Resolution of the 97th Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany
Hambach Castle
April 3, 2019

Hambach Declaration on Artificial Intelligence

Seven data protection requirements

Artificial Intelligence (AI) systems pose a substantial challenge for freedom and democracy in our legal order. AI developments and AI applications must comply with fundamental rights in a democratic and constitutional manner. Not everything that is technically possible and economically desirable may be allowed to be implemented in reality. This applies in particular to the use of self-learning systems which process data on a massive scale and interfere with the rights and freedoms of those concerned by automated individual decisions. Protection of fundamental rights is a key role of all public powers. Essential frameworks for the use of AI need to be defined by legislators and implemented by supervisory authorities. Only if the protection of fundamental rights and data protection can keep pace with the process of digitalisation, a future is possible in which, in the end, human beings and not machines decide over human beings.

I. Artificial intelligence and data protection

Artificial Intelligence is currently being discussed intensively as it promises added value in many areas of business and society. The German government has published an AI strategy with the aim of making Germany world leader in the development of AI. "AI made in Germany" is, at the same time, meant to ensure that even with far-reaching use of artificial intelligence, the basic values and civil liberties which apply in Germany and in the European Union (EU), will continue to play a significant role in our coexistence. The independent federal and state data protection supervisory authorities explicitly welcome this approach of fundamental rights-compatible design of AI.

A generally accepted definition of the term Artificial Intelligence has not yet been found. According to the German government's understanding, AI is about “designing technical systems in such a way that they can handle problems independently and are able to adapt themselves to changing conditions. These systems’ characteristic is the ability to "learn" from new data.”

AI systems are already being used, for example, in medicine to support research and therapy. Even today, neuronal networks are able to automatically recognise complex tumor structures. AI systems can also be used to detect depression disorders based on

behaviour in social networks or based on voice modulation when operating virtual assistants. In the hands of medical professionals, this knowledge can serve the patients' well-being. In the wrong hands, however, it can also be misused.

An AI system was also used to evaluate job application documents with the goal of deciding free from human prejudices. However, the company had hired predominantly male applicants in the past and the AI system had been trained with their successful applications. Subsequently, the AI system assessed women as being much less qualified even though the gender was not only no predetermined evaluation criterion but also unknown to the system. This reveals the danger of discrimination originating in training data and not being eliminated but rather being solidified.

These examples make clear that AI systems often process personal data and this processing poses risks to the rights and freedoms of people. They also demonstrate how important it is to monitor and regulate development and usage of AI systems politically, socially and legally. The independent federal and state data protection supervisory authorities understand the following requirements as a constructive contribution to this vital socio-political project.

II. Data protection requirements for Artificial Intelligence

The General Data Protection Regulation (GDPR) includes important legal requirements for development and use of AI systems processing personal data. They aim at the protection of fundamental rights and freedoms of natural persons. The principles relating to processing of personal data (Article 5 GDPR) also apply to AI systems. According to Article 25 GDPR, these principles must be implemented by the controllers through technical and organisational measures planned at an early stage (data protection by design).

1. AI must not turn human beings into objects

The guarantee of human dignity (Article 1 German Constitution, Article 1 Charter of Fundamental Rights of the EU) demands that an individual must not be objectified, particularly not in the case that AI is being used by public authorities. Fully automated decisions or profiling by AI systems are permitted to a limited extent only. Decisions with legal effect or similar significant interference may not, pursuant to Article 22 GDPR, be left to the machine only. In case that the scope of Article 22 GDPR is not applicable, the basic principles of Article 5 GDPR still apply which protect individual rights in particular through the principles of lawfulness, fairness and accountability. Even when AI systems are used, those affected have the right to the intervention of a real person, to the presentation of his or her point of view and the right to contest a decision.

2. AI may only be used for constitutionally legitimate purposes and may not abrogate the requirement of purpose limitation

AI systems may only be used for constitutionally legitimate purposes. The principle of purpose limitation must also be observed (point (b) of Article 5 (1) GDPR). Article 6 (4) GDPR sets clear limits to changes of purpose of personal data processing. Extended processing purposes must be compatible with the original purpose of collection also with

AI systems. This applies also to the processing of personal data in AI systems for training purposes.

3. AI must be transparent, comprehensible and explainable

Personal data must be processed in a way that is comprehensible to the data subject (point (a) of Article 5 (1) GDPR). This requires, in particular, a transparent processing which comprises easily accessible and understandable information about the procedures of processing and, if necessary, also about the used training data (Article 12 GDPR). Decisions taken on the basis of the use of AI systems must be comprehensible and explainable. Explainability with regard to the result alone is not sufficient. Comprehensibility with regard to the procedures and the decision-making process needs to be ensured, too. According to the GDPR, the logic involved needs to be explained as well. These transparency requirements are to be fulfilled continuously if AI systems are being used to process personal data. The principle of accountability of the controller (Article 5 (2) GDPR) applies.

4. AI must avoid discrimination

Learning systems are highly dependent on the data entered. Insufficient data bases and processing concepts can lead to results with discriminating effects. Discriminating processing are an infringement of the rights and freedoms of the persons concerned. They violate, among other things, certain requirements of the GDPR such as the principle of fairness, the restriction of processing to legitimate purposes and the adequacy of the processing.

Discriminating tendencies are not always apparent from the outset. Therefore, an assessment of risks for the rights and freedoms of people has to aim at a reliable elimination of hidden discriminations through countermeasures before an AI system is being used. Appropriate risk monitoring must be carried out also during the application of AI systems.

5. The principle of data minimisation applies to AI

AI systems typically process large amounts of training data. The principle of data minimisation (point (c) of Article 5 (1) GDPR) also applies for personal data in AI systems. The processing of personal data must, therefore, always be limited to what is necessary. Considering necessity may lead to the result that processing of completely anonymous data is sufficient for achieving a specific legitimate purpose.

6. AI needs responsibility

The parties involved in the use of an AI system must determine and communicate clearly who shall be the responsible controller. And, respectively, the controller needs to take the necessary measures in order to achieve lawful processing, to ensure the rights of a data subject, security of the processing and controllability of the AI system. The controller must ensure that the principles of Article 5 GDPR are being complied with. The controller must fulfil the obligations with regard to the rights of data subjects laid down in Article 12 to Article 22 GDPR. The controllers must ensure security of processing in accordance with Article 32 GDPR and, thus, prevent manipulations by third parties which can affect the

results of the systems. When using an AI system in which personal data are processed, a data protection impact assessment in accordance with Article 35 GDPR will generally be required.

7. AI requires technical and organisational standards

In order to ensure processing in accordance with data protection regulations, technical and organisational measures pursuant to Article 24 and Article 25 GDPR, such as pseudonymisation, must be taken during design and usage of AI systems. This is not achieved solely by the assumption that the individual person will disappear in large amounts of data. As of now, no specific standards or detailed requirements for technical and organisational measures for a data protection compliant use of AI systems exist. Increasing knowledge in this area and developing examples of best practices is an important task for commerce, industry and science. The data protection supervisory authorities will actively accompany this process.

III. AI development requires regulation

The data protection supervisory authorities monitor the application of data protection law, they enforce it and they are to advocate effective protection of fundamental rights in further development of these laws. In view of the high dynamics in the development of AI technologies and the various fields of application, the limits of this development may not yet be foreseen. Similarly, the risks of the processing of personal data in AI systems cannot be rated in a general way. Ethical principles must also be observed. Apart from the scientific community, data protection supervisory authorities and users it is, especially, the political players who are required to accompany and to direct the development of AI in favour of the protection of personal data.