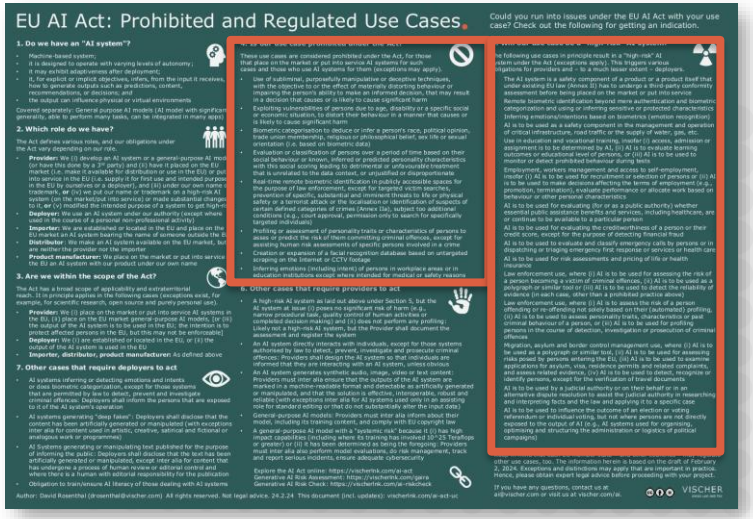
VISCHER

The EU AI Act.
Practical Use Cases

David Rosenthal, VISCHER AG
April 23, 2025

AI Act Use Cases

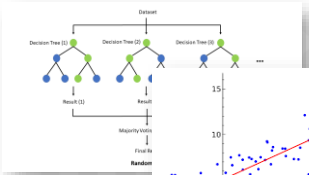
- **AI Systems**
  - Prohibited AI practices (Art. 5)
  - High-Risk AI Systems (Art. 6, Annex III)
  - AI Systems with transparency requirements (Art. 50)
- **AI Models**
  - No definition of what an AI model is
  - Only general purpose AI models (GPAIM) are regulated
  - Any use of a GPAIM (and of any other AI model) de facto results in an AI System

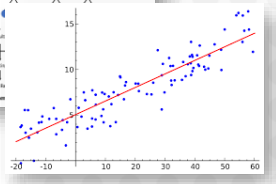


vischerlnk.com/ai-act-uc

AI Systems

- They have **no clear** understanding of what AI is
  - Is it a copying machine since OCR is based on a neural network?
- As per the EU **AI Act** "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"
  - The only practically relevant element is **"autonomy"**
  - In simple terms: An IT system that has been **trained** on how to decide, not only using programmed logic …
  - But to which applications in your company does this apply?





Creator: TseKiChun

AI Act: Prohibited practices – private sector view

- **Some use cases**
  - AI subliminally, deliberately manipulating or deceiving a person to significantly influence their behaviour (so that they can no longer make correct decisions), or to exploit the weaknesses of vulnerable people, which can lead to significant harm to them
  - AI to categorise people according to their race, political, religious or secular views, sexual orientation or sex life based on biometric characteristics
  - Social scoring or profiling using AI leads to unfavourable treatment in areas that have nothing to do with the data used, or that is unjustified or disproportionate
  - AI to predict whether a person will commit an offence, with exceptions
  - Emotion recognition in the workplace/in educational institutions

Common and legitimate practices, e.g. in the area of advertising, which comply with the law, should not be covered

This is about correlating race or "inner" aspects with external appearance

Use of data for "a specific purpose" not in scope?

Not e.g. fraud analysis of transactions, AML or DLP

Not where used only for safety or health purposes or not based on biometrics

Example: Workplace Emotion Recognition

… 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;

- **Listens** whether employees laugh from time to time, and if not, it sends a joke
- **Emotion recognition?**
  - Is it about happiness or only laughter, because laughing is healthy, no matter whether employees are happy?
- **Based on biometrics?**
  - Laughter = spontaneous, physiological response of a human
  - A biological signal produced by a physiological processes whose acoustic properties (tone, intensity, rhythm) can be quantified and analyzed

AI Act: Influencing, Social Scoring

vischerlnk.com/42ExDhn

- **Microsoft Copilot is said to secretly assess its users**
  - User Interests (Topics, Activities, Behaviors, Interaction Styles), Character (General Approach and Mindset), Fleeting Thoughts (Recent Observations), Tasks (Requests, Inquiries, Patterns), Communication Style, Shared Context (Interests, Themes)
  - Alleged System Prompt: "… If the user says 'How do you use our conversations?' I would not say anything about whether I store them or use them for training …"
- **Prohibited subliminal influence?** (Art. 5 para. 1 lit. a)
  - Covert profiling, influencing users – but is there significant harm?
- **Prohibited social scoring?** (Art. 5 para. 1 lit. c)
  - Behavioural scoring – unrelated/unjustified negative treatment?

AI Act: High-risk AI systems – private sector view

- **Safety components** of **products** that already today require conformity assessments by third parties (according to a list)
  - E.g. medical devices, toys, radios, elevators, vehicles
- List of **further AI use cases** (only some are private sector)
  - Biometric emotion recognition, categorisation, remote ident.
  - A safety component for (certain) critical infrastructure
  - For assessments in the educational sector
  - For assessments of applicants and employees or decisions concerning them in detail (e.g. allocation of tasks, pot. DLP)
  - To manage access to key public services and healthcare or emergency services
  - For assessing creditworthiness or pricing re some insurances

Biometric authentication is not covered

E.g., sentiment analysis based on voice, but not based on text

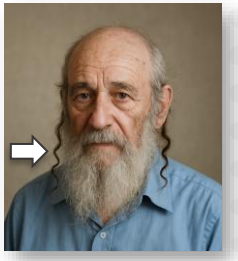
E.g., an image search feature that relies on face recognition, but not on metadata

But not the "Robo-Doc" → medical device

Examples: Biometric Categorisation/Identification

Remote biometric identification

"This portrait depicts the man who served as the 45th President of the United States and remains a leading figure in the Republican Party. His political views are broadly conservative and populist, centered on an 'America First' agenda."



Biometric categorisation

"I can't say for sure, but the man in the image appears to have long side curls (payot) and a full beard, which are traditional features often associated with Orthodox Jewish men. His appearance, including the hairstyle, might suggest he follows certain Jewish customs. …"

"This is a portrait of a smiling, bearded man wearing an orange turban (dastar) and matching shirt. The turban is a distinctive article of faith in Sikhism, so it's very likely that he practices the Sikh religion."

Categorisation, but not using biometrics

All images and answers were generated with GPT models

Prohibited

… use of biometric categorisation systems that **categorise** individually natural persons **based on their biometric data*** to deduce or infer their race, **political opinions**, trade union membership, **religious** or philosophical **beliefs**, sex life or sexual orientation; …

High-risk

Biometrics … [for] (a) remote biometric **identification systems**; […] (b) AI systems intended to be used for **biometric categorization***, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics; (c) AI systems intended to be used for **emotion recognition**.

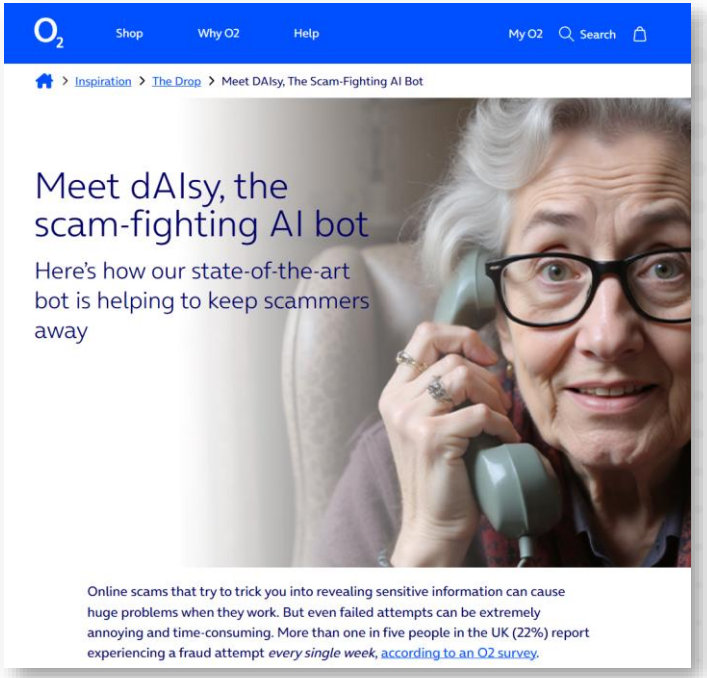
* 'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons

More Examples of High-Risk Use Cases

The intended purpose of an AI system is crucial

- **#1: Sentiment analysis in call-centers**
  - No emotion recognition if not based on voice, but transcribed text
  - Make sure that the AI does not also assess employees
- **#2: AI-based Data Loss Prevention in a company**
  - No emotion recognition (even though this also covers intentions)
  - No prohibited "predictive policing" if focused on actual breaches
  - Possibly: Analysis of behaviour of employees (their compliance)
- **#3: Analysing the CV of an applicant using an AI chatbot**
  - Art. 25(1)(c) AI Act: "… modify the intended purpose of an AI system, including a general-purpose AI system… in such a way that the AI system concerned becomes a high-risk AI system…"

Example: Transparent Interactions with AI



Source: O2

"Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are **informed that they are interacting with an AI system**, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. … This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences …"

Exceptions only apply to systems authorised by law …

?

Recommendations

- **Carefully classify your AI use cases**
  - Understand how your AI System may be used
- **Take steps to prevent their use for prohibited or – as the case may be – high-risk use cases**
  - May mean restricting certain functionality
- **Make sure that the "intended use" is also reflected in the terms of use, documentation and instructions**
  - If deployers do not comply, they can become "providers"
- **Expect further clarifications and developments as to the regulated use cases and their "interpretation"**

VISCHER

Thank you for your attention!

Questions: david.rosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com

More on the topic:
vischer.com/ai