ELİG
GÜRKAYNAK
Attorneys at Law

Generative Artificial Intelligence and Privacy

Authors: Dr. Gönenç Gürkaynak, Ceren Yıldız, Noyan Utkan and Gamze Yalçın of ELIG Gürkaynak Attorneys-at-Law

Admittedly, ubiquity of data processing may be named as one of the most unanticipated outcomes of the digital revolution that overtook the end of twentieth century. Such an unprecedented circulation of data has given way for fascinating developments in the field of "machine learning", wherefrom the densely-debated term "generative artificial intelligence" ("**Generative AI**") has been distinguished to illustrate the ability of machine learning to generate creative solutions to novel problems, by making inferences from previously learned data-sets; a quality previously associated exclusively with human intelligence.

- Definition of "Generative AI"

So far, there is no comprehensive definition for "artificial intelligence" ("**AI**"), let alone for "generative AI." That being said, several research papers have attempted to define both terms.

"International Definitions of Artificial Intelligence", published in September, 2023 ("**Definitions**") through AI Governance Center of International Association of Privacy Professionals ("**IAPP**") includes a compilation of all existing definitions of "artificial intelligence". The term has been extracted as it has been referenced in global and sectoral legislation and legal instruments; guidance, standards, and voluntary frameworks; and industry standards.[1] By way of example, per the Definitions, "artificial intelligence" is defined as "*a machine-based system that can for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environment"* as per the U.S., National Defense Authorization Act for Fiscal Year 2024.

Similarly, in a report titled "Generative Artificial Intelligence and Data Privacy: A Primer" of the Congressional Research Service of the United States ("**CRS Report**") "generative AI" is defined as the type of "*artificial intelligence that can generate new content —such as text, images, and videos—through learning patterns from data*."[2]

While delving into the definition of "generative AI", CRS Report identifies that "generative AI" is the type of AI that is particularly prone to data protection concerns as it requires massive amounts of data as its training data sets, which is obtained (or "*scraped*") from the internet, from sources that vary from a range of Wikipedia entries to digitized text books. Accordingly, generative AI datasets can include information posted on publicly available internet sites, including "personally identifiable information" (i.e. names, phone numbers, addresses, etc.) and sensitive and copyrighted

[1] *See* https://iapp.org/media/pdf/resource_center/international_definitions_of_ai.pdf; Last accessed on November 20, 2023)
[2] *See* https://crsreports.congress.gov/product/pdf/R/R47569 (Last accessed on November 20, 2023)

content, even though generative AI developers may not always provide information with respect to the exact details of their training datasets.

- **Risk Based Approach to Generative AI**

The Proposal for an Artificial Intelligence Act of European Commission of April 21, 2021 with number COM(2021) 206 final 2021/0106(COD) ("Proposal") might be the first landmark document that establishes well-defined standards for AI by stipulating a risk-based approach to generative AI systems regulation.[3] The risk categorisation per the Proposal can be summarized as follows:

- ***Prohibited Generative AI***

Per Article 5 (1) of the Proposal, the following are prohibited "artificial intelligence practices" that are unacceptable as per UN Charter on Human Rights:

- Cognitive behavioural manipulation of people or specific vulnerable groups, for example voice-activated toys that encourage dangerous behaviour in children;
- Social scoring: classifying people based on behaviour, socio-economic status or personal characteristics;
- Real-time and remote biometric identification systems, such as facial recognition.

- ***"High-Risk" Generative AI***

As per Article 6 of the Proposal, the certain practices of AI should be considered "High-Risk AI systems" and therefore be subject to additional compliance requirements throughout their life-cycle. High-Risk AI systems are categorized as the following:

- AI systems that are used in products falling under the EU's product safety legislation.
- AI systems falling into eight specific areas that will have to be registered in an EU database: (i) biometric identification and categorisation of natural persons; (ii) management and operation of critical infrastructure; (iii) education and vocational training; (iv) employment, worker management and access to self-employment; (v) access to and enjoyment of essential private services and public services and benefits; (vi) law enforcement; (vii) migration, asylum and border control management; (viii) assistance in legal interpretation and application of the law.

Compliance requirements of "High-Risk AI" impute obligations on providers, users, and other parties that range from obligations with respect to (i) establishment and operation of risk management systems; (ii) compliance with data governance requirements; (iii) provision of technical documentation; (iv) record-keeping; (vi) transparency and provision of information to users; (vii) human oversight; and (viii) additional measures with respect to accuracy, robustness and cybersecurity. (Article 16 – Article 29 of the Proposal).

[3] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (Last accessed on November 20, 2023*)*

- Law No. 6698 and Artificial Intelligence

In Turkiye, the Turkish Data Protection Authority has published "Recommendations on Protection of Personal Data in the Field of Artificial Intelligence" ("**Recommendations**") wherein the following guiding principles have been advised for systems of artificial intelligence. [4]

- Artificial intelligence and data collection procedures should adopt an approach that protect the fundamental rights and freedoms of individuals, and operate in adherence to the principles of lawfulness, good-faith, accuracy and currentness, proportionality, accountability, transparency, and being for a definite and limited purpose; and founded on the principle of data security;

- Artificial intelligence studies based on processing of personal data must comply with regulations on data protections and all systems must be developed and managed pursuant to data protection law;

- If an artificial intelligence application is perceived as "high-risk" with respect to protection of personal data, then a "privacy impact assessment" must be performed and whether data processing complies with the law must be decided;

- Special categories of personal data must be especially considered and relevant technical and administrative measures should be implemented;

- If a certain outcome can be reached without the processing of personal data during the development of artificial intelligence, then anonymized personal data should be preferred;

- Products and services that expose individuals to decisions based on automatic processing without their exclusive opinions must be avoided;

- Individuals who interact with the AI application, should be informed on the data processing reasons, details on the methods of data processing and possible outcomes of data processing and where necessary a consent mechanism should be established;

- Academic institutions, and independent experts and institutions should be consulted for support in designing an artificial intelligence system based on human rights, ethical, and social considerations and in identifying potential biases therein;

- Individuals should have the right to object against processing actions that effect their opinions and personal development;

- From its design throughout its life-cycle, algorithms that allow for accountability in terms of data protection laws for all stake-holders should be adopted;

[4] *See* https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler (Last accessed on November 20, 2023)

- Appropriate open-sourced based mechanisms should be incentivized to establish a digital ecosystem for safe, fair, legal and ethical sharing of data.

All in all, the existing body of legislation already provides a foundation that forms a basis to regulate the benefit derived from the exponential growth of artificial intelligence while preserving individuals' agency over their personal data. Yet the existing norms might not necessarily always provide explicit references to AI in connection with fundamental principles on data protection and privacy. Therefore, comprehensive set of standards with practical implementation points might be needed so that AI's technological advances are fostered without hindrance to individuals' fundamental rights on privacy and protection of personal data.

Article Contact: Dr. Gönenç Gürkaynak E-mail: gonenc.gurkaynak@elig.com

(First published by Mondaq on November 28, 2023)