Lecture

of the Federal Commissioner for Data Protection and
Freedom of Information

Prof. Ulrich Kelber

„Artificial Intelligence“

1st International Congress on Data Protection

organised by the Turkish Personal Data Protection Authority
in cooperation with the Istanbul University Faculty of Law
and the Turkish-German University Faculty of Law

Istanbul and Digital

12 November 2021

Check against delivery

Dear Ladies and Gentlemen

I. [Introduction]

I am pleased to speak on the topic of artificial intelligence at the 1st International Personal Data Protection Congress today.

Artificial intelligence is a key technology that has just begun to fundamentally change our lives. Disruptive change is predicted, like the transition to the machine age based on fossil fuels in the 18th and 19th century. So we have something big coming up.

We are at the beginning of this transformation. Many potential applications are still in their infancy. I think we are well advised to take a nuanced view of the opportunities and risks of this development. The Data Protection Authorities in particular should help to support wise recommendations for action in the future. Our goal must be to promote innovation while ensuring the best possible data protection. And even though there are – not a few – saying “This is impossible!”, I’ll keep on telling them: “Yes we can! And we will”

AI systems can affect the freedoms and rights of natural persons in many ways. This is because AI presupposes the usability of a lot of (often also personalized) data. For example, enormous amounts of learning data are required, from which the actual problem-solving algorithm is generated. So in many areas we are talking about classic "Big Data" applications.

II. Artificial Intelligence in international formats

While AI will fundamentally change our lives, it’s an important issue in many international formats. It would take more than the time of this speech, if I would present all the initiatives in this field. That’s why I would like to focus on some specific examples.

Before I set out the world's first draft legal framework for AI presented by the European Commission I will present the work done by Data Protection Authorities.

I would like to begin with the Global Privacy Assembly, the GPA. The GPA is a premier global forum for data protection and privacy authorities. The Assembly seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe. Turkey will host the annual conference of the GPA in 2022.

AI is an ongoing work for the GPA. At its 40th Conference in 2018, the GPA endorsed guiding principles, as its core values to preserve human rights in the development of AI. In 2020 the Assembly adopted a resolution on accountability in the development and use of AI.

Recently I took part in the roundtable of G7 Data Protection and Privacy Authorities. In this format the Authorities of the G7 member countries discussed opportunities for closer collaboration.

At this roundtable we agreed that Data protection and privacy authorities must play a leading role in the governance of AI, which is built on personalized data. They should constructively influence the developments of AI systems and create a framework that safeguards human rights, democracy, the common good, and individual freedoms while creating room for innovation and progress. "Red lines" are needed for those AI systems which are not compatible with our values and fundamental rights. To fulfil this task, data protection and privacy authorities need sufficient human and material resources.

The EDPB and the International Working Group on Data Protection in Technology, the so called Berlin Group, are working on guidelines for the areas of biometric identification and devices with audio recognition.

III. The Recommendations for action from Data Protection Authorities

The work done in the international formats leads to recommendations for action. So what are our recommendations in the context of AI?

In my view, we have a clear consensus as Data Protection Authorities on the minimum requirements to be met by AI systems:

First AI must not turn humans into objects. Here, we need to think very fundamentally about which AI applications should cross our "red lines" and be banned as a matter of principle.

Second, AI has a tendency to be intransparent. However, we need a high degree of transparency and traceability of the results and processes of machine-controlled decisions. AI must be made as transparent, comprehensible and explainable as possible.

What do I mean by this? We need transparency about how the decision-making of AI systems works. This transparency is also essential for trust in AI. However, it is anything but trivial to establish this transparency in the first place.

Simply disclosing program codes and training data would fall short. Those affected by AI are generally not IT specialists. And even experts would regularly be overwhelmed by the technical complexity of AI systems.

What we need in any case, in my view, is an explanatory statement on AI systems to make their respective mode of operation comprehensible to the general public. This explanatory statement is important because otherwise the data subjects will hardly be in a position to consent to the corresponding processing. Without it, they would not even know what they were actually consenting to.

Thirdly, AI of course must avoid discrimination. As a matter of principle, data subjects have the right to intervene, explain their position and challenge a decision, even when AI systems are used. The final decision should therefore always be left to a human being, and corrections have to be possible.

This human corrective is indispensable as a guarantee for fair AI. This applies in any case if it is accompanied by impairments for those affected.

But it is also clear that AI is fallible. The reason for this is simple: Errors may have crept in during programming or in the design of the system or its optimization task. Another reason is that the result of an artificial intelligence system depends to a large extent on how it was trained. So what feedback and decision paths were learned here? If the system was trained with erroneous or biased data, this will also be reflected in its decisions.

Unfortunately, these errors and discriminations based on them are often not recognizable in advance. Neutral and thus fair decisions by algorithms simply do not exist - and probably never will. For as long as technology is programmed or designed by humans and based on man-made data sets, it will be subjectively coloured. We are well advised not to rely willingly only on the results of AI. The aspect of effective control therefore also plays an important role in this respect.

Fourth, the data protection principles of purpose limitation and data minimization naturally also apply to AI. Here in particular, it makes sense to use data protection-friendly technologies. Often, for example, the processing of completely anonymized data can be sufficient to achieve the intended purposes.

Fifth, in order to adequately accompany the development of AI, the Data Protection Authorities naturally also need sufficient human and material resources.

IV. European legal framework for AI

The European Commission presented the world's first draft legal framework for AI in April 2021. The draft law is intended to promote the development of AI, ensure a high level of protection for public interests and create a basis of trust for AI systems. The requirements are to apply alongside data protection regulations. Included are obligations for providers, distributors, importers and users of AI systems. The legal requirements shall apply to every placing on the market, commissioning and every type of use of AI systems in the EU.

The draft AI regulation is designed around a risk-based approach with regulatory requirements of varying degrees of stringency:

AI with unacceptable risks will be prohibited. For example, social scoring by public authorities or on their behalf, exploitation of children's vulnerability, or – with exceptions – also "real-time" biometric remote identification for law enforcement purposes. AI applications with inherent high risks have to comply with certain quality requirements. These include data quality, accuracy and robustness of the AI system, and obligations for documentation, traceability, transparency, and ensuring human oversight. Before being placed on the EU market, such AI systems must also undergo a conformity assessment to demonstrate that the AI system meets the requirements of the regulation.

High-risk AI systems are defined in an annex by way of example. AI systems to decide on the accessibility and use of basic private and public services and benefits are qualified as high-risk AI, for example.

Even low-risk AI systems must in principle be designed in such a way that natural persons are informed that they are interacting with an AI system so that there is transparency in this respect.

While the EU Data Protection Authorities in their opinion on the EU draft regulation have welcomed the risk based regulatory approach in general terms, they have also expressed their concerns about missing red lines such as for all forms of social scoring based on artificial intelligence e.g. also for private companies. They have also called for a general ban on any use of AI for automated recognition of human features in publicly accessible space and demand leading oversight competences in this newly regulated field of digitalization.

V. [Final remarks]

To sum it up: Data Protection Authorities are not at all against the technological evolution. We are pro digitization, we clearly see the potential of AI, especially if embedded in a value-oriented digitization. The data protection authorities, among others, are helping to shape a valuable digital future for everyone.

Thank you for your attention.