ TECHNOLÓGIÁK ÉS ALKALMAZÁSOK



(I)IoT és szenzor

0110101
1101010
1101010
BDA



Mesterséges
intelligencia



Mobil



Biztonság(i kamerák)



Felhő alapú
számítástechnika



Társadalmi
Kredit
Rendszere

YOUKU 优酷
世界都在看

Alibaba Group
阿里巴巴集团

微博
weibo.com

Baidu 百度

Közösségi média,
regisztrációhoz kötött oldalak



Vezetékes és vezeték-
nélküli hálózatok



GPS
GIS, GPS



AR, VR, MR

KORMÁNYZATI SZÁNDÉK

A kormány törekvése informatikai eszközökkel és megoldásokkal

- az állam és a társadalom irányítása
- horizontális és vertikális információmegosztás
- a protekcionizmus felszámolása
- a papíralapon levő adatok digitalizálása

ELSŐ LÉPÉS

Minden állampolgár és vállalkozás azonosítható legyen

- egyedi azonosítás (18-digites kód az állampolgároknak) lehetővé tétele minden szükséges helyzetben/helyen
- a beazonosítás nélküli működés (életvitel) lehetetlenné tétele (avatarok, anonim digitális részvétel tiltása)

Adatbázisok összekapcsolásának megtervezése

- hivatalok adatbázisai
- mobiltelefonszám és -előfizetés
- közösségi média
- online szolgáltatások
- biometrikus azonosítás

MÁSODIK LÉPÉS

- Olyan adatbázisok létrehozása, amelyek tartalma az egyedi azonosító alapján összekapcsolható
- Baidu (nem anonim) keresőtalálatainak elemzése, ezeknek az adatbázisok a hozzákapcsolása a többi adatbázishoz

HARMADIK LÉPÉS

- Tárolt adatok és információk feldolgozása és felhasználása
 - Big data elemzés
 - Korrelációszámítás
 - Regressziószámítás
 - Klasszifikáció (osztályozás)
 - Klaszteranalízis (valószínűségszámítás alapján egyének csoportokba sorolása)
 - Szociometria, hálózatkutatás
- Algoritmusok használata
- Feketelisták működésének a fejlesztése

NEGYPEDIK LÉPÉS: HIBAJAVÍTÁS, VÉDEKEZÉS FEJLESZTÉSE

1. Visszaélés az egyén arcával, az arc módosítása, takarása
2. Visszaélés az egyén adataival és eszközeivel
3. Egyén illetéktelen követése
4. Hibásan működő szenzorok és aktuátorok
5. Rendszerelemek közötti kommunikációs hiba
6. Adatbázis – struktúrahiba
7. Adatbázisok összekapcsolási hibája
8. Rossz, hibás adatelemzés és algoritmusok
9. Gépi tanulási hibák
10. A mesterséges intelligencia hibái
11. Hivatalnokok és informatikusok (szándékos) károkozása
12. Hackerek támadása
13. Külföldi gyártók és a mögöttük álló titkosszolgálatok

A TKR INFORMÁCIÓBIZTONSÁGI KIHÍVÁSAI

1. VISSZAÉLÉS AZ EGYÉN ARCÁVAL AZ ARC MÓDOSÍTÁSA, TAKARÁSA



2. VISSZAÉLÉS AZ EGYÉN ADATAIVAL ÉS ESZKÖZEIVEL

- Aktuális kedv (lelki állapot)
- Aktuális tartózkodási hely
- Alvási szokások
- Antropometriai jellemzők
- Arc, arcvonások
- Belépés/kilépés ideje
- Családi állapot
- Email cím
- Fizetési/pénzhasználati szokások
- Fizikai cím (lakcím, tartózkodási hely)
- Hanghordozás, beszédstílus
- Közösségi oldalakon ismerősök, aktivitások, posztolások, lájkolások, megosztások
- Kulturális fogyasztás
- Lakcím
- Médiafogyasztási szokások
- Munkahely(ek)
- Név
- Nyelvismeret és egyéb ismeretek
- Rokonok, ismerősök (kapcsolati háló)
- Szociális készségek
- Szoftver- és alkalmazáshasználat (mit, mikor, mennyi ideig)
- Telefonszám
- Vásárlási szokások
- Végzettségek
- Viselkedés

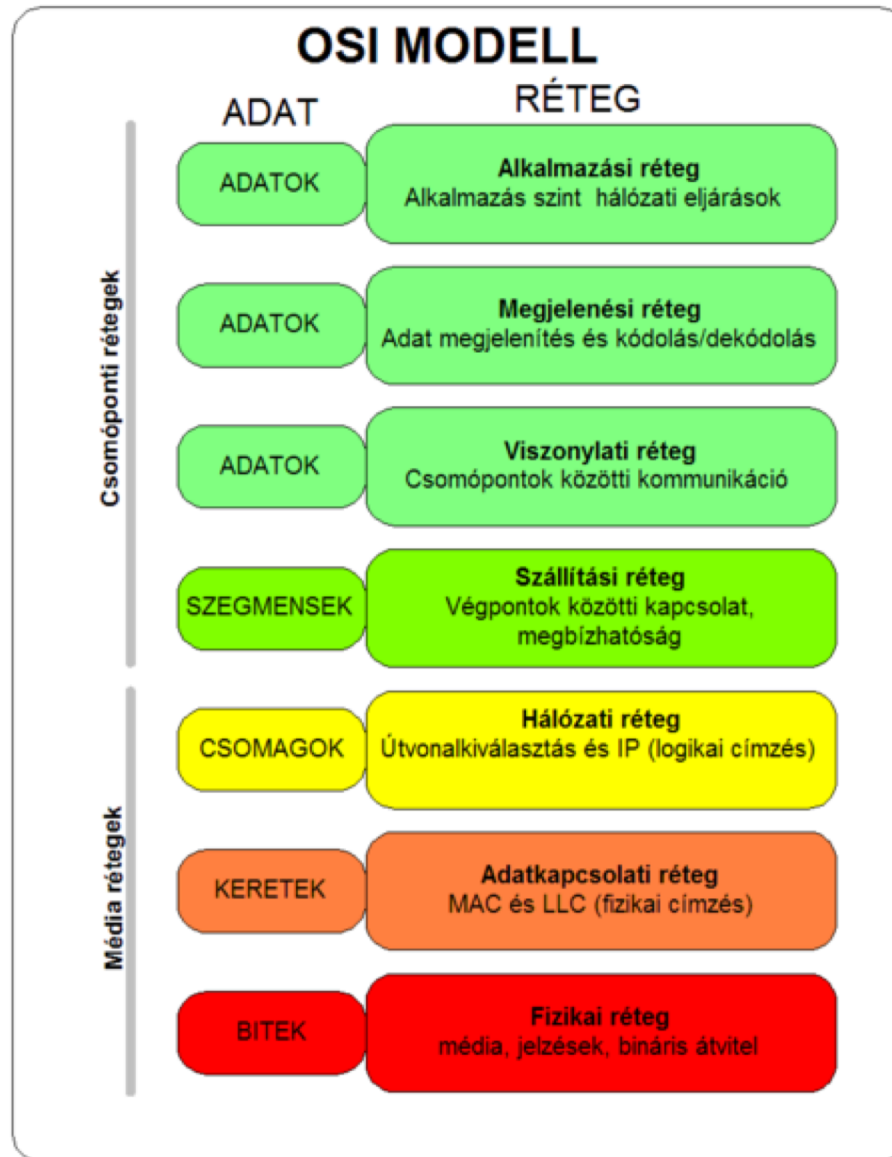
3. EGYÉN ILLETÉKTELEN KÖVETÉSE



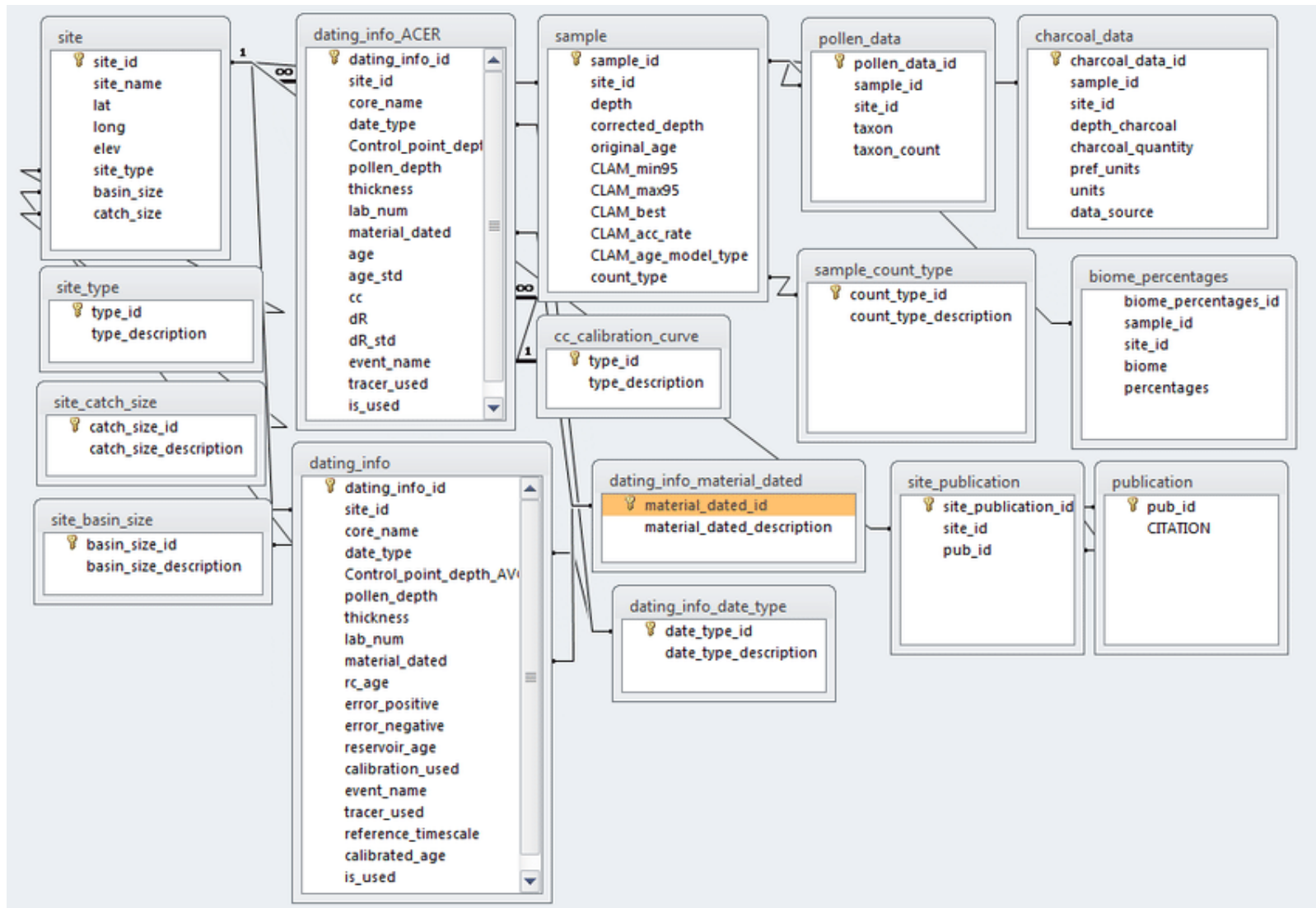
4. HIBÁSAN MŰKÖDŐ SZENZOROK ÉS AKTUÁTOROK

 joystick XY摇杆	 Flame 火焰传感器	 RGB LED 3色灯模块	 Heartbrat 手指测心跳	 Light Cup 魔术光杯	 Hall magnatic 霍尔磁力
 Relay 继电器	 Linear Hall 线性霍尔	 SMD RGB 3色RGB	 7 color flash 7彩闪烁	 Tilt switch 水银开关	 TEMP 18B20
 Big sound 高感应声音	 Touch 人体触摸	 Two-color LED 双色LED	 Laser emit 激光发射	 Ball switch 倾斜开关	 Analog temp 模拟温度
 Small sound 小麦克风	 Digital temp 数字温度	 Two-color 小双色	 Button 按键开关	 Photoresistor 光线	 IR emission 红外发射
 Tracking 循迹	 buzzer 有源蜂鸣器	 Reed switch 磁簧开关	 Shock 震动开关	 Temp and humidity 温湿度	 IR receiver 红外接收
 Avoid 避障	 passive buzzer 无源蜂鸣器	 Mini Reed 迷你磁簧	 Rotary encoders 旋转编码器	 Analog Hall 模拟霍尔	 Tap module 敲击模块 Light blocking 光遮断

5. RENDSZERELEMEK KÖZÖTTI KOMMUNIKÁCIÓS HIBA



6. ADATBÁZIS – STRUKTÚRAHIBA



7. ADATBÁZISOK ÖSSZEKAPCSOLÁSI HIBÁJA



8. ROSSZ, HIBÁS ADATELEMZÉS ÉS ALGORITMUSOK

$$\mu_1^2 = \mu_{\bar{y}_1 - \bar{y}_2}^2 = \frac{2,168 + 12,648}{5+7-2} \left(\frac{1}{5} + \frac{1}{7} \right) = 0,$$

$$\mu_2^2 = \mu_{\bar{y}_1 - \bar{y}_3}^2 = \frac{2,168 + 7,8}{5+9-2} \left(\frac{1}{5} + \frac{1}{9} \right) = 0,$$

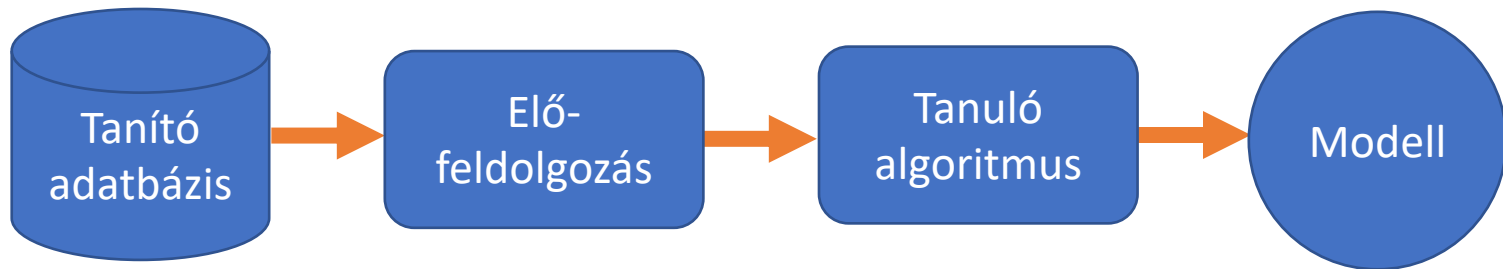
$$\mu_3^2 = \mu_{\bar{y}_2 - \bar{y}_3}^2 = \frac{12,648 + 7,8}{7+9-2} \left(\frac{1}{7} + \frac{1}{9} \right) = 0,$$

$$\mu_1 = 0,71 \quad \mu_2 = 0,508 \quad \mu_3 = 0,508$$

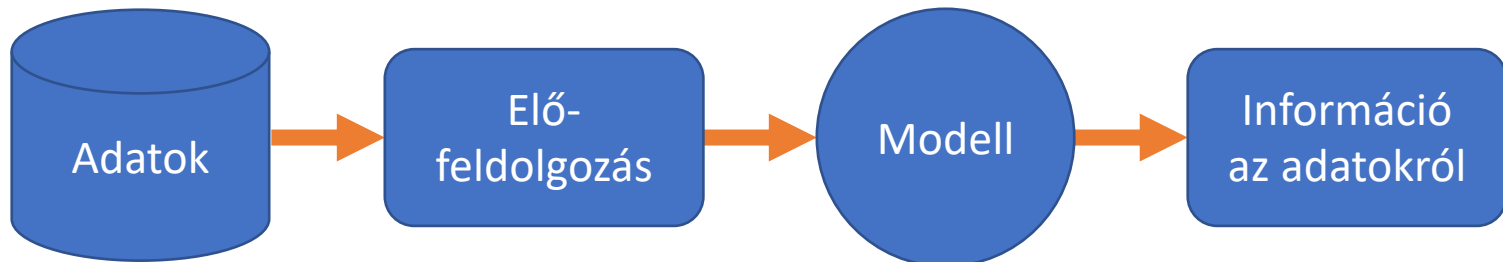
9. GÉPI TANULÁSI HIBÁK

Tanulás

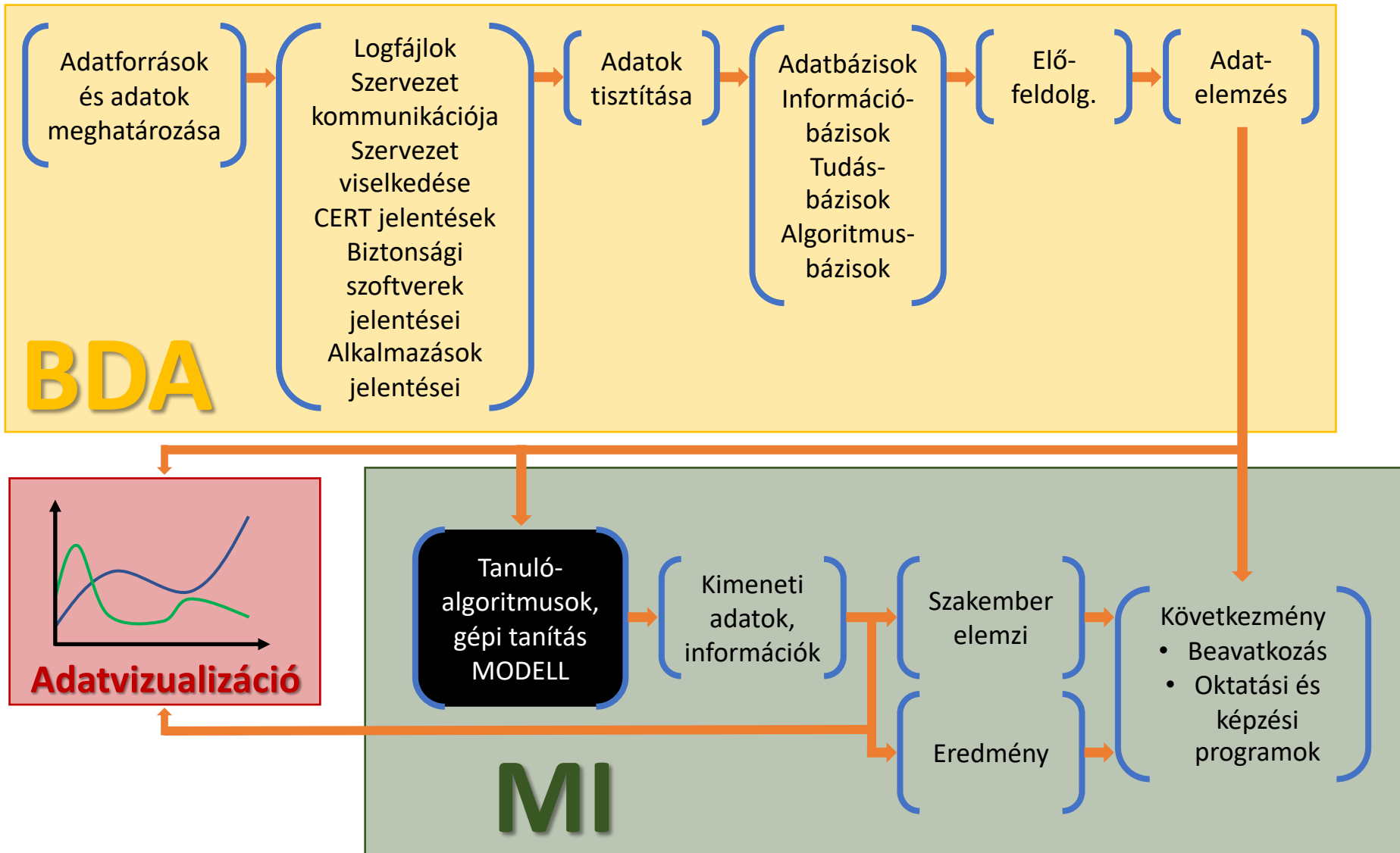
(felügyelt, nem felügyelt, visszacsatolósos, félig felügyelt...)



Felhasználás



10. A MESTERSÉGES INTELLIGENCIA HIBÁI



11. HIVATALNOKOK ÉS INFORMATIKUSOK (SZÁNDÉKOS) KÁROKOZÁSA



12. HACKEREK TÁMADÁSA



13. KÜLFÖLDI GYÁRTÓK ÉS A MÖGÖTTÜK ÁLLÓ TITKOSSZOLGÁLATOK



A TKR GAZDASÁGI ÉS TÁRSADALMI HATÁSAI

POZITÍV HATÁS

- Féken tartja az illegális magatartást, segítheti az egyének és a vállalatok gazdasági megbízhatóságát
- Hozzájárul a társadalmilag és környezetileg felelősségteljes új magatartás kialakításához (nevelés)
- A vállalatok transzparens működésének támogatása
- Az üzleti partnerek jobb megítélése
- Meglevő gazdasági statisztikák jóságának növelése
- A big data elemzések új vállalati lehetőségeket teremtenek
- Megéri „jógyereknek” lenni

NEGATÍV HATÁS

- Nem kiforrott még a technológia és a minősítő rendszer sem, nagy a kockázata a téves értékelésnek
- Folyamatosan nagyon sok adatot kezel a rendszer
 - adatszivárgás révén illetéktelenek kezébe kerülhetnek titkos és személyes adatok
 - nő az adatlopás esélye
 - adatvesztés hatalmas gazdasági károkat okozhat
- Az állam és a vállalatok mindent tudhatnak az emberről
- Megszűnik a magánszféra
- Az üzleti élet szereplői – ha nem képesek betartani a szabályokat – ellehetetlenedhetnek
- Mivel az állam az adatokhoz korlátlanul férhet hozzá, a hivatalnokok a számukra nem szimpatikus egyént/vállalatot ellehetetleníthetik
- Kína üzleti tevékenysége kiszámíthatatlanná válik

NEMZETKÖZI HATÁS

- A nemzetközi vállalatok – hogy elkerüljék a büntetést – megpróbálnak beilleszkedni a rendszerbe
- Adatmegosztás révén a kínai vásárlók adatai külföldre kerülhetnek
- Kína a rendszer révén hozzáférhetne a külföldi vállalatok csúcstechnológiai adataihoz (know-how)

A társadalmi kredit rendszere kiváló exportcikk (nem csak) az olyan országok számára, amelyeknél fontos a gazdaság állami irányításának megerősítése.

A TÁRSADALMI KREDIT MEGJELENÉSE EURÓPÁBAN

Egyesült Királyság

- 2018 New Economics Foundation összehasonlítása a kínai és az angol rendszerekről
- Adatok: polgári kredit pontszám, telefonhasználat, bérleti díj
- Adatok felhasználása: munkaköri alkalmazások szűrése, szociális szolgáltatások igénybevétele, személyre szabott reklámok

Németország

- 2018 február Handelsblatt Global beszámolója
- Lassú közeledés a kínai társadalmi kredit rendszeréhez hasonló rendszer kiépítéséhez
- Adatok: egyetemes hitelminősítő rendszer, földrajzi helyek, egészségügyi nyilvántartások
- Adatok felhasználása: hitelbírálat, egészségbiztosításhoz való hozzáférés



Kitekintés a jövőbe*

*Future Today Institute, Gartner, PREMA, ÓE BGI MIM

A MESTERSÉGES INTELLIGENCIA JÖVŐJE 1.

- Az MI mindenhol megjelenik, köszönhetően a mobileszközökbe integrált MI platformoknak
- A műszaki-informatikai fejlesztések mellett egyre nagyobb hangsúlyt kap az MI etikai és humán oldala
- Az MI lényegesen hatékonyabbá fogja tenni a munkafolyamatokat
- Az MI segítségünkre lesz, hogy a dolgokat jobban csináljuk
- Az MI révén az életünk kényelmesebbé válik
- Szakmák eltűnése, új szakmák születése
- Együtt fogunk dolgozni az MI-ra épülő megoldásokkal

A MESTERSÉGES INTELLIGENCIA JÖVŐJE 2.

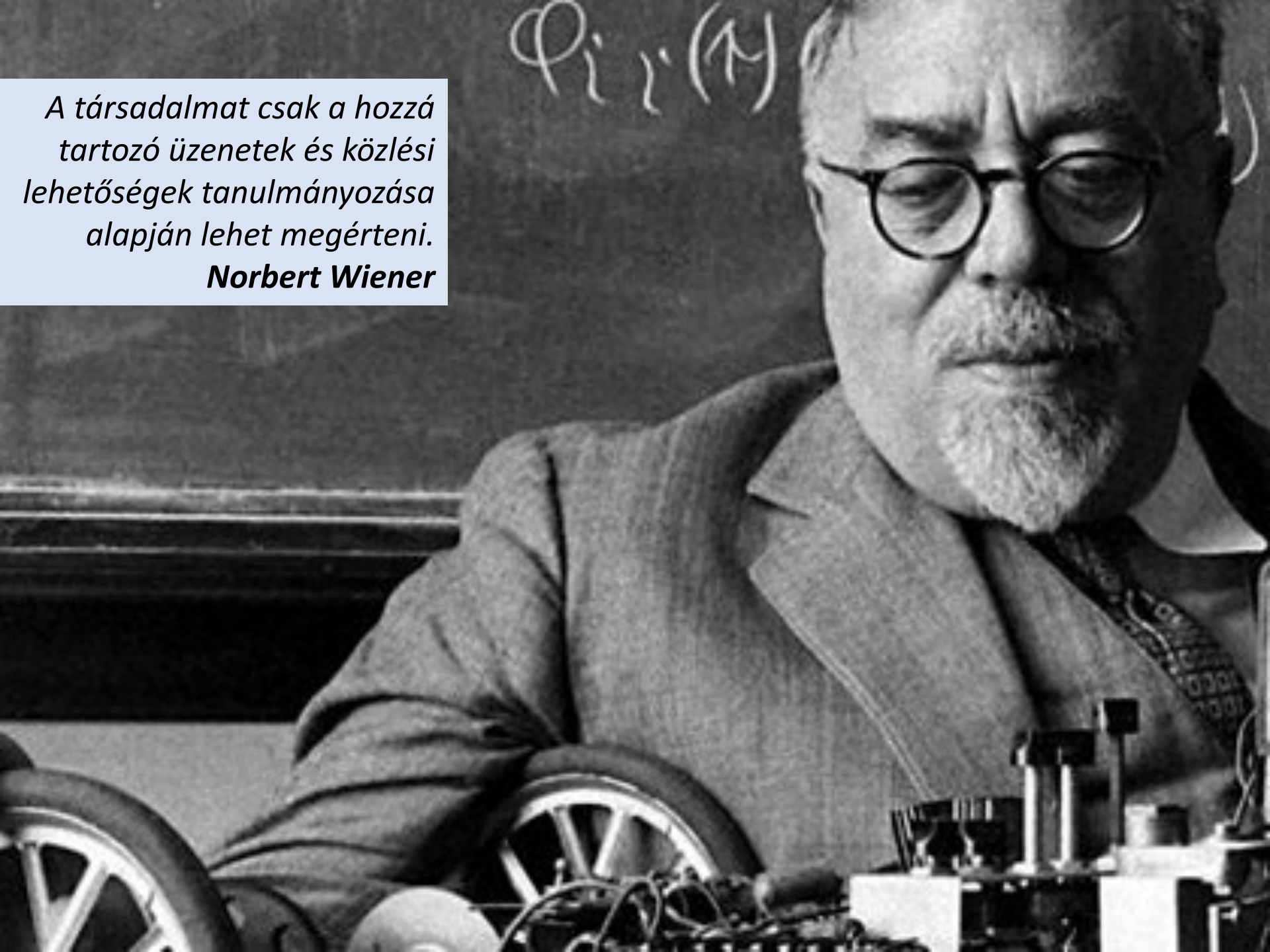
- A veszélyes munkaterületeken az MI-ra épülő megoldások helyettesítik az embert
- Egyre nagyon hangsúlyt kap az MI-vel kapcsolatos informatikai rendszerek védelme
- Új hibajavító algoritmusok fejlesztése
- Megbízható emberek kiválasztása és alkalmazása a hibás mesterséges intelligencia döntéseinek vizsgálatára, elemzésére, módosítására, felülírására
- Új társadalmi gondolkodás megjelenése
- Új törvények elfogadása

A TKR JÖVŐJE

1. Részleteiben szinte minden országban megjelenik
2. Nagyobb hangsúlyt kap az informatikai rendszerek védelme
3. Új hibajavító algoritmusok
4. Megbízható emberek kiválasztása és alkalmazása a hibás mesterséges intelligencia döntéseinek vizsgálatára, elemzésére, módosítására, felülírására
5. Társadalmi értékrend átalakulása és diverzifikálódása (elfogadás, elutasítás, nomádok, egyéni szabadságharcosok, kiskapuk keresése, must go zónák állami felügyelet mellett)
6. Új törvények

*A társadalmat csak a hozzá
tartozó üzenetek és közlési
lehetőségek tanulmányozása
alapján lehet megérteni.*

Norbert Wiener



KÖSZÖNÖM MEGTISZTELŐ FIGYELMÜKET!



Dr. Kollár Csaba PhD

Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

Óbudai Egyetem Biztonságtudományi Doktori Iskola

www.drkollar.hu | www.linkedin.com/in/drkollarcsaba | www.slideshare.net/drkollarcsaba

FELHASZNÁLT KÉPEK FORRÁSA

- <https://brofeed.com/wp-content/uploads/2017/12/810-768x512.jpeg>
- <https://artprojectsforkids.org/wp-content/uploads/2010/05/Outerspace-watercolor-1024x758.jpg>
- <https://i.ytimg.com/vi/LguXfHKsa0c/maxresdefault.jpg>
- https://electronics360.globalspec.com/images/assets/507/10507/11.30_Altoys__1_Anko.jpg
- <https://i.pinimg.com/originals/37/8a/45/378a454827542797eeb9b1372eb1411e.jpg>
- http://concretemedias.hu/wp-content/uploads/2020/01/koronavirus_tudogyulladas_mti_epa_fit_800x10000.jpg
- https://www.delnext.com/blog/wp-content/uploads/2017/02/delnext_blog_tracking-945x630.jpg
- <https://circuits-diy.com/wp-content/uploads/2019/10/212.jpg>
- https://upload.wikimedia.org/wikipedia/hu/thumb/2/20/OSI_mod_2.png/450px-OSI_mod_2.png
- <https://www.researchgate.net/publication/319631062/figure/fig1/AS:613912294735909@1523379505540/ACER-database-structure-in-ACCESS-format.png>
- <https://pixfeeds.com/images/topic/4144/1200-4144-databases-photo3.jpg>
- https://hbr.org/resources/images/article_assets/2014/12/dec14_15_159737162.jpg
- <https://www.brinknews.com/wp-content/uploads/2017/11/sing-office-111348812-1.jpg>
- https://www.total-croatia-news.com/media/k2/items/cache/e8e96c317c84e02199dced757fb971fb_XL.jpg
- <https://images.theconversation.com/files/150392/original/image-20161215-26062-4psy6l.jpg>
- <https://passionatedj.com/wp-content/uploads/2013/03/gypsy-fortune-teller.jpg>
- <https://www.brainpickings.org/2018/06/15/the-human-use-of-human-beings-norbert-wiener/>
- https://blog.talview.com/hs-fs/hubfs/ai_human_handshake-1.jpg?width=1800&name=ai_human_handshake-1.jpg

SZOLGÁLATI KÖZLEMÉNY

A prezentáció az Innovációs és Technológiai Minisztérium ÚNKP-19-3-I-OE-38 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.