EU Unpacked # 6

George Robakidze

Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)

The opinions and conclusions expressed are those of the author/s and do not necessarily reflect the views of the EU Awareness Centre

September 2025

© [2025] EU Awareness Centre. All rights reserved.

Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)

1. What this document is and why it matters

The European Commission's Guidelines explain how to interpret **Article 5** of the EU **Artificial Intelligence Act** (AI Act). Article 5 lists AI uses that are **completely prohibited** across the EU because they are considered incompatible with fundamental rights, democratic values and human dignity. The Guidelines are the Commission's practical reading of those prohibitions: they are **not binding law** (only the Court of Justice can give the final legal interpretation), but they are the official guidance national authorities, providers and users should rely on when applying the ban.

Two timing points are essential: the AI Act itself took effect earlier, but the prohibitions in Article 5 became applicable on **2 February 2025**; the governance and penalties chapters became applicable later (notably from **2 August 2025**). Providers and deployers must therefore already avoid Article 5 practices, even while some enforcement structures were being established.

2. EU approach to AI risk — where "prohibited" sits

The AI Act uses a **risk-based approach**. It groups AI uses into broad tiers:

- **Unacceptable risk** — prohibited (Article 5).
- **High risk** — allowed only under strict requirements (data governance, documentation, human oversight, mandatory assessments, etc.).
- **Transparency risk** — limited obligations (for example, users must be told they interact with AI).
- **Minimal/no risk** — no specific regulation; voluntary codes possible.

Article 5 targets AI uses that, by their nature, are particularly harmful to rights and democratic life — manipulation, exploitation, mass surveillance, socially discriminatory scoring, and certain automated profiling and biometric uses. The Guidelines aim to clarify precisely when an AI practice meets the legal definition of a prohibited practice.

3. The prohibited practices (straightforward list + plain meaning)

Article 5 contains several distinct prohibitions. Below is a short plain-English explanation of each, with the essential limit or exception noted.

1. **Harmful manipulation and deception (Article 5(1)(a))**

   AI systems that use **subliminal techniques** (below conscious awareness) or that deploy **purposeful manipulation or deception** to materially distort a person's behaviour — and that cause or are likely to cause **significant harm** — are prohibited. In short, hidden or highly manipulative AI tricks that make people take harmful decisions are banned.

2. **Exploitation of vulnerabilities (Article 5(1)(b))**

   AI that **targets vulnerabilities** (for example: children, persons with disabilities, or people in acute socio-economic distress) to distort choices in a way that causes or is likely to cause **significant harm** — prohibited. The focus is on exploiting a person's particular weakness.

3. **Social scoring (Article 5(1)(c))**

   AI systems that **evaluate or rate people** based on social behaviour or personality and then subject them to **detrimental or disproportionate treatment in unrelated contexts** (think "credit/privilege/ access" decisions based on irrelevant social data) are banned. The prohibition covers private and public actors alike.

4. **Individual criminal-offence risk assessment/prediction (Article 5(1)(d))**

   AI that **predicts whether a particular person will commit a crime** based solely on profiling or personality characteristics is prohibited. An important carve-out: tools that help a human decision-maker and are based on **objective, verifiable facts directly linked to criminal activity** may be allowed (i.e., the ban targets purely profiling-driven automated predictions).

5. **Untargeted scraping to build facial recognition databases (Article 5(1)(e))**

   AI systems that create or expand facial-recognition databases by **untargeted scraping** of face images from the internet or CCTV (mass harvesting) are prohibited. The aim is to stop bulk, non-consensual collection of biometrics.

6. **Emotion recognition in workplace/education (Article 5(1)(f))**

   AI that **infers emotions** of people in **workplaces or educational institutions** is banned — except where strictly necessary for **medical** or **safety** reasons. (Emotion inference in itself is generally considered high-risk; its use in sensitive contexts is mostly barred.)

7. **Biometric categorisation for sensitive traits (Article 5(1)(g))**

   AI that **derives sensitive attributes** (race, political opinions, trade-union membership, religion, sexual orientation, sex-life) from biometric data and uses that to categorise people is prohibited, with narrow exceptions for legitimate labelling/filtering of lawfully acquired biometric data (e.g., specific law enforcement datasets under strict safeguards).

8. **Real-time remote biometric identification (RBI) in public spaces for law enforcement (Article 5(1)(h))**
   Use of **real-time** biometric identification (for example, live facial recognition in a street or station) by law enforcement in **public spaces** is generally prohibited. There are **very limited, exhaustively-listed exceptions** (targeted searches for victims/missing persons, prevention of imminent threats such as terrorist attacks, and targeted searches for suspects of listed serious offences) — and where permitted, strict prior authorisation, safeguards and reporting obligations apply.

(For the formal legal text and structured table of these prohibitions, see the Guidelines' overview.)

4. How to understand the legal scope — who and what the rules cover

Material scope (what actions)

The prohibitions cover: **placing on the market**, **putting into service**, or **use** of an AI system. For RBI (real-time biometric identification), the ban specifically targets **use** in public spaces; other prohibitions generally cover development, market entry and use. The AI Act's reach includes cloud-based APIs, embedded devices, and online access.

Personal scope (who)

- **Providers** are entities (companies or public bodies) that develop AI or place it on the EU market. They must ensure the system complies before offering it.
- **Deployers** are those who use the AI (for example, employers, police forces); they are responsible for lawful use. A single actor can be both provider and deployer.

Providers are expected to foresee likely misuses and place appropriate design-level safeguards in the product and terms of use. Deployers must not use AI in prohibited ways, even if a contractual clause attempted to permit such use.

5. Important exclusions and limits (where the Act does not apply)

The AI Act contains several targeted exclusions; the Guidelines explain them clearly.

- **National security, defence and military uses** — excluded from the AI Act if the AI is used **exclusively** for military/defence/national security purposes (the test is about purpose, not the type of user). However, "dual-use" systems (military + civilian/law enforcement) fall within the AI Act. Also, the fact of exclusion does not absolve Member States from other EU obligations.
- **Judicial and law-enforcement cooperation with third countries** — limited exclusion may apply where international cooperation frameworks include **adequate safeguards**; recipient EU authorities remain accountable to EU law.
- **Research & development** — R&D before placing AI on the market is excluded to protect innovation and experimentation, but once research yields a system that is placed on the market or tested in real-world conditions, the AI Act's rules apply. Real-world testing is governed by a specific sandbox/regime and may need consent/conditions.
- **Personal non-professional activity** — individuals using AI purely for personal, non-professional use are out of scope as deployers (but the system itself may still be regulated when placed on the market).
- **Open source** — AI released under free/open-source licences is excluded **unless** it is placed on the market or put into service as a high-risk or Article-5 system; the ban on prohibited practices still applies to such systems if they enter the market.

These exclusions are narrowly defined; the Guidelines stress careful case-by-case assessment.

6. Real-time biometric identification: the special, tight regime

Because **real-time RBI in public spaces** is exceptionally intrusive, the Guidelines give it special attention.

- **General rule:** Real-time biometric identification in public spaces for law enforcement is **prohibited**, subject to **three narrowly-defined exceptions** (targeted search for victims/missing persons, prevention of imminent threats, including terrorist attacks, and targeted searches for suspects of certain serious offences). Member States may decide which of the three exceptions they allow in national law.
- **If an exception applies:** use is permitted only under strict conditions: **targeted** (confirm identity of a specifically targeted individual, not general dragnet), prior **authorisation** by a judicial or independent administrative authority (except in urgent cases where retroactive registration is allowed), **fundamental-rights impact assessments**, registration in the EU

database, clear temporal/geographic limits, and reporting/oversight. The aim is to avoid mass surveillance and to ensure necessity and proportionality.

- **Retrospective (non-real-time) use** of facial recognition is **not** banned but is high-risk and subject to the AI Act's high-risk requirements (and to data protection rules).

The Guidelines include concrete examples (e.g., use after a major terror attack may be allowed; systematic screening of protesters or broad searches for shoplifters by police would not).

7. Interplay with other EU laws (GDPR, LED, consumer law, etc.)

The AI Act **does not replace** other EU rules — it works alongside them:

- **Data protection (GDPR/LED/EUDPR):** AI systems that process personal data must still comply with data-protection law. When Article 5 touches biometric processing and law enforcement, Article 16 TFEU provides a specific legal basis, and the Law Enforcement Directive remains relevant. The Guidelines emphasise that compliance with Article 5 is **not** sufficient to comply with data-protection law: both sets of rules apply.
- **Consumer protection, safety, labour law:** AI uses may also be unlawful under consumer law, employment law or product safety rules, even if not explicitly banned by Article 5. For example, social scoring by traders could be an unfair commercial practice; emotion-detection used medically may fall under medical-device rules.
- **Digital Services Act & other sectoral law:** obligations for intermediary platforms and sectoral rules are preserved and must be read together with the AI Act.

In short, operators need a comprehensive compliance checklist that covers the AI Act, as well as privacy, consumer, employment, and sectoral rules.

8. Enforcement and penalties — how the rules will be applied

Who enforces?

National **market surveillance authorities** designated by Member States — and the European Data Protection Supervisor for EU institutions — will enforce the AI Act's product-safety and prohibition rules. They can act ex officio or on complaint; Member States were required to designate authorities by 2 August 2025. When risks cross borders, a Union safeguard procedure exists, allowing the Commission to make a uniform decision.

Penalties:
Violations of Article 5 prohibitions are treated as the **most serious** infringements. Fines may reach **EUR 35,000,000** or, for undertakings, **up to 7% of worldwide annual turnover**, whichever is higher. (Separate caps exist for EU institutions.) The fines regime is tiered across the AI Act according to the seriousness of the offence.

Interim application:

Although penalties and some governance chapters became fully enforceable later (August 2025), Article 5's prohibitions were applicable from **2 February 2025**; this means prohibited uses were already legally forbidden and could be challenged in national courts even before penalties were operational.

Practical effect: providers and deployers must act now: design decisions, contracts and deployment practices must be reviewed to avoid banned uses and to document compliance efforts.

9. What "significant harm" and "material distortion" mean (practical test)

The Guidelines make clear that the Article 5 prohibitions are **cumulative**: several conditions must be met for a practice to be banned (e.g., the technique must be subliminal/manipulative, it must materially distort behaviour, and the distortion must cause or be likely to cause significant harm). This avoids overbroad application: lawful persuasion, marketing that does not cause substantial harm, or high-risk systems with safeguards will not automatically be banned. However, where AI deliberately bypasses conscious choice or exploits vulnerabilities to cause serious harm, the ban applies.

10. Practical examples and likely impact (what citizens, businesses and public authorities should expect)

- **Citizens:** stronger protection against covert manipulation (e.g., hidden messaging, neuro-targeting), mass biometric harvesting, workplace emotion surveillance and discriminatory biometric categorisation. People should expect clearer rights and stronger remedies against abusive AI.
- **Businesses/providers of AI:** must ensure product design excludes the prohibited practices; anticipate obligations to document risk assessments, to write clear "instructions for use", to prevent foreseeable misuse and to build technical safeguards in general-purpose models. Providers of general-purpose models cannot ignore reasonably foreseeable uses that would result in prohibited outcomes.
- **Deployers (employers, platforms, public authorities):** must not use AI in ways that Article 5 bans; where exceptions are narrowly allowed (RBI for certain law-enforcement goals), they must follow authorisation, assessment and reporting procedures. Employers wanting to trial emotion recognition in health/safety contexts must ensure medical/safety grounds and compliance with health/work law and data protection.
- **Law enforcement:** will face strict constraints on live facial recognition; Member States must enact national laws for the exceptions, and authorities must perform fundamental-rights impact assessments and obtain authorisations where required.

11. Key takeaways — simple things to remember

1. **Some AI is simply forbidden in the EU.** The AI Act bans specific practices that are incompatible with fundamental rights and democratic values.
2. **The ban covers providers and users.** Both those who offer AI systems and those who deploy them must avoid prohibited practices.
3. **Real-time biometric ID in public by police is mostly banned** — only narrow, tightly-controlled exceptions exist (targeted victims, imminent threats, targeted suspects of listed crimes).
4. **Other EU laws still apply.** Data protection, consumer, product safety and labour rules must be respected in addition to the AI Act.
5. **Enforcement is real and heavy.** Market surveillance authorities will act, and the maximum fines are substantial (up to €35 million or 7% global turnover).

12. Final note on interpretation and future developments

These Guidelines are the Commission's first comprehensive reading and will be **kept under review** as authorities apply the rules and courts weigh in. The Commission explicitly recognises that applications

will often require **case-by-case** assessment, and it invites stakeholders to contribute further examples and experience so that the guidance can evolve. In short, we now have a clear EU standard that prohibits the most abusive uses of AI, but we can expect evolution as cases, technology, and jurisprudence develop.

September 2025

George Robakidze

George is a diplomat and expert in international politics, security and European integration. During his career in the Georgian public service (2004–2023), he held senior positions focused on political affairs, European and Euro-Atlantic integration and regional security. Beyond diplomacy, he has contributed extensively as an author and researcher, specialising in the rise of radical and populist movements in Eastern Europe. He currently serves as the executive director of the EU Awareness Centre, a Brussels-based NGO promoting democratic reforms, good governance, and EU values. He continues his work as an independent researcher on political and international issues.