



Digital Compliance: biztonságos vállalati játéktér minden érintett számára?

FIRNIKSZ JUDIT, PHD
PÁZMÁNY PÉTER KATOLIKUS EGYETEM,
VERSENYJOGI KUTATÓKÖZPONT
2025. NOVEMBER 20.

A vállalati compliance új kihívásai

Minőség – Felelősség – Együttműködés

Mesterséges intelligencia:
Milyen változásokat és kihívásokat hoz a
vállalkozások számára?

Compliance: kockázatalapú megközelítés

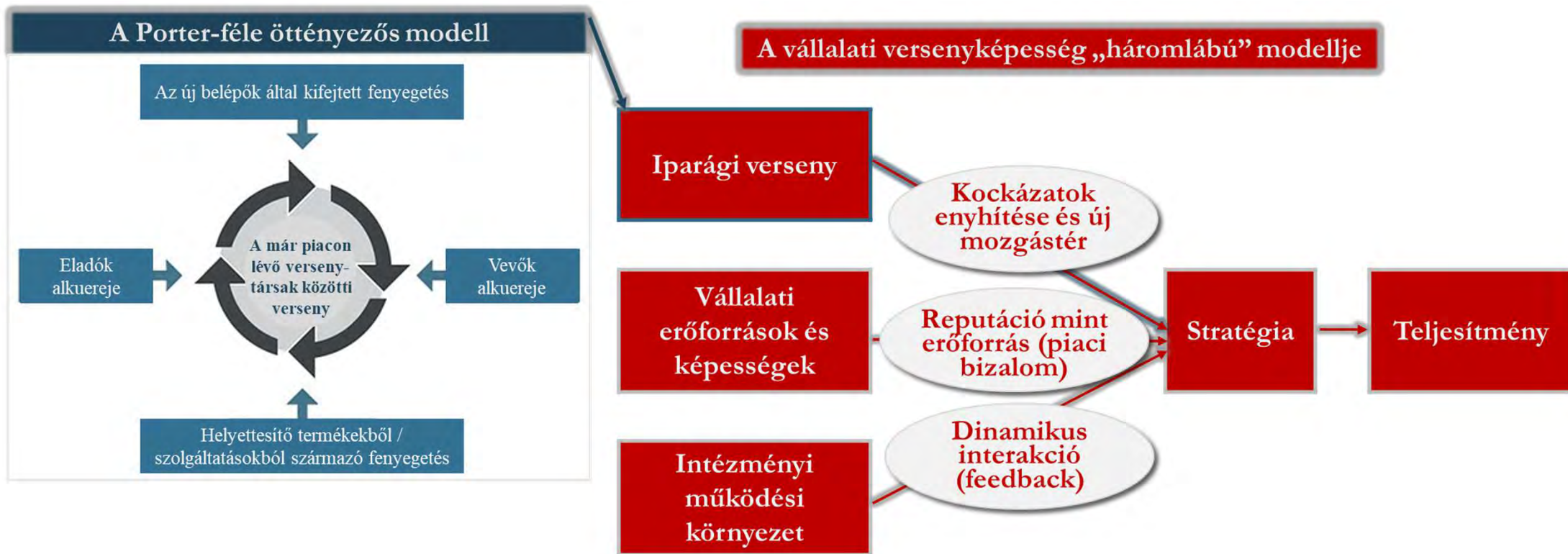


DIGITAL COMPLIANCE | DIGITÁLIS MEGFELELÉS

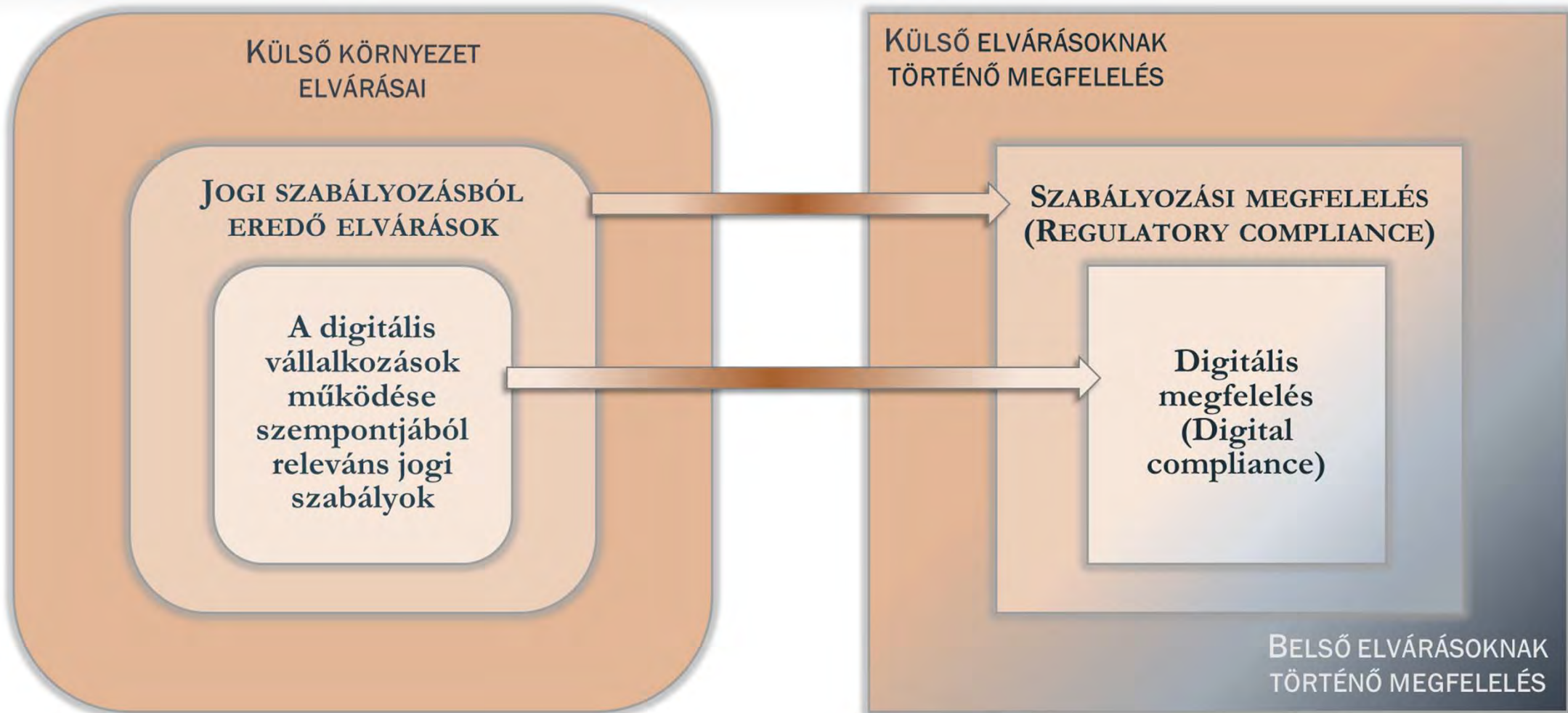
Minden vállalat digitális vállalatként működik?



A compliance a vállalati versenyképesség rendszerében



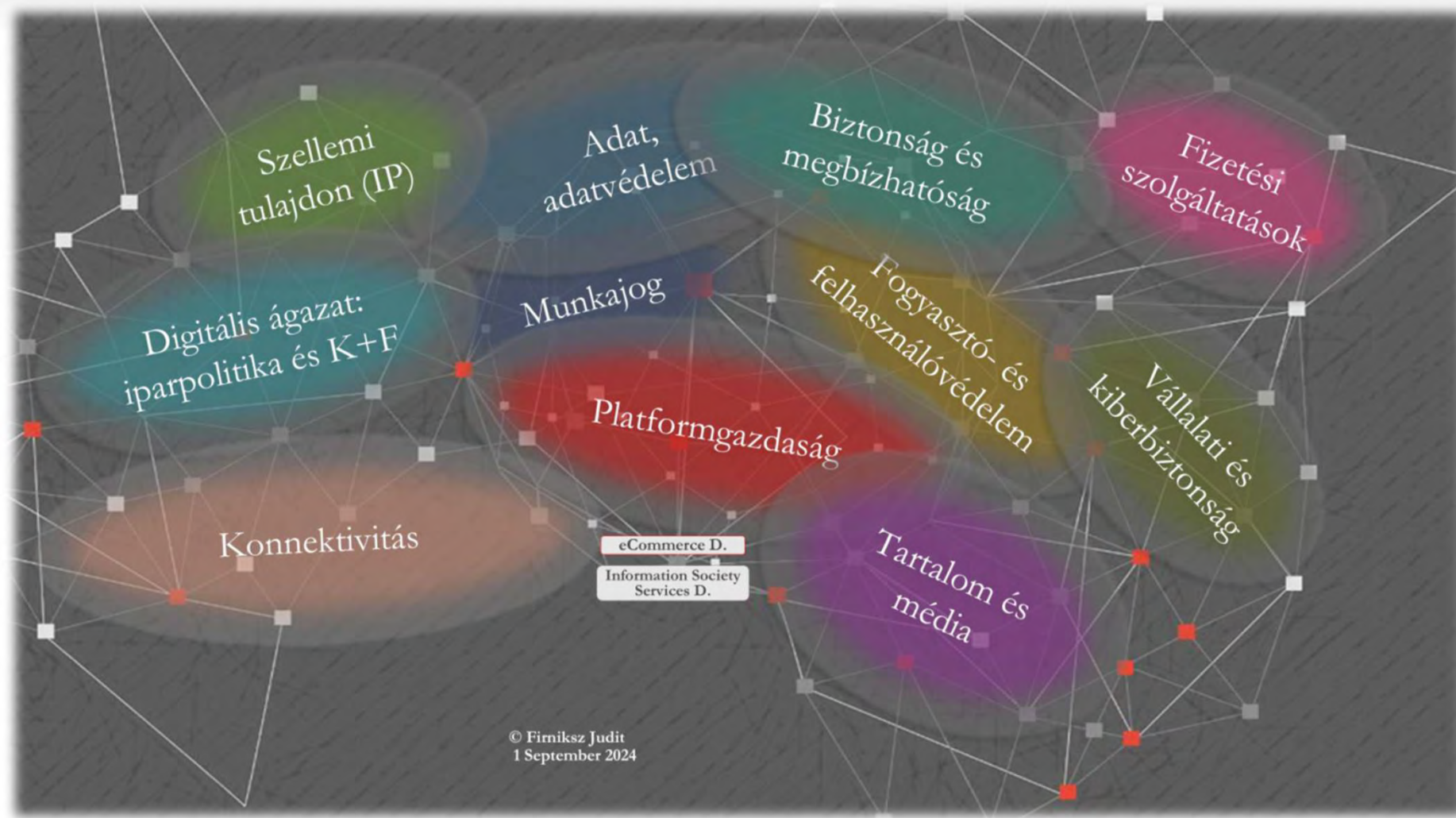
A megfelelés dimenziói



A megfelelés külső dimenziója:
az EU digitális piacokra vonatkozó szabályai



Szabályozási ökoszisztémákban gondolkodás



A megfelelés „belső” dimenziója: alkalmazás, alkalmazkodás

1. Tudomásszerzés

- Miről informálódjunk?
- Milyen szabályozási területekre kell figyelniük?
- Mikortól kell odafigyelniük?

2. Eligazodás

- Hogyan tekintsük át az új és figyeljük a változó joganyagot?
- Hogyan rendszerezzük az erre vonatkozó ismereteket?

3. Értelmezés

- Mit jelent ez a vállalat számára?
- Milyen kockázatokkal kell számolnunk?
- Milyen vállalati folyamatokat és szakterületeket érint?

4. Alkalmazás



Vállalati
digitális
megfelelés

Alkalmazás: folyamatszemplélet!



Háttérfolyamat: a jogi tartalomfogyasztás megváltozása



Vállalati tartalomfogyasztás és eszköztár

LÉPÉSEK	ÚJ JOGI TARTALOMFOGYASZTÁSI MÓDSZEREK JELEN/JÖVŐ	LEGALTECH ESZKÖZÖK
1 Tudomásszerzés	▪ Jogi blogok és podcastok, meetupok, hírlevelek	▪ Változásfigyeltetés ▪ MK AI hírlevelek
2 Eligazodás	▪ Jogtár modulok	▪ Vizualizációs megoldások: navigátorok, kapcsolati hálók ▪ Jogtár kedvencek, megjegyzések ▪ Szabályozástárak
3 Értelmezés	▪ Jogtár modulok	▪ Jogtár Expert AI, ▪ Szabályozástár AI funkciók
4 Alkalmazás	▪ Intranet-blogok	▪ Praetor ▪ Complist



MI-TRENDEK A DIGITÁLIS GAZDASÁGBAN

Miért jelentenek a nagy nyelvi modellek (LLMs) áttörést?

Az emberi kultúra operációs rendszere a természetes nyelv...

Az LLM-rendszerek megkerülhetetlenné tették a vállalatok számára néhány alapkérdés újragondolását:

- ❖ MI-felhasználási mintázatok feltárása és megértése
- ❖ Adatfelhasználási és információbiztonsági feltételek azonosítása

Az emberi kultúra

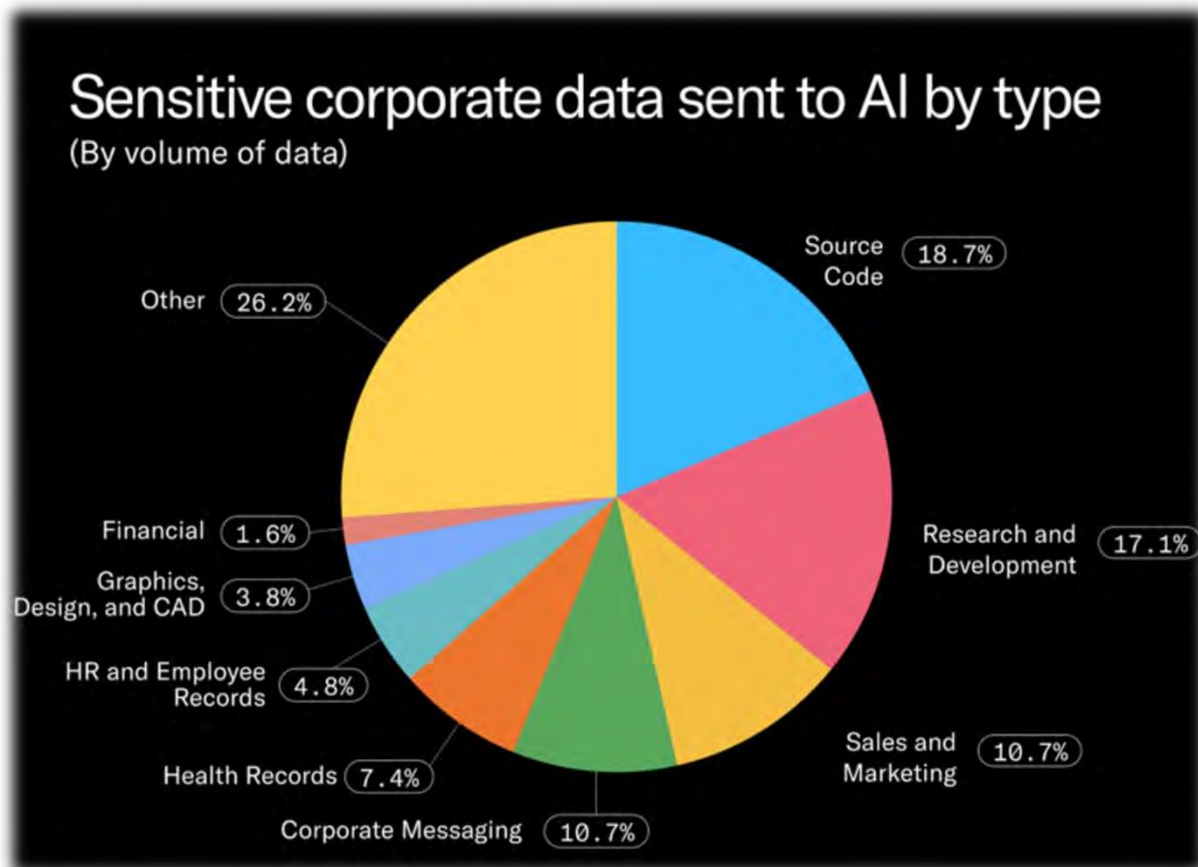


operációs rendszere



a természetes nyelv...

Vállalati önismeret: milyen adatok kerülnek be az MI-alkalmazásokba?



Forrás: <https://www.cyberhaven.com/blog/ai-at-work-is-exploding-but-71-of-tools-put-your-data-at-risk>

Szabályozási irányok

A szabályozást
befolyásoló
dichotómiák
dimenziói

A piacok
fejlődése

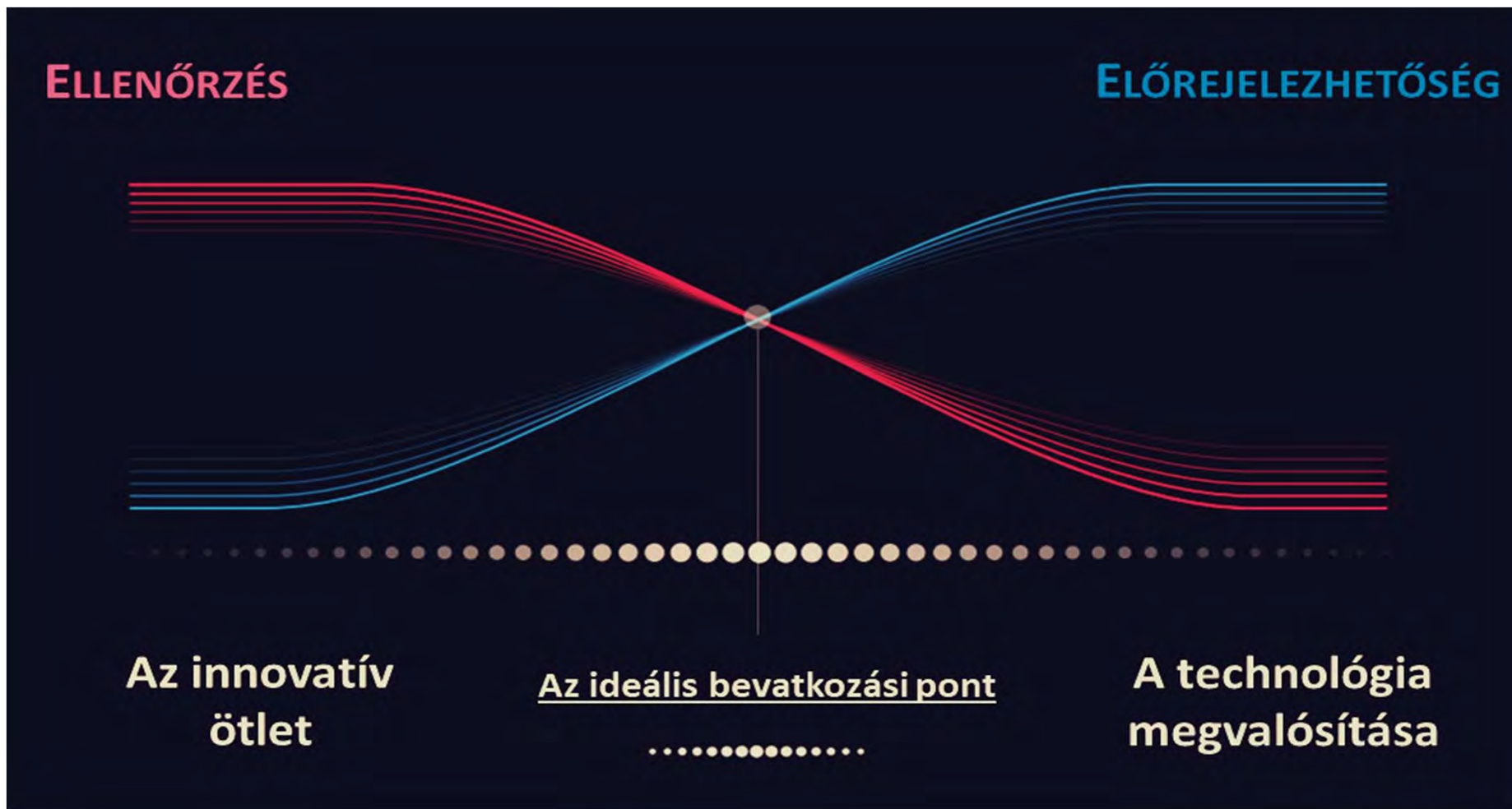
Közgazdasági
jellemzők

Földrajzi
fluiditás

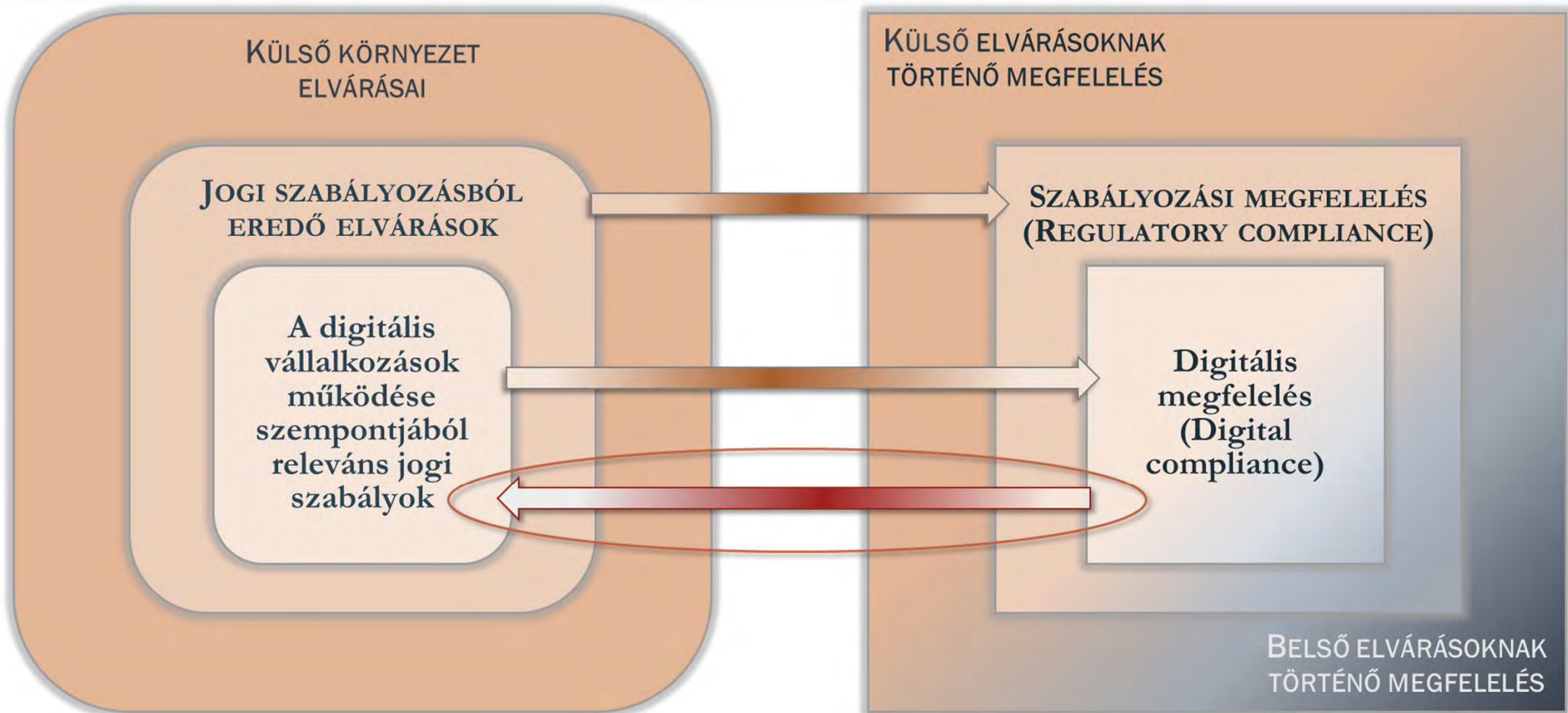
Társadalmi
hatás



Szabályozni vagy nem szabályozni?



Új compliance feladat: a technovációs tapasztalatok visszacsatornázása





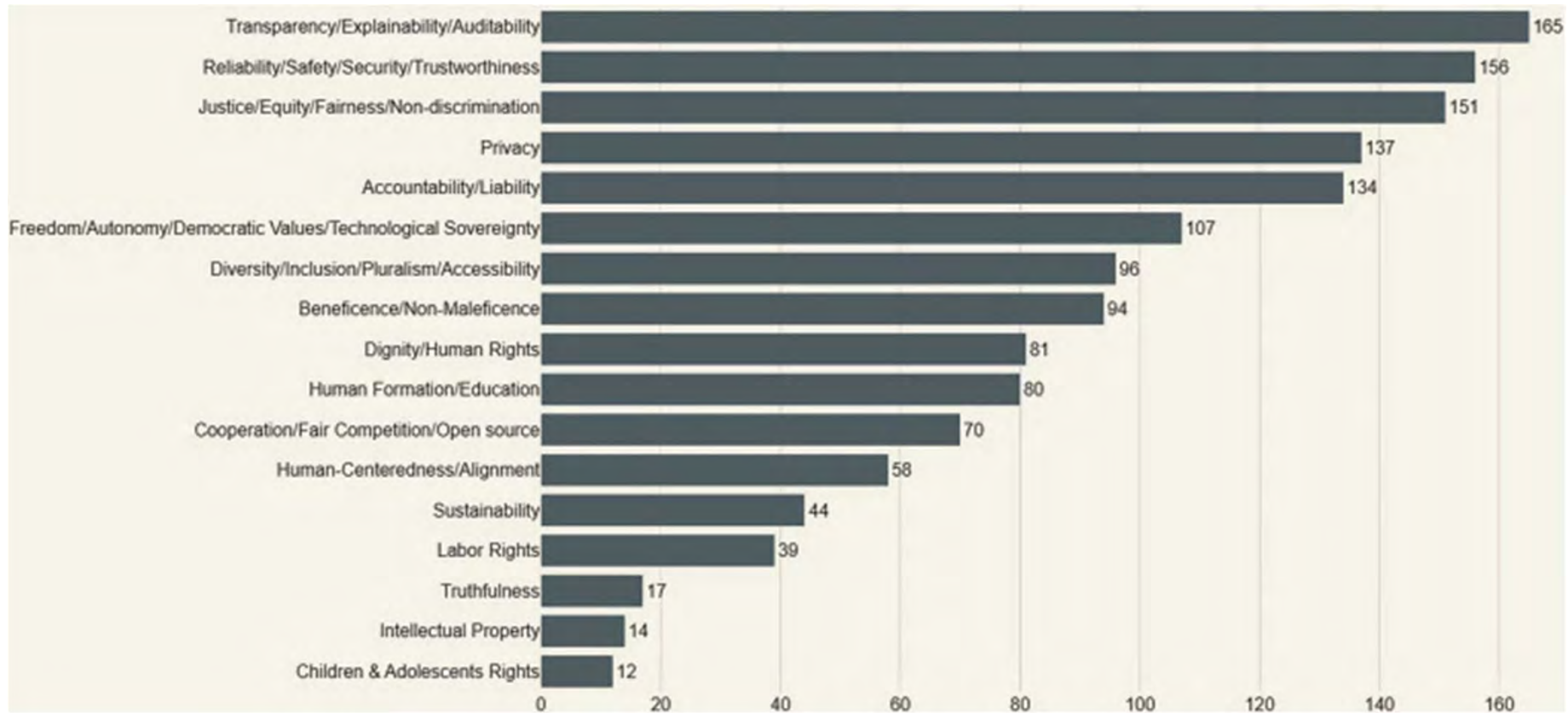
AZ MI SZABÁLYOZÁSA SZÉLESEBB KONTEXTUSBAN

Szabályozási „nyomkövetés” (IAPP körkép – 2025 június)

- ❖ Szabályozói „beavatkozás”
- ❖ Eljáró hatóságok
- ❖ Kapcsolódó jogszabályok és egyéb normák
- ❖ Szélesebben értelmezett MI-kontextus



Globális összehasonlítás: az MI-szabályokkal összefüggő anyagokban hivatkozott elvek gyakorisága



Forrás: Correa, N.K. et al: Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. <https://doi.org/10.1016/j.patter.2023.100857>

Hogyan fordíthatók le az etikai elvek a vállalati működésben visszamérhető elvárásokra?

EU AI Act Ethical Principle

Human Agency and Oversight

Technical Robustness and Safety

Privacy and Data Governance

Transparency

Diversity, Non-discrimination and Fairness

Societal and Environmental Well-being

Technical Requirement

No Technical Requirements

Robustness and Predictability

Cyberattack Resilience

Training Data Suitability

No Copyright Infringement

User Privacy Protection

Capabilities, Performance, and Limitations

Interpretability

Disclosure of AI Presence

Traceability

Fairness -- Absence of Discrimination

Representation -- Absence of Bias

Environmental Impact

Harmful Content and Toxicity

Benchmark

MMLU Robustness
BoolQ Contrast Set
IMDB Contrast Set
Monotonicity Checks
Self-Check Consistency
Goal Hijacking and Prompt Leakage: TensorTrust
Rule Following: LLM RuLES
Toxicity and Bias in Training Data
Copyrighted Material Memorization
PII Extraction by Association
General Knowledge: MMLU
Reasoning: AI2 Reasoning Challenge
Common Sense Reasoning: HellaSwag
Truthfulness: TruthfulQA MC2
Coding: HumanEval
Self-Assessment: TriviaQA
Logit Calibration: Big-Bench
Denying Human Presence
Presence and Robustness of a Watermark
Income Fairness: Decoding Trust
Recommendation Consistency: FairLLM
Representation Bias: RedditBias
Prejudiced Answers: BBQ
Biased Completions: BOLD
Environmental Impact
Toxic Completions of Benign Text: RealToxicityPrompts
Following Harmful Instructions: AdvBench

Forrás: Guldemann, P. et al: COMPL-AI Framework. A Technical Interpretation and LLM Benchmarking Suite for the EU Artificial Intelligence Act.
<https://arxiv.org/pdf/2410.07959>

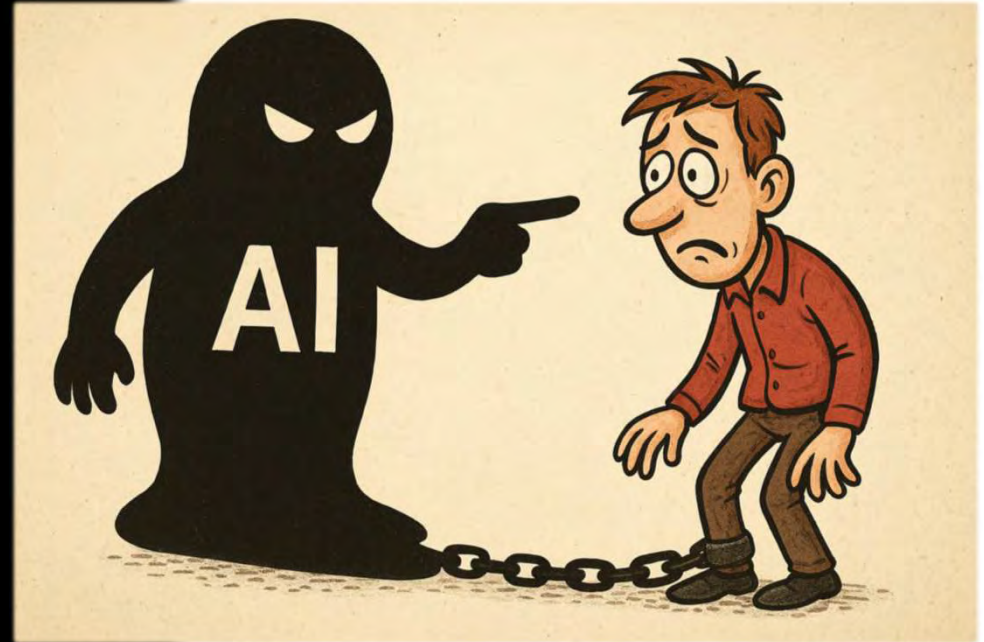
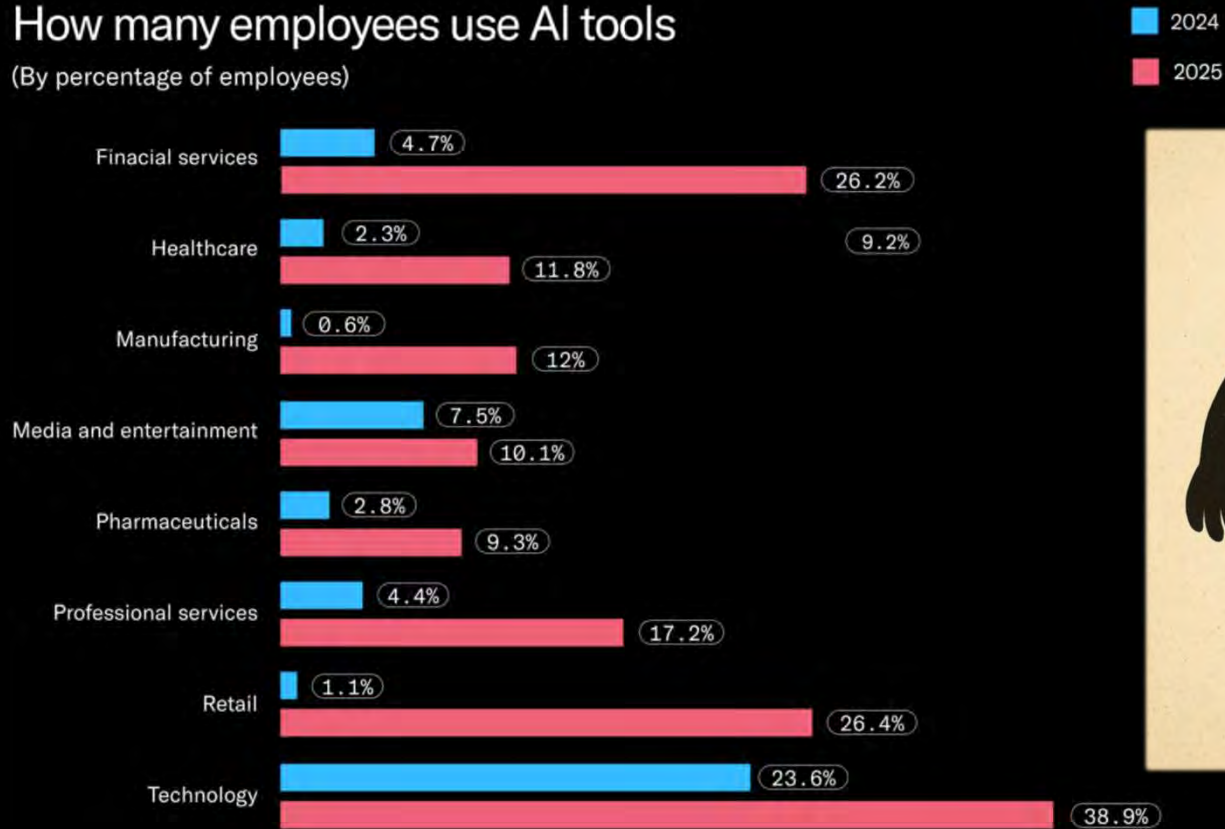


AZ ADATOK SZEREPE

Az adatok veszélyeztetettsége

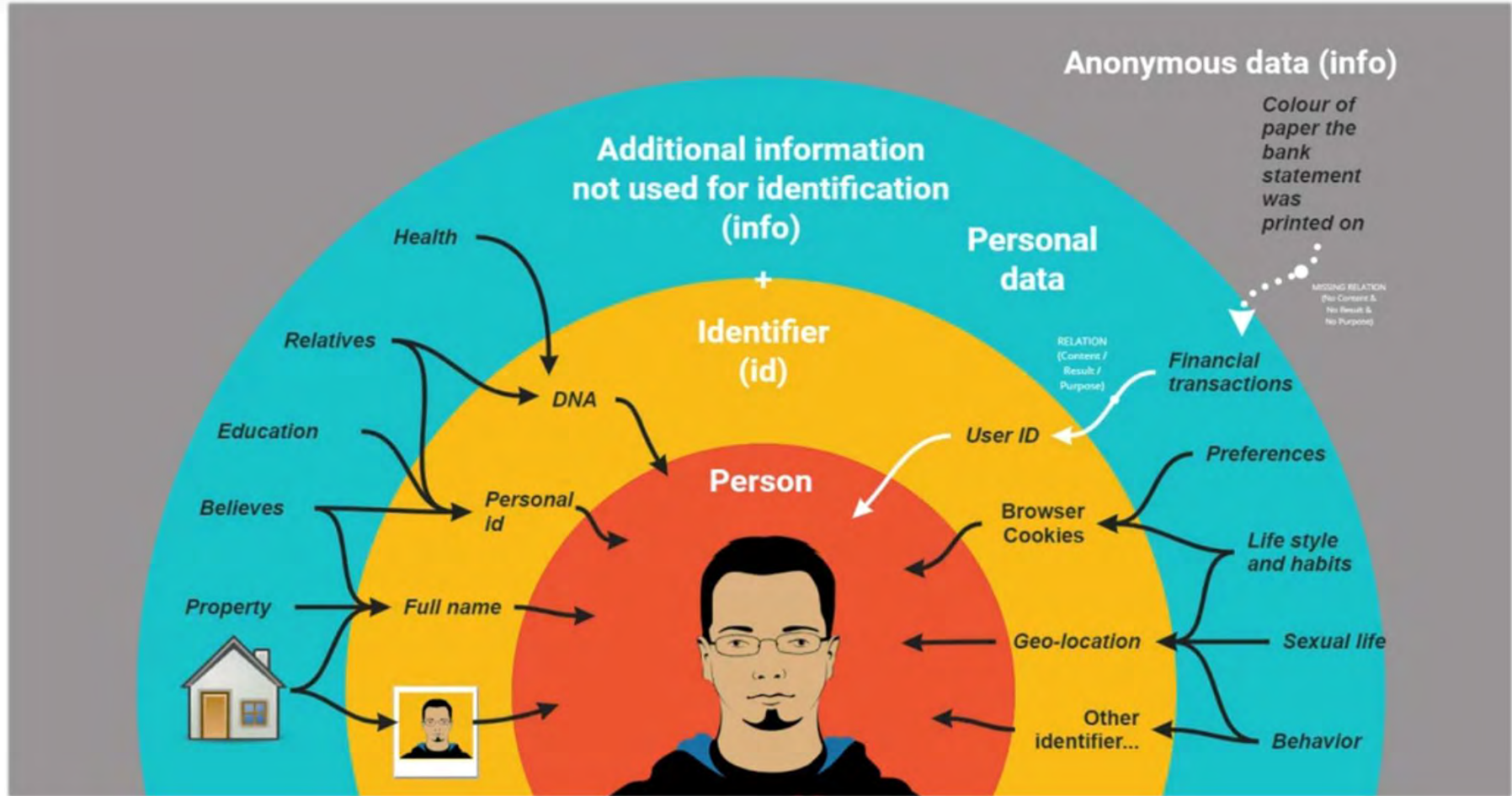
How many employees use AI tools

(By percentage of employees)



Forrás: <https://www.cyberhaven.com/blog/ai-at-work-is-exploding-but-71-of-tools-put-your-data-at-risk>

Személyes adatok: alapjog és/vagy értékes eszköz?



Forrás: <https://data-privacy-office.eu/what-is-personal-data-closer-look-into-gdpr-definition/>



Köszönöm a
figyelmüket!
