



University of
Nottingham

UK | CHINA | MALAYSIA

Upholding EU fundamental rights in a digital era

Dr Mando Rachovitsa, Associate Professor in Human Rights Law,
School of Law, University of Nottingham
Trier, 16 June 2026



Co-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 the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

EU fundamental rights

EU Charter

ECHR

(Art 53 EU Charter)

**General principles of
EU law (domestic)**

**EU law for addressing
algorithmic harms
(e.g., AI Act, DSA)**

**Council of Europe,
Framework Convention on AI,
Human Rights, Democracy
and the Rule of Law**

ratified by EU



Council of Europe Treaty Series - No. 225

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

Vilnius, 5.IX.2024

- first international treaty / ensure that AI activities are fully consistent with human rights, democracy and the rule of law
- does not create new human rights / reinforces the role of existing human rights law
- Being a framework convention, it establishes broad commitments leaving detailed regulation to subsequent agreements, non-binding instruments, or national legislation

human rights law vs ethical approaches to AI

- ✓ binding
- ✓ rights of individual
- ✓ obligations of state
- ✓ remedies

Today's topics

1. Human rights law's capacity to capture novel AI harms
2. Pronounced challenges accessing and assessing evidence
3. Is human rights law relevant in private law relations?
4. The use of certain AI systems incompatible with human rights law?
5. Fundamental rights impact assessments (and remedies?) (case study)

How Dutch activists got an invasive fraud detection algorithm banned

The Dutch government has been using SyRI, a secret algorithm, to detect possible social welfare fraud. Civil rights activists have taken the matter to court and managed to get public organizations to think about less repressive alternatives.

Poland: Government to scrap controversial unemployment scoring system

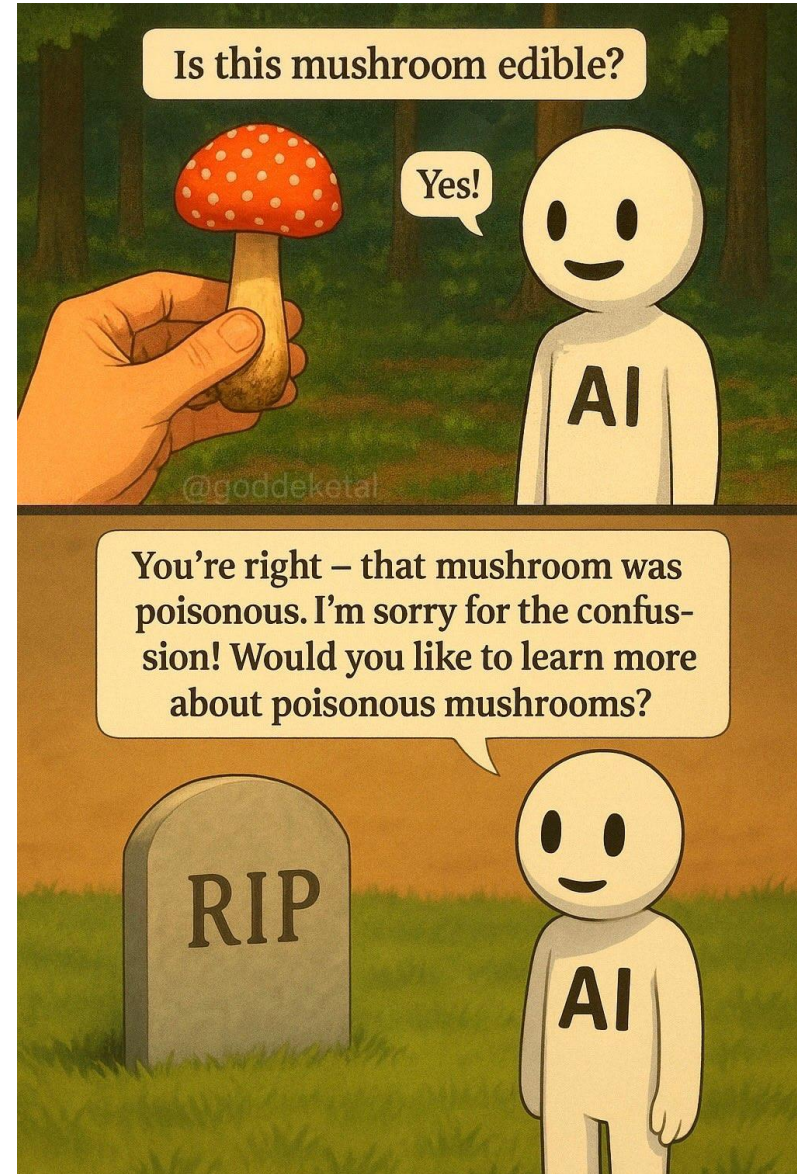
DWP algorithm wrongly flags 200,000 people for possible fraud and error

Exclusive: Two-thirds of housing benefit claims marked as high risk in last three years were legitimate, figures show

The machines that will predict the criminals of the future

The Ministry of Justice will deploy machine learning to identify at-risk children for early intervention and to help prevent them falling into a life of crime

Since 2023....
general-purpose AI systems

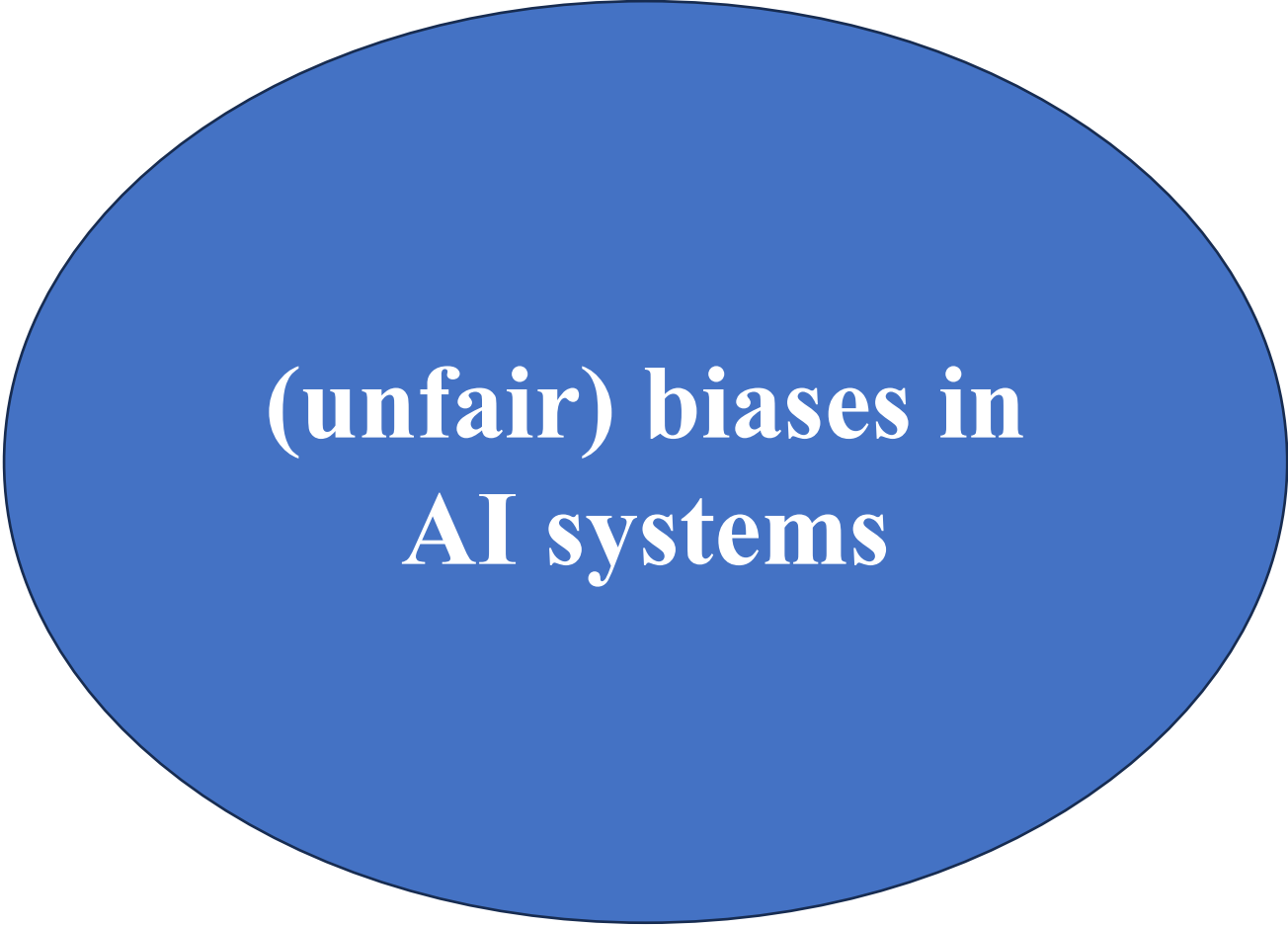


1. Novel AI harms

Figure 1: Sociotechnical harms taxonomy overview.



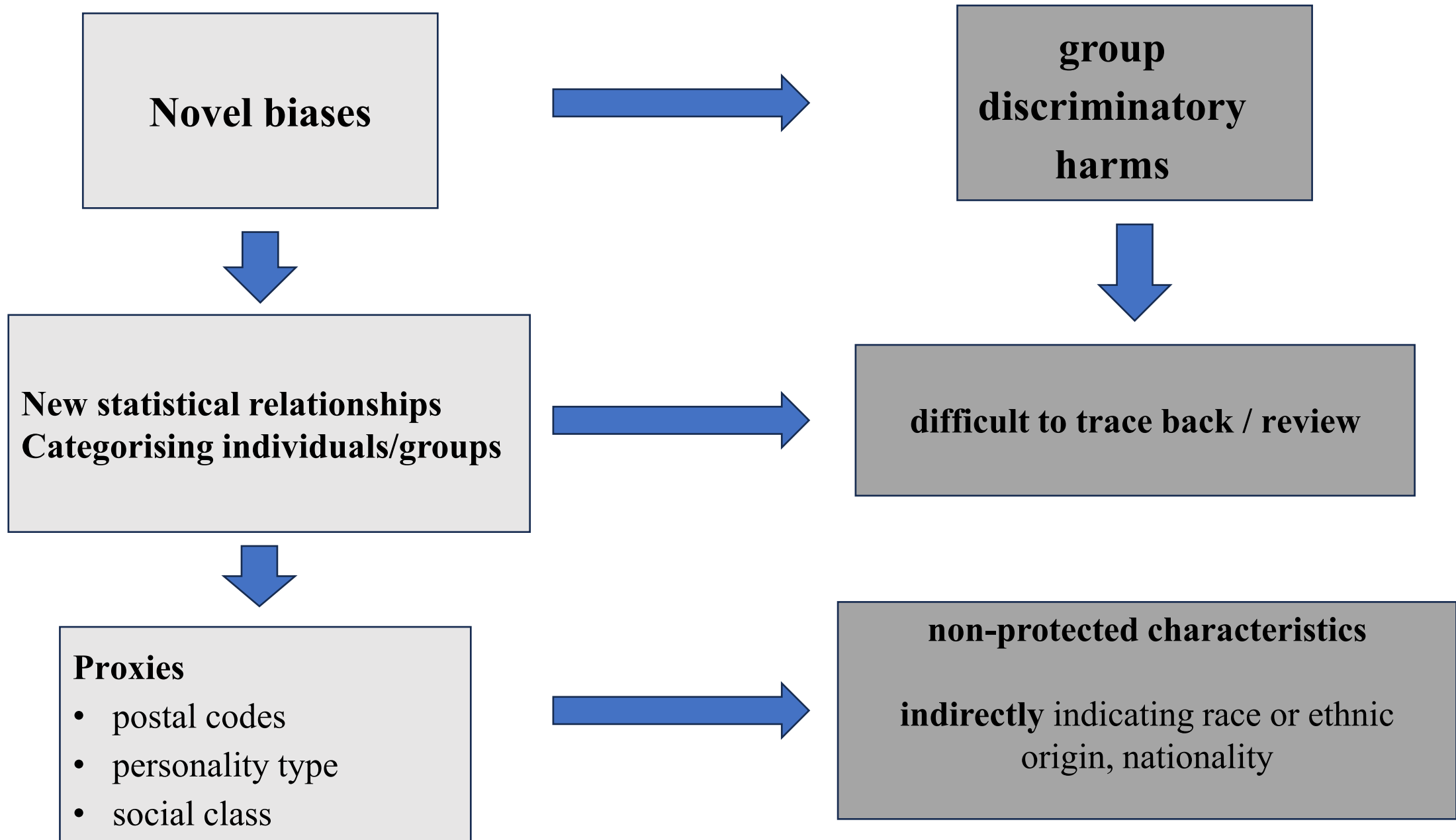
Example 1: discriminatory harms



**(unfair) biases in
AI systems**



**discrimination
in law**



Example 2: manipulation, political participation

[Commission opens formal proceedings against TikTok on election risks under the Digital Services Act](#), 17 December 2024

the Commission has opened formal proceedings against TikTok in relation to TikTok's obligation to properly assess and mitigate systemic risks linked to election integrity, notably in the context of the recent Romanian presidential elections

- undue influence voters and their political behaviour, including casting their vote
- compromise individuals' ability to freely form opinions
- erode the overall environment which gives rise to the formation of political views and political participation

Bradshaw and Others case

- assess the UK's response to the threat of Russian election interference

158. While the Court does not underestimate the threat posed by the spreading of disinformation and the running of “influence campaigns”, their nature is nevertheless such that it is difficult to assess accurately the impact that they may have on individual voters and, by extension, on the outcome of a given election.

difficult to assess accurately the impact on

- individual voters
- the outcome of a given election

Other regulatory approaches

Article 5(2) AI Convention – Integrity of democratic processes and respect for the rule of law

Each Party shall adopt or maintain measures that seek to protect its **democratic processes** in the context of activities within the lifecycle of AI systems, including **individuals' fair access to and participation in public debate**, as well as their **ability to freely form opinions**.

Article 34(1)(c) DSA

VLOPs shall diligently identify, analyse and assess any systemic risks stemming from the design or functioning of their service

- **actual or foreseeable negative effects on electoral processes and civic discourse**

2. Pronounced challenges accessing & assessing evidence

Algorithmic opacity & inability to access evidence on AI systems:

- accessing evidence and burden of proof
- contesting and substantiating claims
- barrier to effective judicial oversight
- inability to prove victim status
- capacity of judges/courts to assess complex evidence

SyRI case

Intentional algorithmic opacity: “game the system”

6.49 The court finds that it is unable to assess the correctness of the position of the State of the precise nature of SyRI because the State has not disclosed the risk model and the indicators of which the risk model is composed or may be composed. In these proceedings the State has also not provided the court with objectively verifiable information to enable the court to assess the viewpoint of the State on the nature of SyRI. The reason the State gives for this is that citizens could then adjust their conduct accordingly. This is a deliberate choice of the State. That choice also coincides with the starting point of the legislator regarding the provision of information on SyRI. The SyRI legislation does not show how the decision model of SyRI functions and which indicators are or can be used in a SyRI project [...], i.e. which factual data make or can make the presence of a certain situation plausible.

- **SyRI case:** use of SyRI has a discriminatory and stigmatising effect?
- **Evidence & burden of proof lies with whom?**

6.93 It is correct that to date SyRI has only been applied to so-labelled ‘problem districts’, as confirmed by the State at the hearing. This in and of itself need not imply that such use is disproportionate or otherwise contrary to Article 8 paragraph 2 ECHR in all cases. However, given the large amounts of data that qualify for processing in SyRI, including special personal data, and the circumstance that risk profiles are used, there is in fact **a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background**

6.95 the court is of the opinion that the SyRI legislation contains **insufficient safeguards** to protect the right to respect for private life in relation to the risk indicators and the risk model which can be used in a concrete SyRI project.
[...]

Inability to prove victim status

- ❑ the otherwise infamous *SyRI* case would have not been decided unless a unique provision in Dutch legislation existed.
- ❑ case was brought by a coalition of Dutch civil society organisations and two Dutch citizens
- ❑ admissibility of the claims, the court noted that two of the claimants were Dutch citizens who lacked standing due to the absence of ‘sufficiently concrete and personal interest’
- ❑ civil society interest groups and were able to benefit from a rather unique public interest litigation provision in the Dutch Civil Code. The court accepted that the civil society groups had a legal interest to bring proceedings seeking to protect the interests of their support base

US Loomis case: **capacity of courts to assess evidence**

❑ predictive algorithms used in sentencing / COMPAS risk assessment tool

due process right to be sentenced based on accurate information

- COMPAS score's use violated his right to an individualised sentence, since the generated data was based on group statistics

not able to understand how his COMPAS score was calculated due to the proprietary nature of system

- prevents a defendant from challenging the scientific validity of the risk assessment

the defendants' right to due process was not violated by the mere fact that they could not gain access to an adequate explanation of the AI since the accuracy of the tools and the capacity of the judges to understand possible malfunctioning were adequate

- despite concerns and empirical evidence that COMPAS disproportionately classified minority offenders as higher risk.

Is the capacity of judges to assess complex evidence overstated?

ECtHR, Yüksel Yalçınkaya v Türkiye (GC)

specific types of evidence (in this instance encrypted electronic data) raise particular difficulties for the judiciary given the fact that technologies involved are complex and **‘may therefore diminish the ability of judges to establish its authenticity, accuracy and integrity’**.

3. Is human rights law relevant in private law relations?



Private governance of AI systems

- Design & deploy technology (e.g., AI chatbot, recommender system)
- Terms & Conditions
- Applicable law
- Private remedies (e.g., moderation, internal complaint mechanisms, out-of-court dispute settlement, META Oversight Board)

1. Do states have an obligation (under human rights law) to regulate relations between individuals/private actors?

→ DSA, AI Act [obligations – no rights to individuals]

2. Art 14 DSA

3. Civil litigation before domestic courts to enforce terms of service (e.g., contract law, consumer law)

Article 14 DSA – terms & conditions

1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions [...]

4. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, **with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights** of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.

Civil litigation before domestic courts to enforce terms of service

Amsterdam District Court, FvD c.s. v Google Ireland Ltd, 2021

- removal of video of a Dutch political party because in violation of T&C

Court of Appeal Ghent, Vandendriessche v Meta Ireland, 2024

- “shadowbanning” / visibility of content

✓ **the standards of reasonableness and fairness under civil law**

✓ **principle of good faith performance of contracts**

Article 10 of the ECHR, which establishes the right to freedom of expression, may have an effect on private law relations, for example through the interpretation of open norms of private law, such as the obligation to act in accordance with the standards of reasonableness and fairness when performing a contract

Only if the obstacles make “*any effective exercise*” impossible, or if “*the essence of the right has been destroyed*”.

4. The use of certain AI systems incompatible with human rights law?

Suggestions highlighted by UN human rights bodies:

- social scoring practices
- remote biometric surveillance systems

raise serious concerns due to their highly intrusive nature and broad impact on many people.

- unclear consensus & hesitance
- AI Convention does not provide any red lines leaves discretion to State parties to assess the need for banning (Article 16(6))
- The AI Act is the only legally binding instrument that prohibits the use of certain AI systems.

Prohibited AI systems - Art 5 AI Act

- manipulation and exploitation of vulnerabilities
- social scoring practices
- predictive policing
- creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV
- sentiment detection
- biometric categorisation systems that categorise individuals based on their biometric data to deduce or infer sensitive characteristics
- real-time remote biometric identification systems in publicly accessible spaces for law-enforcement purposes

Prohibition of the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement (Article 5(1)(h) EU AI Act)

- biometric identification?
- remote (at a distance)
- retrospective use is not prohibited - subject to safeguards for the high-risk AI systems
- publicly accessible space

unless and in so far as such use is strictly necessary for one of the following objectives:

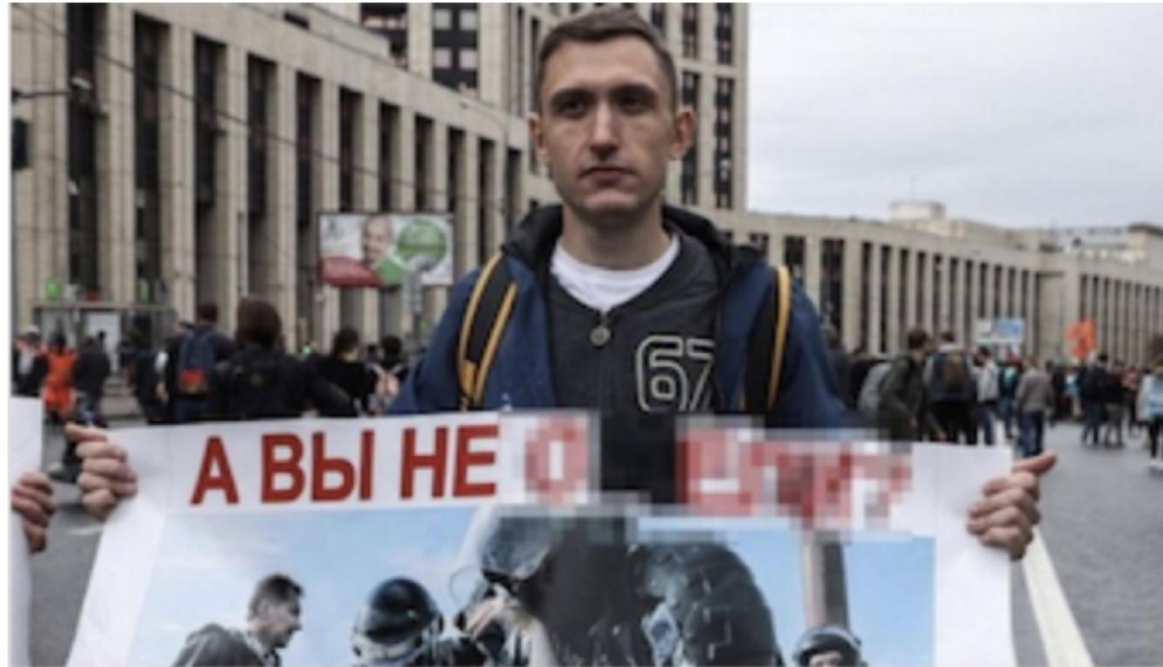
- ❑ the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons
- ❑ the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack
- ❑ the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years

+ **subject to additional safeguards: Art 5(2) and (3))**

- shall be authorised only if the law enforcement authority has completed a **fundamental rights impact assessment**
- **each use [...]** shall be subject to a **prior authorisation** granted by a judicial authority or an independent administrative authority
- comply with **necessary and proportionate** safeguards and conditions
 - the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used
 - the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences

Glukhin v Russia

- first judgment by the ECtHR on facial recognition technology



Mr Konstantin Kotov

88. The Court [...] considers that the use of **highly intrusive** facial recognition technology to identify and arrest participants in peaceful protest actions could have a **chilling effect** in relation to the rights to freedom of expression and assembly.

90. the use of highly intrusive facial recognition technology in the context of the applicant's exercising his Convention right to freedom of expression is **incompatible with the ideals and values of a democratic society** governed by the rule of law, which the Convention was designed to maintain and promote.

societal & human rights law implications of such surveillance?

- may affect the private life of a large part of the population
- evoke a feeling of constant surveillance
- individuals might change their behaviour
- indirectly dissuade the exercise of fundamental rights
- technical inaccuracies - biased results - discriminatory effects

Accounting for, and incorporating, the chilling effect in data protection impact assessments

Information Commissioner's Opinion, [The use of live facial recognition technology in public places](#), 2021

The focus is on the potential for the deployment of LFR to cause any type of direct or indirect impact, and material or non-material damage.

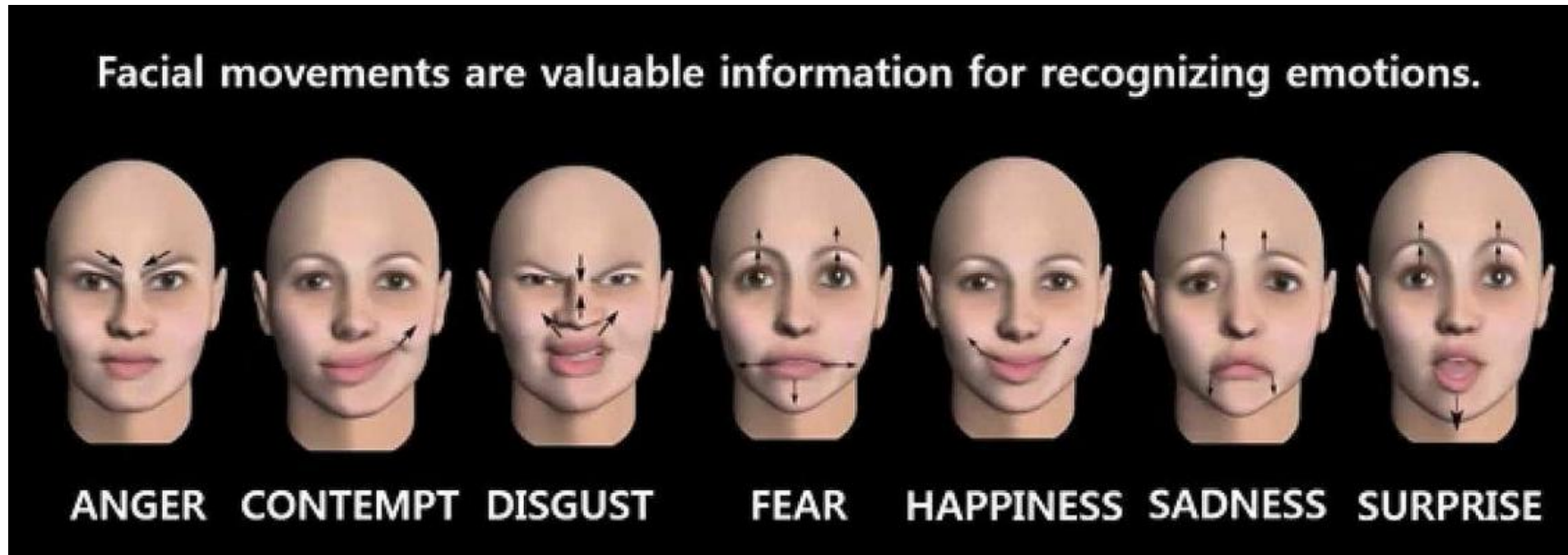
Where LFR is used for the automatic collection of biometric data in public places, controllers should consider at least any potential:

- inability to exercise any legal rights
- inability to exercise any specific data protection rights, including the right to be informed, the right of access and the right to object
- inability to opt-out of the processing
- loss of control over the use of personal data
- inability to access services or opportunities
- direct or indirect impact on individuals' ability to exercise their rights and freedoms in this public setting, such as freedom of expression, assembly and association, including any potential inhibiting effect

sentiment detection (Article 5(1)(h) EU AI Act)

the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of **workplace** and **education** institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons

infer a person's inner emotional state based on physical, physiological or behavioural markers (e.g., facial expressions, vocal tone) and sort them into discrete categories (e.g., angry)



5. Fundamental rights impact assessments (and remedies?)

How do we think about adverse AI impacts at-scale?

Collective, systematic harms cause by AI systems across entire demographics?

**Article 34(1) DSA
risk assessment**

**Article 16 AI Convention
risk & impact assessment**

**Article 27(1) AI Act
fundamental rights impact assessment**

**Netherlands
Canada**

fundamental rights impact assessment (Art 27 AI Act)

- mandatory compliance obligation for high-risk systems
- public + private sector

High-risk AI systems (Art 6 + Annex III)

- significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law
- critical infrastructures (e.g. water, gas, electricity)
- medical devices
- educational institutions or for recruiting people
- law enforcement / border control
- administration of justice
- democratic processes
- biometric identification / categorisation / emotion recognition

Article 27(1) AI Act, Fundamental rights impact assessment for high-risk AI systems

Prior to deploying a high-risk AI system [...] deployers [...] shall perform **an assessment of the impact** on fundamental rights **that the use of such system may produce**.

For that purpose, deployers shall perform an assessment consisting of:

- (a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;
- (b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used
- (c) the categories of natural persons and groups likely to be affected by its use in the specific context;
- (d) the **specific risks of harm likely to have an impact** on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph [...]
- (e) a description of the implementation of human oversight measures, according to the instructions for use;
- (f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

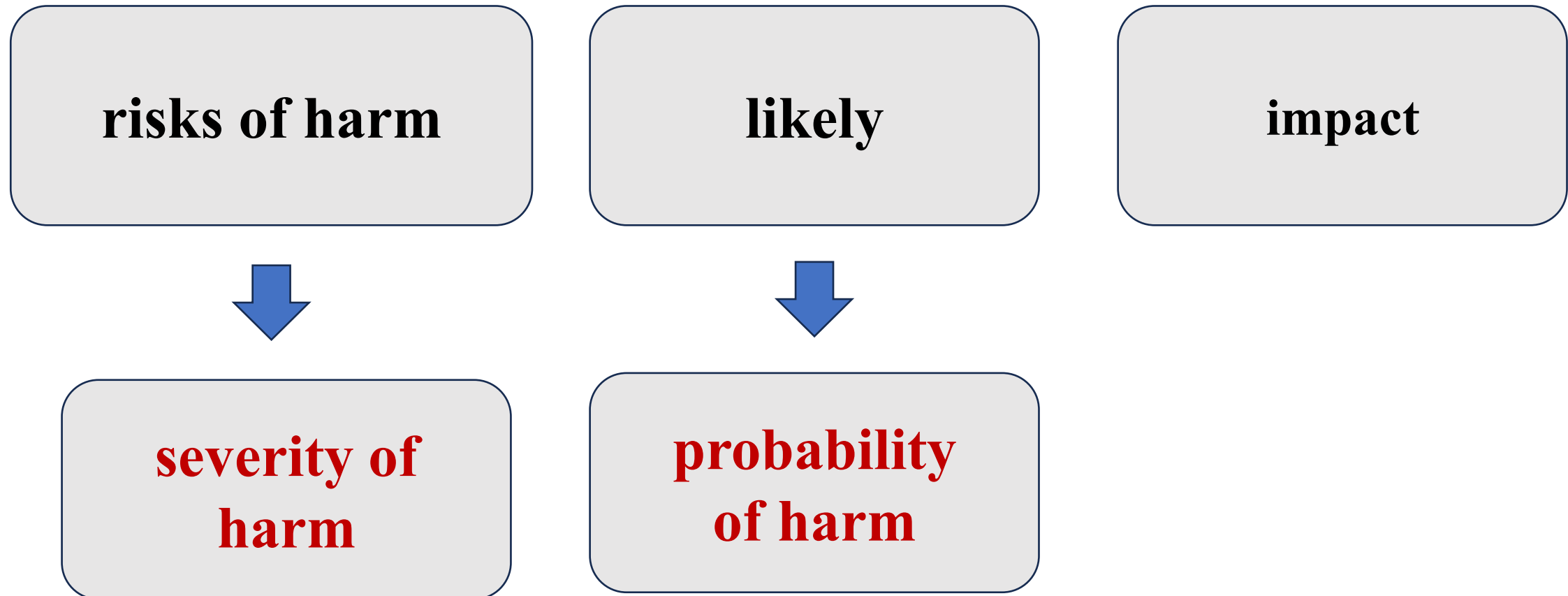
impact assessments do not concern specific individuals / violations

tool to identify, assess, mitigate **adverse impacts at-scale**

impact assessments do **not** reveal real-world harms
exercise trying to capture/ “proxy” real-world harm

‘an assessment of the impact on fundamental rights that the use of such system may produce’

- ‘the specific risks of harm likely to have an impact on individuals/groups’



e.g. human rights (recital 48 AI Act)

- the right to human dignity
- respect for private and family life, protection of personal data
- freedom of expression and information
- freedom of assembly and of association
- the right to non-discrimination
- the right to education
- consumer protection
- workers' rights
- the rights of persons with disabilities
- gender equality
- intellectual property rights,
- the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence
- children's rights
- environmental protection

Scale of the potential adverse impacts

Scope of the potential adverse impacts

- number of persons affected
- protected characteristics or vulnerability of individuals / groups
- timeframe of the impacts

Reversibility of the potential adverse impacts

Probability of the potential adverse impacts

Stakeholder engagement?