European Parliament

Algorithmic discrimination under the AI Act and the GDPR

After the entry into force of the Artificial Intelligence (AI) Act in August 2024, an open question is its interplay with the General Data Protection Regulation (GDPR). The AI Act aims to promote human-centric, trustworthy and sustainable AI, while respecting individuals' fundamental rights and freedoms, including their right to the protection of personal data. One of the AI Act's main objectives is to mitigate discrimination and bias in the development, deployment and use of 'high-risk AI systems'. To achieve this, the act allows 'special categories of personal data' to be processed, based on a set of conditions (e.g. privacy-preserving measures) designed to identify and to avoid discrimination that might occur when using such new technology. The GDPR, however, seems more restrictive in that respect. The legal uncertainty this creates might need to be addressed through legislative reform or further guidance.

AI systems and algorithmic discrimination: Some scenarios

Some AI systems may cause discrimination, and harm individuals' fundamental rights.

- **Generative AI systems**: certain generative AI systems, such as chatbots, do not seem dangerous at first glance, but can still pose threats to fundamental rights and freedoms, for example when they generate hate speech. Generative AI is not classified as high-risk as such. However, some generative AI systems that harm fundamental rights might be included in the high-risk system list that regulators can update periodically, as laid down in the AI Act.
- **Autonomous cars**: discrimination could also arise in insurance calculation or AI machine vision systems – for instance, if autonomous cars are developed in a way that will detect more accurately pedestrians with lighter than those with darker skin.
- **Job recruitment and employment**: algorithms selecting job applicants might contain bias, for example with respect to gender or health.
- **Credit scoring and banking**: AI systems are increasingly used in the banking and credit sectors as a support tool to assess the granting of loans or mortgages. These systems may follow decisional processes that hide discrimination or mask bias based on factors such as clients' residence or ethnicity.

Algorithmic discrimination and special categories of personal data

The AI Act is meant to tackle the issues listed above. To ensure bias detection and correction in AI systems, Article 10(5) AI Act allows for the processing of special categories of personal data 'to the extent that … is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems', conditional on appropriate safeguards for the respect of fundamental rights.

The concept of special categories of personal data is defined in Article 9 GDPR (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, or sexual orientation). Some academics have pointed out that, to detect if an algorithm used in the employment sector discriminates on the grounds of ethnicity, in principle, the organisation concerned needs to know the job applicants' ethnicity.

Article 10(5) AI Act applies to high-risk systems only. The act adopts a 'risk-based approach', in that it classifies AI systems according to the degree of risk they pose to individuals' fundamental rights and freedoms. When determining whether a system is qualified as high-risk (Article 6 AI Act), the emphasis is on a given system's scope and the specific task it performed.

To process special categories of personal data, the specific grounds listed in Article 9 GDPR must be respected (e.g. the data subject's explicit consent). These grounds must also be respected when applying

Author: Stefano De Luca with Marina Federico, Members' Research Service
PE 769.509 – February 2025

Article 10(5) AI Act, which falls within the scope of Article 9 GDPR. The act clarifies that, when the AI Act and the GDPR collide, the GDPR prevails, and states explicitly that its provisions must not affect the GDPR's application.

Some argue that the processing of personal data pursuant to Article 10 AI Act might also be allowed under the GDPR's '**substantial public interest ground**'. Indeed, Article 9(2)(g) GDPR permits processing of special categories of data when

> *necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

In this context, the AI Act would serve as the relevant Union law, and fighting discrimination would be the relevant public interest.

Main challenges

In its September 2024 report, the Belgian Supervisory Authority stressed how correcting bias in training data for AI systems is consistent with both the principle of 'fair processing' of data laid down in the GDPR and the need to ensure that the personal information collected by data processors is accurate.

For Article 10(5) AI Act to be interpreted fully in compliance with the GDPR, some conditions must be met:

- the processing of special categories of personal data has to be carried out with robust cybersecurity measures in order to prevent data leaks, as requested by the GDPR;
- AI systems processing personal data have to comply with such GDPR principles as data minimisation, purpose and storage limitation, integrity and confidentiality, and privacy by design and by default;
- the necessity requirement, a key principle of the GDPR, has to be conceived as allowing entities to process special categories of data only when it is strictly necessary for protecting other fundamental rights, such as non-discrimination;
- the grounds set out in Article 9 GDPR for the processing of sensitive data should be present in order for the data processing to be lawful.

In addition to the **special categories of data** listed in Article 9 GDPR, discrimination may arise as a result of the processing of personal data revealing other factors, such as age or gender. These are not special categories of data pursuant to EU law, but **'merely' personal data**. Therefore, the legal grounds for processing these data will be those listed in Article 6 GDPR.

Article 6 GDPR is broader in content than Article 9 GDPR, providing for a larger number of legal bases for the processing of personal data (e.g. legitimate interest). This means that, when discrimination arises with respect to factors that **are not considered as special categories of personal data**, the processing of data to mitigate bias can occur pursuant to the grounds of Article 6, which are more lenient and easier to prove than public interest or specific consent.

In general terms, shared uncertainty appears to prevail as to how the AI Act's provision on the processing of special categories of personal data for avoiding discrimination should be interpreted. The GDPR, which imposes limits on the processing of special categories of personal data, might prove restrictive in a context dominated by the use of AI in many sectors of the economy, and faced with the mass processing of personal and non-personal data. A reform of the GDPR or further guidelines on its interplay with the AI Act might help address these issues.