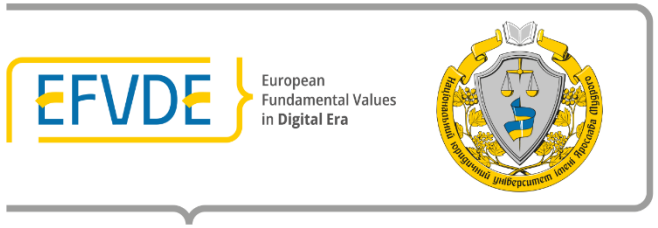
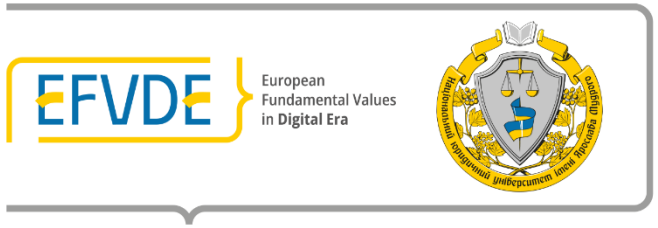


Європейські фундаментальні цінності у цифрову еру,
Центр Досконалості Жана Моне

101085385 - EFVDE - ERASMUS-JMO 2022-HEI-TCH-RSCH

Annual conferences materials

The Jean Monnet Center of Excellence European Fundamental Values in Digital Era, 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.



Європейські фундаментальні цінності у цифрову еру,
Центр Досконалості Жана Моне

101085385 - EFVDE - ERASMUS-JMO 2022-HEI-TCH-RSCH

EFVDE Project Presentation

Yulia Razmetaeva

Co-funded by the European Union

European Fundamental Values in Digital Era (EFVDE)

This project purports **to provide a European Fundamental Values based framework for the issues shaped and brought about by digitalization in Ukraine**. For this purpose, the Interdisciplinary Research Hub on European Fundamental Values and Digitalization is established at Yaroslav Mudryi National Law University.
The project consists of three parts: research, educational (sharing) and policy-making.

ERASMUS-JMO-2022-HEI-TCH-RSCH
ERASMUS-JMO-2022-COE — Jean Monnet Actions in the field of Higher Education: Centres of Excellence
Project: 101085385 — EFVDE

EFVDE European Fundamental Values in Digital Era

Команда проекту EFVDE

Co-funded by the European Union

EFVDE European Fundamental Values in Digital Era

ЮЛІЯ РАЗМЄТАЄВА

НАТАЛІЯ ФІЛАТОВА-БІЛОУС

ПЕТРО СУХОРОЛЬСЬКИЙ

ТЕТЯНА ЦУВІНА

БОГДАН КАРНАУХ

Co-funded by the European Union

Комплексне регулювання

Digital Services Act (DSA), Regulation 2022/2065
Digital Markets Act (DMA), Regulation 2022/1925

Artificial Intelligence Act (a draft EU law)

General Data Protection Regulation (GDPR), Regulation 2016/679

“Технологічний” підхід

Підхід “м’якого права”
White Paper on Artificial Intelligence, Ethics Guidelines for Trustworthy AI and Policy and investment recommendations

EFVDE European Fundamental Values in Digital Era

EFVDE European Fundamentation Values in Digital Era

How artificial intelligence affects
justice and public power in terms of values

VII KHARKIV INTERNATIONAL LEGAL FORUM
Panel discussion
“AI, justice and public power”
26 and 27 September 2023

Yulia Razmetaeva

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

EFVDE European Fundamentation Values in Digital Era

Fundamental values

Human Rights
Democracy
Rule of Law

‘European AI [to be] grounded in our values and fundamental rights such as human dignity and privacy protection’.
(White Paper on Artificial Intelligence – A European Approach to Excellence and Trust’ COM(2020) 65 final)

‘The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail’.
(Consolidated Version of the Treaty on European Union [2008] OJ C115/13, art 2)

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

Human rights and justice

(1) how AI affects fundamental human rights may affect the ideal of human rights in general through the erosion of value bases
(2) AI can attack individual rights in overt and covert manners

Alrogithmic content moderation example
Biometric data example
AIs pre-emptive power example

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

Principles of justice

Embedding them into AI:

- to chose the concept (How? By whom?)
- to describe for machine
- to apply to an unlimited range of cases

The problem of biased humans and biased AIs

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

Can we guarantee the AI that will be involved when applying justice will really understand the law and interpret the law properly?

the speed of text processing and the accuracy of data extraction (+)

machines understand what they ‘read’ (?)

interpret the facts in the light of an infinite number of contexts (?)

justify the decision in such a way as to convince others of its fairness (?)

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

Public and private dynamics

(1) difficult to control, get deployed before it is clear what hazardous long-term consequences
(2) obscurity and incomprehensibility for the general public
(3) private ownership of algorithms, their parts or entire AI systems

→ dependence of the public sector on private actors who create, modify, adjust and maintain algorithm

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

EFVDE European Fundamentation Values in Digital Era

Legitimacy of AI

‘Wait – I did not vote for that algorithm – and it’s already telling me what is just and what not!’

Gradual
Imperceptible
Profound

The requirements for institutions that people consider legitimate have been crystallising over centuries (checks and balances, e.g.)

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

EFVDE European Fundamentation Values in Digital Era

Conclusions

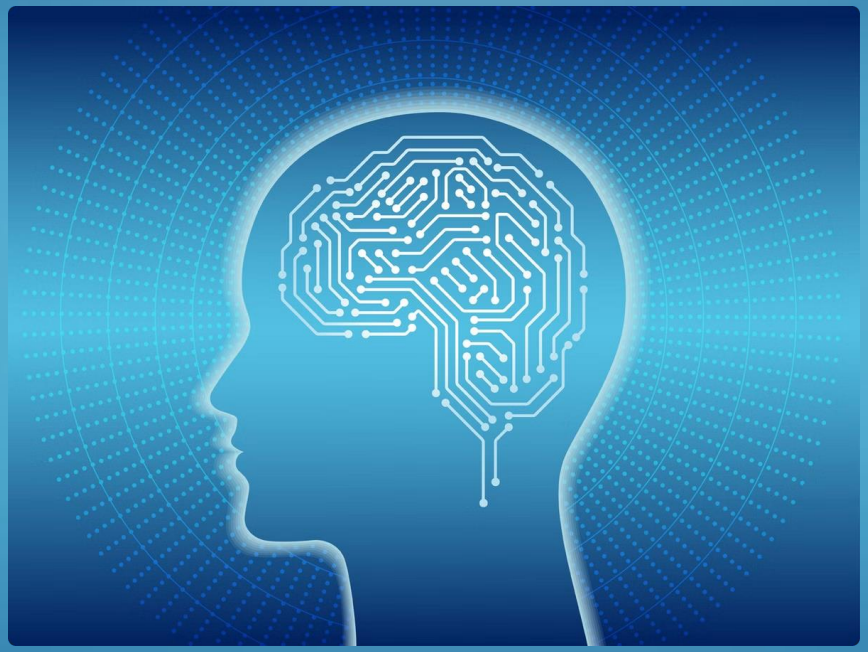
The threats posed by AI do not – and can not – mean we need to abandon AI altogether. All in all, it can create a lot of benefits (efficiency, safety, reducing human errors, etc).

At the same time, it is necessary to take into account that we are not discussing some hypothetical distant future any more, but we consider the future knowing that AI already occupies a significant part of the current life of people and societies.

Co-funded by the European Union

yu.s.razmetaeva@nlu.edu.ua
cledt@nlu.edu.ua

Limitations of AI Transparency



by dr. Gintarė Samuolė
Mykolas Romeris University

Agenda

1 **Global Regulatory Landscape**

Examining the diverse regulatory aspects governing AI their impact on implementation.

2 **Object and Purpose of Transparency**

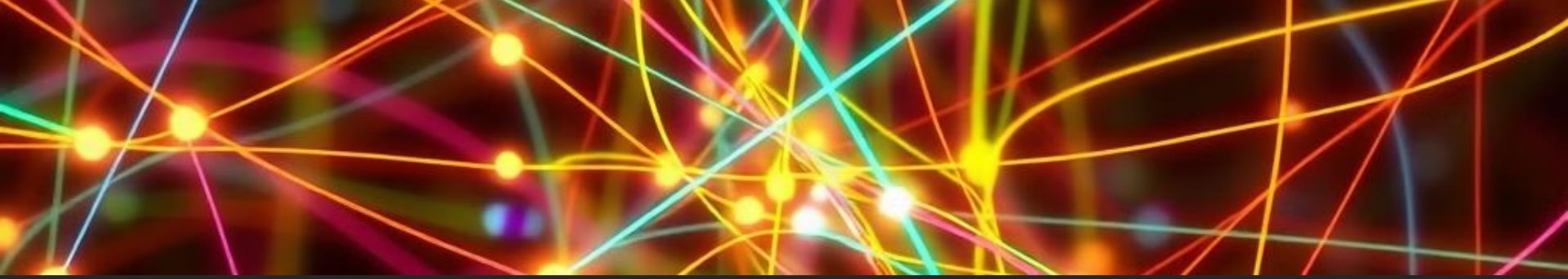
Analyzing the underlying goals, objectives, and concepts driving the driving the pursuit of transparency in AI systems.

3 **AI Transparency Limitations**

Exploring the constraints that limit the scope of AI transparency measures.

4 **Reflections**

Concluding thoughts and insights



The Problem

Complexity and Opacity

AI systems are characterized by intricate algorithms, often making it difficult it difficult to understand their decision-making processes.

Opportunities and Risks

AI has the potential for tremendous benefits but also poses significant risks significant risks that need to be mitigated through transparency.

Balance and Sustainability

Striking a balance between transparency and innovation is crucial to foster a to foster a sustainable AI ecosystem.

EU and AI transparency limitations

How balanced is EU's AI transparency framework to address evolving evolving challenges?

Global Regulatory Landscape of AI

Diversity in Approaches

Global AI regulations vary widely, showcasing different priorities and methods for achieving transparency. transparency.

Micro and Macro Sustainability Sustainability

Examining the effectiveness of transparency measures at both the individual system and the broader ecosystem levels.

Beyond Governmental Transparency

Exploring the unique aspects of AI transparency compared to traditional traditional public sector transparency transparency models.

Object and Purpose of AI Transparency

1

Lack of Subjective Right

Current laws do not formally recognize a subjective right to AI transparency, highlighting the need for further legal development.

2

International Efforts

States and international organizations are actively seeking to address AI transparency issues on a first come – first serve basis

3

Evolving Concept

AI transparency is a dynamic and evolving concept, requiring continuous adaptation to the changing landscape of AI technologies.

4

National Policies

National policies often integrate AI transparency objectives with broader public sector transparency goals, promoting openness in decision-making.

5

EU AI Act

The EU AI Act defines transparency in terms of traceability, explainability, and informing users about their interactions with AI systems.

Object and Purpose (2)

1

Making AI Visible

AI transparency aims to enhance understanding of how AI systems operate, including their decision-making processes, data usage, and potential impacts.

2

Strategic Goal Enhancer

Transparency serves as a crucial tool for regulators to achieve their strategic goals, such as promoting responsible innovation and protecting fundamental rights.

3

Human-Centric and Economic-Centric Goals

EU's AI transparency strategy seeks to balance human well-being and economic growth through responsible AI development.

4

Alternative - China's Strategic Goal

China emphasizes technological innovation aligned with national interest and human rights protection, integrating transparency into its national AI strategy.

5

Targeted Communication

Effective AI transparency requires tailoring communication channels and messages to different audiences, considering their knowledge and needs.

AI Transparency Limitations: principles

Commercial Interests	Principle of Minimum Intervention
AI Disclosure Duties	No Principle of Maximum Disclosure

AI Transparency Limitations: scope of disclosure duty

AI Identification

Transparency measures require clear identification of AI systems, including generative AI and chatbots, to inform users about their interactions. about their interactions.

AI Decision-Making

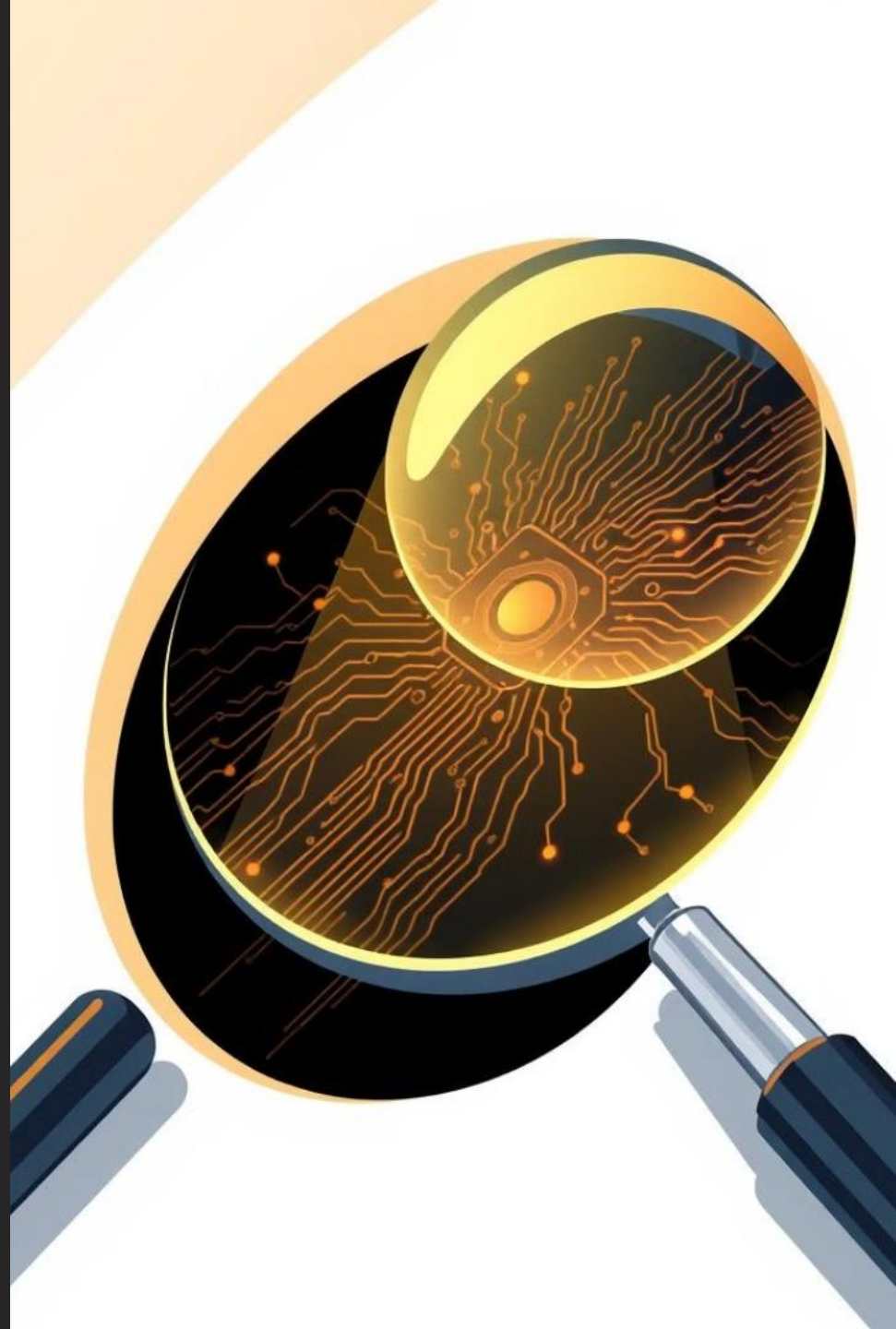
Users should be informed about the use of AI in decision-making processes, especially in regulated services, to understand interactions.

Provider Disclosure

Transparency includes disclosing details about the provider of the AI system, promoting accountability and understanding origins.

Logic, Instructions, and Rights

Transparency encompasses disclosing the logic behind AI algorithms, instructions for use, and users' rights and system.



AI Transparency Limitations: identification

1 Identification Duty: how?

Transparency measures include both implied and direct AI systems through disclaimers, warnings, labeling, acknowledgment.

2 Signals of AI Presence

AI systems can signal their presence through visual cues, verbal statements, and technical indicators, providing users with clear information about their interactions with AI.

3 "Average Consumer" Test

The effectiveness of transparency measures is evaluated "average consumer" test, ensuring that users understand the benefits of interacting with AI.

4 Content Generation and Attribution

Transparency raises questions about the relative importance of content content origin (who created it) versus content creation method (how it (how it was created).

AI Transparency Limitations

Risk-Based Disclosure

Higher-risk AI systems, including those posing systemic risks, require more disclosure, including information about the system's capabilities, conformity risk management, and human oversight.

Supervisory Authority Disclosure

Additional disclosure obligations for high-risk AI systems are primarily supervisory authorities to facilitate effective oversight.

Explanatory Duty

Revealing the identity of the AI system is sufficient for "reasonably understand the general risks and benefits, with more detailed disclosures left discretion of supervisory authorities.

Expert Disclosure

General-purpose AI model providers must provide proportional transparency including documentation and information for downstream deployers.

Full Transparency Zone under the EU AI Act

1 Prohibited Practices

The Full Transparency Zone encompasses AI practices deemed detrimental to democratic values and fundamental rights. This practices such as social scoring and manipulation, which aim to individual behavior or control societal outcomes. Such practices prohibited due to their potential to undermine free decision-autonomy, and individual dignity.

2 Protected Values

This zone prioritizes the protection of fundamental values like free decision-decision-making, freedom from social engineering, freedom of thought, and thought, and individual assessment of personality. The Act aims to prevent prevent the misuse of AI technologies for surveillance, manipulation, and the manipulation, and the creation of biased or discriminatory outcomes. outcomes.

3 Relative Harm Test

In this zone, certain practices, such as remote biometric systems, are subject to a harm test. This test assesses the potential on fundamental rights and determines whether the use of these justified. If the potential harm is deemed significant, the practice classified as a high-risk system subject to stricter transparency

4 Proportionality and Necessity

A crucial aspect of the Full Transparency Zone involves necessity tests. This means that the use of AI systems must be to the intended purpose and that no less restrictive alternatives to achieve the desired outcomes. These tests ensure that AI used responsibly and ethically.

Limited Transparency Zone

High-Risk AI Systems

The Limited Transparency Zone encompasses high-encompasses high-risk AI systems, which pose pose significant potential for harm to individuals or individuals or society. These systems often involve involve sensitive data or have the capability to to influence critical decisions, making transparency transparency a key consideration.

High-risk systems include those used for infrastructure, product safety, law and the administration of justice. In these balancing the protection of fundamental the need for innovation is crucial.

Protected Values

The Limited Transparency Zone seeks to balance balance the protection of fundamental rights with rights with the need for innovation. Transparency is Transparency is essential to ensure that AI systems systems are used responsibly and ethically, especially in sensitive areas like public security, security, individual safety, privacy, and law enforcement.

While transparency is important, the Act that certain exceptions may be necessary to protect national security and public safety. is to strike a balance between transparency need for effective law enforcement and security measures.

Significant Harm Test

AI systems in this zone are subject to a harm test. If an AI system does not pose a significant risk of harm to individuals, not materially influencing decision-making, not be classified as high risk. The test helps identify systems that require greater transparency.

Minimal Transparency Zone

All Other AI Systems

The Minimal Transparency Zone covers all AI systems that do not pose pose a significant risk of harm and are and are not classified as high risk. This This zone aims to ensure that AI systems are developed and used responsibly, while minimizing regulatory burden and encouraging encouraging innovation.

GPAIS

General-Purpose AI Systems (GPAIS) (GPAIS) with no systemic risk are also also included in this zone. GPAIS are are designed for a wide range of applications and are not typically tailored to specific purposes, making making them less likely to pose significant risks.

Transparency

The Minimal Transparency Zone focuses on basic transparency requirements, such as providing information about the purpose functionality of the AI system. The is to promote transparency and accountability, while ensuring development and deployment practical and efficient.

Unregulated Transparency Zone: exemptions

1

AI Framework

The AI Framework Convention establishes a framework for AI governance, including principles. It also sets certain exemptions for national defense-related AI systems and research and development activities.

2

AI Act

The EU AI Act similarly exempts certain AI systems, such as used for national security, purposes, and specific research development activities.

3

Exemptions of the AI Act

Exemptions to transparency requirements are granted to certain certain AI systems, such as those those used for national security, security, defense, and international international cooperation.

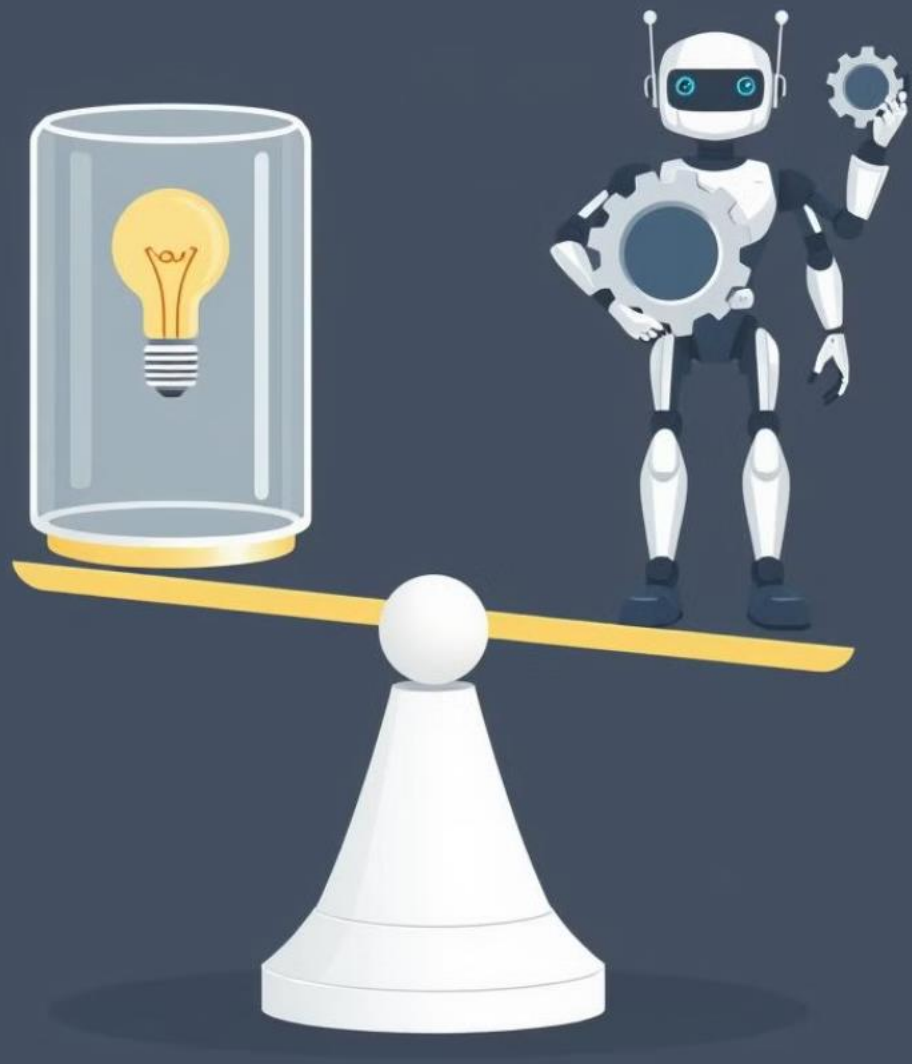
4

Self-Regulation

The AI Act encourages self-regulation for AI systems that do not do not fall under the scope of the the Act. This includes low-scale activities, open-source software, software, and certain research and and development activities. The goal The goal is to promote responsible responsible AI development while while minimizing regulatory intervention.

Final Reflections

Key Considerations	Points to Note
AI Transparency Ownership	Determining the responsibilities and roles of different different actors, including providers, deployers, users, deployers, users, and regulators, in ensuring AI transparency is crucial.
Eisenhower's Principle	Addressing "important but not urgent" risks, such as such as systemic biases and unintended consequences of AI, is essential to prevent long-term long-term harm.
Experimental Nature	The framework for AI transparency is still under under development, and ongoing experimentation experimentation and evaluation are necessary to to ensure its effectiveness.
Ideological Conflict	The global competition in AI development can create create tensions between different nations' approaches to AI transparency, highlighting the need the need for international cooperation and collaboration.



Online platforms and their counteraction to harmful content

Nataliia Filatova-Bilous, PhD in Law, associate professor at the department of Civil Justice, Arbitration and Private International Law of Yaroslav Mudryi National Law University

Cases: examples

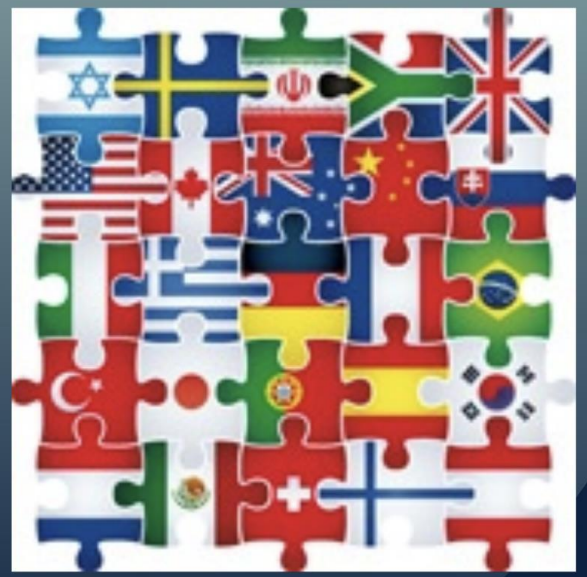
- sharing hateful expressions on Facebook about Rohingya in Myanmar in 2017
- conspiracy theories about COVID-19 and vaccination in 2020-2021
- mass disinformation about the war in Ukraine by pro-Kremlin bloggers from 2022 till now
- Israel-HAMAS armed conflict starting in 2023 ("deluge of online propaganda and disinformation larger than anything seen before" (NYT)

European Commission's assessment 2023

The scope of the concept

Threats and current law

How do platforms and governments respond?



Foreign law responses

Legislative responses in Ukraine

Platform's responses

How does Ukrainian law respond?

- The Strategy of Informational Safety 2021, approved by the President's decree - 'enhancement of liability for sharing disinformation"
- The Law on the prohibition of propaganda of the Russian Nazi totalitarian regime, the armed aggression of the Russian Federation as a terrorist state against Ukraine, and the symbols of the military invasion of Ukraine by the Russian Nazi totalitarian regime, from 22 May 2022
- The Law on the condemnation and prohibition of propaganda of Russian imperial policy in Ukraine and decolonization of place names from 21 March 2023
- A number of bills submitted to the Parliament purporting to impose liability for disinformation

University of Central Lancashire
UCLan Cyprus

CRoLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

Latest regulatory developments in AI in Europe

By Prof. Stéphanie Laulhé Shaelou, Professor of European Law and European Values, Head, School of Law and Jean Monnet Centre of Excellence CRoLEV Director, UCLan Cyprus

D.A.A.D. International Visiting Professor and Chair holder of Common Law in Global Contexts, Institute for International Law of Peace and Armed Conflict (IFHV), University of Ruhr in Bochum, Germany

UNITAR Visiting Professor

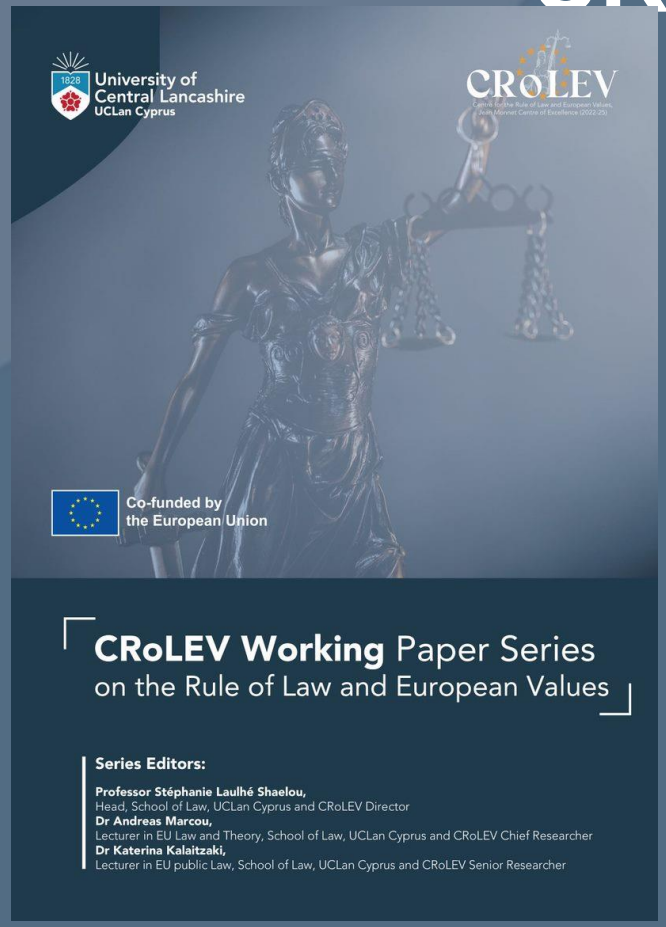
Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CRoLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

CRoLEV JMCE WP Series



Inaugural Working Paper:

S. Laulhé Shaelou and Y. Razmetaeva, 'Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: Shaping the digital legal order while upholding Rule of Law principles and European values' (CRoLEV JMCEWP 1/2023)

https://crolev.eu/working-paper-series/

Co-funded by
the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

Outline

- Inside the European digital legal order: EU AI Act and CoE framework Convention on AI and Human Rights, Democracy and Rule of Law
- AI impact on fundamental human rights
- ‘New’ fundamental rights

Co-funded by
the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

The European digital legal order

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

The advancement of the European digital legal order

- The ‘European digital legal order’ has now gained more importance than the overarching concept of European (public) legal order.
- The European legal order traditionally entails a set of **fundamental human rights, Rule of Law principles and Democratic values** as enshrined in:
  - the UN Charter (1945);
  - the Council of Europe Statute (1949);
  - the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR);
  - the EU Treaties (Articles 2, 6 and 7 TEU);
  - the Charter of Fundamental Rights of the European Union (EU Charter);
  - the case law of the ECtHR and CJEU.

From maintaining the Rule of Law derive the sustainability of Democratic values and freedoms under the law enshrined in fundamental human rights.

This remains unchanged in the digital world: nature, scope and upholding of fundamental human rights, Rule of Law principles and Democratic values.

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

'Inside' the European digital legal order

- No uniform definition of AI or AI systems in the European legal order at large – but several attempts made to provide 'all-encompassing but change-resistant' definitions as AIS's serious impact on fundamental human rights:
  - European Declaration on Digital Rights and Principles for the Digital Decade (anthropocentric interaction vis-à-vis AI systems, digitalisation and algorithmisation);
  - Risk-based EU instruments (General Data Protection Regulation GDPR, Digital Markets Act DMA, Digital Services Act DSA and EU AI Act).
  - Framework approach: CoE framework Convention on AI and Human Rights, Democracy and Rule of Law (Art 2). AI systems are "a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment".
- Need to re-examine potential new/renewed/modernised rights that should enhance and/or supplement the current catalogue of fundamental human rights, as contained in the EU Charter and the ECHR.
- Regulatory standards, especially in relation to AI, should be clearer and not be based on a half-hearted approach.

Co-funded by the European Union

crolev@uclancyprus.ac.cy

Official Journal of the European Union

EN

L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

The EU AI Act

https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

- EU Regulation laying down harmonised rules on AI and amending certain Union legislative Acts agreed with EU MS in December 2023 and adopted on 13th March 2024 by the EP. Published on 12/7/2024.
- Based on the functioning of the internal market (Art 1):
- Lays down a “uniform legal framework for the development, the placing on the market, the putting into service and the use of AI systems in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union, and to support innovation”.
- Ensures the free movement, cross-border, of AI-based goods and services, thus preventing MS from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by the Regulation.

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CRoLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

EU AI Act: Main features

- **Banning** certain AI applications that threaten citizens' rights (facial recognition databases, emotion recognition in certain places, manipulating human behaviour);
- **Limiting** the use of biometric identification systems by law enforcement;
- **Obligations for high-risk systems (Chapter III, sections 1-3, Art 6-27):**
  - **significant potential harm/risk/impact** to health, safety, fundamental rights, environment, democracy and RoL in critical infrastructure, essential private and public services (including banking), law enforcement, democratic processes, etc'.
  - Such systems must 'assess and reduce risks, maintain use **logs**, be **transparent** and accurate and ensure human oversight'.
  - Right of complaints and to receive explanations about decisions based on high-risk AI systems that affect their rights.
- Transparency requirements for General-purpose AI (GPAI) systems and their models: compliance with copyright law and open data training materials. If systemic risks, additional requirements: 'performing model evaluations, assessing and mitigating systemic rights and reporting on incidents'. Deepfakes (artificial or manipulated images/audio/video) must be clearly labelled.
- To support innovation and SMEs, regulatory sandboxes and 'real-world testing' needed at national level before placement on the market.

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

EU AI Act - Next steps

- Entry into force: 20 days after its publication in the EU official Journal;
- Fully applicable: 24 months after its entry into force
- EXCEPT for:
  - bans on prohibited practices: will apply 6 months after the entry into force date;
  - codes of practice: 9 months after entry into force
  - General-purpose AI rules including governance: 12 months after entry into force; and
  - Obligations for high-risk systems: 36 months.

Co-funded by
the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CRoLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

CoE framework Convention on AI and Human Rights, Democracy and Rule of Law

- Adopted on 17 May 2024 by the Committee of Ministers of the Council of Europe at its 133th Session held in Strasbourg, and will be opened for signature on the occasion of the Conference of Ministers of Justice in Vilnius (Lithuania) on 5 September 2024.
- Aim is to ensure compatibility between AI systems throughout their life cycle and HR, Democracy and RoL (Art 1(1)). For this purpose, each Party to the Convention will need to take appropriate measures to ensure that aim – to be deposited to the SG of the CoE (Art 1(2)) with a follow-up mechanism to be put in place (Art 1(3)).
- Scope include not only the AI systems per se, but also their risks and impact, as may be produced or arise from public and private actors (Art 3).
- National security interests fall outside of the scope of the Convention (Art 3(2)). But subject to a broader condition of compliance with international law, international HR obligations and democratic institutions and processes… may not be sufficient for a number of derivative actors.
- R&D activities special provision around testing.
- Convention sets out two general obligations: (i) protection of HR (Art 4); and (ii) integrity of democratic processes and respect for the RoL (Art 5) + Principles related to activities within the lifecycle of AI systems (Chapter III, Arts 6-13).
- There are general provisions for assessment and mitigation of risks/adverse impacts (Chapter V).

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

AI (non-binding) principles

CROLEV
Centre for the Rule of Law and European Values, Jean Monnet Centre of Excellence (2022-25)

European Declaration on Digital Rights and Principles for the Digital Decade and the Ethics guidelines for trustworthy AI of the High-Level Expert Group on Artificial Intelligence (AI HLEG)

1. Human agency and oversight;
2. Technical robustness and safety;
3. Privacy and data governance;
4. Transparency;
5. Diversity, non-discrimination and fairness;
6. Societal and environmental well-being;
7. Accountability.

CoE framework Convention on AI and Human Rights, Democracy and Rule of Law

- **Art 6: subsidiarity**
- **Art 7: human dignity and individual autonomy**
- **Art 8: Transparency and oversight**
- **Art 9: Accountability and responsibility**
- **Art 10: Equality and non-discrimination**
- **Art 11: Privacy and personal data protection**
- **Art 12: Reliability**
- **Art 13: Safe innovation.**

Wider safeguards available (access, public consultation, digital divide, protection of existing HR and non-discrimination, wider protection).

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

AI impact on fundamental human rights

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values, (2022-25)

AI cross-cutting impact on fundamental human rights in Europe

- How AI affects fundamental human rights may affect the ideal of human rights in general through the erosion of value bases and recourse to technological determinism/a more utilitarian approach to regulation and practice.
- AI systems can attack individual rights in overt and covert manners, cross-cutting impact on rights via deployment of technologies. Such attacks may affect primarily, but not only, rights enshrined in the EU Charter and the ECHR:
  - to respect for private and family life (Art 7 EU Charter; Art 8 ECHR)
  - to protection of personal data (Art 8 EU Charter)
  - to freedom of expression and information (Art 11 EU Charter; Art 10 ECHR)
  - to freedom of thought, to conscience and religion (EU Charter, Article 10; ECHR, Article 9)
  - to rights of liberty and security (EU Charter, Article 6; ECHR, Article 5)
  - to the right to a fair trial (EU Charter, Article 47; ECHR, Article 6)
  - to the right to non-discrimination (EU Charter, Article 21; ECHR, Article 14)
  - to equality of men and women (EU Charter, Article 23)
  - to rights of the child (EU Charter, Article 24)
  - to the principle of no punishment without law (ECHR, Article 7)

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

Examples – Solutions?

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

- **Content moderation algorithms** may affect not only freedom of expression, but also freedom of thought, conscience and religion, the right to non-discrimination, equality of men and women, and the rights of the child.
- Algorithms in their design and/or use may be invasive, selective, promote polarisation of opinions and dilute discussions, as well as generally contribute to the formation of a certain picture of the world among users of digital content.
- When describing the impact of AIS on fundamental human rights, it is not always possible to single out specific rights that are affected by these technologies. **Thus, the question arises as to how to best prepare and protect them.**
- **AI technologies used in public spaces by public authorities can go far beyond what is considered acceptable in a democratic society upholding Rule of Law principles and European values as well as fundamental human rights**

- **The ability of AIS to track users both in the public and the private sphere of life** is outstanding.
- That is so particularly because it is not necessary to use technological artefacts directly to be the object of certain tracking actions.
- Bits of information put into the digital space by others can make it easier for non-users to track them because AI can search, process, combine and analyse those bits with astonishing accuracy, as well as keep track of what people have been interested in and weave it into their online searches, intrusively or more subtly.
- Algorithms can establish a match on a photo with a person who did not take or post this photo on the network and may even not have known that it was taken, then determine the location of this person at a certain time.

Co-funded by the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

‘New’ fundamental rights

University of Central Lancashire
UCLan Cyprus

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

Scope of 'new' rights

- A vision of the future with AI systems could open the possibility to create new rights and/or (significantly) change/upgrade the essence and scope of already existing rights.
- Introducing new rights may also mean changing their status from rights that apply to certain categories of persons (such as user rights or data subject rights) to fundamental human rights that are of utmost importance to all human beings.
- New rights do not necessarily fall within the scope of the latest developments on AI in Europe.

Co-funded by
the European Union

crolev@uclancyprus.ac.cy

University of Central Lancashire
UCLan Cyprus

Comparative table

CROLEV
Centre for the Rule of Law and European Values,
Jean Monnet Centre of Excellence (2022-25)

‘New’ rights (not absolute)

1. ‘right not to be subjected to automatic decision-making and automatic processing’ in the broadest sense. Human withdrawal from semi or fully automated decision-making is one of the red lines of the European digital public legal order. The new dimension/broader sense of the right must include the requirement to have human-centered decision-making process controlling the AI decision and being ultimately responsible for it.
2. ‘right to influence one’s digital footprint’. Individuals should have the right to participate in their digital lives in such a way that information is reviewed in accordance with time passed and its significance to the individual and not to society.
3. ‘right not to be measured, analysed or coached’. Since both states and companies are increasingly resorting to mass surveillance and collecting the smallest detailed information about people. Obligations not to resort to mass surveillance, at least in some places that should remain private, and not to resort to 24/7 surveillance.

Existing/extended rights

1. Art 22 GDPR (Automated individual decision-making, including profiling) – limited to ‘seriously impactful events’.
2. Art 17 GDPR (right to erasure)
3. Can new rights be introduced in the EU Charter?
   - ‘right not to be manipulated’
   - ‘right to be neutrally informed online’
   - ‘right to meaningful human contact’

Call on achieving democratic societies based on the Rule of Law and fundamental human rights in which everyone benefits equally from technologies.

Co-funded by the European Union

crolev@uclancyprus.ac.cy

Liability of Online Platform Operator: Tort Law Perspective

Bohdan KARNAUKH

PhD in Law, associate professor at the Department of Civil Law, Yaroslav Mudryi National Law University

EFVDE

European Fundamental Values in Digital Era

Co-funded by the European Union

Mark Zuckerberg’s Senate hearing

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all of the good that connecting people can do. And, as Facebook has grown, people everywhere have gotten a powerful new tool for staying connected to the people they love, for making their voices heard and for building communities and businesses.

But it's clear now that we didn't do enough to prevent these tools from being used for harm, as well. And that goes for fake news, for foreign interference in elections, and hate speech, as well as developers and data privacy.

We didn't take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake. And I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.

So, now, we have to go through our — all of our relationship with people and make sure that we're taking a broad enough view of our responsibility.

It's not enough to just connect people. We have to make sure that those connections are positive. It's not enough to just give people a voice. We need to make sure that people aren't using it to harm other people or to spread misinformation. And it's not enough to just give people control over their information. We need to make sure that the developers they share it with protect their information, too.

Across the board, we have a responsibility to not just build tools, but to make sure that they're used for good. It will take some time to work through all the changes we need to make across the company, but I'm committed to getting this right. This includes the basic responsibility of protecting people's information, which we failed to do with Cambridge Analytica.

Taxonomy of cases

- violation of fundamental human rights
- copyright infringement
- defective products

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

Violation of Human Rights

- ***Force v. Facebook, Inc.,*** *No. 18-397 (2d Cir. 2019)*
- ***Lemmon v. Snap, Inc.****, 995 F.3d 1085 (9th Cir. 2021)*
- ***A.M. v. Omegle.com LLC,*** No. 3:2021cv01674 - Document 36 (D. Or. 2022)

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

Safe Harbor in the US

‘No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider’

- *Section 230 of the Communications Decency Act (CDA)*

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

The immunity applies if:

(i) the action is brought against a defendant who is a ‘provider or user of an interactive computer service’;

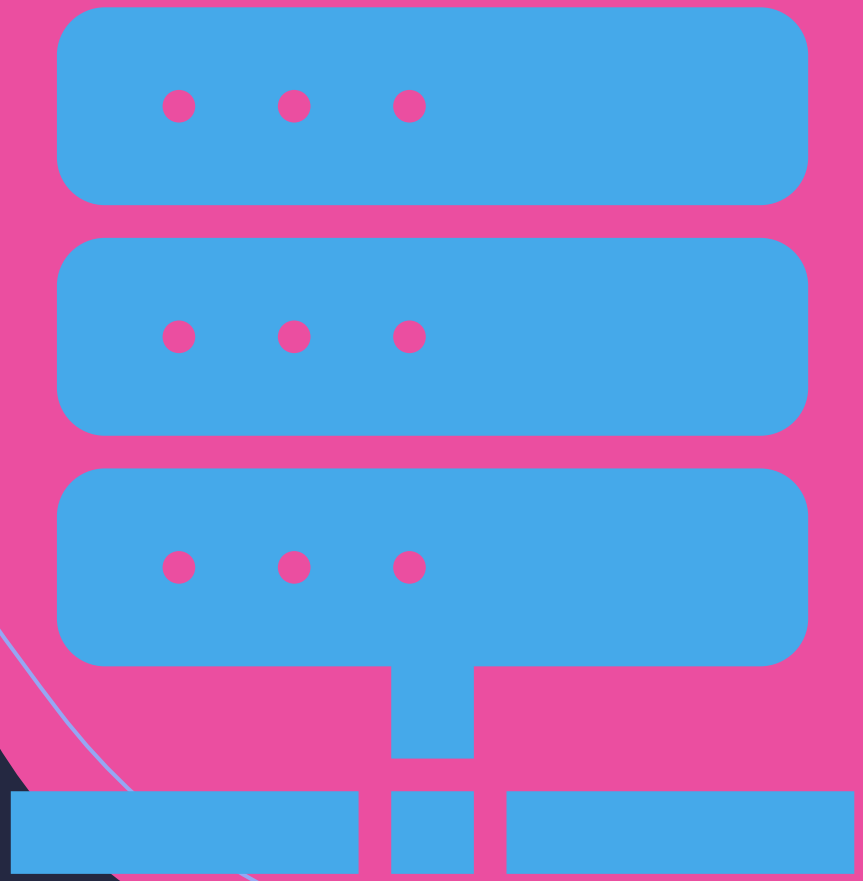
(ii) the claim effectively treats defendant as a ‘publisher or speaker’ of information; and

(iii) the information is provided by another person.

Safe Harbor in the EU

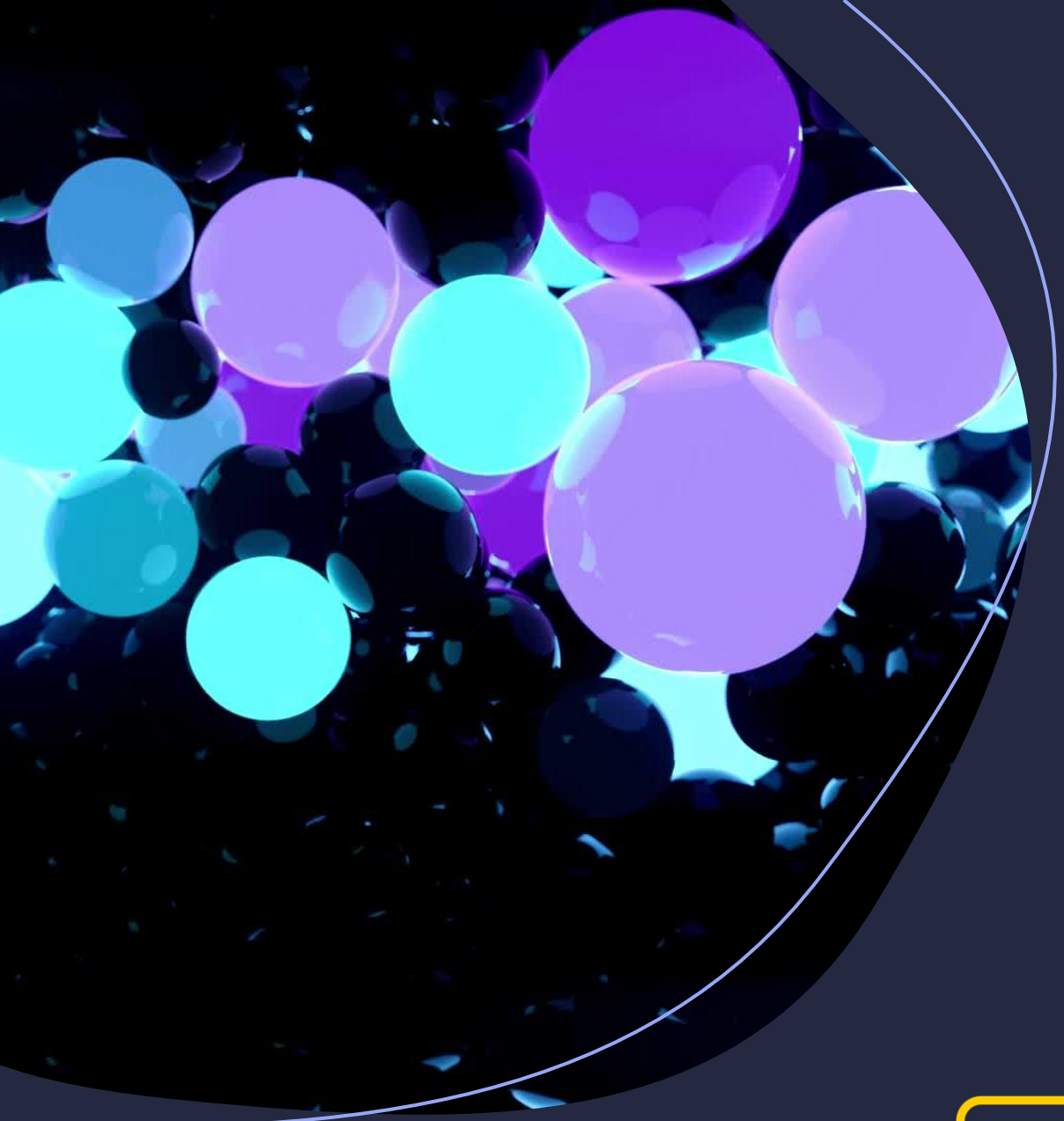
'Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content'.

- Article 14 of Directive 2000/31/EC on e-commerce;
- Article 6 of Regulation (EU) 2022/2065 of October 19, 2022 (Digital Services Act, DSA):



EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union



Frank Peterson v Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH (C 682/18) and *Elsevier Inc. v Cyando AG* (C 683/18)

- (1) can it be deemed that by hosting a third party content, YouTube makes a public communication of a copyrighted work within the meaning of Article 3(1) of the Copyright Directive?
- (2) does the activity of a video hosting platform fall within the scope of Article 14 of Directive 2000/31/EC on e-commerce?
- (3) must actual knowledge of the illegal activity relate to the concrete illegal activity under Article 14(1) of the E-Commerce Directive?

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

Product Liability

- ***Bolger v. Amazon Com LLC*** (2020)
- ***Asociación Profesional Élite Taxi v Uber Systems Spain SL***, (C-434/15)

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

Conclusions

- CONTROL
  - decisive influence & content moderation
- ‘safe harbors’ have limits
- economic considerations

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

See also:

- Karnaukh, B. Scope of platform operator's liability: three categories of cases. *Visegrad Journal on Human Rights*. 2024. No 3. 73-81. https://journal-vjhr.sk/wp-content/uploads/2024/09/Visegrad-3_2024.pdf
- Filatova-Bilous, N. (2021). Once again platform liability: on the edge of the 'Uber' and 'Airbnb' cases. *Internet Policy Review*, 10(2). https://doi.org/10.14763/2021.2.1559.

EFVDE European Fundamental Values in Digital Era

Co-funded by the European Union

The Cyber Resilience Act – Another Piece in the Jigsaw of EU Cybersecurity Legislation

UNIVERSITÄT PASSAU
Juristische Fakultät

Prof. Dr. Meinhard Schröder
27.9.2024

Outline

I. Introduction: Cybersecurity and Fundamental Values

II. Current State of Cybersecurity Legislation of the EU

III. The Cyber Resilience Act

IV. Summary and Outlook

- Importance of information and communications technology
  - backbone of our economic growth
  - critical resource which all economic sectors
  - exercise of many fundamental freedoms is facilitated by it
  - Central to the personality development of many individuals

- Vulnerability of IT systems
  - IT systems are constantly under attack by villains
  - human errors and force majeure are threats to availability, integrity and confidentiality of information processed

- Law as a means to foster cybersecurity
  - Common sense
  - Positive obligations deriving from fundamental rights

- Origins in directives on telecommunication, data protection and e-commerce
- Specific cybersecurity legislation
  - 2004: Establishment of ENISA (now: European Union Agency for Cybersecurity)
  - Cybersecurity strategies since 2013
  - NIS directive 2016/1148 and NIS 2 directive 2022/2555
  - Cybersecurity Act / Regulation (EU) 2019/881
  - Regulation 2021/887 on the European Cybersecurity Competence Centre (ECCC)
  - Regulation 2022/2554 on digital operational resilience for the financial sector

- Legislation dealing inter alia with cybersecurity
  - General Product Safety Regulation
  - Product Liability Directive
  - Radio Equipment Directive, from 8/2025
  - Regulation 2023/1230 on machinery
  - AI Act
  - …

→ Patchwork of laws on cybersecurity

- Act → Regulation
- Will most certainly enter into force until the end of 2024, applicability 3 years later
- Product law, horizontally applicable without limitations to specific sectors
- Why more cybersecurity law?
  - Consumer protection / trust in product quality and security
  - Public interest in cybersecurity
  - Democratic legitimation of cybersecurity standards

- Subject Matter and scope of applicability
  - Article 1 CRA
    - rules for the making available on the market of products with digital elements
    - essential cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity
    - essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes
    - rules on market surveillance, including monitoring, and enforcement of the rules and requirements
  - Definition of “product with digital elements” in Article 3 (1) CRA:
    a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately

- Security requirements
  - Article 6 CRA + Annex I
    - Product-related
    - Manufacturer-related
    - Not only until a product is on the market, but during the whole lifecycle of a product!

- Security levels
  - Determine the level of assurance for conformity required
  - 3-4 levels
    - Most products (~ 90%): self-assessment + declaration of conformity by manufacturer
    - Important products (~10%):
      - Class I: full compliance with harmonised standards + self-assessment or external assessment by notified bodies
      - Class II: external assessment by notified bodies
    - Critical products: “European cybersecurity certificate”

- Additional requirements for
  - importers
  - distributors
  - Open source software stewards

- Enforcement
  - Market surveillance
  - penalties

- The CRA will increase the level of cybersecurity in the EU
- The jigsaw is not finished, promoting cybersecurity with legal means remains a continuing task

Перспективи подальшого запровадження онлайн-судочинства в Україні

Сергій Гришко, партнер Queritius, Голова Queritius Ukraine, Арбітр МКАС при ТПП України

Будапешт | Варшава | Київ | Загреб

План обговорення

I. Єдина судова інформаційно-телекомунікаційна (з березня 2024 р. комунікаційна) система: status quo?

II. Повністю дистанційні засідання поза межами приміщення суду під час війни: чи це можливо?

III. Екстериторіальний онлайн розгляд: ідея чи реальна перспектива?

I. ЄСІТС (ЄСІКС) І Коротка історична ретроспектива | 1

Елементи електронного судочинства до реформи 2017 р.:

- з кінця 1990-х рр. у судах загальної юрисдикції почалось впровадження системи автоматизації документообігу – комп'ютерна програма «Д-3», що застосовується і по сьогодні;
- з 2004 р. фіксування судового процесу технічними засобами;
- з 2007 р. повноцінне запровадження ЄДРСР;
- з 2010 р. встановлено юридичний статус автоматизованого документообігу суду, визначено засади здійснення автоматизованого розподілу справ;
- 2012 р. – можливість відеоконференції з приміщення іншого суду (з 2020 р. – власними технічними засобами, однак лише для учасників справи та їх представників).

I. ЄСІТС (ЄСІКС) І Коротка історична ретроспектива | 2

- Стратегія реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 рр. – необхідність поетапного впровадження інструментів електронного правосуддя;
- Закон № 2147-VIII від 03.10.2017 р. – у судах, ВРП, ВККС, ДСА, Службі судової охорони їхніх органах і підрозділах мало бути забезпечено функціонування ЄСІТС;
- **01.12.2018 р.** – ДСА на веб-порталі судової влади та в газеті «Голос України» було розміщено оголошення ВРП про початок функціонування ЄСІТС;

АЛЕ!

- Наприкінці 2018 р. стався **збій в роботі ЄСІТС**, через який багато сервісів були недоступні більше місяця;
- 28.02.2019 р. ВРП **відкликало** оголошення від 01.12.2018 р. про початок функціонування ЄСІТС;
- Окремі модулі ЄСІТС таки були запущені в дослідну, а згодом користувацьку експлуатацію (Електронний суд та Електронний кабінет), проте очевидною стала **неможливість одночасної комплексної реалізації**.

I. ЄСІТС (ЄСІКС) І Коротка історична ретроспектива | 3

- 27.04.2021 р. – прийнято Закон № 1416-IX «Про внесення змін до деяких законодавчих актів України щодо забезпечення **поетапного** впровадження Єдиної судової інформаційно-телекомунікаційної системи».
- З 05.10.2021 р. офіційно функціонують три підсистеми (модулі): Електронний кабінет, Електронний суд, підсистема відеоконференцзв'язку. Незважаючи на багато технічних проблем та незручний користувацький інтерфейс, Електронний суд є кроком вперед і спрощує роботу адвоката.
- Закон № 3200-IX – **обов'язкова реєстрація в ЄСІКС**:
  - з 18.10.2024 р. для адвокатів, нотаріусів, державних та приватних виконавців, судових експертів, органів державної влади та інших державних органів, органів місцевого самоврядування для участі в господарських, цивільних та адміністративних справах, а також юридичних осіб приватного права – в господарських справах;
  - з 21.02.2024 р. для юридичних осіб приватного права, які є учасниками цивільних та адміністративних справ. **Інші особи реєструють свої електронні кабінети в добровільному порядку!**

I. ЄСІТС (ЄСІКС) l Status quo | 1

У 2023-2024 рр. проведено технічний і функціональний аудити ЄСІТС, за результатами яких підтверджено **технічну застарілість, архітектурну неспроможність і функціональну обмеженість**.

Ключові **недоліки** за Концепцією ЄСІКС (наказ ДСА від 30.04.2025 р. № 178):

- ЄСІКС не є єдиною системою, а швидше являє собою сукупність розрізнених систем, побудованих у різні часи, які використовують різні технології;
- Інформаційні обміни між наявними підсистемами ЄСІКС не завжди відпрацьовують та реалізовані на недостатньо розвиненому рівні;
- Відсутність цілісного підходу до розробки та впровадження системи як єдиної інформаційно-комунікаційної платформи для реалізації повноважень судової гілки влади.

I. ЄСІТС (ЄСІКС) l Status quo | 2

Концепція ЄСІКС (наказ ДСА від 30.04.2025 р. № 178):

- **Доопрацювання** наявних підсистем стає **недоцільним;**
- Пропонується впровадження єдиного централізованого рішення, яке забезпечить інтеграційне середовище реалізації необхідної функціональності;
- Модернізована система забезпечить **перевикористання** наявних сервісів, функціональних компонентів і даних, зробивши їх доступними користувачу через єдиний інтерфейс.

І. ЄСІТС (ЄСІКС) І Плани на майбутнє

Дорожня карта розвитку ІТ-рішень у судовій системі (наказ ДСА від 02.12.2024 р. № 534) та Концепція ЄСІКС (наказ ДСА від 30.04.2025 р. № 178). Створити нову ЄСІКС замість ЄСІТС заплановано до 2028 року у два етапи:

- етап 1 (2025-2026 рр.) містить уже ініційовані проєкти розбудови ЄСІКС і забезпечує розроблення та впровадження ключової функціональності підсистеми Електронний документообіг суду, низки підсистем і компонентів, що доповнюють пріоритетну функціональність ЄСІКС;
- етап 2 (2026-2028 рр.) передбачає доопрацювання додаткової та експериментальної частин функціональності ЄСІКС, зокрема на базі технологій великих даних та штучного інтелекту.

I. ЄСІТС (ЄСІКС) І Чи є майбутнє?

Публічне звернення ВРП до КМУ та Мінфіну від 11.09.2025 р.:

«*У 2025 році фінансування реалізації нової Концепції ЄСІКС* ***з державного бюджету не передбачено****…*

за інформацією ДСА України, модернізація ЄСІТС, а фактично ***створення замість неї нової ЄСІКС, опинилась під загрозою внаслідок припинення фінансування відповідного проєкту з боку Агентства США з міжнародного розвитку (USAID)****. Після припинення підтримки Програми USAID у 2025 році триває пошук донорів для фінансування зазначеного проєкту…*

Міністерство фінансів України в листі від 30 червня 2025 року … повідомило … ***органи судової влади мають … прагнути*** *досягнення цілей шляхом забезпечення якісного надання публічних послуг при залученні мінімального обсягу бюджетних коштів та* ***досягнення максимального результату під час використання визначеного бюджетом обсягу коштів***».

II. Повністю дистанційні засідання поза межами приміщення суду | Безпекові ризики | 1

З 24.02.2022 р. і станом на 16.09.2025 р. **170 приміщень 161 судової установи** зазнали пошкоджень різного ступеня аж до повного руйнування та розкрадання майна:

- 29 березня 2022 року ракетна атака, яка повністю зруйнувала приміщення Господарського суду Миколаївської області, загинули двоє працівників суду;
- 06 грудня 2024 року під час ракетного удару по Кривому Розі постраждала адміністративна будівля Дніпровського апеляційного суду, загинув помічник судді.

II. Повністю дистанційні засідання поза межами приміщення суду | Безпекові ризики | 2

На четвертому році війни процесуальне законодавство не передбачає повністю дистанційних засідань!

Кодекси досі не передбачають можливості брати участь у судовому засіданні поза межами приміщення суду

- судді,
- секретарю судового засідання,
- свідку,
- перекладачу,
- спеціалісту,
- експерту.

II. Повністю дистанційні засідання поза межами приміщення суду | Законодавчі пропозиції | 1

- № 7316 від 26.04.2022 р. – можливість участі секретаря судового засідання, свідка, перекладача, спеціаліста та експерта у судовому засіданні в режимі відеоконференції з використанням власних технічних засобів. **Відхилено та знято з розгляду – 01.07.2022 р.**
- № 8358 від 13.01.2023 р. – аналогічно до № 7316, а також запровадження дистанційного доступу суддів до автоматизованої системи документообігу суду для можливості внесення судових рішень і окремих думок до неї поза межами приміщення суду. **Очікує розгляду більше 2 років.**

II. Повністю дистанційні засідання поза межами приміщення суду | Законодавчі пропозиції | 2

- № 9090 та № 9091 від 10.03.2023 р. – за умов воєнного чи надзвичайного стану в разі виникнення обставин, які зумовлюють загрозу життю, здоров'ю та безпеці судді, учасників судового процесу, судові засідання можуть проводитися в режимі відеоконференції з використанням власних технічних засобів поза межами приміщення суду, **однак**
  - за наявності технічної можливості розгляду **справи за матеріалами в електронній формі**;
  - суддя, секретар судового засідання бере участь у такому **засіданні в межах підконтрольних територій України**;
  - суддя може брати участь у засіданні в режимі відеоконференції поза межами приміщення суду, якщо справа розглядається **одноособово**. **17.07.2025 р. проєкт відкликано** *(це урядових законопроєкт, який відкликаний за фактом зміни уряду, однак новий уряд не переподав його до ВРУ)*.

II. Повністю дистанційні засідання поза межами приміщення суду | Вимоги Єврокомісії

- Звіт Європейської комісії щодо України за 2023 рік

«З огляду на спричинені війною труднощі, включно з переміщенням населення та бізнесу, погіршенням економічної ситуації та зниженням безпеки пересування, ***Україна має ухвалити законодавство, яке би офіційно запровадило дистанційні слухання*** *та врегулювало процедурні аспекти таких слухань з повним дотриманням процесуальних прав сторін. Це підвищило би ефективність судочинства та полегшило би доступ до правосуддя, в тому числі в умовах війни».*

II. Повністю дистанційні засідання поза межами приміщення суду | Знову не в пріоритеті?

- Аналіз Європейської комісії з питань ефективності правосуддя та проєкту Ради Європи «Підтримка судової влади України для забезпечення кращого доступу до правосуддя», жовтень 2022 року

*«Питання про дистанційну (і якщо так, то звідки) або фізичну участь судді в судовому розгляді є **не менш політичним**, ніж юридичним»*.

- Дорожня карта з питань верховенства права:

«Розроблення та прийняття змін до процесуальних кодексів, спрямованих на вдосконалення можливостей дистанційного судочинства» – **IV квартал 2026 р.**

III. Екстериторіальний онлайн розгляд | Ідея

- **Правові аспекти гнучкої територіальної юрисдикції: порівняльний та конституційний аналіз** – спільне дослідження Міністерства юстиції та ЄБРР
- Мін’юст працює над відповідним законопроєктом щодо впровадження екстериторіального розгляду з 2023 р.; його мета – забезпечити рівномірне навантаження між судами в різних регіонах та гарантувати право кожної особи на справедливий суд.

III. Екстериторіальний онлайн розгляд | Ключові терміни

«Юрисдикція» — це юридичний термін, що означає владу або повноваження, буквально право «проголошувати закон»

Юрисдикція як аспект суверенітету охоплює:

- законодавчу юрисдикцію (повноваження встановлювати правила);
- юрисдикцію щодо вирішення судових справ чи судову юрисдикцію (повноваження виносити судові рішення);
- виконавчу юрисдикцію (повноваження примушувати до виконання або карати за невиконання законів чи нормативно-правових актів).

Юрисдикція судів **включає в себе**:

- суб’єктну юрисдикцію (*ratione personae*);
- предметну юрисдикцію (*ratione materiae*);
- територіальну юрисдикцію (*ratione loci*).

III. Екстериторіальний онлайн розгляд | Право на доступ до суду

Національні правила територіальної юрисдикції мають інструментальний характер. Вони **забезпечують практичну доступність судів,** а саме:

- сторони спору можуть легко подати **паперові документи до суду**, який зручно розташований;
- сторони спору **можуть легко ознайомитися з матеріалами справи** на місці; та
- сторони спору можуть **фізично бути присутніми** на судових засіданнях.

Крім того, згідно з науковими джерелами **територіальна юрисдикція**:

- забезпечує **географічний зв'язок** судів зі спором і полегшує **практичний доступ сторін**, включаючи фізичну присутність та участь у процесі;
- **зменшує навантаження на сторони** у зв'язку з подорожами на великі відстані, тим самим знижуючи витрати та логістику, що є ключовим елементом ефективного доступу до правосуддя.

III. Екстериторіальний онлайн розгляд | Право на доступ до суду відповідно до ЄКПЛ | 1

- Законодавство має відповідати загальним вимогам щодо доступу до правосуддя та справедливого судочинства і не створювати надмірних практичних перешкод для сторін, які бажають захистити свої права в суді.
- **Можливість подавати документи та ознайомлюватися з матеріалами справи** не буде порушена через запропоновані зміни оскільки ці правила застосовуватимуться лише до справ, **в яких і позивач, і відповідач зареєстровані в ЄСІТС.**

III. Екстериторіальний онлайн розгляд | Право на доступ до суду відповідно до ЄКПЛ | 2

Можливість бути присутнім на судових засіданнях - ще один аспект доступу до правосуддя, який практично забезпечується правилами територіальної юрисдикції судів.

Екстериторіальна юрисдикція не вплине на можливість сторін бути присутніми на засіданнях, адже:

- справи які відповідно до законопроєкту мають розглядатися поза визначеною територією, зазвичай не вимагають проведення судових засідань;
- якщо в порядку винятку необхідно провести судове засідання, це можна зробити за допомогою відеоконференції;
- судова практика ЄСПЛ розглядає слухання у віддаленому режимі як реальну альтернативу очним слуханням.

III. Екстериторіальний онлайн розгляд | Альтернативні форми територіальної юрисдикції | 1

- Договірний вибір місця розгляду справи (Хорватія, Франція, Німеччина, Італія та Нідерланди);
- Один суд, відповідальний за розгляд усіх справ певного виду (Естонія, Німеччина, Греція, Польща та Словенія);
- Ситуативний перерозподіл справ (за принципом *ad hoc*) (Хорватія, Греція та Нідерланди);
- Випадковий розподіл справ по всій країні (Болгарія та Хорватія).

III. Екстериторіальний онлайн розгляд | Альтернативні форми територіальної юрисдикції | 2

Випадковий розподіл справ по всій країні - модель, яка розглядається для впровадження в Україні

Мета: зменшення дисбалансу навантаження між судами одного рівня та вирівняння швидкості надання судових послуг у різних регіонах країни.

Болгарія: У 2023 році Болгарія внесла кардинальні зміни до ЦПК, переглянувши правила територіальної юрисдикції судів у справах про наказні провадження. Незалежно від того, чи подаються вони в електронній чи паперовій формі всі заяви про наказні провадження мають бути оцифровані, а потім розподілені випадковим чином між усіма судами найнижчого рівня. Розподіл справ має базуватись на алгоритмі, спрямованому на вирівнювання загального навантаження цих судів. Отже, суди з невеликим навантаженням, як очікується, отримуватимуть більшу частку справ про наказні провадження порівняно з перевантаженими судами.

III. Екстериторіальний онлайн розгляд | Альтернативні форми територіальної юрисдикції | 3

Хорватія: У 2015 році запроваджена *«універсальна територіальна юрисдикція»* щодо судів другої інстанції (окружних судів). Скарги на рішення судів першої інстанції розглядаються **випадково обраним окружним судом в межах країни**. Апеляційні справи розподіляються між окружними судами **за допомогою електронної системи випадкового розподілу на основі алгоритму**.

Завдання алгоритму полягає у:

- **зрівнюванні навантаження апеляційних судів по всій Хорватії**;
- забезпеченні однакового темпу розгляду справ та гармонізації судової практики судів другої інстанції;
- **зменшення місцевого впливу**: в результаті розподілу справ по всій країні, справа розглядається в іншому регіоні ніж там, де приймалося рішення.

У Хорватії не існує стандартизованих процедур для організації таких слухань. Однак найбільш реалістичним рішенням було б проведення їх в онлайн форматі, що дозволено процесуальним законодавством.

III. Концепція проєкту Закону України «Про внесення змін до Господарського процесуального кодексу України та Цивільного процесуального кодексу України щодо екстериторіального розгляду в окремих категоріях справ» | 1

Мета: запровадження механізму, який забезпечить **рівномірний розподіл справ між суддями та судами першої інстанції** і, відтак, швидкий та ефективний розгляд справ, що посилить гарантії права на справедливий судовий розгляд відповідно до статті 6 ЄКПЛ.

Законопроєкт передбачає **трансюрисдикційний онлайн розгляд** деяких категорій цивільних та господарських справ на рівні першої інстанції.

Трансюрисдикційний розгляд - процес, при якому **випадковий розподіл справи** між суддями здійснюється не серед суддів одного суду, **а серед усіх суддів, внесених до реєстру на основі алгоритму для визначення коефіцієнта завантаженості кожного судді.**

Трансюрисдикційному онлайн розгляду, якщо і позивач, і відповідач мають електронний обліковий запис в ЄСІТС підлягатимуть такі справи:

- малозначні справи, як визначено в процесуальних кодексах;
- справи, що виникають із трудових відносин;
- справи про надання судом дозволу на тимчасовий виїзд дитини за межі України;
- деякі види справ про безспірні вимоги (у справах наказного провадження).

III. Концепція проєкту Закону України «Про внесення змін до Господарського процесуального кодексу України та Цивільного процесуального кодексу України щодо екстериторіального розгляду в окремих категоріях справ» | 2

Учасники справи, яка розглядається трансюрисдикційно, **мають приєднатися до судового засідання за допомогою засобів відеоконференції поза межами зали судових засідань.**

Процедура оскарження залишається **незмінною,** тобто вона буде відбуватися за традиційними правилами територіальної юрисдикції.

Таким чином законопроєкт **змінює правила територіальної юрисдикції** щодо відповідних справ і передбачає їх **розподіл між усіма суддями відповідного рівня із метою:**

- усунення нерівномірного навантаження в різних регіонах країни;
- вирівнювання швидкості здійснення правосуддя;
- надання судам більшої гнучкості в управлінні операційними труднощами.

III. Екстериторіальний онлайн розгляд | Перспективи | 1

Гнучка територіальна юрисдикція для України:

- Дозволить перерозподіляти справи між регіонами – потенційно за допомогою алгоритмів, що збалансовують навантаження;
- Дозволить виправляти або пом'якшувати диспропорції без ліквідації місцевих судів;
- Зберігатиме доступ до правосуддя в менших громадах, зменшує політичний тиск на суд і підвищує загальну ефективність.

III. Екстериторіальний онлайн розгляд | Перспективи | 2

Запропоновані зміни до процесуальних кодексів:

- відповідають міжнародним зобов’язанням країни за ЄКПЛ;
- не створюють надмірних перешкод для доступу до правосуддя та не порушують право на справедливий суд;
- дозволяють досягти низки легітимних цілей, зокрема:
  - посилення автономії сторін;
  - підвищення процесуальної зручності;
  - сприяння судовій спеціалізації та операційній ефективності, ефективному реагуванню на тимчасові інституційні виклики, такі як накопичення справ або нерівномірне навантаження.

Typical violations in the processing of personal data by AI systems from the perspective of data protection supervisory authorities”

Andrii Hachkevych, PhD in Law, Associate Professor
(Institute of Law, Psychology and Innovative Education,
Lviv Polytechnic National University)

IX KHARKIV INTERNATIONAL LEGAL FORUM

September, 2025

Типові порушення при обробці персональних даних системами штучного інтелекту з позиції наглядових органів із захисту даних

Андрій Гачкевич (Інститут права, психології та інноваційної освіти, Львівський політехнічний національний університет)

IX KHARKIV INTERNATIONAL LEGAL FORUM

September, 2025

План виступу

01

Обробка даних
як поняття

02

Способи
обробки ШІ

03

Огляд кейсів

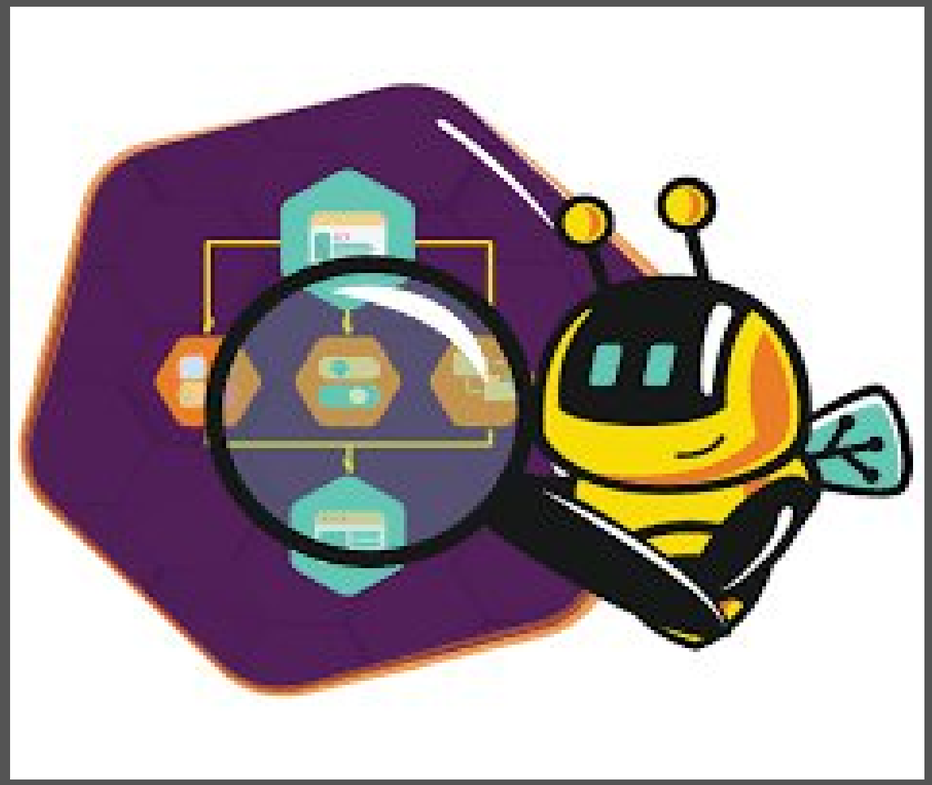
04

Види порушень


GDPR

Які сервіси штучного інтелекту та приватні компанії викликали занепокоєння наглядових органів?

Не тільки розмовні чат-боти та засоби ідентифікації за фото



Обробка персональних даних

Будь-яка операцію або сукупність операцій з персональними даними або наборами персональних даних, незалежно від того, чи вони виконуються автоматизованими засобами, чи ні. До таких операцій належать: **збір, запис, організація, структурування, зберігання, адаптація або зміна, пошук, консультація, використання, розкриття шляхом передачі, поширення або забезпечення доступності інакшим чином, узгодження або поєднання, обмеження, видалення або знищення**

- **ЗБІР** – коли система штучного інтелекту отримує інформацію про фізичну особу і персональні дані стають доступними для використання;
- **ВИКОРИСТАННЯ** – за допомогою персональних даних як ресурсу, здатного до змін, сучасні технології виконують ті чи інші завдання, отримують певні результати;
- **ЗМІНА ЯКОСТІ** – з одного боку, персональні дані можуть бути виправленими – тим самим ставати більш точними, з іншого – зі зниженням рівня якості персональні дані втрачають чутливість, – наслідком десенсибілізації є й підвищення рівня захищеності;
- **ВИДАЛЕННЯ** – коли інформація перестає існувати у системі штучного інтелекту, а отже не підлягає подальшому використанню.

Способи обробки ШІ

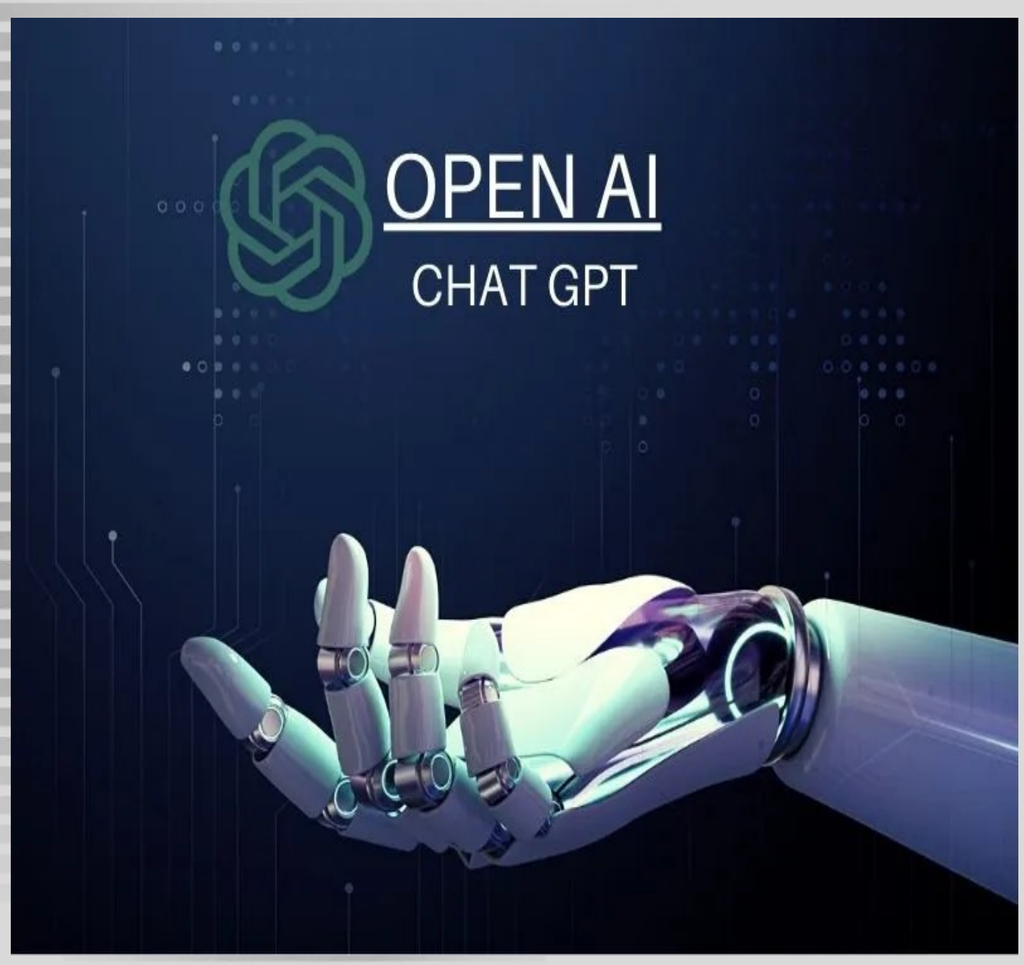
Навчання систем ШІ

Взаємодія з користувачем

Шифрування даних

Маркетингові цілі

Ідентифікація особи



Garante Італії проти OpenAI

3 березня 2023 р. Garante Італії (офіційна назва – Garante per la protezione dei dati personali) з захисту даних до грудня 2024 р. проводив розслідування того, наскільки навчанні та використанні ChatGPT дотримуються положення GDPR

Прогрес технологій v. Захист приватності

- (1) інформування про збір та обробку персональних даних, а також їхній зв’язок з навчанням алгоритмів ChatGPT,(2) надання можливостей відмовитись від обробки персональних даних користувачам та (3) виправляти дані, які не є точними або актуальними, (4) вдосконалення політики конфіденційності та підвищення її видимості,(5) опції перевірки віку, (6) проведення інформаційної кампанії

розблокування	штраф у розмірі 15 млн.євро

CNIL Франції проти Clearview

Наглядовий орган з захисту даних Франції розглядав застосування програмних продуктів Clearview, які дозволяють визначати особу на фотографії

Чи розміщення в Інтернеті робить дані такими, які можна обробляти вільно?

Ст. 6, 12, 15, 17, 31	штраф у розмірі 20 млн.євро


deepseek

Типові порушення

ВИСНОВКИ

Матеріальні порушення

- Недотримання принципів обробки
- Незабезпечення прав суб’єктів
- Відсутність належної підстави
- Загальний режим захисту для окремих категорій персональних даних, насамперед, про дітей

Процедурні порушення

- Відсутність представника в ЄС
- Неготовність оцінки впливів на захист даних
- Відмова взаємодіяти з наглядовими органами (ст. 31)

Європейські фундаментальні цінності у цифрову еру,
Центр Досконалості Жана Моне

101085385 - EFVDE - ERASMUS-JMO 2022-HEI-TCH-RSCH

Особиста автономність
як правова цінність в світлі сучасних технологічних викликів

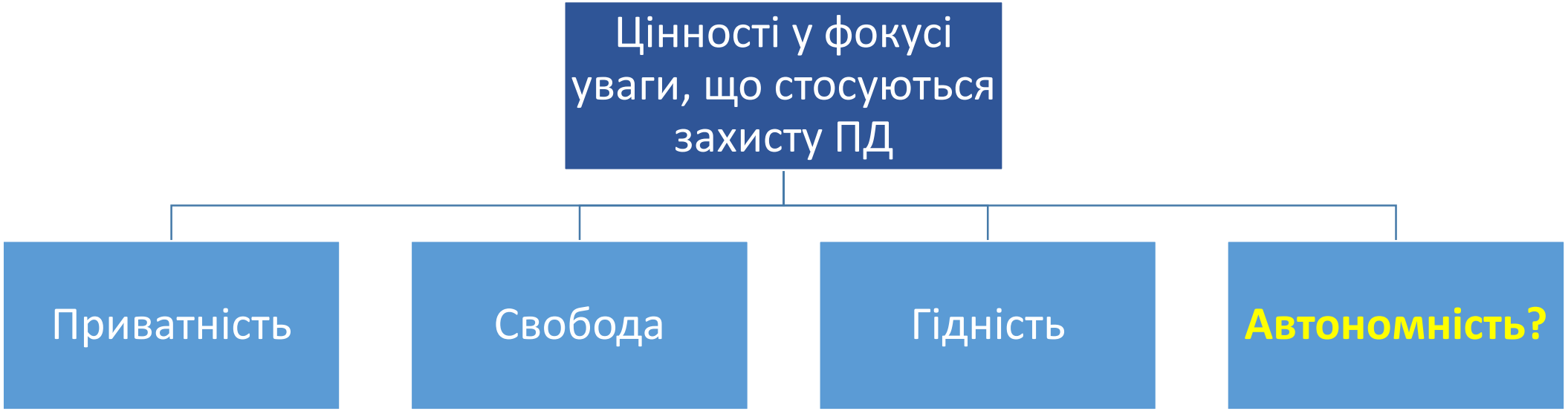
Петро Сухорольський

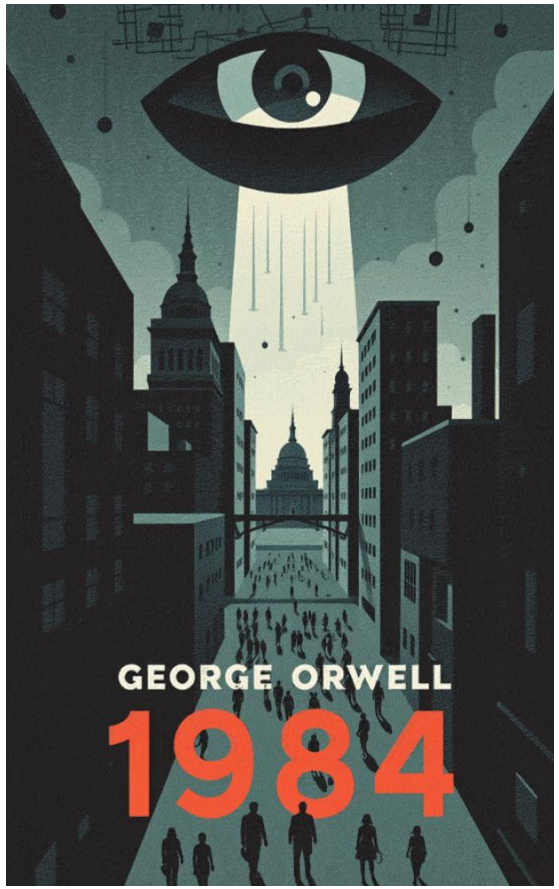
Що саме нам потрібно захищати?

Чому так важлива індивідуальна автономність?

Які загрози створює ШІ для автономності?

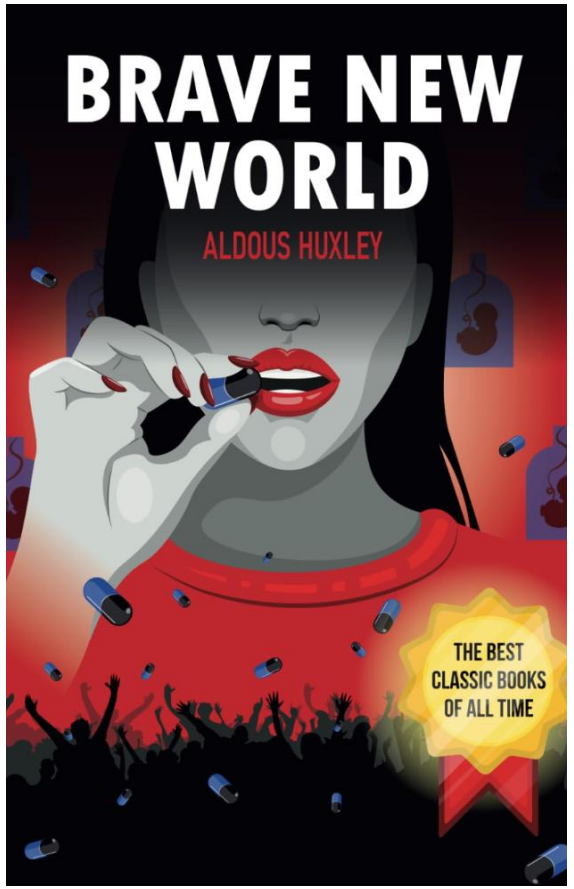
Чи захищають нас правові акти?





Свобода повністю відсутня

Елементи свободи є у пролів, але це не допомагає: «*Пролам можна дозволити свободу, бо в них немає інтелекту*»



Певний варіант свободи є, і це явно видно на прикладі Джона «Дикуна»

Це не допомагає, бо **повністю відсутня автономність**. Неможливість автономності доводить Джона до самогубства

Ніл Мохан, топ-менеджер YouTube: *«Понад **70% часу**, який ви проводите на YouTube, ви переглядаєте ролики, підібрані для вас на основі рекомендацій ШІ»*

Це доказ досконалості алгоритму чи вправних маніпуляцій?

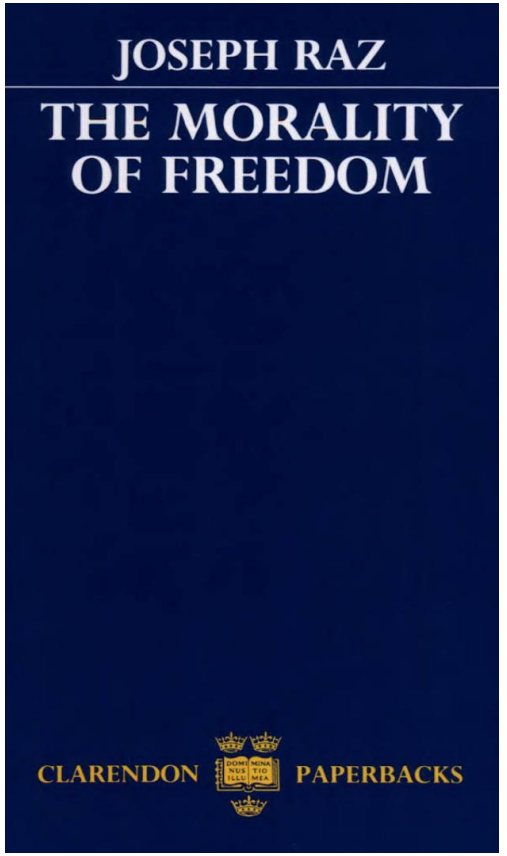
Чи ми НАСПРАВДІ хочемо це дивитися?

- Особиста автономність – найбільш фундаментальна (кінцева) цінність, що є базовою для свободи і гідності
- Людина сама є господарем свого життя, сувереном свого щастя, і **вона сама повинна дозріти до певного рішення**, яке стосується її долі, **сама має зробити вибір і нести за нього відповідальність**
- Автономність включає наявність в людини багатьох цілей та інтересів паралельно, навіть конфліктуючих між собою. І вона в різний час може робити різний вибір, включаючи зміну своїх преференцій

Свобода заслуговує свого імені лише тоді, коли досягнення нашого блага відбувається нашими власними способами.

Принцип свободи вимагає свободи смаків і занять, свободи оформлювати план нашого життя, що відповідає нашому характеру, свободи робити те, що ми хочемо, і приймати можливі наслідки — без жодних перешкод із боку собі подібних, доки те, що ми робимо, не шкодить їм, навіть якщо наша поведінка здається їм дурною, збоченою чи хибною.

Джон Стюарт Мілль



Умови автономності – **колективні блага**. Завдання уряду – їх розвивати.

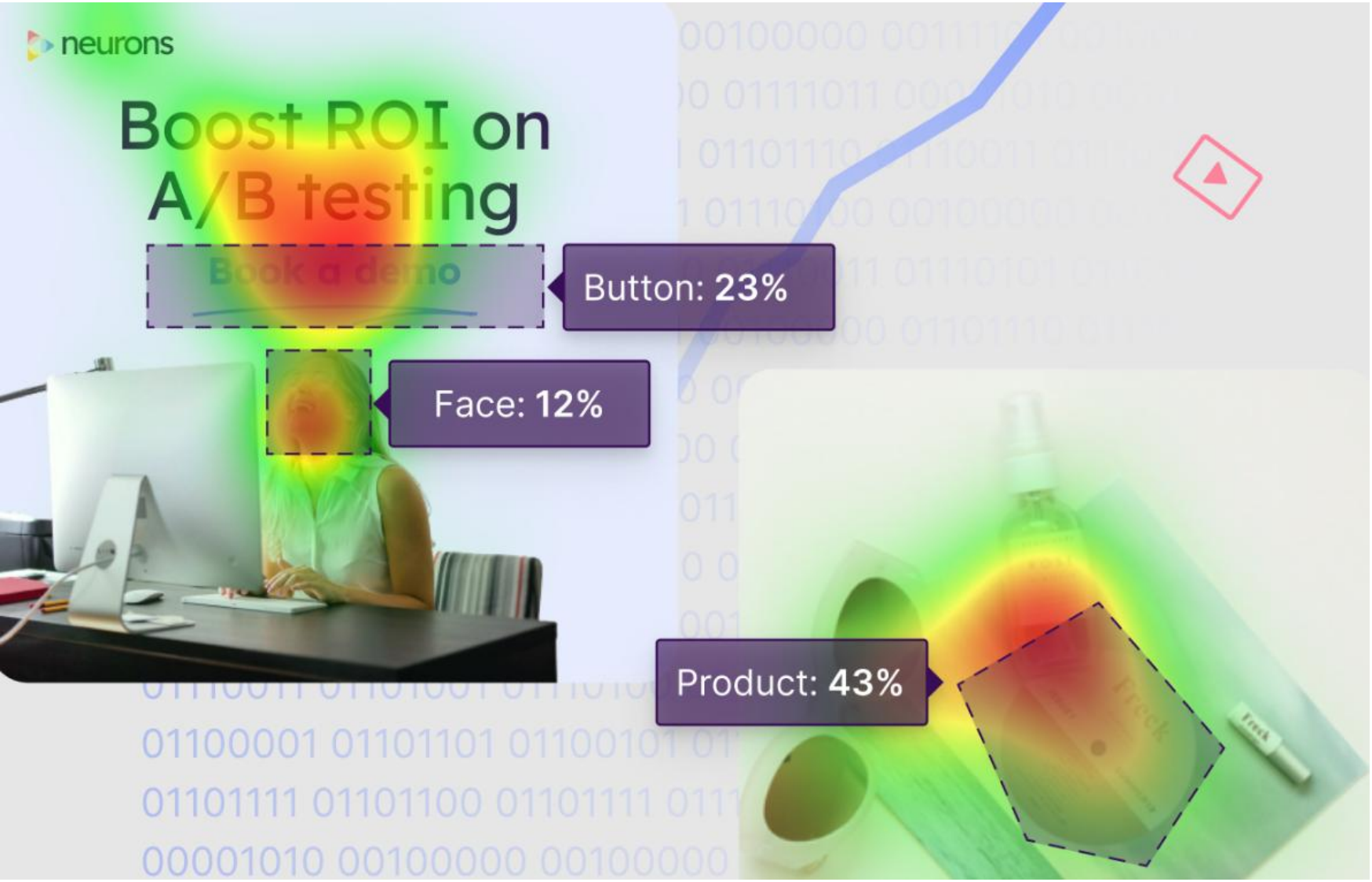
Позитивна свобода отримує свою цінність від свого внеску в особисту автономність. *Обсяг та зміст **позитивної свободи** визначається через внесок спірного елемента в автономність.*

Держава може застосовувати примус (а також маніпуляції), тобто зменшувати персональну автономність однієї людини, лише коли це обґрунтовано захистом персональної автономності інших осіб

Екосистема постійних і витончених онлайн-маніпуляцій: маніпуляції увагою, вибором, відчуттями, станами, середовищем, дизайном тощо

Маніпуляції на всіх етапах користування сервісами

ШІ та досягнення нейронауки допомагають набагато підвищити ефективність і персоналізацію маніпуляцій



Онлайн-платформа чи рекламодавець знають про користувача значно більше, ніж він сам

Хто *клієнт*, а хто *ресурс*?

When we go online, we are **following scripts written by others**

Штучний «*інтелект*»

Алгоритми: «*думають*», «*розпізнають*», «*бачать*», «*розуміють*», «*роблять висновки*».

Cindy Grimm, Professor of robotics: Modern AI or robotic system is still far less complex than the average bacterium and it will just "do" what you want.

Потрібно використовувати **механістичну та педантичну мову**, коли ми говоримо про ШІ

What is an AI Hallucination?

An AI hallucination is a false or misleading output generated by an artificial intelligence system. It can be a confident response by an AI that does not seem to be justified by its training data.

nature human behaviour

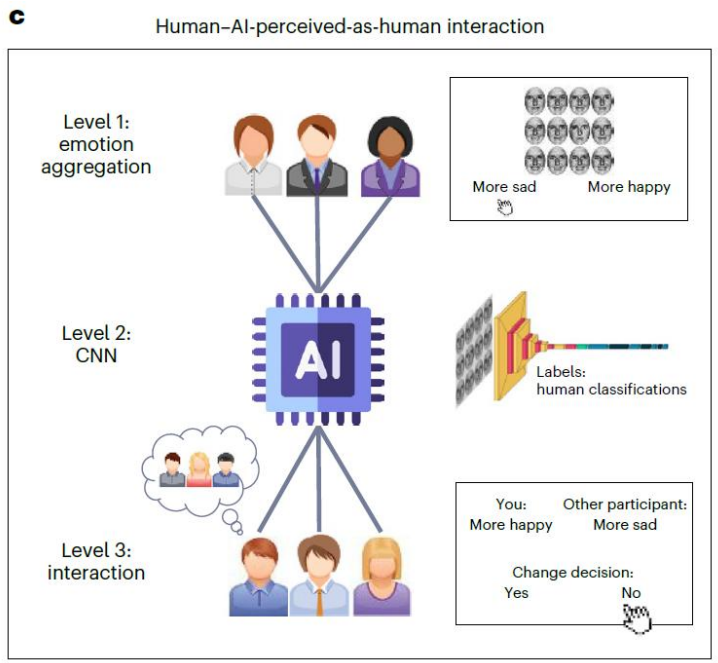
Article

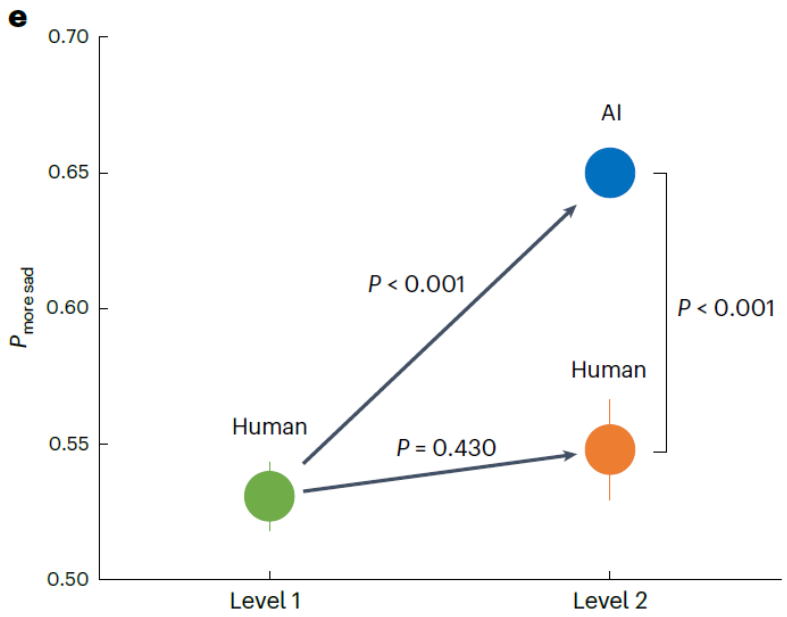
https://doi.org/10.1038/s41562-024-02077-2

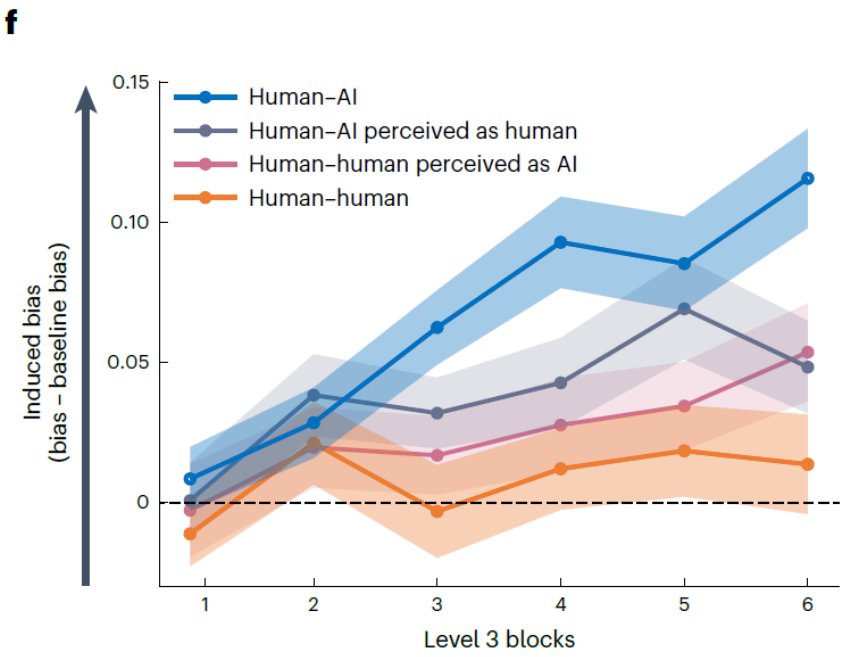
How human–AI feedback loops alter human perceptual, emotional and social judgements

Received: 24 March 2023

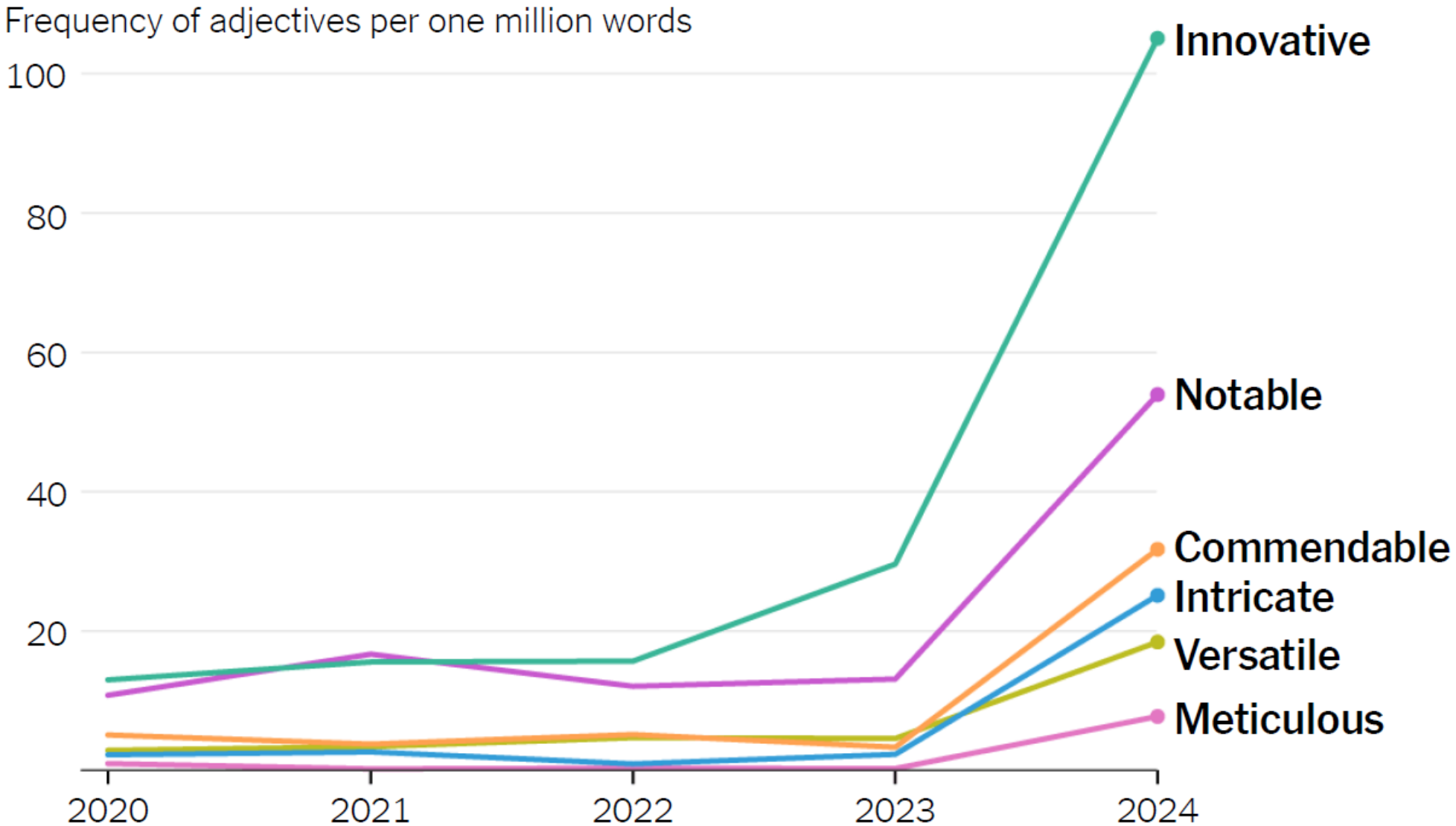
Moshe Glickman [1,2] & Tali Sharot [1,2,3]

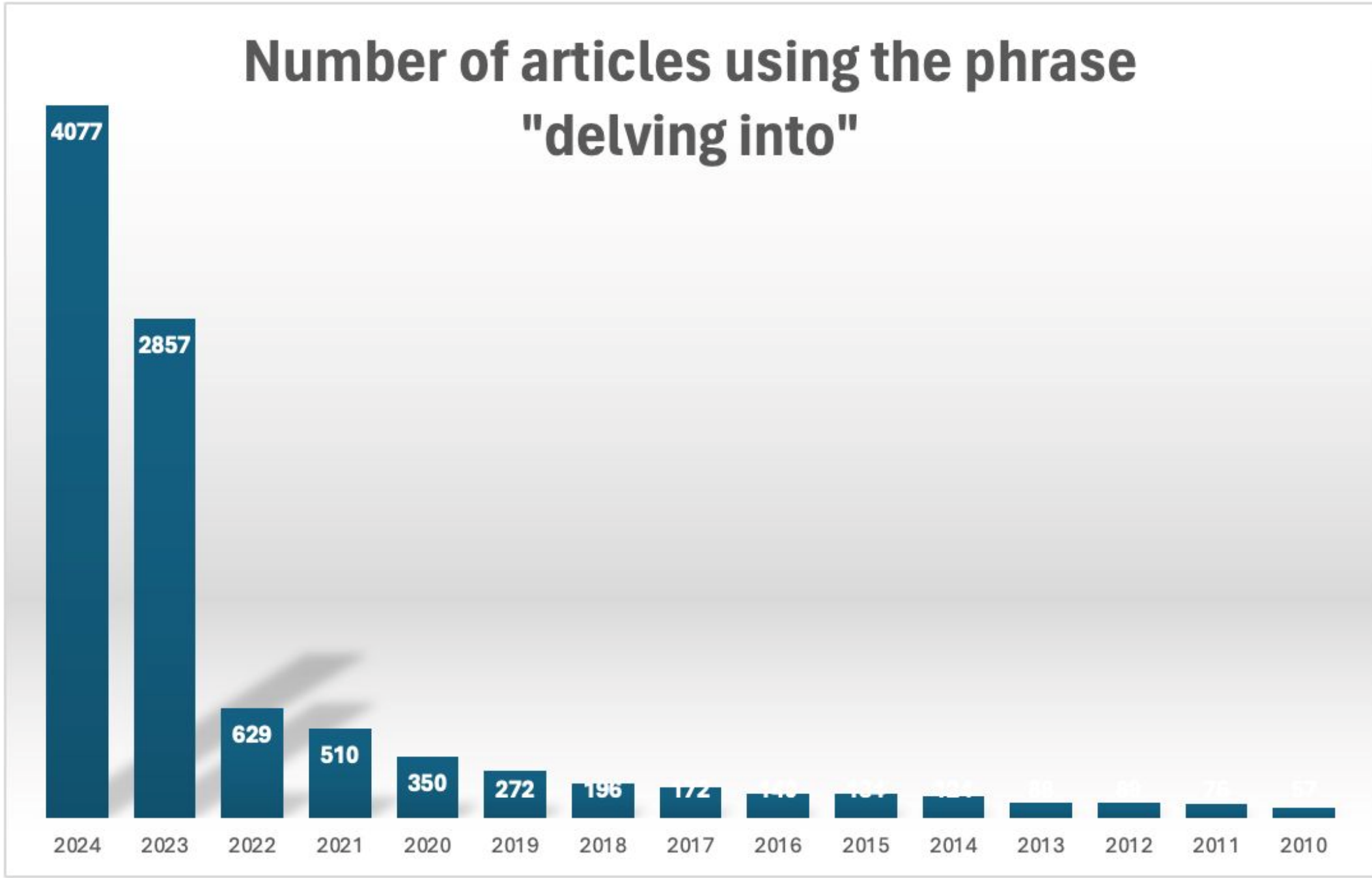






Adjectives associated with A.I.-generated text have increased in peer reviews of scientific papers about A.I.




Number of articles using the phrase "delving into"
4077
2857
629
510
350
272
196
2024
2023
2022
2021
2020
2019
2018
2017
2016
2015
2014
2013
2012
2011
2010

The New York Times

https://www.nytimes.com/2024/03/29/opinion/ai-internet-x-youtube.html

GUEST ESSAY

A.I.-Generated Garbage Is Polluting Our Culture

March 29, 2024

By Erik Hoel
Mr. Hoel is a neuroscientist and novelist and the author of The Intrinsic Perspective newsletter.

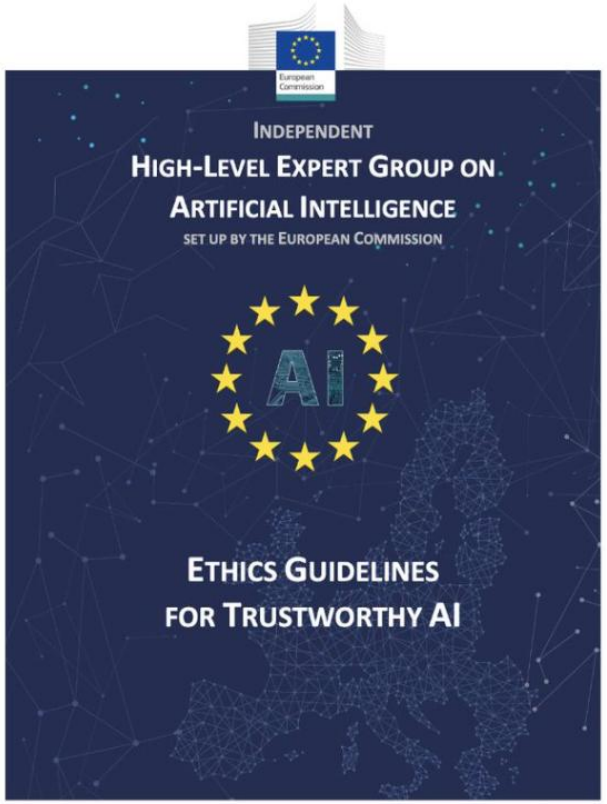
Einstein supposedly said: “If you want your children to be intelligent, read them fairy tales. If you want them to be very intelligent, read them more fairy tales.” But what happens when a toddler is consuming mostly A.I.-generated dream-slop?

There’s so much synthetic garbage on the internet now that A.I. companies and researchers are themselves worried, not about the health of the culture, but about what’s going to happen with their models.

Питання персональної автономності у актах щодо регулювання ШІ

European Commission's High-Level Expert Group's Ethics Guidelines for Trustworthy AI

Respect for human autonomy is strongly associated with the right to human dignity and liberty. AI systems should not unjustifiably subordinate, coerce, deceive, manipulate, condition or herd humans and should be designed to augment, complement and empower human cognitive and cultural skills.



Montreal Declaration for Responsible AI

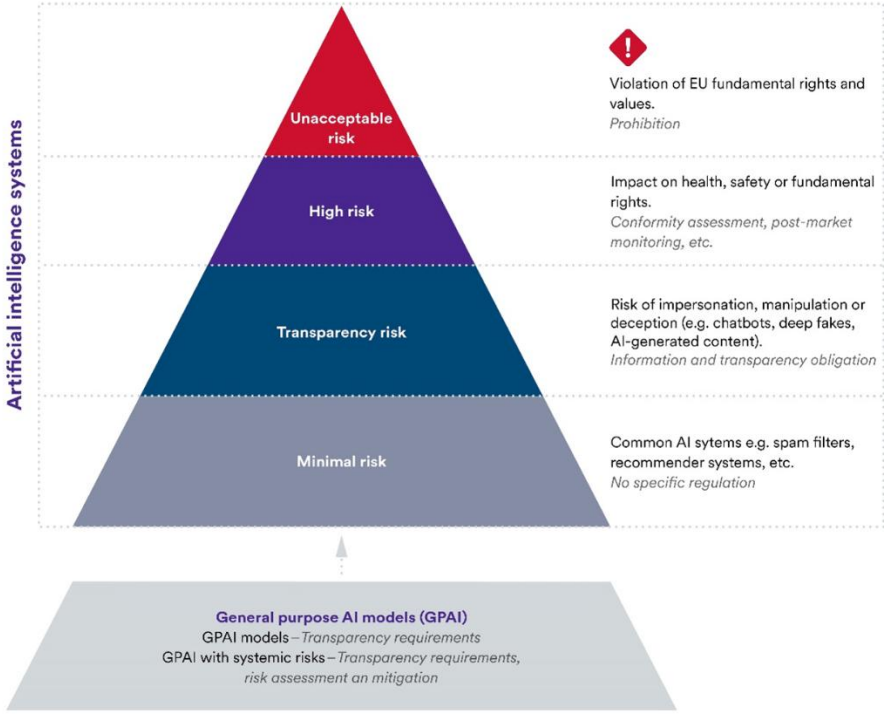
Principle of respect for autonomy. The right of persons to achieve their goals and live in accordance with their values and ethical beliefs. Goverments and companies should not promote or discredit a certain conception of the good life. We must empower citizens by ensuring access to relevant forms of knowledge, promoting the learning of fundamental skills and encouraging the development of critical thinking.

AI Act

Питання особистої автономності відсунуті на периферію: автономність згадано лише 2 рази в преамбулі і жодного разу в статтях.

Ст. 5 забороняє використання ШІ-систем, які «deploys **subliminal techniques** beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to **cause that person, another person or group of persons significant harm**».

1) Як довести, що техніки «підсвідомі»?
2) Головна шкода – соціальна, а не для особи чи групи.
3) Стандартні інтерпретації прав людини не враховують розглянуті загрози для автономності.



Рішення з боку політико-правової системи

Неефективність механізму згоди на опрацювання персональних даних чи розміщення кукіз

Замінити її на оцінку ризиків в межах співпраці великого бізнесу і влади

Чи сприяє таке рішення збільшенню автономності людини?

Конвенція Ради Європи про ШІ

Роль і загрози для автономності чітко відзначені.

Повага до індивідуальної автономності поряд із повагою до гідності закріплена у окремій статті як ключовий принцип – перший у переліку із семи принципів.

Преамбула Конвенції: *artificial intelligence systems may undermine human dignity and individual autonomy, human rights, democracy and the rule of law*

Конвенція відводить для автономності фундаментальне місце – поряд з гідністю та перед правами людини, демократією і верховенством права

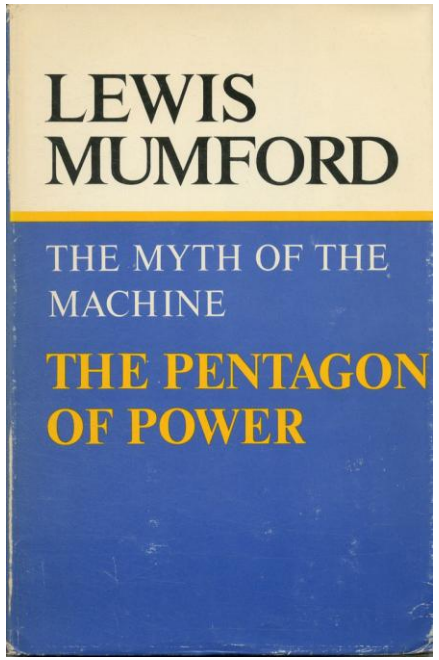
Article 7 – Human dignity and individual autonomy

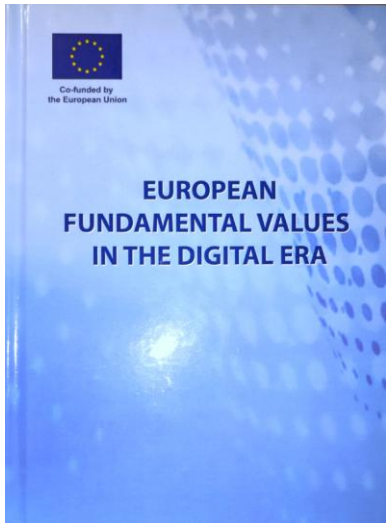
Each Party shall adopt or maintain measures to respect human dignity and individual autonomy in relation to activities within the lifecycle of artificial intelligence systems.

За допомогою цієї нової «мегатехніки» домінантна меншість створить однорідну, всеохопну, супер-планетарну структуру, призначену для автоматичної роботи. Замість того, щоб активно функціонувати **як автономна особистість**, людина **стане пасивною, безцільною, машинно обумовленою твариною**.

Всезегальний нагляд — це не просто вторгнення в приватне життя, а повне знищення автономності: власне, розкладання людської душі.

Льюїс Мамфорд, 1967





Література

- Sukhorolskyi P.M. Respect for Personal Autonomy in AI Regulatory Framework. *Problems of Legality*. 2025. 168. P. 6-25.
- Sukhorolskyi P. Fundamental Values of Data Protection Law: Autonomy vs the Megamachine. *European Fundamental Values in the Digital Era* : [monograph] / eds.: Yulia Razmetaeva, Nataliia Filatova-Bilous. Kharkiv : Pravo, 2024. P. 79–103.