euro one

U.S. COMMERCIAL SERVICE
United States of America Department of Commerce

Cyber Summit Budapest 2025

Legal Traps in AI

Éva Kerecsen dr. LLM

Managing Partner – Lawit Legal

Hewlett Packard Enterprise

NETWITNESS

paloalto NETWORKS

TREND MICRO

Legal Traps in AI

What Every Company Needs to Know

Éva Kerecsen dr. LLM

law it
LEGAL SERVICES
EST. 2019

“AI told me to do it.”
Sounds ridiculous?
Not in 2025.

AI Risk Isn't Always Where You Expect

Special attention to the high-risk layer (conformity assessment, certifying etc.)

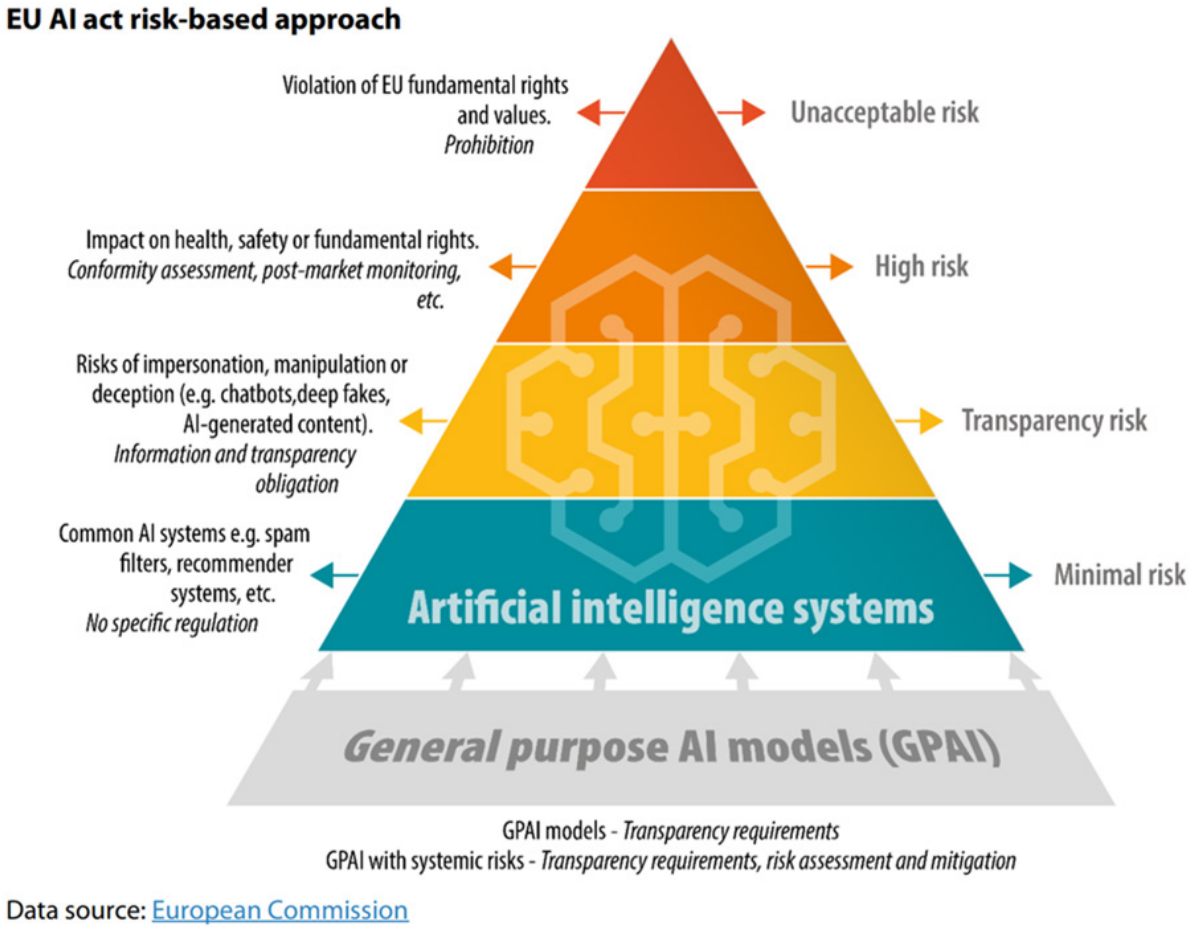
But some AI systems are just… **talking**

Minimal Transparency

Still cause real-world harm:

- Dangerous suggestions
- Hallucination
- Misinformation

Strict Product Liability?



Data source: European Commission

AI Systems Fall Under the New EU Product Liability Directive

1. **New Technology, Same Liability**
   AI systems + software are treated like traditional products.
   If defective and harmful → **strict liability** applies

2. **Wider Scope of Compensable Damage**
   Covers not only death, injury, and property damage, but also **medically certified psychological harm** (e.g. AI-driven emotional distress).

3. **Black-Box Presumption**
   If the provider can't explain how or why the system caused harm, courts may **presume defectiveness and causation**.

AI Defamation Can Cause Psychological Harm

“Turley case”:

“False accusations, reputational harm, emotional damage — caused by a product on the market.”

Under EU product liability rules, when an AI system causes harm, it’s treated like any other defective product — regardless of whether it’s made of code or metal.

AI Misrepresentation Triggers Corporate Liability

"Air Canada Voucher Case"

When your AI gives wrong instructions, it's not just a glitch — it's your liability.

In this case, it was a refund. Next time, it could be thousands in free tickets.

AI Impersonation of Expertise Creates Legal Risk

“DoNotPay case”:

The moment your AI acts like a licensed expert — you’re on the hook for its mistakes.

Presenting it as professional creates professional-level responsibility.

DoNotPay

Copyright infringement with AI

- **AI Training Needs Data — Publicly available ≠ Public domain**

- **Copyright protection**
  - Original works: texts, images, photos, videos, music, code, articles, designs, etc.
  - Protected regardless of whether they are publicly available online.
- **Sui generis database protection (EU)**
  - Database structures that required substantial investment in obtaining, verifying or presenting the data.
  - Protection applies even if the individual data points are not protected.

- **Key point:**
  - Using protected content for AI training may require licenses or fall under limited exceptions.

Scraping Third-Party Content: A Costly Shortcut?

Using protected datasets without proper rights — even at startup or internal development stage — can lead to costly copyright and database disputes.

AI Use and Data Leaks: Business Secrets at Risk

Sensitive company data often feeds AI tools:

- internal emails
- salary structures
- financial models
- product roadmaps
- client contracts

The Risk:

If AI tools store data for further training or processing, business secrets may leak — even violating NDAs or trade secret protections.

Preventing Data Leaks in AI Usage

Safe vs risky scenarios:

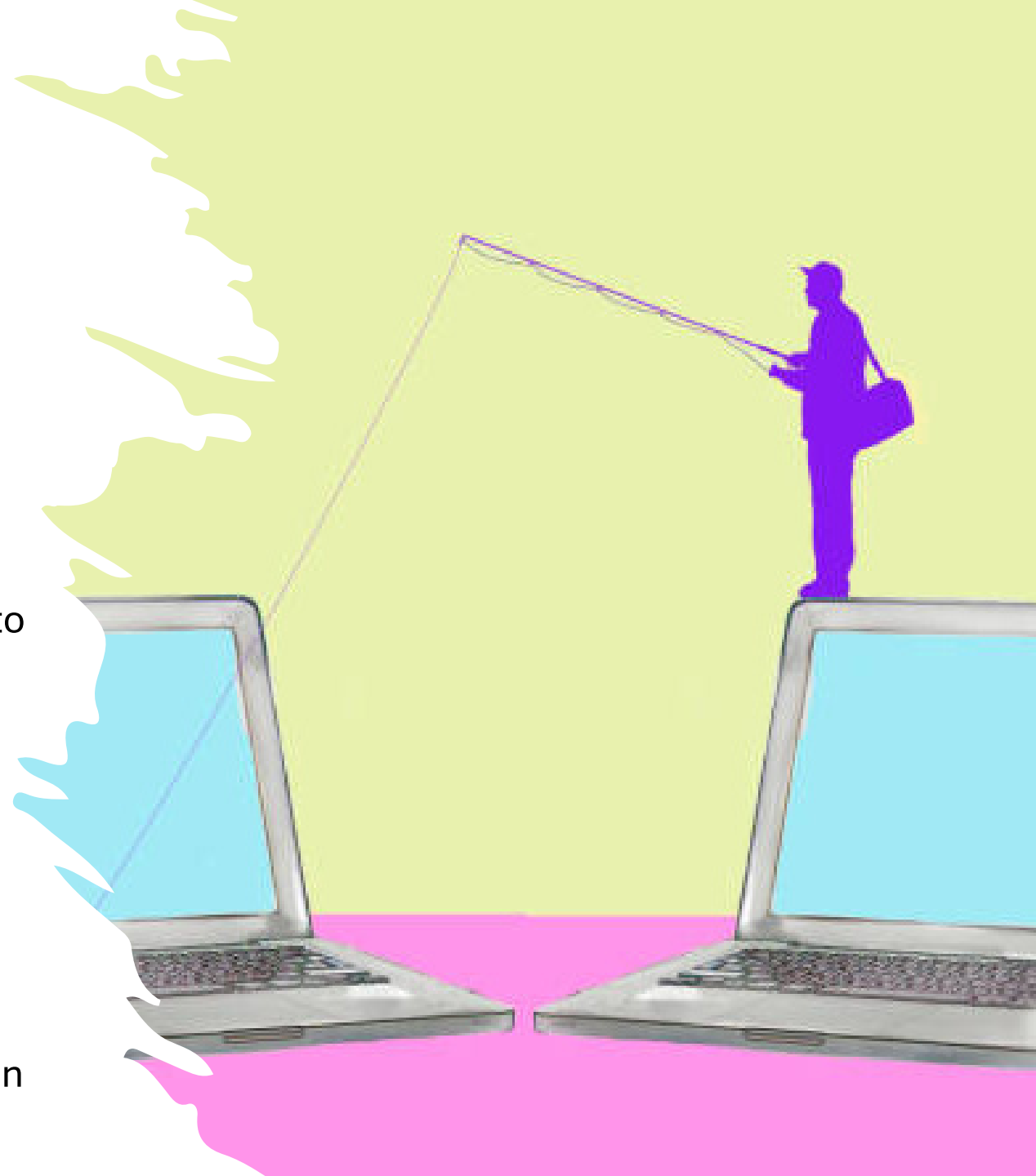
✅ Copilot for Microsoft 365 (Enterprise), ChatGPT Teams: enterprise-level isolation, no training on customer prompts

❌ Personal/free AI accounts: potential data exposure to provider's model training or 3rd parties

Key takeaway:

Internal AI policies must clearly regulate:

- which AI tools are approved
- which data may be shared
- how employees should handle confidential information



Best Practices to Minimize AI Risk

1) **Visibility & Inventory**
Maintain a clear overview of all AI tools in use (AI Tool Repository).

2) Risk Classification
Assess and classify AI systems based on:

- EU AI Act risk levels.
- Internal business risks (e.g. pricing decisions = high risk even if not high-risk under AI Act).

3) Contractual Safeguards
Include proper liability allocation and limitation clauses depending on your role

- AI developer → limit liability.
- AI user/client → ensure sufficient vendor accountability.

4) AI Usage Policy
Clear internal guidelines:

- What is allowed? Vs What is restricted or prohibited?

5)AI Awareness & Training
Regular training to ensure employees understand risks, rules, and responsible AI use.

Let’s continue!

+36 20 665 5442

eva.kerecsen@lawit.hu

www.lawit.hu

www.linkedin.com/in/eva-kerecsen/

SCAN ME