November 22, 2023

Regulatory Turning Points in AI Worldwide

Client Updates

Recently, there have been significant developments in the regulation of Artificial Intelligence ("**AI**"). As the European Union's comprehensive AI Act reaches its critical stages, the US has also taken a significant step on the matter with the issuance of the Executive Order on "Safe, Secure and Trustworthy Artificial Intelligence ("**EO**") by President Joe Biden. Additionally, the G7 has published the International Code of Conduct for Organizations Developing Advanced AI Systems (the "**Code of Conduct**"). Below is a short summary of each of these important developments.

The EU AI Act is getting close to the finish line

As discussed in our previous client update, the AI act is now being negotiated as part of the "trialogue" between the Council of the European Union, the European Parliament and the European Commission. There are several issues still subject to negotiations, two of which have arisen in the past weeks. The first relates to balancing between enforcement at the member state and at a centralized EU level. The second and more significant point is the opposition of several member states to the proposed regulatory approach for foundation models, which suggests following a tiered approach by introducing tighter rules for the most influential companies.

The next significant step in the legislation process would be the meeting scheduled for December 6, 2023 – the last day of the trialogue for this year. It appears that if an agreement will not be reached by that date, the legislation process would be significantly postponed.

President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI

The EO follows the Blueprint for an AI Bill of Rights, the AI Risk Management Framework, and Executive Order 14091 of February 16, 2023, and is intended to establish guidelines, standards, and best practices for ensuring safe and responsible use and development of AI. The EO highlights various areas of concern related to the use of AI, such as cybersecurity, privacy, labor, competition and health, the main of which are detailed below:

- **Cybersecurity**: the EO imposes certain obligations on leading AI companies, including notification, reporting and disclosure obligations.
- **Data Privacy**: the EO emphasizes that the implementation of robust and comprehensive data protection measures is crucial for ensuring the security and integrity of personal information. In

that regard, the EO also underscores the need for the enactment of data privacy legislation by Congress.

- **Equity and Civil Rights**: the EO details action that should be taken to prevent bias and promote fairness in the use of AI , such as addressing algorithmic discrimination through training and technical assistance, and developing best practices for the use of AI in the criminal justice system, particularly in sentencing, parole, and probation.

- **Implications for Employers**: according to the EO, guidelines that will address job displacement risks, labor standards, job quality, and employers' AI-related collection and use of data about workers should be developed, in order to mitigate AI's potential harms to employees' well-being and maximize its potential benefits.

- **Healthcare and Biosecurity**: The EO directs the development of policies and frameworks on responsible deployments and us of AI and AI-enabled technologies.

The implementation of the Executive Order is expected to be a protracted process, marked by nonbinding deadlines that span from November 2023 to early 2025.

The G7 Code of Conduct

The Code of Conduct has the objective of promoting worldwide adoption of safe, secure and trustworthy AI and includes a non-exhaustive voluntary action, that can be taken by organizations, while following a risk-based approach. The actions suggested in the Code of Conduct, include, **inter alia**, the following:

- Develop AI responsibly, and identify, evaluate, and mitigate risks across the AI lifecycle.
- Identify and mitigate vulnerabilities, and encourage incident reporting and information sharing.
- Publicly report advanced AI capabilities and limitations to ensure transparency.
- Develop and disclose AI governance and risk management policies including privacy policies and mitigation measures.
- Invest in and implement robust security controls (including physical security and cybersecurity).
- Develop and deploy reliable content authentication mechanisms to enable users to identify AI-generated content.
- Advance the development and adoption of international technical standards.
- Develop and adopt global technical standards while safeguarding personal data and intellectual property.

There have also been recent legislative efforts in China on the regulation of use of AI technologies – we will review these in a separate client update to be published soon.

Please feel free to contact us with any questions that you have on this matter.

Key Contacts

Netta Shaked-Stadler
Partner

Assaf Harel
Partner

Rebecca Genis Shepetovsky
Senior Associate