Statement

Statement on Section 5 "An ecosystem of trust" within the White Paper on AI of the European Commission

Federation of German Industries

Version: 19.06.2020

Table of contents

Management Summary

- The BDI welcomes the efforts of the European Commission (Commission) to create an ecosystem for excellence and trust. A selective adaptation of the existing legal framework for AI can increase legal certainty for companies.

- Up to now known high-risk AI applications can already be effectively regulated through existing national or European law. Additional legislation going beyond a selective adaptation of the existing legal framework may only be considered if there is a proven need. Should the Commission decide to introduce a new legislation specifically on AI, it should be based on a horizontal approach, which should be specified sector-specifically or transferred to already existing sector-specific legislation.

- In the view of the BDI, the currently existing national and European legal provisions on safety and liability issues are largely fit for purpose and provide generally an adequate legal framework that also covers AI as a source of risk in principle. A cautious adjustment is conceivable, but a fundamental readjustment of the liability framework is not necessary.

- In the event of any AI-specific legislation, a differentiated and risk-based approach is the right way forward. However, too much emphasis is put on the sectoral nature of an AI application. Sector affiliation will indeed play a role in assessing the risk, nevertheless it does not seem to be very useful to define it as one of two main criteria. More important than the sector is the specific field of application in which the AI application is used.

- When defining requirements for AI systems, a distinction should be made between B2C and B2B applications. The requirements in the B2C area are different from those in the B2B area, since consumer rights must be specially protected by law (for example, via product liability). In the B2B area, companies can negotiate legal aspects among themselves in contracts.

- As described in the White Paper on AI, conformity assessments for AI should primarily be part of the existing conformity assessment mechanisms. Conformity assessments should be designed in a user-friendly way and should take the form of a self-assessment with clearly defined standards.

Federation of German Industries
Member Association of
BUSINESSEUROPE

Address
Breite Straße 29
10178 Berlin

Contact person
Clemens Otte
T: +49-30-2028-1614
E-Mail: c.otte@bdi.eu

Internet
www.bdi.eu

Detailed statement on section 5 of the Commission's White Paper on AI

The Commission should critically examine whether lack of trust is really a main factor holding back a broader uptake of AI

The White Paper on AI, on page 9, identifies lack of trust as a "main factor holding back a broader uptake of AI." At the European level, it is often argued that a trustworthy AI can promote social acceptance of the technology and help the European economy to differentiate itself in the international competition for AI. Generally, the BDI also sees this as a valid strategy. However, the Commission should at least critically examine whether lack of trust is really a main factor holding back a broader uptake on AI. Analogous to the so-called privacy paradox, a discrepancy between concerns about the trustworthiness of an application and the actual user behaviour is also apparent in the case of AI. Thus, even a minimal additional benefit or cost saving could be sufficient to induce consumers to use less trustworthy AI applications. In this respect, it is questionable whether supposedly more trustworthy applications from Europe can compete better on the international market.

The Commission should use concrete positive examples to show how high-risk AI applications can already be addressed by the existing legislative framework

The public debate often focuses on AI applications that are not wanted by European society or the European economy, such as applications that can detect the sexual orientation of people or applications used in other regions of the world for systematic surveillance of citizens. Such examples stir up fears in society and increase mistrust in AI. However, not everyone knows that such applications are generally not compatible with the existing European legal framework. Therefore, broader knowledge of the existing applications and legal limits of AI is necessary to counteract fears and objections of society. The Commission should use concrete examples to show that particularly critical AI applications can already be adequately addressed by the existing legal framework. Furthermore, this could also reveal concrete gaps in law enforcement that need to be closed as part of the Commission's regulatory efforts.

A Problem definition

Enabling individualisation

Possible new requirements for non-discrimination must take account of the fact that non-discriminatory individualisation of offers also has a strong positive impact and must remain possible.

B Possible adjustments to existing EU legislative framework relating to AI

There are currently no fundamental legislative gaps

The paper rightly points out that many challenges related to the use of AI can be addressed by the existing regulatory framework. As described in the introduction to section five, the EU Commission should therefore, before introducing new legislation, "examine whether current legislation is able to address the risks of AI and can be effectively enforced ". In the view of the BDI, there are currently no fundamental regulatory gaps that cannot be closed by a selective adjustment of the existing regulatory framework.

The Commission should choose a combination of a horizontal approach and sectoral specification when introducing new legislation

If the Commission considers it necessary to introduce new legislation, a horizontal approach with general requirements should be taken, which should be specified sector-specifically or transferred to already existing sector-specific legislation. In this way, the Commission could, on the one hand, achieve a minimum degree of cross-sectoral coherence and, at the same time, take into account that AI is a basic technology that poses different challenges depending on the context of application, the AI technology used and the overall socio-economic system.

A fundamental readjustment of the liability framework is not necessary

From the point of view of the BDI, the extensive body of existing national and European legal provisions on safety and liability issues is largely appropriate, sufficient and balanced and provides an adequate legal framework that generally also covers AI applications as a source of risk. A cautious adjustment could possibly be considered, this however does not justify a fundamental readjustment of the liability framework. Due to the special characteristics of AI applications, further investigations should be carried out for the time being. In particular, the existing regulations should be examined in detail in order to finally identify actual liability gaps and problems of proof.

Only thereafter and if necessary, legal adjustments could be made accordingly, taking into account the specific risk factors. The decision to introduce new regulations must not be an end in itself, but must ensure both effective protection against AI and sufficient scope for technological innovation. It is important to balance innovation and consumer protection appropriately.

The possibilities of the existing product liability directive (85/374/EEC) should be reviewed in combination with the safety legislation in order to provide clarity on the core concept of "product". For example, in line with the view of the Commission, it should be made clear to what extent independent software applications or digital services are also covered by product safety legislation.

In any case, the Commission should take into account differences between B2C and B2B applications when adapting existing legislation. In the B2C area, the requirements are higher than in the B2B area. Consumer rights are to be protected under the Product Liability Directive, while companies can effectively regulate liability and other legal aspects through contracts, especially in the "high-risk" sectors. In addition, special rules in the B2C sector could be useful, as there might be situations in the future where AI applications learn from the consumer's input and responsibility may shift to the consumer accordingly.

As a matter of principle, it must be guaranteed that all parties involved along the production chain should be obliged according to their individual casual contribution. Ultimately, the aim is to fill unacceptable liability gaps in such a way that no party is unfairly burdened.

C Scope of a future EU regulatory framework

Additional requirements should apply to all technologies concerned

Many of the issues and challenges raised in the White Paper on AI are not specific to AI, such as changing functionality of systems or uncertainties in the allocation of responsibilities. In the light of the above, generally there should not be laid down different requirements for AI than for those "traditional" algorithmic or numerical systems that are also affected by the challenges. AI functionalities can rarely be clearly distinguished from non-AI-based functionalities. Furthermore, there will be a multitude of hybrid systems. New requirements must always keep up with the state of the art, be updated and then be applied to all systems.

Sectoral affiliation is unsuitable as a main criterion

A differentiated and risk-based approach is the right way forward for any regulation. However, too much weight is attached to the sector of an AI application. Sector affiliation will indeed play a role in risk assessment. However, it does not seem to be suitable to define it as one of two main criteria. A sectoral differentiation would only make sense if the vast majority of AI applications used in a given sector pose a significant risk or if the vast majority of AI applications from a given sector are completely risk-free. The BDI doubts that such a clear distinction is possible. More important than the sector affiliation is the concrete field of application of the AI system. In addition, the criterion of sector affiliation is softened by the considered exceptions and therefore appears to be inconsistent. If sector affiliation is nevertheless chosen as one of the main criteria, it must be clearly visible according to which criteria the sectors are chosen.

A more precise definition of 'significant risk' is necessary

Clear criteria must be determined to exactly define what is meant by a "significant risk". The paper is still very vague in this respect and leaves too much room for interpretation. Risk matrices which are also used in the area of product safety can serve as a guide. Here the probability of occurrence is multiplied by the possible extent of damage and threshold values for classification are defined.

Level of decision autonomy and level of learning autonomy should be included as criteria in the risk assessment

The level of decision autonomy and the level of learning autonomy should be taken into account both in assessing the risk and in defining appropriate requirements for AI applications. The level of *decision autonomy* depends on whether an AI application is merely a source of information, provides a support function for human decision making, or can decide completely autonomously without human involvement. The level of *learning autonomy* depends on whether a re-training of an AI system is a) completely possible b) only for limited, non-safety relevant parameters or c) not possible at all. According to this classification, limits of action could be defined for the respective AI systems. For example, safety-relevant parameters should be defined, which may not be re-trained in the field without a new conformity assessment.

It must be clearly defined who asseses whether an application poses a high risk

The paper does not clarify who assesses whether an application poses a "high risk" and how this assessment should be made in a legally secure manner. The assessment could lead to a considerable amount of bureaucracy for companies and government or notified bodies. Practical mechanisms need to be developed which, on the one hand, ensure rapid market introduction and, on the other, provide sufficient legal certainty for companies. In addition, the assessment must be carried out uniformly throughout Europe and coordinated across all EU countries.

D Types of requirements

Practical challenges in the data and record-keeping must be considered

The requirement (b) "keeping of records and data" may be appropriate in certain cases. However, it poses practical challenges for companies that need to be considered. Cataloguing and managing data and data models requires a considerable administrative and financial effort. Excessive requirements for the data and record-keeping could result in certain AI applications no longer being economically viable. The reference on page 23 that the data sets themselves should only be kept in "certain justified cases" is to be welcomed. It is important that the Commission adheres to this restriction. After all, it is the AI model that is decisive for the evaluation of an AI system. The model cannot be reconstructed from the data sets alone, as the chosen parameterisation is an important factor. Furthermore, the long-term storage of data sets must remain compatible with the requirements of the GDPR, in particular the "right to erasure". Particular attention must be paid to IoT systems or edge devices that learn during operation and have limited storage capacity. For capacity reasons, comprehensive data storage is difficult or technically impossible. If necessary, periodic spot-checks can be considered to verify compliance with the requirements. In this way, the amount of data stored could be kept to a minimum.

E Addressees

The "cheapest cost avoiders" principle proposed by the Commission may lead to legal uncertainties

BDI takes a critical view of the Commission's proposal that any obligations should be distributed to those players who are best placed to address potential risks. Those companies that are actually most responsible for causing a risk must not be allowed to shirk their producer responsibility and should be included in the obligations to minimise the risk ("polluter pays principle" vs. "cheapest cost avoider"). Moreover, it can be highly open to interpretation and explanation as to which actor is actually best able to address the potential risks. This could lead to great legal uncertainty and a high level of bureaucracy for the bodies involved. The detailed case-by-case consideration required in cases of doubt would collide with the character of a generally valid regulation.

F Compliance and enforcement

The conformity assessments should primarily be carried out by the companies themselves and should be designed in a user-friendly manner

The current market entry regulations are already very far-reaching and time-consuming. The introduction of additional, AI-specific mechanisms for conformity assessment must be very well justified and designed in a user-friendly way. First and foremost, conformity assessment by the manufacturer - analogous to the CE mark - should take the form of self-assessment with clearly defined standards and effective market surveillance. If companies have to put too much effort in a conformity assessment, they could tend to abandon AI applications in case of doubt and use "traditional" systems instead. This would lead to less uptake of AI in "high risk" applications. Moreover, the additional work involved in conformity assessment could have a negative impact especially for small and medium-sized enterprises. The fixed regulatory costs are disproportionate to their small size in comparison to larger companies.

It must be clearly defined when a new conformity assessment is necessary

The White Paper on AI points out that the functionality of AI systems can change over time. This raises the question of the cycles in which a conformity assessment should be carried out. Conformity assessment at each update would not be practical and would significantly limit the uptake of AI. According to current regulation, a renewed conformity assessment is only necessary if fundamental safety-relevant parameters of the product change. A comparable scheme can also be applied with regard to self-learning systems or software updates. At this point, a clear definition of the risk-relevant parameters is required, whose change makes a renewed conformity assessment necessary.

Strengthening audit and assessment capacity

In order to be able to introduce and carry out proper and independent audits, the existing authorities, institutions and agencies must be given the necessary human, technical and financial resources. The assessment of many AI applications will require the cooperation of different bodies, e.g. in cancer detection, where image evaluation algorithms, mathematical models, laboratory tests and data from the operating theatre will merge. In addition, test scenarios, methods and standards must be developed to ensure the security of the

algorithms and self-learning systems used throughout the product life cycle. This also includes developing methods and standards that counteract the use of "biased data". Test scenarios should focus on compliance with prescribed processes and methods, such as ISO 26262 (Functional Safety).

G Voluntary labelling for no-high risk applications

The added value of voluntary labelling is not apparent

We are critical of voluntary labelling in addition to proven markings such as the CE mark. This could rather confuse the user. Moreover, if an AI application is not regarded as high risk, voluntary labelling does not create any additional added value, but only additional work for companies. It is also questionable whether "horizontal" certification can meet the needs of the large number of different AI applications. More important than voluntary labelling are clear and transparent set of rules based on international standards.

About BDI

The Federation of German Industries (BDI) communicates German industries' interests to the political authorities concerned. She offers strong support for companies in global competition. The BDI has access to a wide-spread network both within Germany and Europe, to all the important markets and to international organizations. The BDI accompanies the capturing of international markets politically. Also, she offers information and politico-economic guidance on all issues relevant to industries. The BDI is the leading organization of German industries and related service providers. She represents 36 inter-trade organizations and more than 100.000 companies with their approximately 8 million employees. Membership is optional. 15 federal representations are advocating industries' interests on a regional level.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Contact persons

Clemens Otte
Deputy Head of Department
Digitalisation and Innovation
T: +49 30 2028-1614
c.otte@bdi.eu

Kathrin Hintner
Senior Manager
Law, Competition and Consumer Policy
T: +32 2 792 1008
k.hintner@bdi.eu

BDI Dokumentennummer: D 1203