ODIHR – NHRI Academy 2022: AI and Human Rights

20-24 June 2022, Tirana, Albania

Day 2 – Session 4

ONGOING REGIONAL REGULATORY INITIATIVES ON AI: THE EU AND COUNCIL OF EUROPE

Trainer: Francesca Fanucci

European Center for Not-for-Profit Law

www.ecnl.org

@enablingNGOLaw

CoE (CAHAI) Possible Elements for AI regulatory framework

Legally binding transversal instrument:

- Setting out general principles and specific legal norms governing the development, design and application of AI systems
- Preventing and/or mitigating risks emanating from applications of AI systems with the potential to interfere with the enjoyment of human rights, the functioning of democracy and the observance of the rule of law
- Facilitating accession by States outside of the region that share CoE standards.

+ sectoral binding/non-binding instruments

Copyright © 2021 ECNL

CoE (CAHAI) Possible Elements for AI regulatory framework

Scope of framework:

- Matters relating to **national defence** not covered
- Inclusion of "dual use" (military/civil) systems and "national security" to be discussed

Copyright © 2021 ECNL

CoE (CAHAI) Possible Elements for AI regulatory framework

General approach:

- Applicable to the development, design and application of AI systems, **irrespective of** whether these activities are undertaken by **public or private actors**
- Nature of risk posed to human rights, democracy and the rule of law => proportionate legal requirements to the design, development and use of AI systems
- Basic principles (e.g., transparency) applicable to ***all*** AI systems as precondition to identify risks
- **Positive rights** of individuals in relation to the development, design and application of AI systems + **related obligations** upon Member States
- Possibility of putting a **full or partial moratorium or ban** on the application of AI systems with unacceptable risks

Copyright © 2021 ECNL

CoE (CAHAI) Possible Elements for AI regulatory framework

Risk Assessment

Methodology for risk classification of AI systems with an emphasis on human rights, democracy, and the rule of law:

- **All AI systems** should undergo **an initial review** ("**risk assessment**") to assess "*potential risk on the enjoyment of human rights, the functioning of democracy and the observance of the rule of law*" & determine **risk classification** (e.g., low, high, unacceptable);
- Where "**clear and objective indications of relevant risks emanating from the application of an AI system**" are identified => more detailed Human Rights, Democracy and Rule of Law Impact Assessment ("**HUDERIA**")

Copyright © 2021 ECNL

CoE (CAHAI) Possible Elements for AI regulatory framework

Other recommended provisions:

- Prevention of "**unlawful harm**" potentially stemming from the development, design, and application of AI systems (including clarifying the concept of "unlawful harm");
- Respect of **equal treatment and nondiscrimination** of individuals in relation to the development, design, and application of AI systems;
- ensuring **gender equality** and **rights related to vulnerable groups and people in vulnerable situations**, **including children** throughout lifecycle of AI systems
- Requirement to establish **data governance mechanisms** to assess and ensure the data accuracy, integrity, security and representativeness
- Provisions on **robustness, safety** and **cybersecurity, transparency, explainability**, **auditability, accountability** and **necessary level of human oversight**
- **Protection of whistleblowers**
- **Safeguards:**
  - effective remedy before a national authority (including judicial authorities)
  - right to be informed about the application of an AI system in the decision-making process;
  - right to choose interaction with a human in addition to or instead of an AI system,
  - right to know that one is interacting with an AI system rather than with a human

Copyright © 2021 ECNL

CoE (CAHAI) Possible Elements for AI regulatory framework

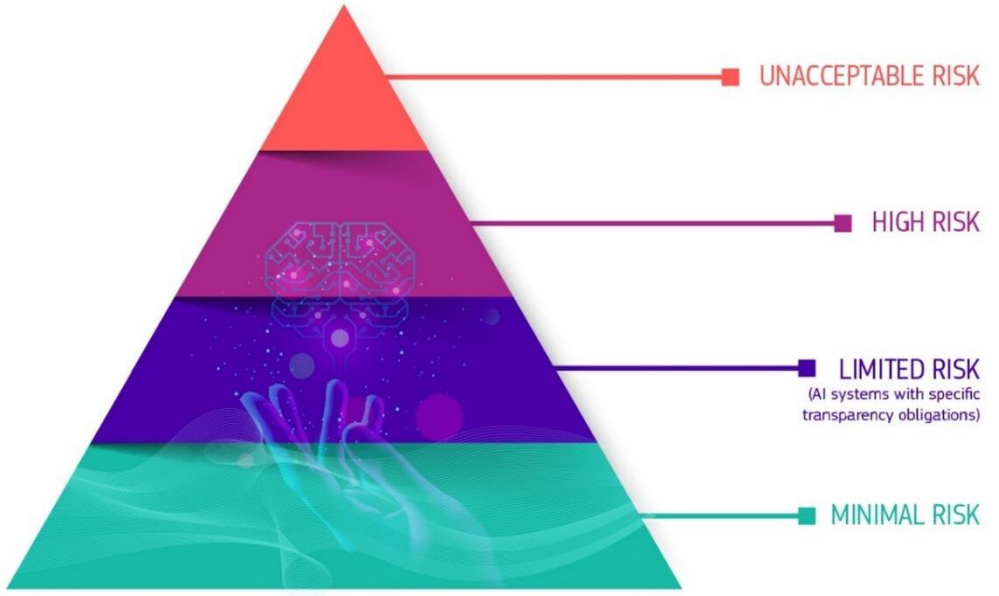
Recommended provisions for AI in the public sector:

- **Access to effective remedy**
- **Right to human review** of decisions taken or informed by an AI system (except when there are "competing legitimate overriding grounds")
- **Meaningful information**
- Establishment of **public registers** listing AI systems used in the public sector

Copyright © 2021 ECNL

EU Artificial Intelligence Act - overview

- **Scope: all AI systems used in the EU or whose outputs are used in the EU (no matter where the company is based),** ***except:***
  - Those developed or used **exclusively for military purposes**
  - Those that are **part of large-scale IT systems already placed on the market** (Article 83 and List IX)
- Risk-based approach with **four categories of risk**: unacceptable, high, limited, minimal
- **4 unacceptable (prohibited) uses of AI:** social scoring, real-time biometric identification (with exceptions!), systems which manipulate or exploit certain vulnerabilities
- Updatable list of high-risk AI systems
- Compliance obligations focused on **providers (developers) o high-risk** AI systems
- Public database of high-risk AI systems (only for providers)



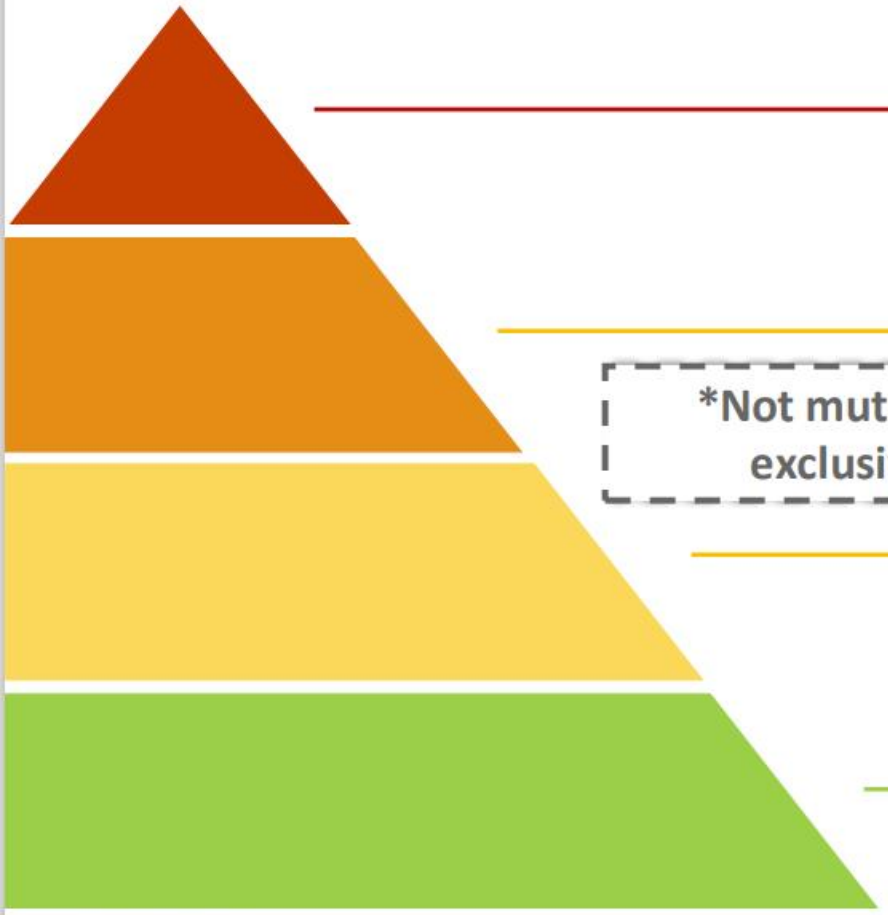
Source: European Commission

Copyright © 2021 ECNL

What does the exemption of "large-scale IT systems already placed on the market " cover?

EU IT-Systems operating in area of Freedom, Security and Justice:

- Schengen Information System for the **return of illegally staying third-country nationals**
- Establishment, operation and use of the Schengen Information System (SIS) in the **field of border checks**
- Establishment, operation and use of the Schengen Information System (SIS) in the field of **police cooperation and judicial cooperation in criminal matters**
- **Visa Information System**
- **Eurodac** system for
  - comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on **Asylum and Migration Management**] and of Regulation (EU) XXX/XXX [**Resettlement Regulation**]
  - for **identifying an illegally staying third-country national or stateless person**
  - **comparison with Eurodac data** by Member States' law enforcement authorities and Europol **for law enforcement purposes**
- **Entry/Exit** Systems
- **European Travel Information and Authorisation System**
- European **Criminal Records Information System on third-country nationals and stateless persons**
- **Interoperability** between EU information systems in the field of **borders and visa, police and judicial cooperation, asylum and migration**



Unacceptable risk
e.g. social scoring

Prohibited

High risk
e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

*Not mutually exclusive

AI with specific transparency obligations
'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

Minimal or no risk

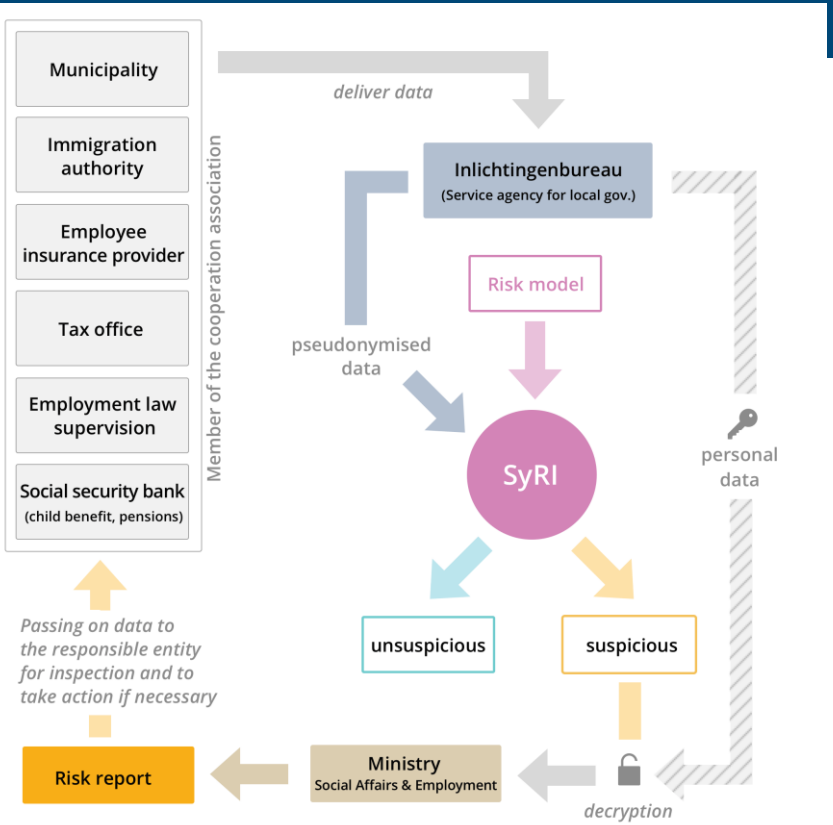
Permitted with no restrictions

European Commission

Copyright © 2021 ECNL

Fundamental rights in the EU AI Act

- Risk/conformity assessment performed by providers of AI systems focuses on **technical aspects**
- No fundamental rights impact assessment or transparency obligations on users (deployers) of AI
- No individual rights or collective rights
- No complaint mechanism
- Role of **national fundamental rights agencies**:
  - Access to data and documentation
  - Participation in evaluation of compliance where risks to fundamental rights are identified by the market surveillance authority



Source: Algorithm Watch

Copyright © 2021 ECNL

EU AI Act – Role of national fundamental rights bodies

Article 63, paras 3, 5:

- National public authorities or **bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights in relation to the use of high-risk AI systems** referred to in Annex III shall have the **power to request and access any documentation created or maintained under this Regulation** when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body **shall inform the market surveillance authority** of the Member State concerned of any such request.
- **Where the documentation** referred to in paragraph 3 **is insufficient to ascertain whether a breach of obligations under Union law intended to protect fundamental rights has occurred, the public authority or body** referred to paragraph 3 **may make a reasoned request to the market surveillance authority to organise testing of the high-risk AI system** through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within reasonable time following the request.

Article 65, para 2:

- **Where the market surveillance authority** of a Member State has **sufficient reasons to consider** that an AI system presents a risk as referred to in paragraph 1 **[risks to the health or safety or to the protection of fundamental rights of persons], they shall carry out an evaluation of the AI system concerned** in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to the protection of fundamental rights are present, the market surveillance authority **shall also inform the relevant national public authorities or bodies.**

European Center for Not-for-Profit Law

Copyright © 2021 ECNL

CoE and EU on AI

How would you expect the EU AI Act and a future CoE Convention on AI to complement each other?

Copyright © 2021 ECNL

Sources/reading materials

Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law (2021), https://rm.coe.int/possible-elements-of-a-legal-framework-on-artificial-intelligence/1680a5ae6b

European Union, Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)and amending certain Union legislative acts (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

Copyright © 2021 ECNL