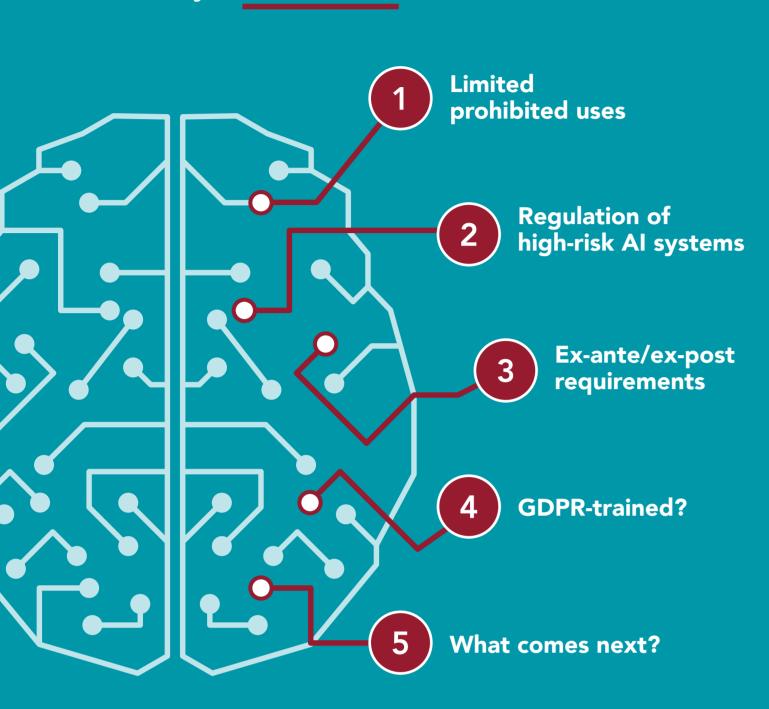
Key aspects

On April 21, 2021 the EU Commission published its proposal for an Artificial Intelligence Act.

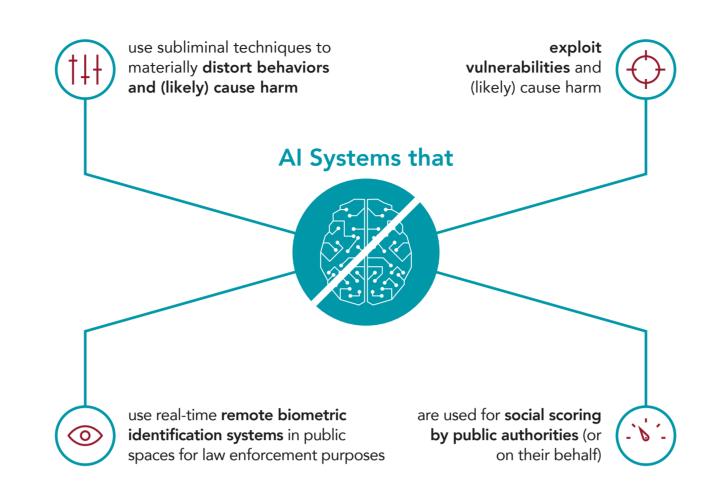
Here is what you need to know





The Regulation identifies a series of AI practices that are prohibited because they

go against the EU values or because they violate EU individuals' fundamental rights.





targeted search for victims

EU

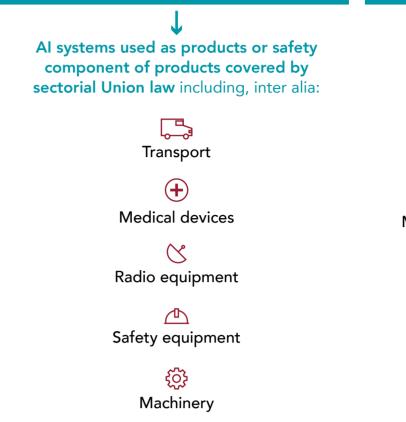
prevention of specific, substantial and imminent threats or terrorist attacks

detection, localization, identification or prosecution of a perpetrator or suspect of certain criminal offences



HIGH-RISK AI SYSTEMS

The proposal primarily focuses on high-risk AI applications and impose stringent requirements on 'providers' and 'users' of Al applications, as well as across the supply chain. In-scope uses are listed in 2 annexes.



ANNEX II

Other high risk AI applications including, inter alia:

ANNEX III

Biometric identification and categorization of natural persons

Management of critical infrastructure

Education and vocational training

Employment

Access to essential private

Administration of justice

and public services

The lists should be **updated by the EU Commission through delegated acts**.

Specific information requirements for other AI systems that interact with humans; use emotion recognition or biometric categorization systems; or manipulate content (videos, images, etc.) to generate 'deep fake'.

EX-ANTE REQUIREMENTS VETTED BY A CONFORMITY ASSESSMENT

Before the placement of AI systems on the market or their putting into service, high-risk Al systems should undergo a conformity assessment to ensure they are in line with the requirements of the Regulation.

Transparency obligations including mandatory information to

be provided in users' instructions Use of high-quality datasets for training Logging of activities to and testing the system ensure traceability of results টাটাটা Robustness, accuracy, and **Human oversight** – appropriate human-machine interface tools cybersecurity requirements Compliance that should apply throughout for natural persons to prevent or minimize risks Risk management **Documentation**

What's the process?

EU declaration of conformity +

systems

Registration in

an EU database

requirements

on the market / in service

EX-POST REQUIREMENTS

Post-market requirements (monitoring system, reporting of serious incidents and malfunctioning) and surveillance.

A REGULATION TRAINED WITH GDPR DATA?

Various elements of the Regulation echo the GDPR.

EXTRATERRITORIAL SCOPE the Regulation seeks to apply to providers and users (even if based outside the EU) that place AI systems on the market or put them into service in the EU and to providers and users of Al systems where the output produced by the system is used in the EU

PRINCIPLE OF ACCOUNTABILITY amongst others, providers need to put in place a quality management system that ensures compliance with the Regulation and is documented through written policies and procedures and technical documentation

GDPR

EU REPRESENTATIVE

obligation for providers based outside the EU to appoint an authorized representative when an importer cannot be identified

INCIDENT NOTIFICATIONS ex-post obligations include the requirement to put in place a

monitoring system and to notify the competent authorities in case of serious incidents or malfunctions in the systems within 15 days after they become aware of the breach

that can go up to 30 million or 6% of the total worldwide annual turnover of the preceding financial year

minded

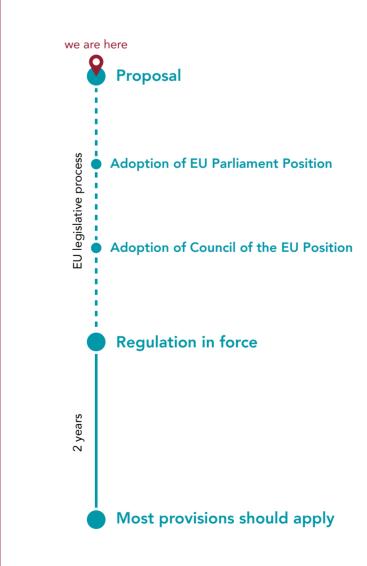
empowered national supervisory authorities and a European Artificial Intelligence Board to supervise the consistent application of the Regulation and issue interpretative guidance



WHAT COMES NEXT?

The proposal will have to undergo the **EU legislative process**, which might take quite some time and lead to significant changes.

In its current format, most provisions should apply 2 years after the entry into force of the Regulation.





"Recommendation of the Council on AI"

NATO 2019 "Coherent Implementation Strategy on Emerging and Disruptive Technologies"

UNESCO 2020 "Comprehensive global standard-setting instrument to provide AI with a strong

ethical basis" (draft) **COUNCIL OF EUROPE** "Legal framework on AI design, development

standards" (feasibility study)

Global Partnership on Artificial Intelligence

and application based on Council of Europe



The **EU** is shaking the AI ecosystem and stepping in as a **key regulator**. This competes with other 'principles-based' regional approaches, such as

We will closely follow the developments of the Regulation to help understand how the "AI EU way" will play out.

AUTHORS



Diletta De Cicco ddecicco@steptoe.com



Charles-Albert Helleputte (Head of EU cybersecurity, data & privacy) chelleputte@steptoe.com

OTHER CONTACTS

or your regular Steptoe contact



Charlotte Brett Policy Advisor



Partner cwhiddington@steptoe.com

Charles Whiddington



David O'Sullivan Senior Counselor dosullivan@steptoe.com



Of Counsel phughes@steptoe.com