Artificial Intelligence in Civil Security – a European Commission Perspective

popAI Final Event: "Towards a European AI hub for Law Enforcement Agencies (LEAs) supporting the ethical use of AI in policing"

19 September 2023

Aleksandra Oczko-Dolny, Unit F2
DG Home Affairs and Migration

Overall context

- Unit F2 in charge of coordinating DG HOME's policy on AI as key area of attention – Important interconnection between policy priorities and research results.
- In research - addressed horizontally across all security areas.
- Use of AI tools for security purposes as supportive technology, enabler or aim:
  need for AI, use of AI so far, obstacles to use AI (legal, technical)
  Identifying opportunities/addressing risks)

Opportunities: AI tools have the potential to significantly enhance the capacities of LEAs/security actors by developing and deploying AI solutions that have positive impacts on society.

Finding a proper balance

Risks: Intensifying inequalities, discrimination. Algorithms, machine-learning risk repeating, contributing to or amplifying unfair biases that are the result of specific data selection. So need to ensure that such use remains trustworthy, fully compatible with European values and ethical principles.

Important AI dedicated initiatives

- **AP4AI** a web-based tool to help practitioners self-assess their compliance with the accountability principles, to identify areas for improvement, and enhance the ethical use of AI in their work.
- **STARLIGHT**, **ALIGNER**, **popAI** AI for LE the same cluster of calls from H2020
- **Operational (capacity), Governance (roadmap), Ethics**
- **popAI** recommendations to policymakers, EU legislators on the identified needs or concerns. Complement the forthcoming provisions of the AIA. Non legal supportive measures.

AI as global priority

State of the Union 2023 President **Ursula VON DER LEYEN**

“Mitigating the **risk of extinction** from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.”

“I believe Europe, together with partners, should **lead the way on a new global framework** for AI, built on three pillars: **guardrails, governance and guiding innovation**.”

Guardrails: AI Act – the world's **first comprehensive pro-innovation AI law. A blueprint for the whole world**.

Governance: body for AI **– on the risks and its benefits for humanity.**

Guiding innovation in a responsible way: an **open dialogue** with those that **develop and deploy AI.**

European Commission

AI ACT Regulatory framework proposal

Legislative state of play:

- The Council ‘General Approach’ from December - sufficient account of law enforcement concerns.

- The EP position (approved at committee level (IMCO internal market and consumer protection/LIBE Committee on Civil Liberties, Justice and Home Affairs) May - much less favorable and more likely to impact security activities, especially the list of prohibited practices and of high risk uses.

- Negotiations will now pick up speed. Starting of the trilogues, with a view to achieving a political agreement by the end of the year.

- Most of the main issues of interest for security/migration/borders are likely to be discussed at the next trilogue, on 3rd October and again during subsequent trilogues.

- DG HOME will be in touch with DG CNECT throughout the process to support the negotiations to work on possible compromise wording.

Proposal for a Regulation on AI

A single EU law for AI in the 27 EU Member States

- Two main objectives: address **risks to safety and fundamental rights** and **create a EU single market for AI**
- "Classic" internal market harmonised rules for the **placing on the market, putting into service and use of** AI
- **Horizontal in scope**: public and private sector
  - Excluded: military, research
- Without prejudice and complementary to existing EU law (e.g. data protection, criminal procedural law)

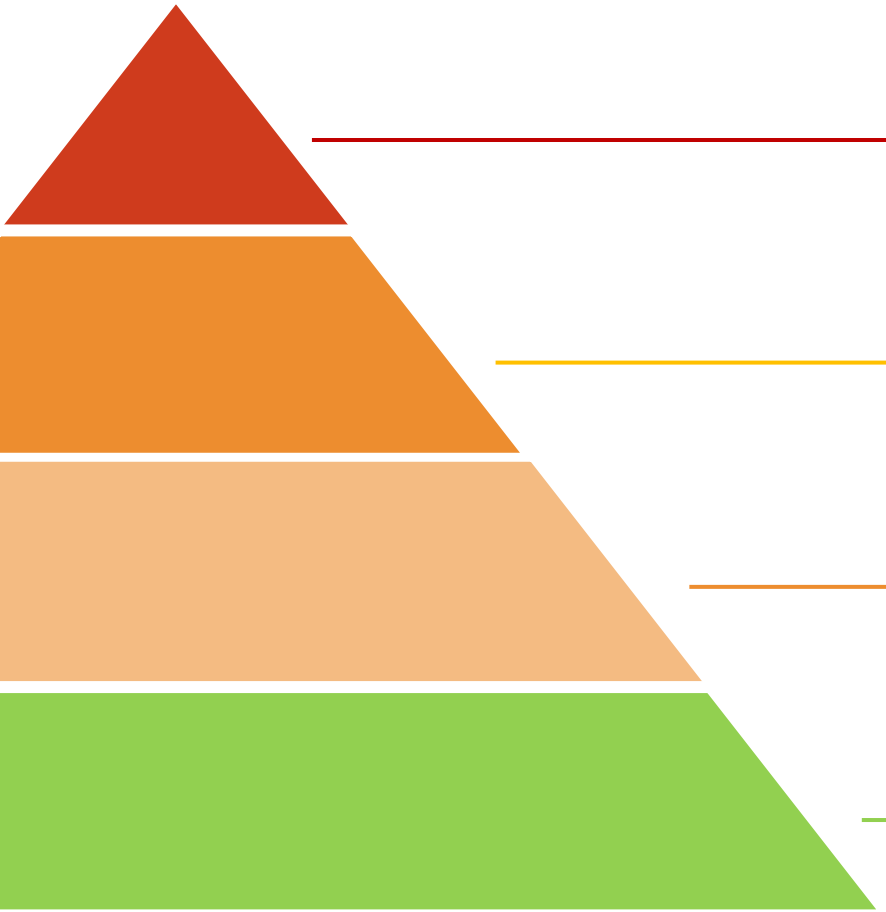
Innovation-friendly and risk-based legislation

- Provide **legal certainty** to operators and stimulate **trust** in the market
- No overregulation: designed to intervene only where strictly needed following a risk-based approach

Creates a level playing field for EU and non-EU players

- Applicable independent of origin of producer or user

A risk-based approach to regulation



Unacceptable risk
e.g. social scoring

Prohibited

High risk
e.g. recruitment, medical devices, law enforcement

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

AI with specific transparency obligations
(e.g. Chat bots, deep fakes)

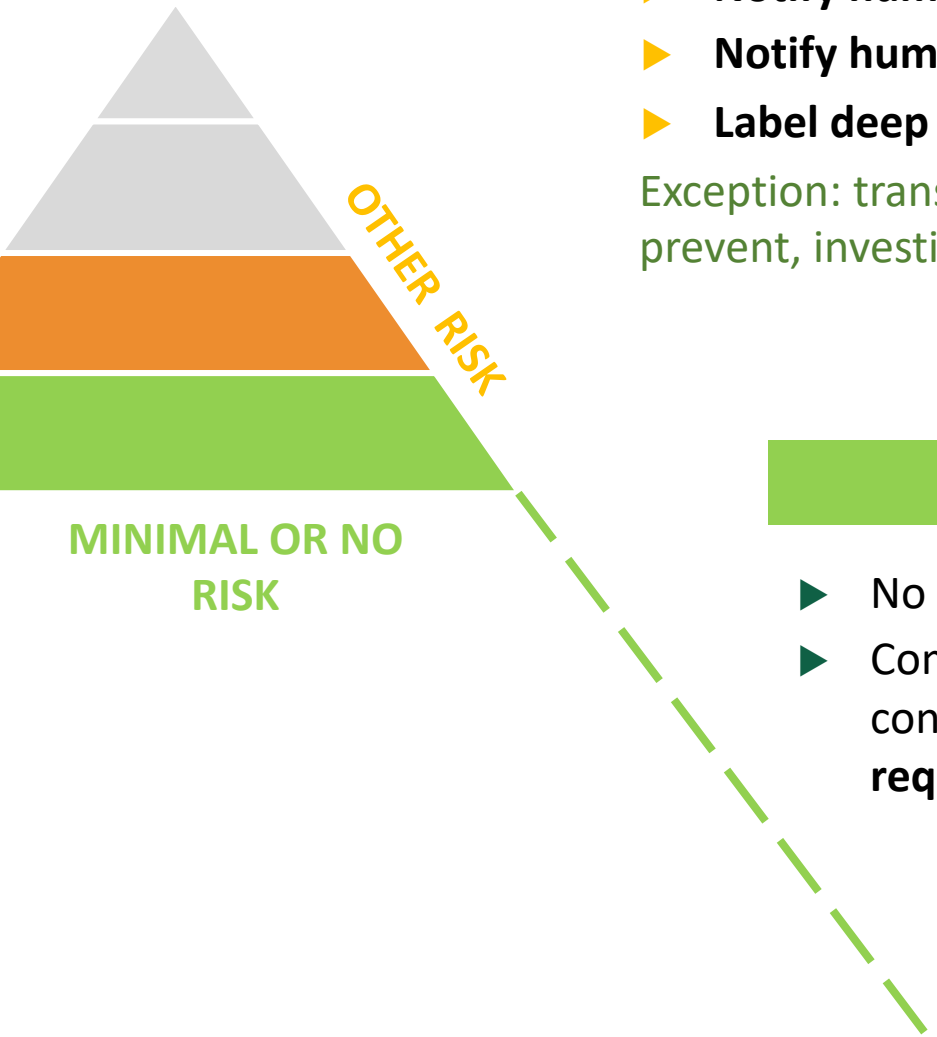
Permitted but subject to information/transparency Obligations

Minimal or no risk

Permitted with no restrictions

European Commission

Most AI systems will not be high-risk (Titles IV, IX)



New transparency obligations for certain AI systems (Art. 52)

- **Notify humans** that they are **interacting with an AI system**
- **Notify humans** that **emotional recognition or biometric categorisation systems**
- **Label deep fakes**

Exception: transparency obligations do not apply when authorised by law to detect, prevent, investigate and prosecute criminal offences

Possible voluntary codes of conduct for AI (Art. 69)

- No mandatory obligations
- Commission and AI Board to encourage drawing up of codes of conduct intended to foster the **voluntary application of requirements to low-risk AI systems**

High-risk Artificial Intelligence Systems (Title III, Annexes II and III)

Certain applications in the following fields:

1 **AI SAFETY COMPONENTS OF REGULATED PRODUCTS**

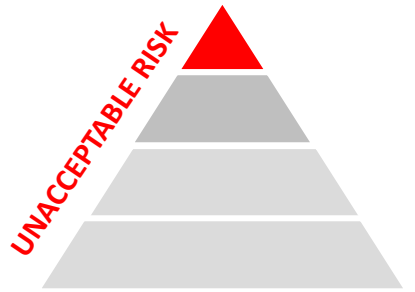
(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

2 **CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS**

- ✓ Biometric identification and categorisation of natural persons
- ✓ Management and operation of critical infrastructure
- ✓ Education and vocational training
- ✓ Employment and workers management, access to self-employment
- ✓ Access to and enjoyment of essential private services and public services and benefits
- ✓ Law enforcement
- ✓ Migration, asylum and border control management
- ✓ Administration of justice and democratic processes

NB! Not all use cases in the law enforcement sector are high-risk, but only a few explicitly listed in Annex III. The Commission can amend the list to keep it future-proof, following a common methodology and impact assessment.

AI practices that contradict EU values are prohibited (Title II, Article 5)



✗ **Subliminal manipulation** resulting in physical/ psychological harm

✗ **General purpose social scoring by public authorities**

✗ **Exploitation of children or mentally disabled persons** resulting in physical/psychological harm

✗ **Real-time remote biometric identification for** law enforcement purposes in publicly accessible spaces (with exceptions)

Annex III, 6 - Law enforcement

Art. 3(40) AIA: defined as in the Law Enforcement Directive

The following AI systems **intended to be used by *'law enforcement authorities':***

a) for making **individual risk assessments of natural persons** in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences

b) **polygraphs** and similar tools or to detect the **emotional state** of a natural

c) for detection of **deep fakes**

d) for **evaluation of the reliability of evidence** in the course of investigation or prosecution of criminal offences

e) **predicting the occurrence or reoccurrence of an actual or potential criminal offence** based on i) profiling of natural persons or ii) assessing personality traits and characteristics or past criminal behaviour of natural persons or groups

f) for **profiling of natural persons in the course of detection, investigation or prosecution** of criminal offences

g) for **crime analytics** regarding natural persons, allowing law enforcement authorities to search **complex related and unrelated large data sets** available in different data sources or in different data formats in order **to identify unknown patterns or discover hidden relationships in the data**

Annex III, 7 - Migration, asylum and border control management

The following AI systems **intended to be used by 'competent public authorities':**

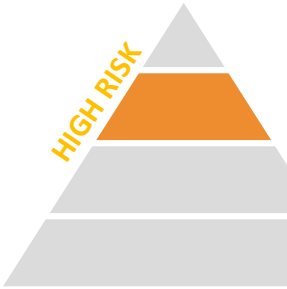
a) **polygraphs** and similar tools or to **detect the emotional state** of a natural person

b) to **assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person** who intends to enter or has entered into the territory of a Member State

c) for the **verification of the authenticity of travel documents and supporting documentation of natural persons** and detect non-authentic documents by checking their security features

d) for the **examination of applications for asylum, visa and residence permits and associated complaints** with regard to the eligibility of the natural persons applying for a status.

Requirements for high-risk AI (Title III, chapter 2)



Establish and implement **risk management** processes

- Use high-quality **training, validation and testing data** (relevant, representative etc.)
- Establish **documentation** and design **logging** features (traceability & auditability)
  - for RBI applications - enhanced logging requirements
- Ensure appropriate degree of **transparency** and provide users with **information** (on how to use the system, its capabilities and limitations)
- Enable **human oversight** (measures built into the system and/or to be implemented by users)
  - Enhanced oversight for RBI applications - “Four eyes” principle
- Ensure **robustness**, **accuracy** and **cybersecurity**

Obligations of operators of high risk AI systems

Provider obligations (incl. Tech providers or LEAs developing in-house)

- Undergo **conformity assessment** to check compliance with the requirements (**self-assessment** for Annex III except for RBI) - time-limited derogation possible for public security - art. 47
- Implement **quality management** system in its organisation
- Draw-up and keep up-to-date **technical documentation**
- **Register** stand-alone high risk AI system in public EU database (no disclosure of instructions of use not to jeopardize security/investigation)
- Conduct **post-market monitoring** and take **corrective action**
- **Report serious incidents and malfunction** that infringe fundamental rights
- **Collaborate** with market surveillance authorities (enhanced confidentiality and security safeguards for LEAs)

User obligations (in-house AI or bought off the shelf)

- Ensure **human oversight** and operate AI system in accordance with the **instructions of use**
- **Monitor** operation for possible risks
- **Inform the provider or distributor about any serious incident** or any malfunctioning
- Use the information given by the provider for the **data protection impact assessment** (where applicable)

⚠ **Existing legal obligations** for users continue to apply (e.g. LED, criminal procedural law – see also recital 31)

European Standardisation Bodies and the AI Act

- The European Commission can ask the European Standardization Organizations to develop **harmonized European standards** in support of EU legislation

- Manufacturers that implement these standards benefit from a **presumption of conformity** with the legislation

- European Standards are automatically transposed into national standards in CEN and CENELEC members' countries and **conflicting national standards are withdrawn**

- In April 2023, the European Commission formally requested CEN & CENELEC to develop such standards

The upcoming standardization Request

CEN & CENELEC Joint Technical Committee 21 "Artificial Intelligence" is ready to take on this challenge

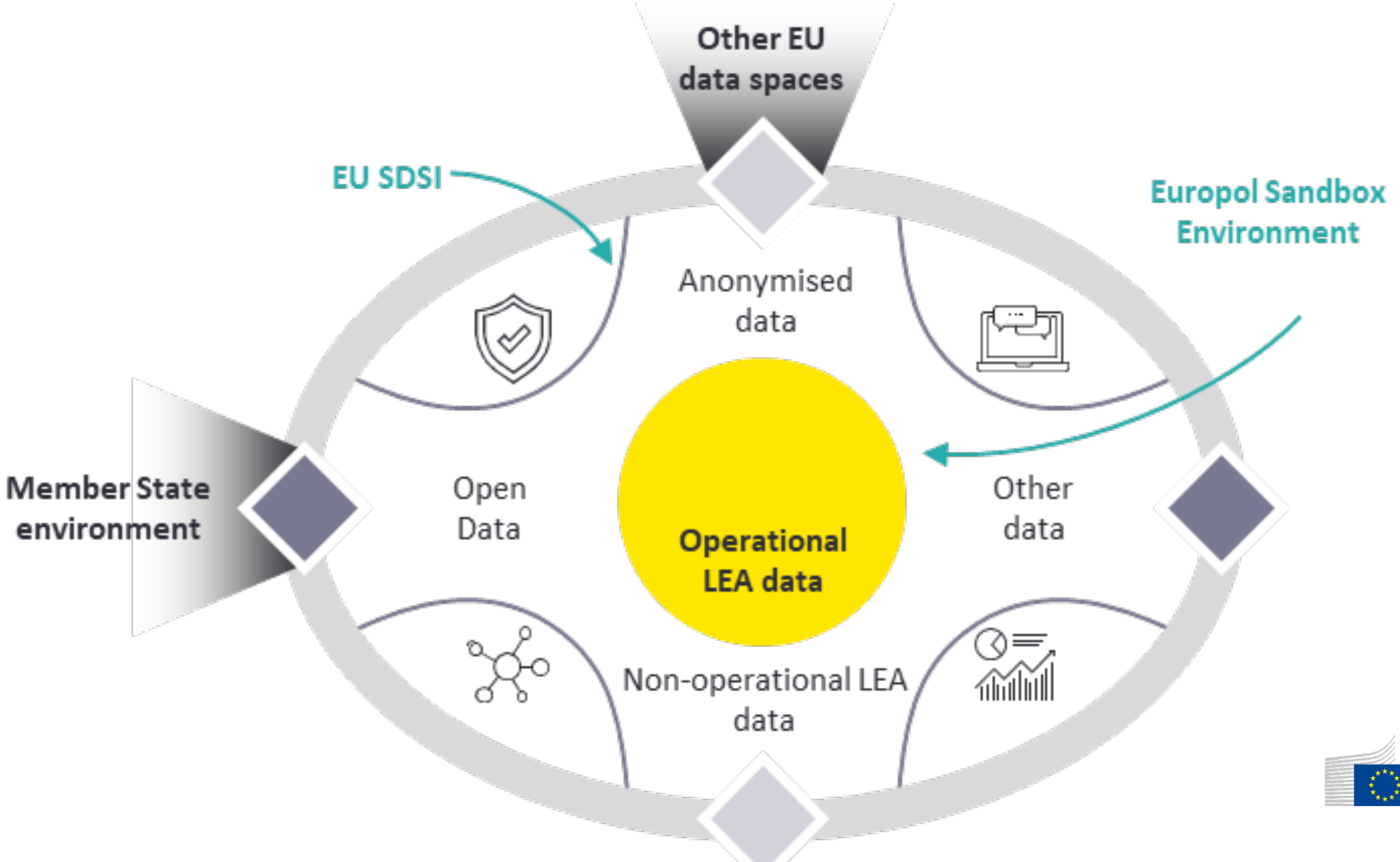
Extensive stakeholder participation of many stakeholders:

28 CEN & CENELEC member countries	ANEC, SBS, ETUC, the Commission, ENISA, …	Liaisons with many Technical Committees

Ongoing dialogue between with the European Commission increase this even further

- AI as a driver for larger mobilization of stakeholders and experts.
- Special focus on the involvement of SMEs and civil society organizations in the standardisation process

Long-term vision: European Security Data Space for Innovation (EU SDSI)



European Commission

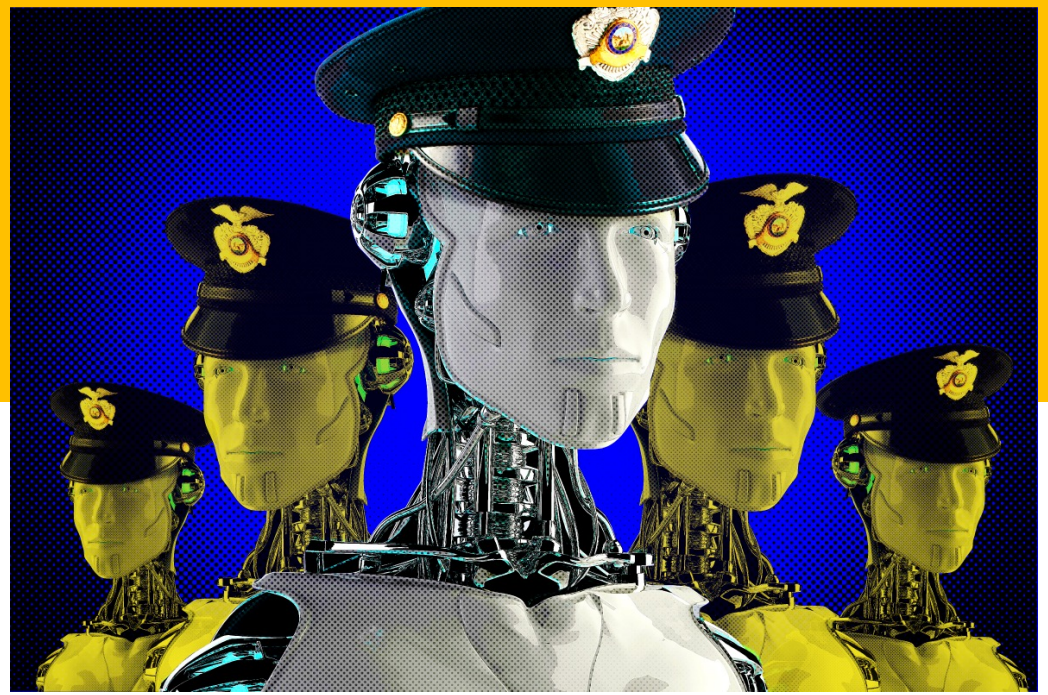
(EU SDSI)

- Aims at fulfilling European Strategy for Data and creating a single European market for data.
- Data environment for innovation to improve the access of national LE authorities to high-quality and high-quantity data to test, train and validate algorithms.
- An ISF Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation, by Ernst & Young (EY) concluded there is clear appetite and need for such a solution, however very problematic.
- Step by step approach. Possibly starting with Europol sandbox environment and only then further stages. Strengthened mandate (Art. 18(2)(e) and 33 (a) of the Europol Regulation). Member States can connect their sensitive (operational) data with non-sensitive data from the EU SDSI to test, train and validate AI algorithms

EU Innovation Hub

- The European Commission, represented by DG HOME, forms part of the Hub team and Steering Committee together JHA agencies.
- The Networks that interact with the Innovation Hub, such as I-LEAD, EACTDA, CYCLOPS etc… are all developed and funded through DG HOME funds (Security research or Internal Security Fund)

European Commission



Thank you!
Questions?

Aleksandra.OCZKO-DOLNY@ec.europa.eu

European Commission