POSITION PAPER

eco position paper on the Handling of Artificial Intelligence

Berlin, 26.09.2023

Artificial intelligence – AI is fundamentally changing our society, economy and science. In recent years, AI systems have been significantly developed in many areas, enabling their use in more and more application scenarios in everyday life and business. It can be assumed that this trend will intensify even further. Today, it is already clear that great opportunities arise from the integration of artificial intelligence into many areas of life and work. For example, for companies, the use of AI can enhance value creation and relieve employees of monotonous and simple tasks. What's more, in the field of science, AI systems can also effectively support the knowledge acquisition and help to achieve faster and more precise results, thus contributing to combatting diseases or climate change, for example.

Given the enormous potential of AI systems, it is also important to be aware of the risks and possible undesirable side effects and to address these prudently. In order to increase or maintain society's trust and acceptance of AI systems, this is absolutely essential. It is important not to lose sight of the balance between legitimate concerns, such as an increase in state surveillance and the benefits of the technology: for example, for health research. It is therefore important that the deployment and development of this technology must adhere to rules that are defined in a democratic process, whether in the form of either regulatory or voluntary commitments. At the same time, the rules must not lead to Europe falling behind in international competition.

In a global comparison, Europe is already lagging behind other world regions in terms of the deployment and development of AI systems. [Globally](), 73% of the major AI models come from the United States, with an additional 15% coming from China. The EU does not have the share in the field of AI that corresponds to its global economic importance. This situation jeopardises the competitiveness of the European economy and also poses the risk that European standards and values will not play a role in the development of a key technology of the future.

To accompany the various discussions and put them in the context of current technological developments, eco – Association of the Internet Industry has formulated the following guidelines.

1. In favour of risk-based regulation with a sense of proportion

Various approaches to the regulation of AI systems are currently being discussed worldwide. With the AI Act, the EU has opted for a risk-based approach. According to this approach, systems used in areas posing only a low risk to society will have few requirements. In contrast, AI systems that fall into a high-risk category will be subject to significantly higher conditions and more obligations. eco supports the risk-based approach in principle. Artificial intelligence is a technology with a wide range of applications, some of which are not yet foreseeable, which means that clear assessments of the opportunities and risks in certain application areas are not always possible. It therefore makes no sense to regulate or ban artificial intelligence as a whole, but only in cases where it is necessary to counter legitimate dangers. Moreover, it is important to bear in mind that ex ante regulation of use cases is not commensurate with the complexity of artificial intelligence and its areas of application, and this could also weaken Europe's innovation capacity. New systems and innovations need room to grow and should therefore not be banned from the outset or be exposed to too much bureaucracy. In addition, the regulatory approach should be flexible enough to be able to react to future developments if necessary. Last but not least, duplicate regulations and overlaps with existing regulations, such as the DSA, should be avoided in order to prevent legal uncertainties and to avoid excessive bureaucracy.

Europe is closely integrated into the global market and the digital industry has been international since its inception. The development of AI applications has, however, been based on data and foundation models that were often not collected or developed in Europe. In addition, European companies also rely on the global market to grow and remain competitive. Accordingly, AI regulation in Europe must be internationally compatible, especially with regard to the definition of AI. It should not impose significantly more complicated and complex rules on European companies than those applicable to their competitors in other parts of the world. Moreover, it is also important within the European Union to also ensure the functionality of the EU single market for AI products. A fragmentation of the single market through a multitude of individual national rules must be avoided, especially in order to provide startups with simple and unbureaucratic access to the entire European market.

2. Codes of conduct must be supported

In addition to government regulation for artificial intelligence, relevant stakeholders should be encouraged and supported in developing their own codes of conduct. Many companies are already taking the lead in this regard, which is why it is possible to draw on existing examples of voluntary commitments that have already proven their worth in practice. These codes of conduct are often tailored to the specific business models and use cases, enabling a faster response to new technological developments and associated issues than the state regulation can offer. In both the United States and the EU, there are already approaches for such
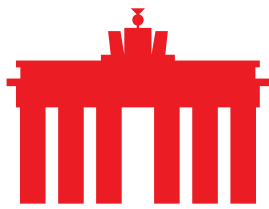
voluntary commitments between companies and governments. These approaches should also be coordinated as closely as possible internationally – for example, within the framework of the TTC (EU-US Trade and Technology Council) or the OECD, so that they can have an impact beyond Europe and create a common value space for AI. The codes of conduct must also be developed in multi-stakeholder formats with the participation of associations and standardisation bodies, in order to ensure that they are as practical as possible and that all relevant stakeholders are involved.

3. Acceptance of artificial intelligence must be promoted

Trust in any form of technology is an important foundation for its acceptance by society. Only through a high level of trust can widespread application in business and society be achieved, and the potential of artificial intelligence can be fully harnessed. To establish this trust, transparency is also needed regarding how artificial intelligence works. To create this transparency, manufacturers should specify what a system can do and what it was designed for. In addition, we at eco believe that a dialogue on the labelling of AI or its outputs would be useful. Here, issues concerning press freedom and artistic freedom should also be considered. In addition, new questions also arise in the area of product liability as a result of the proliferation of AI systems. These should be addressed in order to create legal certainty and trust in AI systems. The solutions to these issues should be based on the established principles of product liability and must not impose stricter or more far-reaching requirements on the developers of AI systems.

In order to enable acceptance, it is also necessary to address the legitimate concerns associated with AI systems. In principle, a technology is neither bad nor good, but the use of artificial intelligence opens up new possibilities that can also be misused by various actors or have unintended side effects. AI systems, especially when used in sensitive areas, should be inherently monitorable and correctable in order to prevent people from being harmed by errors in algorithmic modelling, training and programming. Artificial intelligence, for example, significantly expands the possibilities for the surveillance of people. This is particularly problematic when the state utilises these options, such as in the area of law enforcement or communication monitoring. Particularly in connection with state social scoring or so-called dark patterns, there are examples of use cases in which artificial intelligence has the potential to pose a threat to fundamental democratic rights or digital self-determination, or to intensify existing risks. Therefore, we support calls for a ban on surveillance or social scoring by the government.

4. Recognising the societal value of data

The availability of data is an important prerequisite for the training of foundation models. Depending on the area of application, models require both data from people and generated data: for example, in the IoT context. Since the application fields of artificial intelligence are extremely broad – e.g., medicine, traffic, logistics –

the challenge here is to create rules that are as universally valid as possible and that can be applied by all parties involved (research and science, business, administration and citizens) and that ensure high quality and a high level of trust in digital services. The challenge of a responsible data policy is therefore, on the one hand, to meet the high requirements of data protection as prescribed by the General Data Protection Regulation (GDPR) and, on the other hand, to provide as comprehensive and high-quality a database as possible that can be used for training and operating artificial intelligence.

The GDPR, with its standards and principles, provides a good basis in this context. The societal value of data must not be overlooked in this debate. Information that, for example, enables artificial intelligence to better detect tumors in X-ray images may well touch on personal data on a pseudonymised level; but ultimately, it can also contribute to better healthcare for all when used as training material for the corresponding algorithms.

A broad base of training data is also important to prevent bias or false conditioning of the systems towards certain characteristics. If more data is available from different contexts and regions, the bias or false conditioning can be better avoided.

This requires a dismantling of barriers to the international exchange of data. In Europe, as much data as possible must also be available for training AI systems. In addition, there is a need for legally compliant procedures for anonymising and pseudonymising personal data, so that this data can also be used for training AI systems in compliance with the GDPR.

5. Adapting copyright to the digital age

With the emergence of generative AI systems, copyright issues in connection with the training of AI systems are increasingly being raised. Discussions revolve around how owners of copyrighted material can enforce their rights or how they can object to the use of their works for training AI models. In addition, there are also various ideas about how to structure the use of copyrighted material in a fair mannerIt is important to emphasise that the data is only used for training purposes, and that no further copyright-relevant exploitation or use is intended. Nevertheless, a discussion about a fair design of the use is important. eco supports the interpretation of the EU Commission with regard to Article 4 of the EUCD, which gives rights holders such as publishers the option to opt out of text and data mining. This approach remains correct and appropriate; however, there should also be discussions on ways to make it easier for copyright holders to assert their refusal of usage. In this regard, this requires standards that are as international as possible, or that are at least harmonised throughout Europe.

Ultimately, in our view, only a fair balancing of the interests of all stakeholders can help to ensure that as much data as possible can be used for training and that all stakeholders involved can benefit from generative AI systems. From our

perspective, this does not require full disclosure obligations for developers of AI foundation models, which would be difficult to implement in practice, and which could also undermine the protection of trade secrets.

6. Enabling a sovereign approach to AI

For us, it is important that citizens are empowered to handle AI systems with sovereignty. This requires education on the fundamentals of AI and training for practical use in the workplace and in the private sphere. Some systems will require human supervision, while others will deliver results or recommendations that need to be interpreted and classified by humans. Therefore, competencies in the field of AI need to be promoted, be it in schools or government institutions, awareness campaigns or through further training in companies.

In this context, a certain degree of knowledge about the capabilities of artificial intelligence can also help to reduce uncertainty regarding potential dangers. Knowledge of the capabilities of generative AI, for example, can help to detect deepfakes or to react more critically to images or videos that do not align with personal experiences. Education and information, as well as the teaching of skills, can thus make an important contribution to protecting against disinformation. This can thus help to adequately address possible dangers for the likes of democracy.

It is already clear that the use of AI systems will also change the labour market. Existing professions and occupational fields will change, and new ones will emerge. In order to prepare employees for these changes, they must be able to acquire the necessary skills so that they are supported in the transformation of the working world. This should also be taken into account when designing training programmes. Overall, the use of AI systems in many fields of work will be able to relieve people of simple and monotonous tasks. It is therefore just as important to see AI as an opportunity to reduce the workload of employees, and not as a threat. Nevertheless, a broad societal debate should be held on how to shape the transformation of the working world. This is required in order to meet the upcoming changes for the use of artificial intelligence in an active and societally acceptable manner, and to prepare employees for future job profiles and requirement.

7. Enabling innovation in Europe

Europe needs to catch up in the development and application of AI in order to maintain its future viability and to ensure that European values and standards remain relevant in setting international standards. In doing so, however, a number of prerequisites to enable more innovation in the field of AI are lacking within the EU.

Firstly, AI research needs to be more strongly supported within the EU. This applies both to research conducted by public institutions and by private companies.

Secondly, access to large computing capacities, which are particularly relevant for the development of foundation models, is often lacking. Currently, only a handful of companies and research institutions – most of which are not located in Europe – can provide these capacities. It is therefore essential to create similar capacities in Europe and to enable business and science to have uncomplicated and unbureaucratic access to these. Especially for small companies and start-ups, protected test rooms can be helpful to test their systems for compliance with various regulations and to fix potential problems. eco endorses the use of test rooms and areas for AI, such as those laid out in the AI Act. SMEs should have easy access to these test rooms if they wish to do so.

8. Paying attention to artificial intelligence in legislation

The possibilities of artificial intelligence must be taken into account in future legislation and in the evaluation of the existing legal situation in many areas. In view of the fact that artificial intelligence can not only process sensitive data but potentially generate data itself through links, the aspect of security is one of the factors of central importance. On the one hand, securing the systems and applications themselves (integrity) is crucial; on the other hand, artificial intelligence can contribute to the automated detection and prevention of threats and attacks. What can improve security for all is network security and the closing of security vulnerabilities and errors in computer programmes that enable attacks, given that responses to attacks on information technology systems can occur more quickly and on an automated basis. In addition, AI raises new issues in the area of privacy and data security. AI systems are capable of aggregating and analysing large amounts of data and creating precise profiles.

In addition, biometric surveillance systems also make it easier to establish movement patterns. Legislators must be aware of these facts when evaluating relevant laws as well as future legislative projects, and should discuss the implications for legislation in a broad-based dialogue.

Summary

Currently, there is a controversial debate about artificial intelligence, its capabilities, its use and its implications for society, the economy and science. In this debate, eco – Association of the Internet Industry advocates for a pragmatic approach to artificial intelligence. In our view, it is important to be able to harness the positive potential of this technology, while at the same time not ignoring potential problems. Specifically, we advocate the following principles for dealing with AI in Europe:

- In favour of risk-based regulation with a sense of proportion

Artificial intelligence should be regulated with moderation in order to avoid jeopardising Europe's competitiveness and to make the benefits of AI systems

accessible to European companies and citizens. AI systems should only be specifically regulated in those application fields that are clearly defined high-risk areas. In addition, ex ante regulation should be avoided in order not to block innovations from the outset and to give European companies room for new developments. Moreover, the European single market must not be jeopardised by measures at the Member State level. Liability rules for AI systems should be based on already established principles of product liability, while overlaps with other regulations, such as the DSA, should be avoided when regulating AI.

- Support for codes of conduct

Codes of conduct, which can be a flexible and unbureaucratic alternative to state regulation in some areas, are also suitable for preventing possible undesirable developments. These codes should therefore be developed in multi-stakeholder formats and supported and recognised by the EU.

- Enabling a sovereign approach to AI

In order to counter the concerns in some sections of society regarding AI systems and to ensure acceptance of the technology, the Internet industry believes that the first thing that is needed is increased communication of knowledge about artificial intelligence. Addressing concerns about job displacement should be countered with a societal debate on how changes in the working world should be shaped, in addition to responses to further training. Ultimately, problematic practices such as AI systems for state surveillance should be banned in order to counter undesirable developments.

- Better availability of data

Availability of high-quality data is an important prerequisite for the training of AI base models and the overall development of AI systems. It is therefore important that barriers to the transfer of data to or from Europe are as low as possible. In addition, there is a need for legal certainty in the handling of personal and non-personal data. Especially in connection with the use of personal data, there is therefore a need for legally secure options for pseudonymisation and anonymisation.

- Stronger promotion of innovations

A large proportion of AI innovations do not come from Europe, despite AI being one of the central technologies of the future. In order to catch up with other regions of the world, we need not only a regulation that is as unbureaucratic as possible, but also increased support and focus on AI research, both by public and private actors.

In addition, European SMEs and start-ups also need access to the computing capacities required for the development of foundation models. Corresponding initiatives to create such capacities should be supported and encouraged by the Member States and the EU.

- Copyright must be digitalised

The copyright law has not yet been sufficiently adapted to the digital age. This becomes clear in the context of generative AI systems. eco supports the option for rights holders to object to the use of their works for training AI, as provided in the EUCD. At the same time, there needs to be a debate about a fair balance of interests for all stakeholders. This must also be based on the digital realities of the 21st century and how AI systems work. By contrast, we do not consider a full disclosure obligation for developers of AI models to be practicable and appropriate, also with regard to trade secrets.

- Adapt legislation to new technical possibilities

When it comes to the areas of cybersecurity and IT security, alongside citizens' rights – such as the right to privacy – new issues are continuing to emerge from the increased use of AI systems, both today and in the future. From the perspective of the Internet industry, existing laws and infrastructures in these areas must be adapted and strengthened to accommodate these developments. At eco, we are of the opinion that the use of artificial intelligence can also contribute to strengthening cybersecurity and IT security and that the new technical possibilities can also offer many opportunities in other areas. In eco's view, legislators must take the emergence of AI systems into account in their future legislative projects and also seek a dialogue about necessary adjustments to the existing legal framework in the relevant areas.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.