AI, Law Enforcement and the EU

The introduction of a not-so-new technology called „neural networks“, „big data“ or „machine learning“ under the brand name „Artificial Intelligence“ by the EU Commission

A genre picture

OERAK

2024 02 09

Inviso by Insikt Intelligence 2,1 mio € 2017

HORIZON 2020

Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization

Fact Sheet | Results in Brief | Reporting | Results | News & Multimedia

DE EN ES FR IT PL

INVISO: No respite for the radicalised on social media

Soon, social media platforms will have no more than an hour to delete users' extremist content after it's been published. While extremely positive, this EU measure doesn't eradicate the problem at its source and reinforces Law Enforcement Agencies' need for real-time analysis capabilities. To answer this need, INSIKT Intelligence suggests INVISO – a threat intelligence platform.

Aida + Grace + Infinity 21 mio € 2019

⇨ ***H2020 projects***

In 2019, Europol participated in four H2020 funding proposals, three of which were successfully granted: AIDA, GRACE and INFINITY. The projects aim at developing AI and machine learning-based tools to enhance the efficiency of Europol's support to Member States. The Europol Innovation Lab team has taken over the coordination of the implementation of these three H2020 projects. Currently, the Europol Innovation Lab is coordinating the recruitment of dedicated contract agents who will work on the projects.

Furthermore, the Innovation Lab has joined three consortia as a Senior Law Enforcement Agency User to submit project proposals to H2020 calls on AI and Security. Together with more than 16 Law Enforcement Agency partners, the Europol Innovation Lab plans to play a driving role in the development of a European research roadmap on AI in support of Law Enforcement[5].

Powerful machine learning 7 mio € 2020

Augmented reality to help law enforcement agencies fight crime

When fighting crime, law enforcement agencies (LEAs) are required to respond and make decisions in a very short period of time. With this in mind, the EU-funded DARLENE project aims to offer European LEAs a proactive security solution that will enable them to sort through massive volumes of data to predict, anticipate and prevent criminal activities. To achieve this, the project will combine augmented reality (AR) capabilities with powerful machine learning algorithms, sensor information fusion techniques, 3D reconstruction, wearable technology and personalised context-aware recommendations. It will therefore develop practical and beneficial policing applications through the use of affordable, lightweight and inconspicuous AR glasses.

New powers & Big Data for Europol Feb 2021

(2) Policy options addressing objective II: analysing large and complex datasets to detect cross-border links

- policy option 4: enabling Europol to analyse large and complex datasets
- policy option 5: introducing a new category of data subjects (persons not related to a crime) whose data Europol can process

(3) Policy options addressing objective III: use of new technologies for law enforcement

- policy option 6: regulating Europol's support to the EU security research programme, the innovation lab at Europol, and Europol's support to the EU innovation hub
- policy option 7: enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

Draft AI Act on high-risk AI systems Nov 2021

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(~~2~~3)

High-risk AI systems pursuant to Article 6(~~2~~3) are the AI systems listed in any of the following areas:

1. Biometric **systems** ~~identification and categorisation of natural persons~~:

   (a) ~~AI systems~~ **Biometric identification system** intended to be used for the 'real-time' and 'post' ~~remote~~ biometric identification of natural persons **without their agreement**;

2. ~~Management and operation of~~ ~~c~~**C**ritical infrastructure **and protection of environment**:

   (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity**;**

Even more high-risk AI systems Nov 2021

(a) AI systems intended to be used by law enforcement authorities **or on their behalf** 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 for **a natural person to become a** potential victims of criminal offences;

(b) AI systems intended to be used by law enforcement authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;

(c) AI systems intended to be used by law enforcement authorities **or on their behalf for law enforcement purposes** to detect deep fakes as referred to in article 52(3);

And yet more high-risk AI systems Nov 2021

(d) AI systems intended to be used by law enforcement authorities **or on their behalf** for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities **or on their behalf** for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities **or on their behalf** for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

Europol hoarding petabytes of data Jan 2022

THE EDPS THEREFORE ORDERS AS FOLLOWS:

1. As from the day following the notification of the present decision, Europol shall, for each contribution, proceed to data subject categorisation within the meaning of Article 18(5) of the Europol Regulation within six months as from the date of reception of that contribution. Datasets lacking data subject categorisation at the expiry of the six months period referred in the previous sentence shall be erased.

2. By way of derogation from point 1 above, Europol shall proceed to data subject categorisation within the meaning of Article 18(5) of the Europol Regulation of all datasets existing on the day of notification of the present decision within twelve months from the day of said notification. Datasets lacking data subject categorisation at the expiry of the twelve months period referred in the previous sentence shall be erased.

Large scale pilots in LEA premises 58 mio €

DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI - Security (law enforcement): AI-based pilots

Objectives

The overall objective is to enable the final validation and to foster the uptake of artificial intelligence (AI) systems for law enforcement (LE) by running large scale pilots in Law Enforcement Agencies (LEAs)[23] premises. This is necessary, as AI systems for LE need, in most cases, a final validation on real operational datasets[24] that can only be accessed in stand-alone secured environments.

This action will contribute to close the gap between prototypes that have been developed with the support of EU funded security research and innovation programmes (i.e. up to TRL 7) and systems proven in operational environment that bring clear added value to police practitioners (i.e. TRL 8/9).

The stern lady of dubious numbers

„Chat Control“ started May 2022

EUROPEAN
COMMISSION

Brussels, XXX
COM(2022) 209/2

2022/0155 (COD)
SENSITIVE*
UNTIL ADOPTION

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

Impact assessment „chat control“ May 2022

EU-Kommission

What are the costs of the preferred option (if any, otherwise of main ones)?

The main costs in the preferred option are those of:

- **service providers**, to comply with the obligations to **detect, report** and **remove** child sexual abuse online (estimated at one-off costs of **EUR 1.6 billion** and annual costs of **EUR 1.5 billion**);
- **public authorities**, to deal with the **increase in reports** (estimated at one-off costs of **EUR 5.4m** and annual costs of **EUR 825.6m**);
- **the EU centre** (estimated at one-off costs of **EUR 5m** and annual costs of **EUR 25.7m**).

What are the impacts on SMEs and competitiveness?

The most significant impacts on SMEs arise from the **obligation to detect, report and remove** child sexual abuse online found in their services. The economic impact will be mitigated by the **free access to technology** to detect, report and remove, which the EU centre will facilitate. **Uniform rules** related to the fight against child sexual abuse will help SMEs operate across the **Single Market**, helping scale-ups and innovators, while facilitating a safer online environment for children.

Remote biometric ID & the AI Act May 2022

Joint civil society recommendations for an EU Artificial Intelligence Act for Fundamental Rights
Biometrics Part 1: Article 3(36) and Article 5(1)(d)

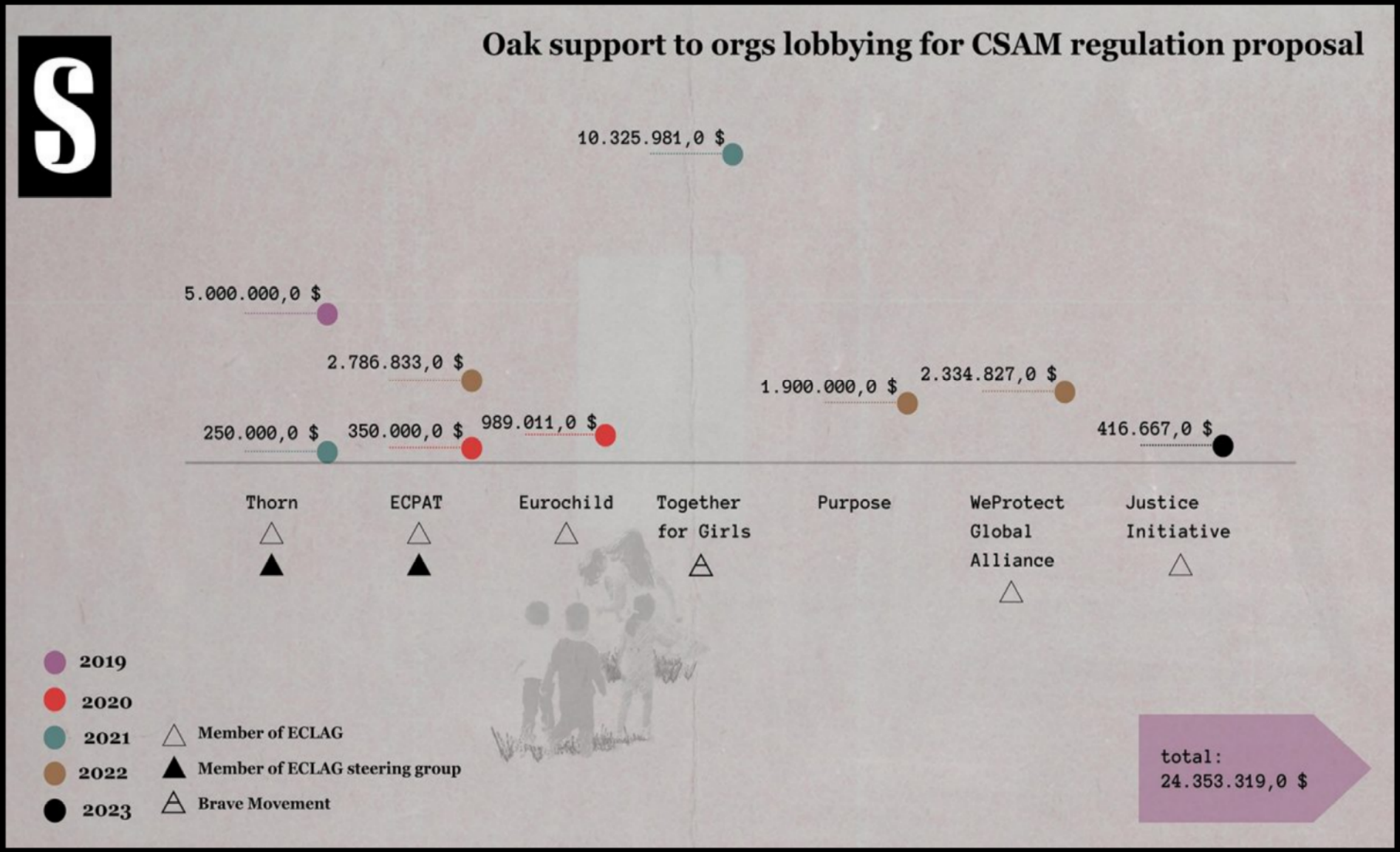
Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces

What is Remote Biometric Identification (RBI)?

Nota bene: *biometric identification is the technical process of identifying one person among many, on the basis of their biometric data (as defined in GDPR article 4.14). This is different from biometric verification, which uses someone's biometric data to confirm that they match specific biometric data which have been stored locally, under their control. An example of biometric verification would be unlocking your mobile phone by comparing your fingerprint to the fingerprint template you created when you set up your device. Another would be going through an*

The Eva Kaili & Ashton Kutcher Show Nov 2022

One foundation to pay them all (by Balkan Insight)



The philanthropist alliance behind the scenes

- Thorn - rather a start-up than a child welfare NGO
- „WeProtect“ foundation : security agencies, police, governments, IT industry, PR firms & EU commission
- 25 mio from the Oak Foundation philanthropists for WeProtect, Thorn, ECPAT, Brave et al since 2019
- EU officials in dual roles, Europol officers changing sides.
- A microtargeting campaign by the Commission on „X“

7 b. Is strongly concerned about the revelations on conflicts of interests involving high level Commission's officials and the use of X advertising campaign related to the Child Sexual Abuse regulation; calls on the Commission to publish all documents requested by the Parliament and make full transparency on this case;

Where have all the safeguards gone? Art. 29

In any case, such AI system for post remote biometric identification shall not be used for law enforcement purposes in an untargeted way, without any link to a criminal offence, a criminal proceeding, ~~or the prevention of~~ a ***genuine and present*** *or genuine and foreseeable* ***threat of a criminal offence*** ~~criminal offence~~ or the search for ***a*** specific missing person~~s~~.

It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities solely based on the output of these post remote biometric identification systems.

This paragraph is without prejudice to the provisions of Article 10 of the Directive (EU) 2016/680 and Article 9 of the GDPR for the processing of biometric data. ~~for purposes other than law enforcement~~.

Tnx for your patience!

https://moechel.com/kontakt
secure upload form, pgp key

https://moechel.com/reporting
Alle Artikel 1999 - 2022

@harkank@chaos.social