

BRUSSELS VS SKYNET - EC UNVEILS AGENDA FOR POLICING AI

06 May 2021 | Insight
Legal Briefings

EC makes pioneering bid to regulate AI as policymakers strive to ensure public trust. Can it work?

The European Union Commission released its long awaited [proposed regulation of artificial intelligence](#) on 21 April 2021 (see press release [here](#)), which sets out a risk-based approach to regulation designed to increase trust in the technology and ensure the safety of people and businesses above all. The regulation has extra-territorial scope meaning that AI providers located outside of the EU whose technology is used either directly or indirectly in the EU will be affected by the proposal. This wide ranging applicability and the ambitious nature of the proposal have afforded it intense scrutiny, as it is the first regulation of its kind. Although it provides for fines of up to EUR 30 million or 6% of the total worldwide annual turnover, the proposal would impose controls on what are the most risky forms of AI – potentially leaving unaffected many AI applications which are in use today.

BROAD SCOPE OF APPLICATION

AI is broadly defined in the proposal and the assessment of whether a piece of software is covered will be based on key functional characteristics of the software - in particular, its ability to generate outputs in response to a set of given human defined objectives. AI can also have varying levels of autonomy and can be either free standing or a component of a product.

To prevent the circumvention of the regulation and to ensure effective protection of natural persons located in the EU, the regulation applies to:

- any provider of AI systems irrespective of whether they are based inside or outside the EU, if their systems are used directly in the EU or if the output of their system would

impact a natural person in the EU; and

- to individuals, public or private entities using these AI systems in the EU (the ‘users’), except where the AI system is used in the course of a personal non-professional activity.

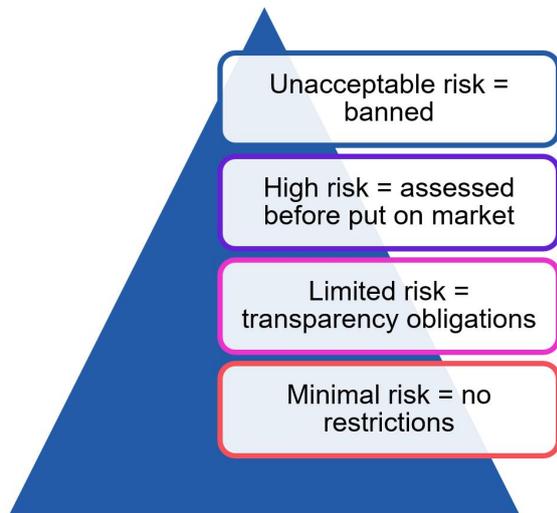
For example, where an EU operator subcontracts the use of an AI system to a provider outside of the EU, and the output of such use would have an impact on people in the EU, then the provider would be obliged to comply with the regulation if using a “high-risk” AI system.

This wide scope of application is not unusual for the Commission, as a similar approach was adopted for the protection of personal data under the GDPR and in the draft EU Digital Services Act and the draft ePrivacy Regulation.

RISK BASED APPROACH

The proposal sets out four categories of AI systems based on the risk they present to human safety.

1. Those systems which unequivocally harm individuals are banned, such as AI applications which manipulate human behaviour through subliminal techniques, circumvent the user’s free will or systems which allow ‘social scoring’. Operating an AI system in violation of such a prohibition may lead to the maximum penalty of up to EUR 30 million or 6% of the total worldwide annual turnover.
2. The most extensive set of provisions deal with “high-risk” AI systems and start applying during their development, before they are made accessible on the EU market. Such regulatory requirements include obligations for ex-ante testing, risk management and human oversight to preserve fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. AI systems relating to critical infrastructure (e.g. autonomous vehicles or the supply of utilities) also fall within this risk category. The classification of an AI system as “high-risk” depends not only on the purpose of the system but also on the potential affected persons, the dependency of these persons on the output and the irreversibility of harms they could suffer. In particular, the regulation requires that the data sets which are used to train the AI algorithm be of high quality to ensure their accuracy and their non-discriminatory nature.



3. Those AI systems which present limited risks to fundamental rights will be subject to transparency obligations. For instance when users are interacting with chatbots, the user should be made aware that the chatbot is powered by an AI algorithm.
4. The majority of AI applications in use today present minimal risks to citizens' rights or safety (e.g. AI enabled video games and spam filters), which means no restrictions are imposed on their use by the proposal.

IMPACT

If the proposal is passed (see the **What's next?** section below), this would generate a significant compliance burden on companies developing and marketing "high risk" AI systems, including providing risk assessments to regulatory authorities that demonstrate their safety (effectively giving those authorities the right to determine what is acceptable and what is unacceptable). In light of this, industry stakeholders will welcome the proposed 24 month grace period after the regulation is finalised before the legislation will apply.

The regulation could also have a significant impact outside the EU given European regulations such as the GDPR have influenced regulations abroad. We have seen regulators so far shy away from being the first to act when it comes to AI because of concerns about constraining innovation and investment. Therefore this action by the Commission could be a catalyst for other regulators to act.

The proposal provides for the creation of an 'EU AI Board' to set standards and help national regulators with enforcement. This approach differs from that of the GDPR (which created a single regulator) as national competent authorities would be in charge of monitoring and enforcing the provisions.

The fines imposed by the proposed regulation mainly relate to an absence of cooperation or incomplete notification of the competent authorities, but could be significant:

- developing and placing a blacklisted AI system on the market or putting it into service could trigger a fine of up to EUR 30 million or 6% of the total worldwide annual turnover of the preceding financial year (whichever is higher);
- failing to fulfill the obligations of cooperation with the national competent authorities, including their investigations could amount to up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year in fines (whichever is higher);
or
- supplying incorrect, incomplete or false information to notified authorities could cost up to EUR 10 million or 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

WHAT'S NEXT?

It will likely take a number of years for the proposal to be passed into law. It must first be debated and adopted by the European Parliament and the Member States before it becomes directly applicable in all Member States. The current provisions may be changed during this process and further clarification may be brought to concepts such as obligations imposed on users. In addition, the Commission has retained the ability to add onto the list of AI prohibited or highly regulated in order to adapt the regulation to any future developments of the technology.

MARKET RESPONSE

Privacy activists have questioned the loopholes in the regulation which seek to ban real-time remote biometric identification in public spaces, except where law enforcement uses such facial recognition for:

- the search for potential victims of crime, including missing children;
- certain threats to the life or physical safety of natural persons or of a terrorist attack; or
- the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences.

Business will be closely monitoring the development of the proposal as it goes through the legislative process and how it impacts current and future activities, especially in areas like advertising. If passed, the proposal would have wide ranging consequences on businesses using AI systems as it will impact how the AI algorithm is created as well as regulatory monitoring during the life of the technology.

BACKGROUND

The proposal is part of a set of initiatives to set up Europe for the digital age. Fueling innovation in AI has been part of the EU's agenda to create jobs and attract investments. First, in 2018 the [Commission published a strategy paper](#) putting AI at the center of its agenda, followed by [guidelines for building trust in human centric AI](#) published in 2019 - after extensive stakeholder consultation (see our previous blogpost [here](#)). It has also encouraged collaboration and coordination between Member States in order to create AI hubs in Europe by releasing a [Coordinated Plan on AI in 2018](#) - which has been updated with the release of the proposal (see the New [Coordinated Plan on AI 2021](#)).

The Commission also published a [White Paper on AI](#) in 2020 which set the scene for the proposal by setting out the European vision for a future built around AI excellence and trust (see our previous blogpost [here](#)). The White Paper was also accompanied by a '[Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics](#)' which highlighted the gaps in the current safety legislation and lead the Commission to release a new [Machinery Regulation](#) alongside the proposal.

SHARE

[Share to Facebook](#) [Share to Twitter](#) [Share to LinkedIn](#) [Email](#) [Print](#)

Show Share Links

RELATED TOPICS

[Digital Transformation](#)

[Emerging Technologies](#)

[Tech Regulation](#)

[Digital Transformation](#)

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:



-

TECH, DIGITAL & DATA



-

GEOPOLITICS AND BUSINESS



[NEW BUSINESS LANDSCAPE](#)

RELATED ARTICLES



UPDATED: UK NATIONAL SECURITY ACT 2021 - WHAT INVESTORS NEED TO KNOW



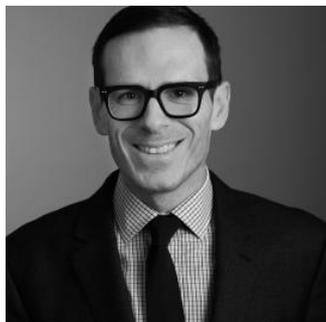
Foreign investment: Rising tides of politics in regulation



Comply or Explain to mandatory climate-related reporting

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



AARON WHITE
PARTNER, BRISBANE

+44 20 7466 2188
aaron.white@hsf.com



CLAIRE WISEMAN
PROFESSIONAL
SUPPORT LAWYER,
LONDON

+44 20 7466 2267
Claire.Wiseman@hsf.com



**GHISLAINE
NOBILEAU**
ASSOCIATE, LONDON

+44 20 7466 7503
ghislaine.nobileau@hsf.com