Position Paper

Bitkom views on the ICDPPC Declaration on Ethics and Data Protection in Artificial Intelligence

25/01/2019

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Introduction

Bitkom welcomes the International Conference of Data Protection and Privacy Commissioners' (ICDPPC) Declaration on Ethics and Data Protection in Artificial Intelligence and we support the establishment of the permanent working group for Ethics & AI. We also welcome the ever increasing work and dialogue regarding the topic. The digital revolution is probably not only the most exciting development from an economic and technological point of view, but also the fastest. The rapid progress of technology in the increasing digitalization of all kinds of processes is always closely linked to data and the will to constantly improve data analysis. In recent years, technological progress has enabled us to make enormous leaps in the field of automated decisions, machine learning and AI. But while for past industrial revolutions we often had the opportunity for several decades to test, change and improve our approach and systems and, if necessary, to impose conditions or prohibitions on their use, extensive "testing" of new technologies today happens "on the run" - and this changes the mechanisms of development, control and also the targeted promotion of developments that serve the prosperity of society. The developments therefore call for new kinds of interdisciplinary dialogues.

The diverse application possibilities and potentials should always be discussed in the overall context. Especially because AI has the potential to positively influence nearly all areas of our daily lives, a balance needs to be struck between enabling use while going with a responsible approach to developing

and using AI. The use of personal data or the automated evaluation of such data involves, among other things, a danger of discrimination, which is why the use of automated decisions also requires certain limits. We must always check, in a dynamic process, which applications are socially acceptable. Society and politics are not only faced with the challenge of preventing the misuse of developed technologies, but must also actively work to safeguard fundamental rights. Our current regulatory framework already addresses most of the issues but some areas of application need our constant evaluation and assessment. The preservation and strengthening of democratic values cannot be achieved by regulation alone. In addition, companies also need "self-regulation" and the development of ethical guidelines in companies. This can and should be accompanied by an open discourse. It is also of the utmost importance to always differentiate between legal obligations and ethically, socially desirable development and application of AI. Furthermore, when assessing whether additional ethical guidance is needed a differentiation needs to be made between guidelines for legislators and guidelines for businesses. We recommend to strengthen this aspect in this Declaration as well.

International cooperation and dialogue that may hopefully result in cross-regional recommendations are particularly welcome. The current policy discussions on AI around the world revolve around the same challenges and opportunities, and the nature of AI requires cross-border policy approaches in order to appropriately address AI's risks and enable its full benefits. The ICDPPC Guidelines can help provide further guidance and strengthen a common understanding on the subject. We therefore welcome that the Declaration is open to public consultation, which will hopefully contribute to a constructive public debate on data protection and artificial intelligence.

We also believe that when an "ethics by design" process is chosen, the development and use of AI systems would benefit greatly – not at least because in our view one of the necessary cornerstones of a successful AI framework is the trust of all citizens and users. When choosing such an approach ethics principles and values are taken into account when AI is developed and used and throughout

the process to ensure that the values and criteria are upheld. It also provides the necessary flexibility for such a dynamic field.

As we think that only an interdisciplinary dialogue will help us find answers regarding a responsible development and use of AI, we support the acknowledgement of the need for data protection and privacy authorities to work with other authorities (f.i. institutions addressing human rights). However, one of our concerns lies in the fact that that the DPAs are challenged even today with regard to their available resources and their specific tasks should remain closely related to Data Protection whilst seeking expertise on other issues in the respective institutions.

We would therefore like to comment on the Declaration of the ICDPPC as follows:

2. Preamble

2.1. Development and Application

The preamble of the Declaration addresses important aspects of AI, highlights the chances and the potential of the technology and raises important challenges with regard to the technology. We welcome that the Declaration refers explicitly to the great potential of AI. However, the aspects listed in the preamble only refer to the development of AI, not the application. In our view, both should be included in this section, especially because in dynamic and evolving processes such as AI the development process is basically never completed. It is also important to keep in mind that development and application of AI-technologies may need different approaches depending on the sector they are built for. Where there is need for human re-evaluation and decision making, the process should always include the human element in the loop. And where humans rely on decisions suggested by AI whey should be trained appropriately.

2.2. A Risk to Data Protection and Privacy?

The preamble states that the respect of the rights to privacy and data protection are increasingly challenged by the development of AI. In our view such a

statement is too undifferentiated and should be amended. We do acknowledge that the use of large data sets can seem like a conflict of objectives but we do not see a risk for privacy and data protection in the use of data for AI in general.

As anonymous data does not pose a privacy risk to the users, strides and innovations should be encouraged in this regard. Reliable guidance from the data protection authorities would help companies develop tools to anonymize data and therefore mitigate the possible challenges AI poses with regard to privacy and data protection. There is, however, a debate about how to anonymize properly as data can, in some cases, be combined afterwards and allow re-identification of the data subjects. We recommend that a legal "barrier" is assessed in this regard – to prohibit the re-identification after anonymization took place. The Working Party29 already recommended a subsequent obligation of care for the party that anonymized the data. Besides anonymization, pseudonymization can be a useful step to enhance protection. In the GDPR context, pseudonymization is considered one of the tools to mitigate risks and enhance data protection. Such tools need to be strengthened and their development encouraged. As the GDPR already provides a comprehensive rule in this regard set we believe that no further rules are needed but rather guidance and assistance in implementing them would improve protection and legal certainty. As such, it is not an ethical but rather a legal question and should be addressed accordingly.

2.3. Strengthening different players in the AI environment

The preamble refers to potential risks induced by the current trend of market concentration in the field of artificial intelligence. Scalability and cross-border cooperation are regularly critical factors determining the success of digital business models and the associated investment and innovation incentives, especially in AI related developments. In our view, competition law should facilitate these factors by creating more generous criteria for cooperation between companies, as these are indispensable, especially for core technologies, standardisation efforts and business alliances. Facilitating cooperation at f.i. the EU level would also lead to increased legal certainty. This would also counteract

the existing scepticism as well as the widespread silo thinking of the industrial sector, which blocks cooperation and the associated advantages.

2.4. Discrimination and Bias

In the preamble, the ICDPPC also points out that some data sets used to train machine learning-based and artificial intelligence systems have been found to contain inherent bias resulting in decisions which can unfairly discriminate against certain individuals or groups, potentially restricting the availability of certain services or content, and thus interfering with individuals' rights such as freedom of expression and information or resulting in the exclusion of people from certain aspects of personal, social, professional life.

While we agree that bias can occur in AI based systems we would argue for more differentiation in this regard.

2.5. Liability issues should be addressed separately

As recommended in the Preamble, we think it is necessary to clearly distinguish between binding, legal obligations and ethical guidelines. Liability issues are in their core a legal issue (which needs to be addressed and the current legal framework assessed in this regard), not an ethical one. Furthermore, questions about liability touch upon civil law rather than data protection law and should therefore be discussed in a wider context with regulators, rather than within groups of data protection professionals.

2.6. International Approach

We welcome that the ICDPPC Declaration argues for the need for the adoption of an international approach and standards. For such an alliance and approach a dialogue with especially the High Level Expert Group on AI and other competent groups should be initiated to avoid fragmented solutions.

3. Guiding Principles

3.1. Collective Impact on Groups

Section 1 (b) argues that Artificial intelligence and machine learning technologies should be designed, developed and used in respect of fundamental human rights and in accordance with the fairness principle, in particular by taking into consideration not only the impact that the use of artificial intelligence may have on the individual, but also the collective impact on groups and on society at large.

In our view, ensuring that individuals are not negatively affected is a necessary and desirable aim and must always be kept in mind when developing and applying AI; impact on groups and society, however, will be ambiguous and difficult to assess. We also would like to raise the question whether Data Protection Authorities should ascribe such a task to themselves. Furthermore, the demands and requirements placed on the design of the procedures would then be higher that data protection does actually require. We hence suggest amending that section.

3.2. Collective Impact on Groups

In Principle 2 (d), the ICDPPC argues that the continued attention and vigilance, as well as accountability, for the potential effects and consequences of, artificial intelligence systems should be ensured, in particular by establishing demonstrable governance processes for all relevant actors, such as relying on trusted third parties or the setting up of independent ethics committees. With regard to such committees we would like to raise the question by whom such groups would be nominated and which countries would be part of these groups.

3.3. Research in explainable AI

In principle 3 (a) the ICDPPC argues that AI system transparency and intelligibility should be improved, with the objective of effective implementation, in particular

by investing in public and private scientific research on explainable AI. Bitkom supports this objective as certain techniques are opaque and not comprehensible.

In our view, procedures that are transparent by design should be promoted and encouraged more. Innovations in the field of explainable AI should therefore also be supported, the respective research funded. It is our conviction that trust in the technology is important and therefore transparency and explainable models are needed.

We would also, however, like to point out that a full disclosure of the software code, the algorithms used would neither help with regard to transparency of the processing nor uphold our standards for trade secrets and their protection. Furthermore, as the applications and the code regularly evolve and change, a disclosure of such would not benefit either party. We suggest a risk based approach in this regard and that the assessment how much transparency is needed is done on a case by case basis while taking the context of the application into account.

3.4. Bias and Discrimination

The ICDPPC refer to the issue of bias in principle 6. It states that unlawful biases or discriminations that may result from the use of data in artificial intelligence should be reduced and mitigated, including by:

- ensuring the respect of international legal instruments on human rights and non-discrimination,
- investing in research into technical ways to identify, address and mitigate biases,
- taking reasonable steps to ensure the personal data and information used in automated decision making is accurate, up-to-date and as complete as possible, and
- elaborating specific guidance and principles in addressing biases and discrimination, and promoting individuals' and stakeholders' awareness.

We welcome that this issue is raised. The basis for AI-supported decisions is data that contributes to the decision-making process. Just like a human decision, algorithms based on incomplete or erroneous data make an erroneous decision. Similar to human decision making, due to the complexity of the system, a relationship of trust with the data supplier remains the strongest guarantee for the correctness of the information supplied.

When addressing fairness and machine bias it is, however, important to keep in mind that not all AI applications need personal data to work with. Applying principles that were developed for personal data might therefore be inconsistent. Also, data quality and origin cannot always be traced back to the source. It is possible that only aggregated or non-personal data will be added for a profiling or clustering of users. The exact detail data are therefore not available or may not be passed on. Bitkom recommends that developers and user of AI should specify the data to be used, the data categories and the criteria according to which data can be introduced into self-learning systems, checked for sources of error and documented as comprehensibly as possible.

Before using an AI system, all involved parties should carefully check the use of data and the criteria according to which data can be introduced into self-learning systems, checked for sources of error and documented as comprehensibly as possible.