AI ACT OF THE EUROPEAN UNION

2024 MARCH

BACS
Blockchain Arbitration & Commerce Society

WHAT IS BACS?

Blockchain, Arbitration, and Commerce Society (BACS) is an international private law association that promotes international trade using new technologies (blockchain, crypto assets, and artificial intelligence).

We have the first specialized Tribunal of International Arbitration with international recognition, whose sentences are directly enforceable through Smart Contracts without the need for judicial authority. More information: https://bacsociety.com/en/

CONDUCT AN ARTIFICIAL INTELLIGENCE COMPLIANCE TEST WITH BACS

BACS is working on a beta platform for artificial intelligence compliance based on this regulation.

Do you use artificial intelligence and want to take the test?

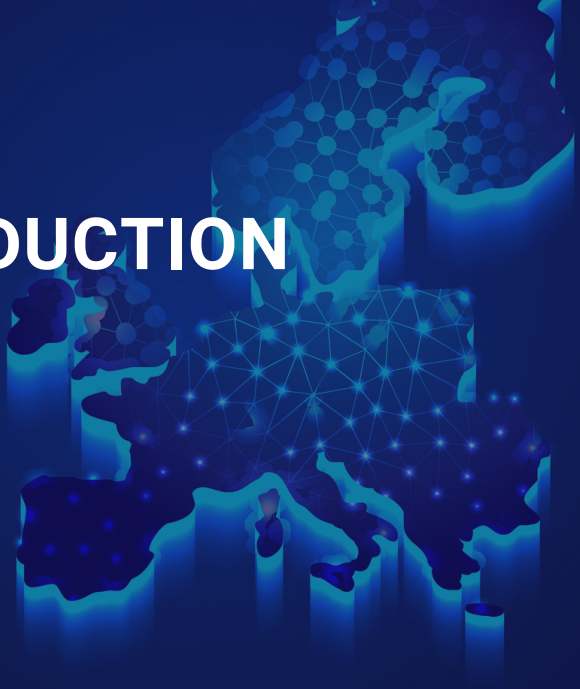
Contact us by writing to info@bacsociety.com

BACS Blockchain Arbitration & Commerce Society

INDEX:

01

INTRODUCTION



The European Union has been actively working on establishing comprehensive regulations for Artificial Intelligence (AI), aiming to address the ethical, legal, and societal challenges posed by AI technologies.

The EU's approach to AI regulation is part of a broader digital strategy to ensure that AI systems are developed and deployed in a way that respects EU values and fundamental rights, including privacy, non-discrimination, and consumer protection.

THE EU'S PROPOSED AI REGULATION

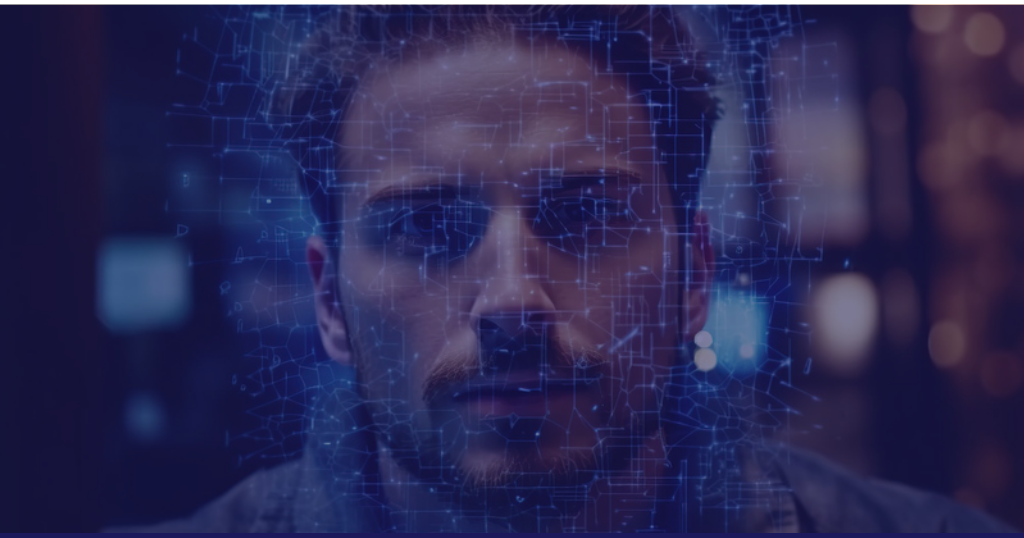
In April 2021, the European Commission proposed the first-ever legal framework on AI, known as the AI Act. This proposal aims to create a harmonized set of rules for the development, deployment, and use of AI across the EU member states.

02

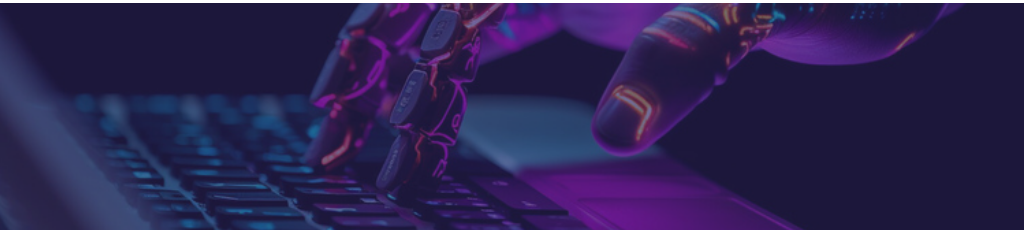
OBJECTIVES AND CONCERNS

The objectives of the EU's AI Act are to ensure the safety and fundamental rights of individuals and businesses while fostering innovation, investment, and the development of AI across the EU.

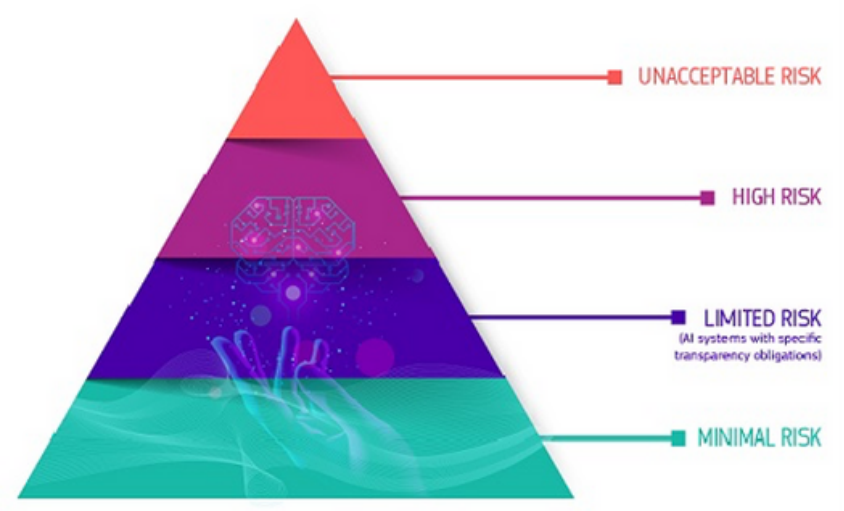
However, the proposal has sparked a debate among stakeholders, including businesses, civil society, and academia, over concerns such as the potential for overregulation, the impact on innovation and competitiveness, and the challenges of enforcement and compliance.



03 RISK-BASED APPROACH



The framework categorizes AI systems according to the level of risk they pose to rights and safety. It ranges from an unacceptable risk, to high-risk and to Lower-risk AI applications.



Source: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

04

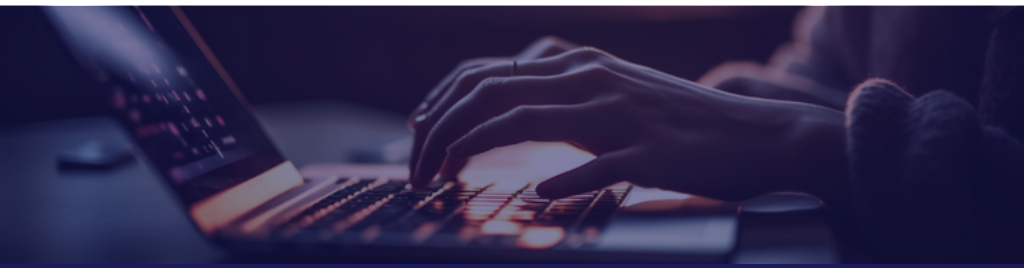
UNACCEPTABLE RISK

AI systems are systems considered a threat to people will be banned.

They include:

- Cognitive behavioural manipulation of people or specific vulnerable groups: for example, voice-activated toys that encourage dangerous behaviour in children.
- Social scoring: classifying people based on behaviour, socio-economic status or personal characteristics.
- Biometric identification and categorisation of people.
- Real-time and remote biometric identification systems, such as facial recognition.

Some exceptions may be allowed for law enforcement purposes. “Real-time” remote biometric identification systems will be allowed in a limited number of serious cases, while “post” remote biometric identification systems, where identification occurs after a significant delay, will be allowed to prosecute serious crimes and only after court approval.



05

HIGH-RISK SYSTEMS

Included Assumptions:

- critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);
- essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- migration, asylum and border control management (e.g. automated examination of visa applications);
- administration of justice and democratic processes (e.g. AI solutions to search for court rulings).

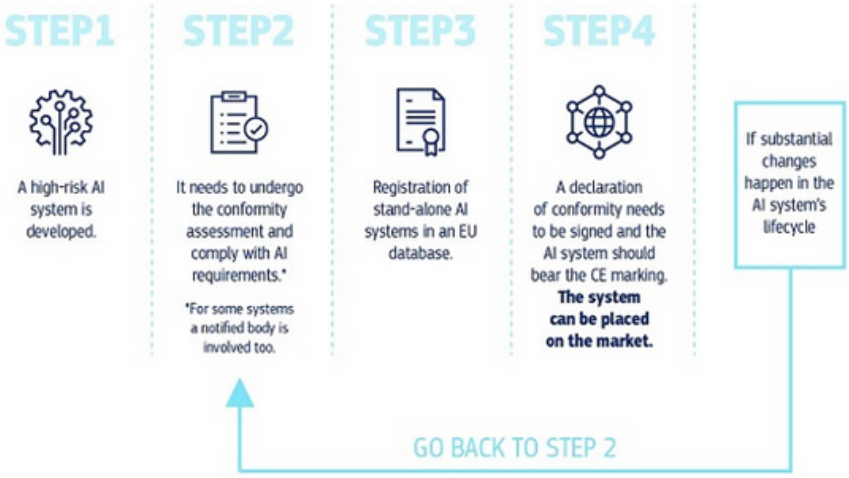
Obligations to be fulfilled before they can be marketed:

- Adequate risk assessment and mitigation systems;
- High quality of the datasets feeding the system to minimise risks and discriminatory outcomes;
- Logging of activity to ensure traceability of results;
- Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance;
- Clear and adequate information to the deployer;
- Appropriate human oversight measures to minimise risk;
- High level of robustness, security and accuracy.

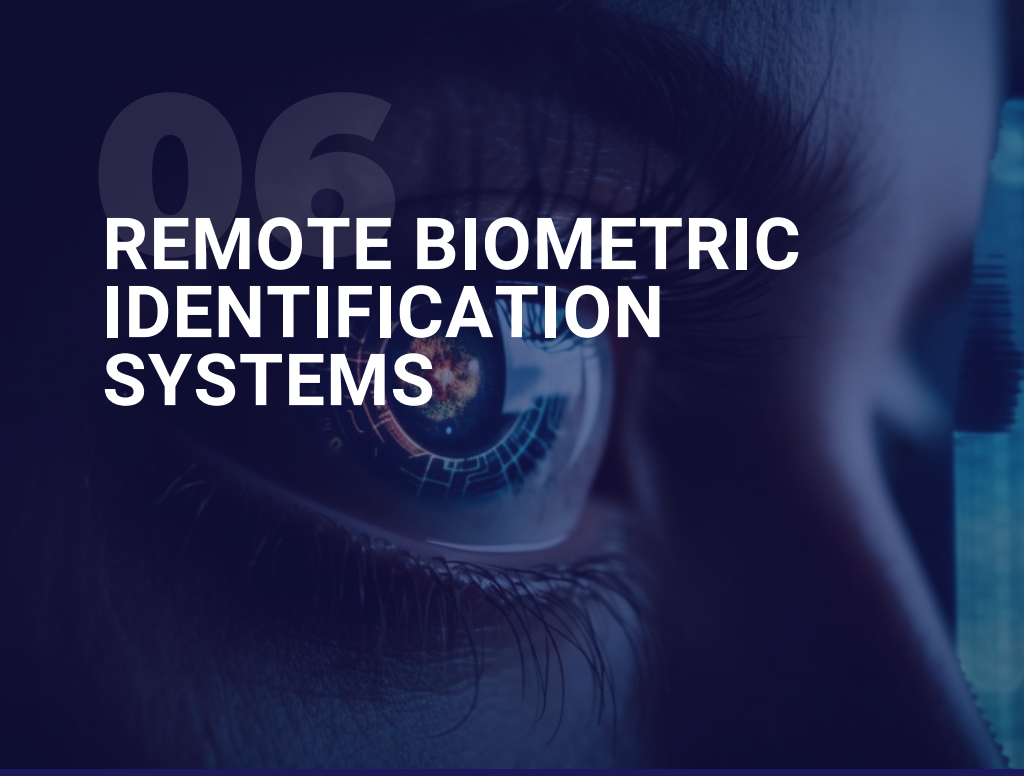
How does all this work in practice for high-risk AI system providers?

Once an AI system is on the market, authorities will be in charge of market surveillance. Implementers will ensure human oversight and monitoring, and providers must have a post-market monitoring system in place. Providers and implementers will also report serious incidents and malfunctions.

If you are an implementer or provider, you can conduct a compliance test with BACS (info@bacsociety.com).



Source: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai



06

REMOTE BIOMETRIC IDENTIFICATION SYSTEMS

Which biometric systems are not allowed

- For identification and categorisation of people.
- Real-time and remote biometric identification systems, such as facial recognition.
- The use of remote biometric identification in publicly accessible spaces for law enforcement purposes is, in principle, prohibited.

High-risk and subject to strict requirements: All remote biometric identification systems.

Exceptions to biometric systems (and may be allowed)

Such as when necessary to search for a missing child, to prevent a specific and imminent terrorist threat or to detect, locate, identify or prosecute a perpetrator or suspect of a serious criminal offence.

Those usages are subject to authorisation by a judicial or other independent body and to appropriate limits in time, geographic reach and the databases searched.

07

REQUIREMENTS FOR MINIMAL OR NO RISK

The AI Act allows the free use of minimal-risk AI. This includes applications such as AI-enabled video games or spam filters. The vast majority of AI systems currently used in the EU fall into this category.

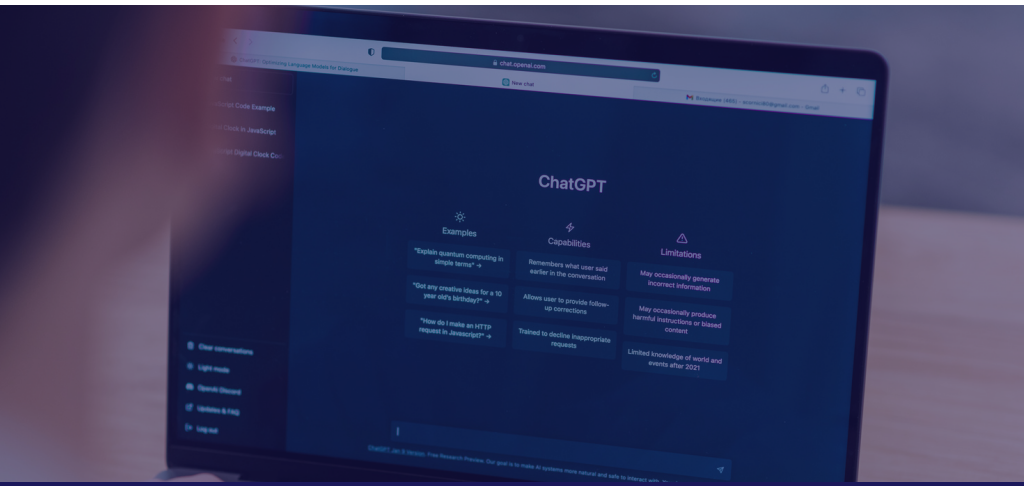
08

GENERATIVE ARTIFICIAL INTELLIGENCE, LIKE CHATGPT

General rule: will not be classified as high-risk

However, it must comply with transparency requirements and EU copyright law. Specifically:

- Disclosing that the content was generated by AI.
- Designing the model to prevent it from generating illegal content.
- Publishing summaries of the copyrighted data used for training.

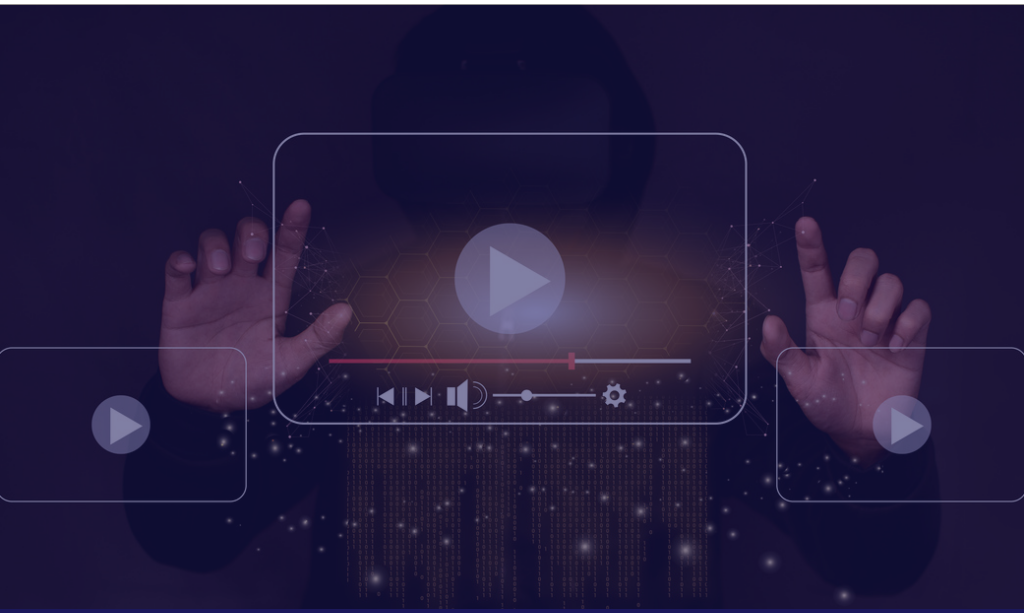


High-impact AI models that could represent a systemic risk (GPT-4)

This applies to the most advanced AI model, GPT-4. Such models would have to undergo comprehensive assessments, and any serious incidents would have to be reported to the European Commission.

Images, audio, or video files generated by AI

This content, which is generated or modified with the help of AI, needs to be clearly labeled as AI-generated so that users are aware when they encounter such content.



09

ENFORCEMENT AND IMPLEMENTATION

December 2023, the European Parliament and the Council of the EU reached a political agreement on the AI Act.

The text is in the process of being formally adopted and translated. The AI Act will enter into force 20 days after its publication in the Official Journal, and will be fully applicable 2 years later, with some exceptions:

- Prohibitions will take effect after six months.
- Governance rules and the obligations for general-purpose AI models become applicable after 12 months and the rules for AI systems - embedded into regulated products - will apply after 36 months.
- Codes of practice will apply nine months after entry into force.

Support from the community.

To facilitate the transition to the new regulatory framework, the Commission has launched the AI Pact, a voluntary initiative that seeks to support the future implementation and invites AI developers from Europe and beyond to comply with the key obligations of the AI Act ahead of time.

BACS

Blockchain Arbitration
& Commerce Society

VISIT OUR WEB

C/ Antonio Acuña 9, 2º izq.
Madrid (Spain)

info@bacsociety.com
+34 91 018 29 46