The final agreement maintains the risk-based approach proposed by the Commission and classifies AI systems into several risk categories, with different degrees of regulation applying.

- **Prohibited AI practices**. The final text prohibits a wider range of AI practices as originally proposed by the Commission because of their harmful impact:
  - AI systems using subliminal or manipulative or deceptive techniques to distort people's or a group of people's behaviour and impair informed decision-making, leading to significant harm;
  - AI systems exploiting vulnerabilities due to age, disability, or social or economic situations, causing significant harm;
  - Biometric categorisation systems inferring race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation (except for lawful labelling or filtering in law-enforcement purposes);
  - AI systems evaluating or classifying individuals or groups based on social behaviour or personal characteristics, leading to detrimental or disproportionate treatment in unrelated contexts or unjustified or disproportionate to their behaviour;
  - 'Real-time' remote biometric identification in public spaces for law enforcement (except for specific necessary objectives such as searching for victims of abduction, sexual exploitation or missing persons, preventing certain substantial and imminent threats to safety, or identifying suspects in serious crimes);
  - AI systems assessing the risk of individuals committing criminal offences based solely on profiling or personality traits and characteristics (except when supporting human assessments based on objective, verifiable facts linked to a criminal activity);
  - AI systems creating or expanding facial recognition databases through untargeted scraping from the internet or CCTV footage;
  - AI systems inferring emotions in workplaces or educational institutions, except for medical or safety reasons.
- **High-risk AI systems**. The AI act identifies a number of use cases in which AI systems are to be considered high risk because they can potentially create an adverse impact on people's health, safety or their fundamental rights.
  - The **risk classification** is based on the intended purpose of the AI system. The function performed by the AI system and the specific purpose and modalities for which the system is used are key to determine if an AI system is high-risk or not. High-risk AI systems can be safety components of products covered by **sectoral EU law** (e.g. medical devices) or AI systems that, as a matter of principle, are considered to be high-risk when they are used in **specific areas** listed in an annex.[13] The Commission is tasked with maintaining an EU database for the high-risk AI systems listed in this annex.
  - A new test has been enshrined at the Parliament's request (**'filter provision'**), according to which AI systems will not be considered high-risk if they do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons.[14] However, an AI system will always be considered high-risk if the AI system performs profiling of natural persons.
  - Providers of such high-risk AI systems will have to run a **conformity assessment procedure** before their products can be sold and used in the EU. They will need to comply with a range of requirements including for testing, data training and cybersecurity and, in some cases, will have to conduct a fundamental rights impact assessment to ensure their systems comply with EU law. The conformity assessment should be carried out either based on