Volume 4, No. 6 | November–December 2021

The Journal of Robotics, Artificial Intelligence & Law

European Commission's Proposed Regulation on Artificial Intelligence: Requirements for High-Risk AI Systems

Karen L. Neuman, Hilary Bonaccorsi, Michael P. Tierney, and Madeleine White

fastcase FULL COURT PRESS

European Commission's Proposed Regulation on Artificial Intelligence: Requirements for High-Risk AI Systems

Karen L. Neuman, Hilary Bonaccorsi, Michael P. Tierney, and Madeleine White*

This article describes "high-risk" artificial intelligence ("AI") systems under an AI regulation proposed by the European Commission, summarizes key requirements for these systems, discusses corresponding obligations for providers of high-risk AI, and identifies some strategic considerations for providers and other impacted organizations.

The European Commission's ("EC") proposed regulation[1] ("Proposed Regulation") for "trustworthy" artificial Intelligence ("AI") systems establishes rules for the development, placement on the EU market, and use of AI. Rather than regulating all AI to the same degree, the Proposed Regulation takes a proportionate, risk-based approach by distinguishing between "harmful" AI practices,[2] which are prohibited, and other AI uses that carry risk, but are permitted. The bulk of the Proposed Regulation focuses on "high-risk" AI.

This article (1) describes "high-risk" AI systems under the Proposed Regulation; (2) summarizes key requirements for these systems; and (3) discusses corresponding obligations for "providers" of high-risk AI. This article also identifies some strategic considerations for providers and other impacted organizations.

The Proposed Regulation may evolve during the public consultation and negotiation periods. The Proposed Regulation also may become a global blueprint for lawmakers and regulators already examining AI, including in the United States, where the Federal Trade Commission has spotlighted its interest in AI.[3] Now is the time for providers (and users)[4] of high-risk AI to familiarize themselves with applicable provisions in the Proposed Regulation to gain a head-start on understanding the potential impacts on their businesses.

Robotics, Artificial Intelligence & Law / November–December 2021, Vol. 4, No. 6, pp. 441–449.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

What Is High-Risk AI?

The Proposed Regulation creates two main categories of high-risk AI. The first is AI intended for use as a "safety component" of a product, or which is itself a safety component, such as a "collision avoidance system" in a car. These AI systems are already subject to existing EU conformity (product integrity) assessment procedures, governance, and enforcement mechanisms. The EC anticipates that these frameworks will be updated to account for the Proposed Regulation's new requirements.[5]

The second category of high-risk AI is "stand-alone" AI systems. The Proposed Regulation and accompanying Explanatory Memorandum attempt to future-proof the law through technology-neutral requirements but list specific technologies in annexes. These annexes can be updated from time to time as technology evolves.

The high-risk AI systems annex (Annex III) lists the following AI systems as high risk:[6]

- *Biometric identification and categorization*: AI systems intended to be used for real-time and post remote (e.g., CCTV footage) biometric identification of individuals.[7]
- *Management and operation of critical infrastructure*: AI systems intended to be used as safety components in the management and operation of road traffic and supply of water, gas, heating, and electricity.
- *Education and vocational training*: AI systems intended to be used for determining access or assigning individuals to educational and vocational training institutions, or for the purpose of assessing students in educational institutions.
- *Employment, workers management, and access to self-employment*: AI systems intended to be used for recruitment or selection of individuals, notably, advertising vacancies, or for making decisions on monitoring and evaluating workplace performance.
- *Access to and enjoyment of essential private services and public services and benefits*: AI systems intended to be used by or on behalf of public authorities to evaluate individuals for public assistance benefits and services, or to evaluate the creditworthiness of individuals.

The EC can add new high-risk AI systems when: (1) the AI system is intended to be used in any of the areas already listed in

the annex, and (2) the AI system poses a risk to health, safety, or fundamental rights that is equal or greater to that posed by the high-risk AI systems already set forth in the annex. Factors to be considered by the EC when assessing these risks include the intended purpose of the AI system and whether the AI system has already caused harm to health and safety, or has had an adverse impact on fundamental rights.

Summary of Key Requirements for High-Risk AI

Risk Management System

High-risk AI systems are required to have a risk management system in place throughout their entire life cycle. These systems must, among other things: (1) identify known and foreseeable risks associated with the AI system; (2) estimate and evaluate risks that "may emerge" when the system is "used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse"; and (3) include risk management measures. Residual risks must be "acceptable" and communicated to users. Among other requirements, high-risk AI systems must also be tested prior to being placed on the market or put into service in order to identify the most appropriate risk management measures.

Data and Data Governance

Data sets used to train, validate, and test AI systems must meet certain quality criteria. For example, the data sets must be "relevant, representative, free of errors and complete" and consider the "characteristics or elements" that are specific to the "geographic, behavioral, or functional setting" in which the related AI system is intended to operate. Providers and users of high-risk AI must continually examine possible biases and identify potential gaps in the data sets used to make the AI function.

Technical Documentation

High-risk AI systems must be accompanied by technical documentation. The documentation must contain information necessary for regulators to assess the AI system's compliance with the

Proposed Regulation. This includes information on the system's capabilities and limitations, algorithms, data, training, testing, and validation processes used, as well as documentation that describes how identified risks have been managed.

Recordkeeping

The Proposed Regulation requires high-risk AI systems to possess automatic logging capabilities. The Proposed Regulation anticipates that AI will generally operate by comparing and analyzing new "input data" (e.g., data regarding employee applicants, healthcare patients, etc.) against a background data set that is used to develop and train the AI system and generate results. At a minimum, the required logging functionality must provide a record of each time an AI system is used, the reference database against which input data has been checked by the AI system, the input data which led to a "match" (i.e., each time a decision is made against background data), and the identities of the people responsible for overseeing and verifying the AI.

Transparency

High-risk AI systems must be accompanied by "instructions for use" that are "concise, complete, correct, and clear" so that users can "interpret" a system's output and "use it appropriately." Disclosures to be provided include:

- The AI system's intended purpose;
- The level of accuracy, robustness, and cybersecurity against which the AI was tested and validated;
- Any known or foreseeable circumstance that may lead to risks to health, safety, or fundamental rights; and
- The AI system's performance with respect to the people on whom it is intended to be used.

Subject to certain exceptions, providers of AI that is intended to interact with individuals are required to inform those individuals that they are interacting with AI. In addition, users of an emotion recognition system or a biometric categorization system must tell the individuals exposed to that system of its operation.

Human Oversight

High-risk AI systems must allow for human oversight that enables the person overseeing the system to fully understand its capabilities and limitations and effectively monitor it for signs of dysfunction. Humans must be able to intervene and halt a system's functions through a "stop button."

Primary Obligations for Providers of High-Risk AI

Providers of high-risk AI must comply with specific requirements under the Proposed Regulation, including:

- Implement a quality management system and adopt written policies, procedures, and instructions to ensure compliance with the requirements for high-risk AI in the Proposed Regulation. The system must incorporate many features, including risk management, post-market monitoring, procedures for reporting incidents (e.g., data breaches, system malfunctioning, and identification of risks that were not previously apparent), and testing and validation procedures for data management. The system can be "proportionate to the size of the [providers'] organization[s]."
- Draw up technical documentation and keep logs to accompany high-risk AI systems and, subject to certain exceptions, keep the automatically generated logs that AI systems must generate.
- Conduct a conformity assessment before placing the system on the market or putting it into service. The applicable conformity assessment procedure, and whether it must be conducted internally or by a third party, depends on the category and type of AI at issue.

Providers of high-risk AI must also implement other measures, which include:

- Taking corrective action if the AI system they have placed on the market or put into service is not in conformity with the Proposed Regulation;
- Providing information to and cooperating with authorities;

- Appointing an authorized representative in the European Union (if located outside the European Union); and, where applicable,
- Registering their high-risk AI systems in the EU database of such systems to be created under the Proposed Regulation.

Strategic Considerations and Sector-Specific Challenges

The Proposed Regulation has already been criticized by stakeholders who contend that exceptions could dilute protections and give way to increased use of real-time remote biometric identification systems by law enforcement in public spaces. Other stakeholders contend that the Proposed Regulation could threaten innovation in the European market. Users of high-risk systems will want to start assessing now the impact of the Proposed Regulation on their sectors, including the following.

How to Balance Transparency with the Protection of Trade Secrets

The Explanatory Memorandum asserts that "increased transparency obligations will [] not disproportionately affect the right to protection of intellectual property . . . since they will be limited only to the minimum necessary information." Nevertheless, given the robust transparency requirements, providers of high-risk AI will need to consider if they will be able to satisfy these requirements and still protect their trade secrets. Sector-specific trade groups may seek to develop standard disclosures to align with regulatory expectations.

Whether and When AdTech is a High-Risk AI System

The Proposed Regulation does not expressly regulate the AdTech sector or consider AdTech in and of itself to be a high-risk AI system or use of AI. The only reference to "advertising" in the list of high-risk AI systems relates to those used for job recruitment, including "advertising vacancies." AdTech providers (or users) will nonetheless want to compare their uses of AI with the list of high-risk AI.

For example, algorithms and models that target ads to some populations but exclude others may, indirectly, exclude these populations from learning about employment, educational, or training opportunities. Likewise, algorithms and models could exclude some populations from learning about public services and benefits for which they may qualify. Put simply, AdTech itself may not be high-risk, but the uses to which it is put could potentially be high risk under certain circumstances.

How to Decide Whether an AI System Interacts with Humans

There are special transparency obligations for AI systems that are intended to interact with individuals (e.g., chatbots). Companies may want to assess whether their seemingly invisible AI systems, such as AI-driven apps, tools that make eligibility decisions, or tools that monitor daily routines or health information, may, in fact, be ones that are "intended to interact with" humans.

How to Navigate the Requirements in the Proposed Regulation in Relation to GDPR

Providers of high-risk AI may be subject to competing or duplicative obligations under the GDPR. For example, companies that are not established in the European Union, but otherwise offer goods and services in the region or monitor the behavior of data subjects in the EEA, are required to designate an EU representative under the GDPR. Similarly, under the Proposed Regulation, providers of high-risk AI systems (if located outside of the European Union) that offer the system in the European Union must also designate an EU representative. Non-EU providers will want to consider whether they therefore must designate two EU representatives.

Consider What It Means for a Quality Management System to Be "Proportionate to the Size of the Provider's Organization"

Companies may want to consider what it means for a "quality management" system to be "proportionate to the size of the

provider's organization" in practice. For example, whether "size" refers to number of employees, the provider's annual revenues, the "impact" that its high-risk AI system has, or something else.

Other regulators have permitted a "balancing" approach like the one suggested in the Proposed Regulation. For example, when Massachusetts adopted a requirement for companies processing Massachusetts residents' personal information to adopt a written information security program, it required the program to be "appropriate to" the "size, scope, and type of business," "the amount of resources available," and "the amount of stored data."

While early drafts of the GDPR included certain derogations and exemptions for smaller companies, these largely disappeared in the later drafts in favor of a proportionality vis-à-vis the processing activities approach. For example, as part of the controller's obligation to implement appropriate technical and organizational measures under the GDPR, a controller need only implement appropriate data protection policies "where proportionate in relation to processing activities," thereby looking to the processing in question rather than the controller organization. Companies will therefore be mindful that the proportionality approach in the current draft of the Proposed Regulation may change during the legislative process.

What Obligations Apply When Using a Biometric Categorization System

More than just facial features or fingerprints, biometric data may also relate to an individual's physiology, such as the way a person walks, speaks, or even how a person makes strokes on a keyboard. Companies that use AI systems to assign individuals to specific categories based on their biometric data must adequately and transparently disclose to users that they are using them.

How to Address AI Risks Contractually

Users of high-risk AI systems that introduce these systems into the European market will have obligations like those of a provider. To mitigate potential risks, users of high-risk AI systems will want the providers of those systems to represent that they comply with the Proposed Regulation, use good quality data, and ensure that the

assumptions that go into an AI's logic base are vetted and overseen by a team of people that are representative of relevant populations.

Providers may want to consider creating industry-standard and/or competitive representations to include on their own paper.

Notes

* Karen L. Neuman is the co-chair of Dechert's Privacy & Cybersecurity Practice; the co-authors are lawyers in Dechert's Privacy & Cybersecurity Practice. Ms. Neuman can be reached at karen.neuman@dechert.com.

1. *Available at* https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

2. Prohibited AI includes AI that deploys subliminal techniques to materially distort behavior in a manner that causes a person physical or psychological harm, exploits a specific group's vulnerabilities, is used for social scoring or, subject to some exceptions, for real time biometric identification in public places for law enforcement purposes.

3. *Available at* https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai?_vx_workflow=26428.

4. Under the Proposed Regulation, "Provider" means "a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge." "User" means "any natural or legal person, public authority, agency or other body using an AI system," except when used during a personal non-professional activity.

5. *See, e.g., Explanatory Memorandum*, at Section 1.3, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

6. Annex III of the Proposed Regulation includes other high-risk uses, including those related to law enforcement, migration, asylum and border control management, and the administration of justice.

7. The Proposed Regulation expressly prohibits AI used for real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement, unless such use is strictly necessary for a targeted crime search, the prevention of substantial threats, or is being used in other very limited circumstances.