

Point of View

Artificial Intelligence Act EU Attempts to Tame the Tech Dragon

EU AI Act

Abstract

The rapid advancement of AI technologies is shaping government policies worldwide. In the EU, lawmakers and experts started working on a regulatory approach for AI with the establishment of a special committee on Artificial Intelligence in Digital Age (AIDA) in 2020. A draft proposal of the EU AI Act was unveiled in 2021, aiming to develop human-centric AI that prioritizes privacy and safety. The AI Act takes a risk-based approach to categorize systems into different risk categories (unacceptable/high/medium/low). High risk AI systems will be subject to most stringent regulations and requirements.

After last-minute amendments to cover Generative AI and Foundation models, EU lawmakers reached a preliminary deal in Apr'2023, and the bill is likely to pass by the end of 2023 after parliamentary negotiations. Once adopted, the EU AI Act will be the first of its kind landmark horizontal regulation on AI.

The year 1950 was a watershed moment in human history, and its events have left an enduring legacy on the world. The first universal credit card (made of cardboard) was introduced in the US; Gwendolyn Brooks won a Pulitzer prize for her poetry book *Annie Allen* becoming the first African American to do so; Disney released *Cinderella*, which became its highest-grossing movie of the year; *Peanuts*, the famous cartoon strip by Charles M. Schulz began as a daily strip in seven newspapers; US declared its support to develop the Hydrogen bomb, and Winston Churchill lost the general elections as the Labour party won but with a much-reduced majority.

In the same year, **Alan Turing** released a path-breaking and prophetic paper called “Computing Machinery and Intelligence,” popularly known as *Imitation Game*, where he raised the question - “can machines think?”. This was much before the term Artificial Intelligence (AI) was coined in 1955.

Turing came up with an idea for a test that would measure a machine’s ability to exhibit intelligent behavior equivalent to or indistinguishable from a human’s. This test became known as the **Turing test**.

Turing proposed that a human judge would converse with a **machine** and a **human** without knowing which was which. If the judge could not reliably distinguish the machine’s responses from the human’s, then the machine would be considered to have passed the test and be considered as having human-like intelligence.

Years passed, and many attempts were made to create machines that could pass the Turing test. Some came close, but none were able to convince the judges that they were fully human. Nonetheless, the pursuit of AI continued to drive progress in computer science and robotics.

Then, in 1997, **Deep Blue**, developed by IBM, defeated Garry Kasparov, the world chess champion. Today, we are seeing AI systems that appear to be truly intelligent machines that can not only mimic human behavior but also learn, reason, and solve complex problems in ways that were once thought impossible.

Machines and algorithms are being used across different industries to bring positive impact on our world, such as predicting weather patterns and natural disasters, optimizing energy consumption in buildings, enabling virtual tutors in various languages, early detection of diseases, robotic-assisted surgeries, optimizing routes for transport and logistics, working in hazardous environments, quality control and inventory management, using smart cameras to avoid bird deaths by wind turbines and so on.

The world of business and finance has seen increased use of AI in automating routine and repetitive tasks, analysis of large amounts of data with speed and accuracy, helping make better-informed decisions, enhancing customer experience through chatbots and personalized financial services, real-time fraud detection through identification of suspicious transactions, identifying potential risks such as credit risk/market risk/operational risk, improving investment and trading strategies, and identifying regulatory and compliance violations.

While AI offers significant benefits, it raises an important question: *Are algorithms and machines above morality and, more importantly, above the law?*

Regulators are now working on creating effective regulations that will help shape the future of AI in a way that is safe, ethical, and beneficial for all.

The European Union **(EU) AI Act** is a proposed piece of legislation that seeks to regulate the development and deployment of AI systems across the EU.

EU AI Act

History and Timeline

EU Commission president Ursula Van Der Leyen talked about making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy through AI Ethics guidelines.

2018

EU Commission started a pilot project on Explainable AI.

2019

2020

Consultation and evaluation of the pilot phase of AI Ethics guidelines began. Ursula Van Der Leyen released the white book for AI and data strategy and said that the EU wanted to attract €20 billion per year through AI.

Draft of the Artificial Intelligence Act was unveiled. The act imposed checks on technologies considered high-risk and included a ban on most surveillance and live facial scanning as well as AI systems to filter out school, job, or credit scoring.

2021

2022

First AI Regulatory Sandbox launched.

Addition of subcategories of “General Purpose AI” and “Foundation Models” to put stricter obligations on generative AI tools

2023

EU AI Act

Definition of AI

The act establishes a neutral definition of AI, intending to cover all AI (symbolic AI, Machine Learning (ML), and hybrid systems), and includes techniques that are not yet known or developed.



A software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

Source: Article 3 of EU AI Act (<https://artificialintelligenceact.eu/the-act/>)



The quality of a robust law is that it is open and abstract, e.g., our constitution. Keeping this in mind, AI regulations are also being drafted so that any future technology advancement and use cases can be brought into the regulatory framework easily.

EU AI Act

Summary of Ethical Guidelines

As per the Act, a trustworthy AI should be lawful, ethical, and robust. AI systems must satisfy **the seven assessment guidelines:**

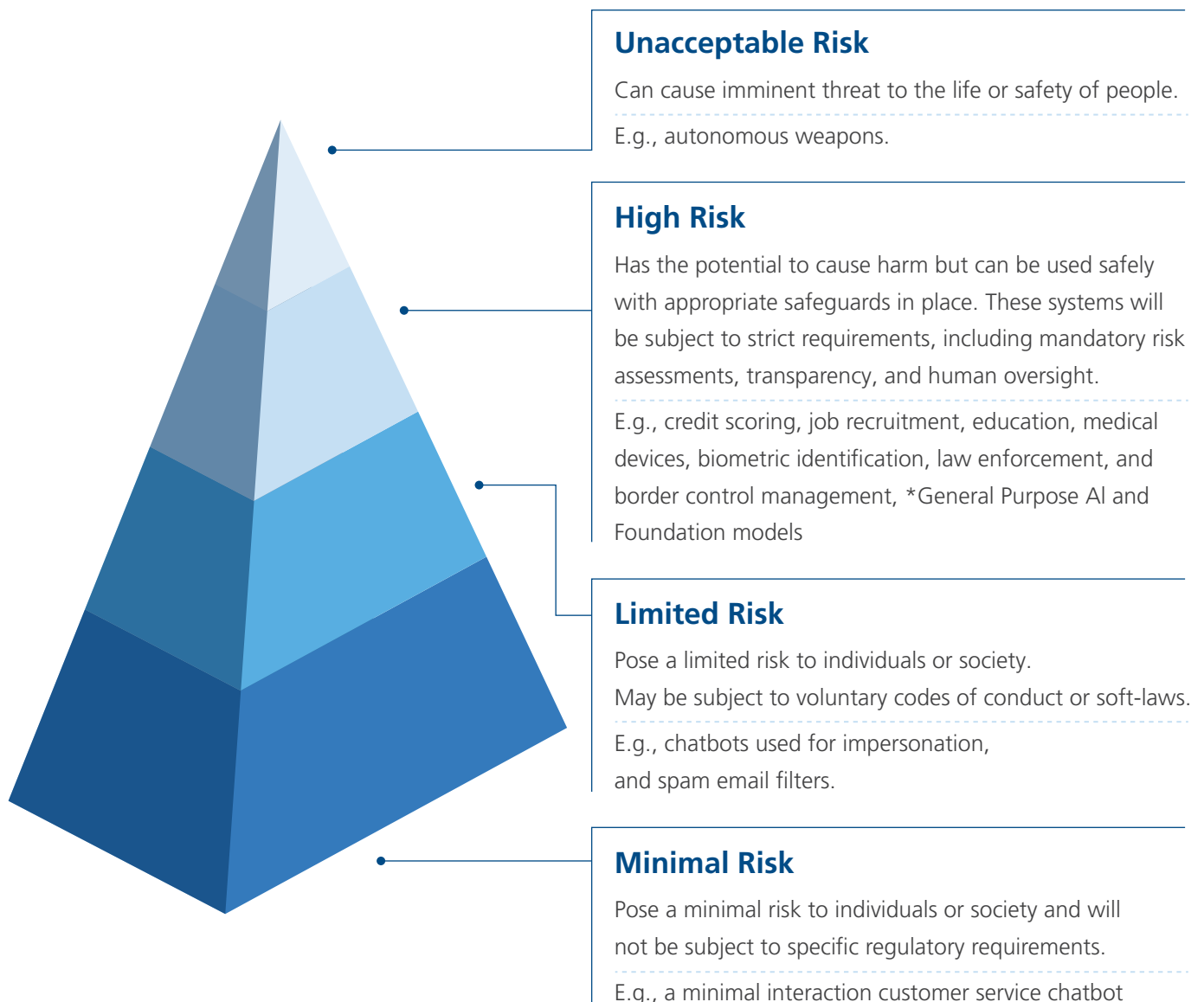


EU AI Act

A Risk-Based Approach

The risk-based approach of the EU Commission's AI Act draft refers to how the regulation categorizes different types of AI systems according to their potential risks to human health, safety, and fundamental rights.

The AI Act classifies AI systems into the following four categories:



EU AI Act

What Could it Mean for the Financial Services Industry?

The provisions of the Act are not expected to impact most of the core business of banks, but only the AI systems, which are high risk. Financial services will have obligations as software importers, providers, distributors, and users.

Under the purview will be any system that uses ML/statistical methods or is logic-knowledge based.

Fines for violation of the rules can be up to **6% of global turnover** or **30 million euros** for private entities.

The below table summarizes how the AI Act will impact the financial industry.

	AI Act Risk Category	Use-case in Finance	Guidelines
Credit Scoring	High	<ul style="list-style-type: none"> › Evaluate an individual's creditworthiness and credit score. › Evaluate the credit default risk category of a customer. 	<ul style="list-style-type: none"> › Register the AI system as high-risk under the EU database. › Continuously monitor software behavior, outcomes, and use. › Set up governance with respective banking regulators. › Regulate the use of personal data used by credit scoring algorithms, as this impacts a person's privacy and fundamental rights.

<p>Biometrics</p> <ul style="list-style-type: none"> > Face > Fingerprint > Voice > Iris 	<p>High</p>	<ul style="list-style-type: none"> > Digital ID for customers using cloud-based authentication. > Fraud detection and prevention. 	<ul style="list-style-type: none"> > Maintain strict data privacy, as some biometric characteristics can reveal secondary information which may affect a person's fundamental rights. > Ensure no bias, as biometrics is known to not work accurately for people of color and women due to biased training datasets and can lead to discrimination. > Maintain transparency to enable individuals to know when their biometric information is being processed.
<p>People Management</p>	<p>High</p>	<ul style="list-style-type: none"> > Use of AI for hiring and promotion decisions. 	<ul style="list-style-type: none"> > Avoid discrimination towards specific categories of people. > Set up continuous monitoring. > Add mandatory human oversight.
<p>Chatbots</p>	<p>Limited</p>	<ul style="list-style-type: none"> > Customer service chatbot. 	<ul style="list-style-type: none"> > An AI system impersonating a human through audio/video must make it clear to users that it is a machine they are interacting with to avoid the risk of manipulation or deceit. > With the latest developments in Large Language Models (LLM), e.g., OpenAI's ChatGPT, and Generative AI, e.g., image generation tool Midjourney, these have come under the purview of the high-risk category.

<p>Securities Market</p> <ul style="list-style-type: none"> > Stock trading > Algorithmic and high-frequency trading > Asset management 	<p>High</p>	<ul style="list-style-type: none"> > Robo-advisors > Natural Language Processing (NLP) techniques used to analyze company reports to generate real-time assessments. > ML models used to execute large trades optimally across different regions and times. 	<ul style="list-style-type: none"> > Fund houses and brokerage firms to create transparency with investors whenever they leverage AI/ML tools for decision making. > Ensure that the NLP techniques and prediction algorithms are bias-free. > Ensure consent and privacy guidelines while collecting investors' personal data for use by robo-advisors. > Maintain transparency and explainability for algorithms, as GDPR's right to explanation allows users to ask about the logic involved in algorithmic decisions.
<p>General Guidelines</p>	<ul style="list-style-type: none"> > Set up governance and monitoring of AI systems. > Perform data quality checks on training, validation, and testing data for algorithms to ensure data transparency, completeness, and fairness. > Ensure robustness, privacy, and cybersecurity. > Encourage responsible innovation. 		

Conformité Européenne (CE) indicates that a high-risk AI system complies with the regulation after undergoing a conformity assessment procedure.

EU AI Act

The Political Will Backing this Regulation

EU's vision for AI

Through the Horizon Europe and Digital Europe programs, the Commission plans to invest €1 billion per year in AI and generate €20 billion in revenue per year in the future. Paul Nemitz, a key contributor to GDPR and now actively involved in forming the EU AI Act, explains how unregulated AI can be a threat to Democracy.

“There has been reshaping of public space of discourse as algorithms are deciding what political news we see on the internet. There may be a different variety of messages being sent from the same party, which might not match their published manifesto. This is contrary to newspapers publishing the same news and point of view for everyone.”

EU Commission wants to propose a regulation of the Election Party Register that will provide a comparative overview of all messages a party pays for online discourse.

Nemitz adds further: “Code is upgraded on a daily basis which is difficult to keep check on. The big tech giants can take advantage of this for their business benefits while no one else can transparently understand the changes.”



The Brussels Effect

Anu Bradford is a Finnish-American author, Professor of Law and International Organization at Columbia Law School, and expert in international trade law. She is the author of **“The Brussels Effect: How the European Union Rules the World.”**

In her book, she explains ‘The Brussels Effect’, as a process of regulatory globalization. Companies must comply with EU regulations and standards to gain access to its markets.

As a result, the EU can set global standards through its **regulatory power**. With the AI Act, the EU will have a starter advantage, as organizations would also push to have a consistent global framework to comply with, and hence EU regulations will get worldwide acceptance.

Recent EU AI Act Amendment for General Purpose AI and Foundation Models

On Apr 27th 2023, members of the European Parliament reached a preliminary deal to push the draft AI Act, with significant last-minute amendments introduced to put stricter obligations on generative AI models.

Distinct definitions for **'General Purpose AI'** and **'Foundation models'** have been introduced. Foundation models (like GPT4, Stable Diffusion) are defined as – “AI systems that are trained on broad data at scale, are designed for generality of output, and can be adapted to a wide range of distinctive tasks”. A general Purpose AI system is “any AI system that is intended by the provider to perform general applicable functions”.

Generative AI tools (like OpenAI's ChatGPT and Midjourney) will now have to disclose any copyrighted material used for training their models, provide details of personal data usage, create a transparent privacy policy, provide better control on maintaining data history and follow EU law and fundamental rights.

EU Commission maintains that the Act is pro-innovation and provides guardrails to avoid misuse instead of a ban on the technology.

Conclusion

AI can be both powerful and unpredictable. Harnessing its power to improve our lives and solve our greatest challenges requires understanding how this technology works by improving our knowledge and skills.

The EU has laid out a comprehensive strategy for using AI-related applications in Europe, under programs like AI4EU, EuroHPC, AI Watch, ELISE, AI4Media, and SHERPA. It plans to take forward AI initiatives in areas of healthcare, transportation, environment and sustainability, social inclusion, education, and agriculture to improve people's lives.

Creating frameworks to bring transparency and ensure the use of AI for good will be key in shaping the future. The Artificial Intelligence Act is an important step in this direction as the EU looks towards AI innovation for its economic growth. The draft still has loopholes; however, with government, organizations, and people's support, the regulation can be strengthened with time. In parallel, we are seeing legal frameworks for AI systems management being formulated by other strong democracies of the world like the U.S., Britain, France, Canada, Japan, and India.

For everyone's benefit, we hope that the EU and the rest of the world can train and channel the power of the sharp-clawed beast called AI.

References Links

<https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

https://single-market-economy.ec.europa.eu/single-market/ce-marking_en

<https://artificialintelligenceact.eu/developments/>

<https://futurium.ec.europa.eu/en/european-ai-alliance>

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN.pdf

White Paper on Artificial Intelligence A European approach to excellence and trust -

https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

EU's Digital Strategy – <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

EU's Horizon Europe program -

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en)

<https://www.law.columbia.edu/faculty/anu-bradford>



Surabhi Mathur

Director - Projects, BFS

Surabhi leads the Data Science Products and Innovations team in the Banking and Finance vertical of LTIMindtree. She has a keen interest in AI ethics, data fairness and bias, building responsible AI, algorithm explainability, and ethical investing.



LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700+ clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by more than 84,546+ talented and entrepreneurial professionals across 30 countries, LTIMindtree – a Larsen & Toubro Group company – combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit www.ltimindtree.com.