DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Committee on European Affairs

on the Public Consultation of the European Commission on the White Paper On Artificial Intelligence – A European approach to excellence and trust (COM(2020) 65 final)

Position Paper No.: 40/2020 Berlin/Brussels, June 2020

Members of the Committee on European Affairs

- Rechtsanwältin Dr. Claudia Seibel, Frankfurt am Main (Chair)
- Rechtsanwältin Béatrice Deshayes, Paris (Rapporteur)
- Rechtsanwalt Prof. Dr. Christian Duve, Frankfurt am Main (Rapporteur)
- Rechtsanwalt Prof. Dr. Thomas Gasteyer, LL.M., Frankfurt am Main
- Rechtsanwalt Prof. Dr. Hans-Jürgen Hellwig, Frankfurt am Main
- Rechtsanwalt Dr. Ulrich Karpenstein, Berlin
- Rechtsanwältin Gül Pinar, Hamburg
- Rechtsanwalt Prof. Dr. Dirk Uwer, Düsseldorf
- Rechtsanwalt Michael Jürgen Werner, Brussels

Responsible DAV-Director and contact in Brussels:

- Rechtsanwältin Eva Schriever, LL.M.

Members of the Committee on Civil Law

- Rechtsanwalt Dr. Christian Bereska, Celle (Chair and Rapporteur)
- Rechtsanwalt Dr. Rupert Bellinghausen, Frankfurt (Rapporteur)

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparency Register ID number:
87980341522-66

www.anwaltverein.de

- Rechtsanwalt Dr. Markus Beaumart, Köln
- Rechtsanwalt Dr. Tobias Heinrich Boecken, Berlin
- Rechtsanwältin Petra Heinicke, München
- Rechtsanwältin Dr. Sylvia Kaufhold, Maître en droit, Dresden
- Rechtsanwalt Dr. Dr. h.c. Georg Maier-Reimer, LL.M., Köln
- Rechtsanwalt (BGH) Dr. Michael Schultz, Karlsruhe

Responsible DAV-Director:

- Rechtsanwältin Christine Martin

Mailing List

Europe

European Commission

- Directorate-General for Justice and Consumers
- Directorate-General for Communications Networks, Content and Technologies

European Parliament

- Committee on Civil Liberties, Justice and Home Affairs
- Committee on Legal Affairs
- Committee on Internal Market and Consumer Protection

Council of the European Union

Permanent Representation of the Federal Republic of Germany to the EU

Legal Advisers of the Permanent Representations of the German Bundesländer to the EU

Council of Bars and Law Societies of Europe (CCBE)

Vertreter der Freien Berufe in Brussels (BFB)

DIHK Brussels

BDI Brussels

Germany

Bundesministerium der Justiz und für Verbraucherschutz

Bundesministerium für Wirtschaft und Energie

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag

Ausschuss für Wirtschaft und Energie im Deutschen Bundestag

Ausschuss Digitale Agenda im Deutschen Bundestag

Ausschuss für die Angelegenheiten der Europäischen Union

Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und –senatsverwaltungen der Länder

Rechtsausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland

Bundesrechtsanwaltskammer

Bundesnotarkammer

Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Ver.di, Recht und Politik
stiftung neue verantwortung e.V.
DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Press

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion heise online
JurPC

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising more than 62.000 German lawyers. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession.

A. Preface

1 With this paper and a separate document, replying to the questionnaire of the EU Commission, the DAV submits its views in the context of the consultation regarding the “White Paper on Artificial Intelligence (AI) – A European approach to excellence and trust”.

2 In this paper, the DAV will respond to those questions which were specifically directed to the DAV by the Fundamental Rights Unit of the Directorate General for Justice and Consumer Protection of the European Commission in its e-mail of 2nd April 2020.

3 In a separate document, the DAV answers directly to the questions raised in the EU Commission’s consultation questionnaire.

B. Key Findings and Recommendations

4 Acknowledging the increasing importance of artificial intelligence in modern society, and the expected benefits when used at the service of the legal profession, the DAV invites the Commission to consider the following key findings when drafting a new framework on AI:

5 1) The introduction of AI systems in the field of justice entails particularly high fundamental rights risks and should, therefore, be subject to strict requirements.

6 2) Judicial and similarly intervening binding decisions by state actors must never be fully automated.

7 3) Where this is not absolutely necessary, comprehensive and meaningful transparency obligations must be complied with.

8 4) In addition, liability rules must be extended at the EU level with regard to AI. Likewise, effective redress and control mechanisms must be established for the use of AI in the justice and public administration sector.

9 5) Finally, in order to guarantee the human centric approach, national governments and the EU must ensure that the increasing automation of services does not lead to a reduction of jobs in the justice sector but rather to additional training for legal professionals in the field of AI and to an intensified knowledge-sharing.

C. Introduction

10 The futurist Ray Kurzweil has forecasted that artificial intelligence may reach or exceed levels of human intelligence by 2029. It does not matter whether the timing of the prediction is accurate. What matters is how we deal with a technology that has the potential to outpace human development. Therefore, challenges underlying this consultation are of an existential nature and a forward-looking regulation is required in order to protect a humane society and human rights.

11 Today, we can observe the rapid progression of self-driving cars or robots in healthcare. What we have not yet seen to the same degree is how human judgment is taken over by AI. If we want to preserve a human society where humans continue to make the final decisions, we need, however, to make sure that humans remain in control. These considerations hold particularly true for the areas of justice, law enforcement, and public administration. While still in its early stages, digitization is also advancing in these sectors which are central to the functioning of each democratic society.

12 Stressing the importance of a human society is not denying the benefits of innovation and progress. For example, studies have shown that less than 50% of the population have access to the legal system in some jurisdictions.[1] Technology – including AI-based instruments – can help broaden such access due to lower costs and easy access. Intelligent systems could, for instance, be used to largely automate the submission of briefs and the issuing of court orders in civil

[1] Marr, Bernard, The Future of Lawyers: Legal Tech, AI, Big Data and Online Courts, Forbes, January 17, 2020, available at: <https://www.forbes.com/sites/bernardmarr/2020/01/17/the-future-of-lawyers-legal-tech-ai-big-data-and-online-courts> [accessed on May 12, 2020].

proceedings. However, once AI-based technology is applied in the courtroom or in the decision-making process, fundamental legal rights could be seriously affected.

13 While lawyers will adapt their working methods and use new technologies, they will continue to consider themselves as advocates of those who need them and as guardians of the rule of law as an overarching principle of freedom and democracy. Following this mission, the legal profession also needs to point out developments that could negatively affect the rule of law.

I. Question 1: In which concrete situations does the use of AI applications increase or lead to risks for fundamental rights, including a high level of consumer protection?

14 As long as AI facilitates the logistics of administrative or judicial proceedings or the well-targeted assembling of relevant information, it can certainly make life easier for those who look for orientation or are going through a legal process. It becomes much more sensitive when AI is being used to identify and retrieve information as part of adjudicatory proceedings and, more specifically, as part of a decision-making process. Alternatively, fundamental rights could be affected if AI-based technology was applied in the courtroom to read faces, similar to a lie detector, or to otherwise interpret human behavior.

15 In the following sections, we will first examine examples of AI tools used in the justice sector (1). We will explain why the ultimate decision-making power needs to reside with a judge. We will set out why any effort to replace a human judge through AI would violate the fundamental rights of citizens to be heard and judged by a human being. In a second section, we shall explain that a similar reasoning applies to the extent that judges retain the decision-making power, but largely rely on AI systems. Under such circumstances, it would be very difficult for them to exercise their own independent judgment. Examples regarding the use of predictive justice tools in the sentencing practice in the United States and the Netherlands show, in a third section, how real the threats to the rule of law have already become in jurisdictions outside and inside the EU. With respect to the administration of justice, an example from Poland shows how the independence of

the judicial system can also be affected by the use of algorithms in the allocation of cases.

16 We will further outline examples of AI systems used in law enforcement (2) and public administration (3) that pose risks to fundamental rights and which will have a direct or indirect impact on legal practitioners, as these systems can either be adopted in court proceedings (such as video-based lie detectors) or play a role as evidence in legal proceedings as they may form the basis of administrative or enforcement decisions (such as intelligent video surveillance and credit score systems).

1. AI used in the judiciary

17 While AI-tools so far have been mostly utilized by lawyers, some applications are beginning to be introduced by the judiciary. Such applications can affect basic tenants of the legal system, such as fairness, accountability, impartiality, non-discrimination, autonomy and due process and, thus, the rule of law. Three main fields in which AI can be used by justice professionals can be distinguished:

18 Firstly, AI may be used as an assistive tool to predict a certain outcome of a case. Taken to the extreme, this application could potentially be used to substituting a human judge’s decision.

19 Secondly, AI tools can be applied prior to a hearing as an analytical tool, for instance, to search databases or other documents for relevant information and to generate parts of written judgements based on these outcomes.

20 Thirdly, AI can be applied in the administrative system of courts, for instance, as intelligent distribution systems or as a tool to communicate basic information on legal processes or hearings to the public via chatbots.

21 In the following, the risks of these different categories of AI-applications will be examined, starting with the most far-reaching and thus risk-inherent practical example, namely the possibility of replacing a human judge with AI-technology.

a) AI used to replace a human decision in court

22 In Estonia a pilot project created a “robot judge” that adjudicates small claims disputes of less than EUR 7.000 focusing especially on contract disputes. The

concept foresees that the AI-system issues a decision in an entirely autonomous way, solely based on uploaded documents by the parties. The case will be adjudicated by a human judge only on appeal.[2]

23 Similarly, in China, three years ago, the so-called ‘cyber-court’ transferred the whole administrative procedure for the handling of a case (- from case filing to the publication of the judgement -) online.[3] Further, the Supreme People’s Court runs a ‘mobile court’ pilot program since the beginning of 2019. In this ‘mobile court’, an AI-driven chatbot “judge” manages civil procedures through the country’s social media platform WeChat and the evidence is entered into a blockchain. It seems that the cases are still adjudicated by a human judge.[4]

24 Replacing a human judge with AI-controlled software touches on a number of fundamental rights:

25 First of all, based on today’s understanding of the rule of law, a software program cannot fulfil each individual’s right to be heard by an impartial and independent tribunal as laid down in Art. 47 para (2) of the European Charter of Fundamental Rights (“EChFR”). Likewise, the German Basic law (Grundgesetz, GG) demands that no one may be deprived of his or her ‘legal judge’ (Art. 101 para (1) sent (2) GG).

26 Legislation demonstrates that justice always required a decision to be made by a human actor. This is illustrated by statutes, such as the provision that the status of a judge can only be granted to a person "for life" (Section 27 (1) of the German Judges Act, DRiG). The expectation at the time of legislation as well as the choice of language clearly presumed the judge to be a human being.[5]

27 When thinking about the judge, the creators of constitutional and legal rights, of course, had more in mind than an analytical machine. They imagined humans to

[2] Niller, Eric, Can AI Be a Fair Judge in Court? Estonia Thinks So, WIRED, March 25, 2020, <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so> [accessed on May 12, 2020].
[3] Feng, Zhen/Xia, Helen, China: Three Cyberspace Courts now online and open for business, October 16, 2018, available at: <https://www.jdsupra.com/legalnews/three-cyberspace-courts-now-online-and-91459> [accessed on May 12, 2020].
[4] Cui, Yadong, Artificial Intelligence and Judicial Modernization, Shanghai: Springer 2020, p. 26; Harris, Briony, Could an AI ever replace a judge in court?, July 11, 2018, available at: <https://www.worldgovernmentsummit.org/observer/articles/could-an-ai-ever-replace-a-judge-in-court> [accessed on May 12, 2020].
[5] Enders, Peter, Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 2018, 721 (723).

be judged by humans who would make use of their intuition and experience in addition to their knowledge and skills. By listening to and engaging with the arguments of the court participants, judges make it easier for people to accept even adverse decisions. This is a necessary prerequisite to create trust in judicial systems.

28 Furthermore, even if Art. 47 para (2) EChFR were interpreted differently and, in principle, allowed a non-human to qualify for judicial functions, it would not be able to satisfy the requirement of 'hearing' a party. The right to be heard, enshrined in Art. 47 para (2) EChFR, serves to enable individuals to participate in and influence decision-making in the judicial process by entering into a dialogue with the decision-making authority.[6] Such a dialogue, characterized by mutual exchange and influence as well as speech and counter-speech can currently not yet take place with a machine. However, the movie "Her" illustrates how such an exchange could work in the future. Accordingly, such a hearing might technically well be conceivable. However, such a hearing would leave the realm of human to human communication, judgment and control if a machine took over.

29 Finally, at this time it would be practically impossible to verify whether an AI-judge could have the ability to be 'impartial' in the sense of Art. 47 para (2) EChFR. Since it is impossible to anticipate the facts and cases a machine would be dealing with or whether it was trained with insufficient or biased, it would be impossible to verify whether an AI judge would satisfy standards of impartiality. Furthermore, impartiality also requires that the deciding judge can be identified. AI systems, however, do not have legal personality and could therefore not be held responsible for a decision.

30 Thus, replacing a judicial decision with AI-technology would constitute an infringement of the right to be heard by an independent and impartial judge.

31 From a systemic perspective, the protection of human rights could be fundamentally threatened if the role of the legal profession was weakened as a result of an increasing digitalization of adjudicatory proceedings: If the role of lawyers is not sufficiently protected, there could be dire consequences for

[6] Hillebrand Pohl, Jens, The Right to Be Heard in European Union Law and the International Minimum Standard- Due Process, Transparency and the Rule of Law, June 8, 2018, available at: <https://ssrn.com/abstract=3192858>, p. 3 [accessed on May 12, 2020].

democracies and the rule of law. Less democratic regimes could use automation and algorithms to the detriment of critical citizens. If proceedings were ultimately decided without oral proceedings and without an independent human decision, civil liberties would be at risk.

b) AI used to assist the decision-making process

32 Even if there is no doubt that the ultimate decision-making power needs to reside with a human judge, one might wonder whether AI systems may be used to assist at least in the decision-making process.

(1) AI-tools used by judges and prosecutors as assistance

(2) Use of predictive justice tools in adjudicatory proceedings

33 From a fundamental rights perspective, the most far-reaching and, therefore, intrusive AI-tools are those attempting to predict a certain outcome of a case. Such AI tools are currently in their very early stages and primarily developed for lawyers but could potentially be applied by the judiciary. In France, for instance, two civil courts of appeal in Rennes and Douai tested a predictive justice system ("*Prédictice*") in spring 2017.[7]

34 In the light of the above findings, the fundamental rights risks are evident here too. If the use of the system were to lead to an automatic adoption of the decision judges would risk becoming nothing more than a conduit for delivering machine-generated decisions. Hence, if the ultimate decision constituted a mere formality, the right to be heard would be unduly restricted. The admissibility of such an instrument therefore depends on whether it leaves the judge concerned with sufficient discretion to enable him[8] to take an autonomous, impartial and unbiased decision. Consequently, a judge's decision should be based on reasoning that is sufficiently independent of the instrument's outcome so as to ensure a clear separation between the two. In other words, a judge should clearly display her or

[7] Ronsin, Xavier/Lampos, Vasileios, Appendix I – In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data, in: European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Strasbourg, CEPEJ - Commission Européene pour l'Efficacité de la Justice, 2018, available at: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>, p. 42 [accessed on May 12, 2020].

[8] For reasons of readability, the masculine form has been chosen in the text, the information, however, refers to members of both genders.

his own reasoning, stating verifiable reasons for following (or rejecting) a decision predicted by the AI system.

35 However, even in situations, where the predictive justice tool does not automatically lead to a pre-defined decision, a judge may be unduly influenced by data that he does neither know nor feel comfortable to assess. The judge will most likely not know the reasons why the system reached a certain conclusion and won't be able to verify the data which the system gathered and/or evaluated. Accordingly, the reasoning could be biased and, thus, result in a discriminatory outcome for individuals or groups.

36 If the judge relies on data and algorithms that he cannot verify, he would at least need to make sure that his judgment will not be influenced by the predicted outcome before he builds his own view. To mitigate this risk, a judge may need to take his decision before consulting the AI's predicted outcome. The judge could be obliged to make a formal declaration thereon in the course of the proceedings.[9]

37 The need to come up with an independent human reasoning for a judicial decision will sustain the ambition, creativity and logic of the human mind. And the preservation of such human judgment is crucial beyond the individual level: As a democratic society, based on the rule of law, we rely on the multitude of different opinions and their ongoing amendment and refinement. In the legal world, such development and progress, following changing attitudes over time, is reflected by the ongoing further development of case law (*Rechtsfortbildung*). Such case law over time may lead to new legislation and, either way, keeps a legal system alive. The reliance on AI systems, which necessarily base their analysis on existing case law and more formal patterns of analysis, could lead to a structural limitation of the courts' initiative to actively pursue further legal development, asking questions, central to the facts, and using general legal methodology. This applies, in particular, to situations which deviate from the typical case, as anticipated by the initial legislation, and therefore, may create a contradiction between the text of the law and its ratio legis. Such legal gaps are typically closed by using recognized methods of interpretation, such as a historic analysis, a systematic interpretation or a teleological reduction or extension. If predictive justice tools are over-used,

[9] *Cf.* fn. 5.

however, the further development of the law could slow down or eventually cease to take place.

(i) Use of post sentencing predictive justice tools

38 Another practical, frequently debated example of a predictive justice tool that could potentially be used by the judiciary concerns the post-trial behavior of a crime offender. Recidivism tools determine the risk of re-offending and may be used to define the crime-offender's length of imprisonment.

39 Applications similar to the most prominent AI-tool *COMPAS*, which is used in several US States, are emerging in EU Member State's law enforcement systems, for instance the *ProKid* AI-tool that is being used in the Netherlands. ProKid aims to identify the risk of recidivism among twelve-year old children who have previously been suspected of a criminal offence by the police.[10] A similar tool ("*SAVRY*") is used by Spanish authorities.[11]

40 In this context, essentially the same fundamental rights risks arise as in the cases cited above: Firstly, the right to a fair trial could be violated if the system is trained on biased and discriminatory data. This effect is even aggravated in cases where the algorithmic system's functioning is not made publicly available since there is no opportunity to contest a decision based on the data. Even if such data were available, the situation would not be much better for the affected parties as they would carry the costly and time-intense burden to analyze the data. Such a burden would significantly deteriorate their situation in the proceedings and violate the due process.

(ii) Use of intelligent legal research tools

41 Intelligent legal research tools are another practical example of AI used by legal professionals. The Italian program *TOGA*, for instance, is used as an intelligent database for prosecutors (and lawyers).[12]

[10] Algorithm Watch, Automating Society – Taking Stock of Automated Decision-Making in the EU, January 2019, pp. 100, available at: <https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf> [accessed on May 12, 2020].
[11] *Cf.* fn. 10, pp. 122.
[12] *Cf.* TOGA, available at: <https://toga.cloud/>.

42 The use of these tools is generally welcome. Nonetheless, from a fundamental rights perspective, the selection of the search tool could pre-define the outcome of a prosecutor's decision, as the system could weigh some searched keywords more than others. It could, thereby, influence the process of decision-making and lead to a partial decision.

(3) Predictive analytical AI-tools used by lawyers

43 Lawyers and insurers are increasingly relying on AI-tools, especially those aimed at predicting a judge's decision. A typical example is *Jurimetria*, a statistical and predictive jurisprudential software that helps legal professionals in Spain analyze their cases. It systemizes and extracts content from more than 10 million judicial decisions, coming from all instances and jurisdictional orders in Spain[13]. Another prominent example is *Casecruncher* Alpha, which In October 2017, won a week-long competition against human commercial lawyers with an accuracy of 86.6% of the predictions made.[14]

44 At first glance, predictive analytical tools used by lawyers do not appear to hinder access to justice. However, it is important to keep in mind that the work of lawyers goes by far beyond providing a brief legal response to a simple question.

45 The work of a lawyer is much more multifaceted than the mere provision of legal analysis. AI may be able to carry out a legal analysis more quickly and accurately than a lawyer, as it can draw on a vast data pool and evaluate it within a very short time. However, a client who can only answer binary questions will not necessarily get the most appropriate advice in many situations. At the beginning of an exchange between a lawyer and a client, it is often not clear, even to the client, what the real problem is. And it is only in the course of time that the facts relevant to the settlement of a legal dispute as well as the personal and commercial interests emerge. Behind the legal issues, personal or economic interests may play a major role. Therefore, everyone should have the opportunity to receive comprehensive advice from competent, experienced people lawyers who

[13] *Cf.* Jurimetría, available at: <https://jurimetria.laleynext.es/content/Inicio.aspx>.
[14] Hill, Caroline, 'Machine beats man' in Casecrunch lawyer challenge, Legal IT Insider, October 30, 2017, available at: <https://legaltechnology.com/machine-beats-man-in-casecrunch-lawyer-challenge/> [accessed on May 12, 2020].

understand to ask the appropriate questions and to explore the facts in order to develop the best solution with the client.

46 While lawyers can use AI resources in a supportive manner, they also need to make sure that they preserve their ability to ask the appropriate questions, explore the facts with the clients and jointly build the appropriate solutions. Otherwise, a negative prediction might prematurely prevent individuals to file a case solely based on a machine's opinion. This could be problematic not only in cases where the machine simply produces a wrong outcome, but even more so in cases where only minor, but potentially decisive features of a case differ from apparently similar cases. Taken to the extreme, a systematic use of such machines could also have an adverse effect on the further development of case law by judges. Such development of case law, however, has always been part of changes in societies and innovation in legal systems.

c) AI used within the court's administrative system

47 The use of AI in courts' administrative systems could also affect fundamental rights, if used in a targeted manner. Such concerns became real, when the Ministry of Justice in Poland introduced a system of algorithm-driven allegedly random allocation of cases. The digital system assigns cases to particular judges across the country on a once-per-day basis. If the system were truly random and left no discretion to its operator, this would not appear problematic at first sight. With regard to this particular tool, however, it was argued that the Prosecutor General could unduly influence the process. Belonging to the administering Ministry of Justice and being a party to criminal proceedings, the Prosecutor General, could control how cases would be assigned. If such influence took place, it could ultimately result in a violation of the right to a fair trial.[15] The concerns in this example were aggravated by the fact that the Ministry was unwilling to disclose the workings of the algorithm used for the system.[16]

[15] Matczak, Marcin, 10 Facts on Poland for the Consideration of the European Court of Justice, May 13, 2018, available at: <https://verfassungsblog.de/10-facts-on-poland-for-the-consideration-of-the-european-court-of-justice/>, citing Case of Daktaras v. Lithuania – Application no. 42095/98 [accessed on May 12, 2020].
[16] *Cf.* fn. 10, pp. 107-108.

2. AI used in law enforcement

48 The rule of law might further be endangered by the use of AI-tools used in law enforcement. Tools already used there could be applied directly in the courtroom or play an indirect role as a basis for a decision challenged in a court proceeding. The challenge in this context results from the fact that affected individuals usually are not aware that such tools are being used to their detriment. Furthermore, the police may not want to publicly disclose which criteria determine the system's outcome, how they are weighed and which data are being used to train the system's algorithms. Such systems prevent access to justice, as in most cases the affected individuals can neither detect nor prove whether they have been subject to an erroneous or unfair decision. Risks further arise as the systems collect considerable amounts of data which may be hacked and lead to grave data protection and privacy infringements.

49 One particularly critical example is the EU-funded iBorderCtrl-project (Intelligent Border Control System) which tests software that aims to detect persons lying at border controls[17]: Third-country nationals are asked to answer questions from a computer-animated border guard avatar which analyses the micro-gestures of travelers to figure out if the interviewee is lying.[18] According to an analysis by Algorithm Watch, the system contained a strong risk of racial bias, as it was mostly trained on white European men and also had a high error rate of 25%.[19] It further raised fair trial concerns due to legitimate doubts about the scientific accuracy and reliability of a lie detector. Such tools could technically and hypothetically also be used in the context of court hearings which would increase the due process concerns even further.

50 Other critical examples of AI use in law enforcement involve intelligent video surveillance or predictive policing tools based on facial recognition which are increasingly being used all over the EU. In the German city of Mannheim, for instance, an experiment has been used to enable AI-supported recognition of social situations based on automatic image processing. The camera system

[17] *Cf.* iBorderCtrl, available at: <https://www.iborderctrl.eu/>.
[18] *Cf.* iBorderCtrl, Intelligent Portable Control System, Project Presentation, available at: <https://www.iborderctrl.eu/sites/default/files/publications/iBorderCtrl%20global%20presentation%20v5.pdf> [accessed on May 12, 2020].
[19] *Cf.* fn. 10, pp. 36-37.

informs the police when it detects actions that could be considered as assault or theft. It is then possible to track the people involved throughout the entire camera system.[20] Such behavioral scanners firstly exert a strong conformity pressure and are vulnerable to generating false alarms. With regard to access to justice rights, the main risk results from the fact that the system does not disclose to which 'unnatural movements' the algorithms are trained to react.

3. AI used in public administration

51 Another sector in which lawyers have a specific task to ensure that the rule of law is observed is in the context of AI-technology used by public administration. The opacity of such systems – exemplified in practical examples in the following – shows that discriminatory or biased outcomes also threaten due process as they are difficult to detect and to contest in front of a judge.

52 A particularly critical example is that of profiling or credit scoring systems. In the Danish city of Gladsaxe, for instance, a tracing tool was introduced as part of the country's *ghetto plan* in January 2018 to detect children in vulnerable circumstances at an early stage. Municipalities were allowed to collect and combine information on children from different public sources and to categorize it according to specific "risk indicators". The system then assigned a score to the family based on information such as attendance of doctor's appointments, employment and family status, mental health and similar criteria.

53 In December 2018, the Gladsaxe municipality was subject to a leakage which exposed data of more than 20000 citizens' personal data, including gender, age, welfare benefits and the family's special conditions. [21] This case exemplifies the typical implications that come along with profiling: Not only do such programs expose significant privacy and data protection risks, they also may be used in a discriminatory way. Most people were not even aware that they had been subject to the program and were, therefore, also prevented from taking action against the program.

---

[20] Mannheim testet verhaltensbasierte Videoüberwachung, Heise Online, December 3, 2018, available at: <https://www.heise.de/newsticker/meldung/Mannheim-testet-verhaltensbasierte-Videoueberwachung-4239279.html> [accessed 12 May 2020].

[21] *Cf.* fn. 10, pp. 36–37*; cf.* also Enforcement Tracker, available at: <https://www.enforcementtracker.com>.

54 In other administrative systems, administrative tasks have been automated. Such applications may generally serve as positive use cases of AI. However, if programmed incorrectly or if the data are trained insufficiently, such applications may affect certain social groups to a greater extent than others and, therefore, increase social inequalities. For example, a tax collection system in Australia in 2018, which in many respects was flawed, affected people from weaker social backgrounds financially to a significantly higher extent than others.[22] Hence, the risk of increasing inequalities associated with the use of AI also needs to be taken into account.

II. Question 2: Which situations do you view as high-risk situations from a fundamental rights perspective? How would you define high-risk situations in this regard?

55 According to the White Paper, a new regulatory framework for AI may contain mandatory requirements only with regard to high-risk applications of AI. The DAV suggests a more nuanced approach. From the DAV's point of view, a concept should be developed which has at least five stages, within the framework of which AI-applications must comply with certain transparency, security and monitoring requirements depending on the intensity of their intervention. The area of use and the hazard potential should be key factors for classification. In the following, two concrete examples of high-risk applications will be presented. Subsequently, a risk assessment concept is developed on the basis of precise indications. Lastly, a risk matrix is designed based on the preceding findings.

1. High-risk situations

56 There are a variety of situations that may qualify as high-risk situations from a fundamental rights perspective. In the following, two exemplary situations in the context of the judiciary and law enforcement will be outlined.

a) Situation 1: Predictive justice tools

57 Given the observations under question (1), AI used within the justice sector, law enforcement and administration is particularly critical. The highest risk arises

[22] Djeffal, Christian, Artificial Intelligence and Public Governance Normative Guidelines for Artificial Intelligence in Government and Public Administration, in: Wischmeyer, Thomas/Rademacher, Timo (edt) Regulating Artificial Intelligence, Cham: Springer 2019, p. 281.

where a legally binding decision is solely based on an autonomous decision and, thus, replaces human rationale. It is a high-risk situation, as the decision is likely to be non-transparent, may be biased and might cause harm of an unlimited extent as – ultimately – it could lead to severe financial damage or to innocent individuals being imprisoned.

b) Situation 2: Biometric identification schemes

58 Another high-risk situation within the judiciary, law enforcement and administration is where legally binding decisions are primarily based on biometric identification systems. The use of such tools is highly risk-inherent, as the likelihood of grave violations to basic rights, such as privacy and principles of non-discrimination is very high and may lead to far-reaching consequences for the affected individual. The systems also often tend to have high error rates and are vulnerable to manipulation.

2. Definition of high risk – gradual approach required

59 The White Paper follows a two-fold risk-assessment approach and splits AI applications in high-risk and low-risk categories. 'High risk' applications are defined as those which involve significant risks, both in a sector and in its intended use.

60 In the view of the DAV, dividing AI systems into two categories only, namely high and low-risk applications by way of an exhaustive list, does not reflect the complexity and variety of real-life use cases. It is further likely to lead to an artificial splitting of applications. This could cause either sensitive regulatory gaps or, on the other hand, lead to over-regulation if, for the sake of caution, too many applications were included into the high-risk category.

61 Accordingly, the DAV suggests developing a risk matrix. Such risk matrix could follow a gradual approach and – following the suggestion of the German Data Ethics Commission – divide applications into at least five different risk levels.[23]

[23] Data Ethics Commission of the Federal Government, Opinion of the Data Ethics Commission, January 22, 2020, available at: <https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.html>, p. 177 [accessed on May 12, 2020].

Every risk category would, in turn, lead to a different set and degree of legal requirements.[24]

62 When assessing potential risks, both the affected sector as well as individual aspects of the concrete AI measure should be taken into account. In the following, sectors that are of utmost importance for the systemic functioning of a state will be identified (a). In the subsequent section, criteria for a concrete risk assessment of an individual application will be developed.

a) High risk sectors

63 Given the significance of the risks identified under Question (1), the judicial system should be marked as systemically relevant and particularly critical for democracies which are built on the idea of the balance of powers. If decisions in this sector are fully automated, but not transparent, there is an overarching risk that a government that is in control of the technology might disrespect crucial elements of democracy. Accordingly, AI tools could be used by authoritarian regimes to exercise control over societies and strengthen their repressive capabilities.

64 Other sectors which are relevant for the systemic functioning of a state, such as the health and energy sectors, need to be particularly safeguarded. This certainly became obvious during the outbreak of the Covid-19 pandemic. All these sectors need to be categorized as particularly risk-inherent to ensure that basic needs of the population can be fulfilled – with or without the use of AI.

b) High risk applications

65 The White Paper currently lacks clear guidance on what constitutes a concrete critical application. Two major factors should be taken into account, namely the *likelihood of the occurrence of an identified risk* (i) and the *severity of a potential damage* (ii).

---

[24] The risk assessment procedure and the risk matrix are inspired by: Opinion of the Data Ethics Commission from January 22, 2020, *cf.* fn. 23; Martini, Mario, Grundlinien Eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse, available at: <https://www.uni-speyer.de/fileadmin/Lehrstuehle/Martini/2019_Gutachten_GrundlageneinesKontrollsystemendgueltig.pdf>; Zweig, Katharina, Algorithmische Entscheidungen: Transparenz und Kontrolle, January 2019, available at: <https://www.kas.de/documents/252038/4521287/AA338+Algorithmische+Entscheidungen.pdf/533ef913-e567-987d-54c3-1906395cdb81?version=1.0&t=1548228380797>, [all accessed on May 12, 2020].

(1) Likelihood of the occurrence of an identified risk

66 Under this section, the classic risk-assessment regarding the causal link between an action and a likely consequence must be evaluated. Whether the end user has the possibility to re-evaluate and, thus, mitigate the automated decision also plays a decisive role.

(2) Severity of a potential damage

67 When assessing the severity of a potential damage, both its nature (a) and its likely extent (b), need to be considered.

68 As regards the type of damage (a), criteria such as whether the envisaged damage would be reversible or irreversible need to be included in the assessment. Another crucial aspect is the type of the affected fundamental right: In this regard, potential physical harm and, thus, a violation of the right to physical integrity (as enshrined in Art. 3 EChFR) need to be placed at the highest level.

69 With regard to the extent of the potential damage (b), criteria such as the number of individuals affected, the impact on other fundamental rights, the circumstances, frequency and duration of the adverse effect need to be taken into consideration.

(3) Risk matrix

70 The classification of a specific application into one of the risk categories should lead to different legal requirements. These could be based on the following risk matrix:

(i) Risk-level (1):

71 At the lowest level of intervention, only ex-post transparency obligations may be necessary. This would mean that no permanent control processes would need to be installed. Upon request, an ad hoc analysis would need to be carried out and the risk assessment repeated. AI systems used to suggest products to consumers or to display them in a certain order on social networks, for example, could fall under this category.

(ii) Risk-level (2):

72 At a second risk level, a general monitoring of the system would be required. In order to facilitate monitoring, the system’s operator would be obliged to indicate

the quality measures and the learning process of the system and disclose how the system relates to the ultimate decision, i.e. the degree to which the decision is influenced or based on the system's output. The monitoring could be performed by external third-party auditors. Dynamic or personalized pricing techniques could fall under this category.

(iii) Risk-level (3):

73 At a third level, comprehensive transparency obligations may be legally required in addition to monitoring. This obligation would need to include the disclosure of all relevant factors and criteria used as a basis for the automated decision and all training data, but without disclosing other technical functions of the system.

74 Third-party monitoring may be accompanied by governmental information and inspection rights. Recording requirements may also apply. The regulations of the German Securities Trading Act (WpHG) on algorithmic trading with financial instruments could serve as a regulatory model (Section 6 (4) WpHG).

75 Furthermore, the entity making use of the system would be required to name a responsible person within the company to perform risk management tasks. This person could be held responsible for failures of the systems vis-à-vis third parties.

76 As regards the use of AI by the government, purely informative tools used within the administration, such as the "Bobbi" chatbot used by the administration of the Land of Berlin[25], could fall into this category.

(iv) Risk-level (4):

77 At the next level, a full explanation of the system would be required. In this class, if something went wrong, the possible damages would be so high that AI-systems with a learning component may only use explainable methods of machine learning. Such explanation could be given, for example, by means of explanation or decryption algorithms. If business or trade secrets were to hinder the full disclosure of an algorithm's logic, the business entity would be required at least to disclose them to an authorized state body or agency. Furthermore, preventive admissions procedures could be required to ensure compliance with relevant law prior to its use.

[25] *Cf.* Chatbot Bobbi, available at: <https://service.berlin.de/chatbot/chatbot-bobbi-606279.php>.

78 In addition, ongoing dynamic operator obligations would need to be installed. These would make operators responsible for the results of decisions and the procedural correctness of the system even after its admission to the market.

79 Such requirements could apply to AI used within such areas as the judiciary and law enforcement or for the examination and allocation of benefits. Prior checking may also be appropriate for applications which may have a significant impact on those areas of life which are of systemic importance for the functioning of the state and the free and democratic order (in particular elections or the formation of public opinion).

(v) Risk-level (5):

80 The highest level of intervention would apply only to exceptional applications, such as automated lethal weapons. In addition to the previously listed obligations, one would need to consider whether their use could be limited, for example, to non-learning AI systems, i.e. those based on linear regression, or whether other reliable, safe limitations could be found to ensure full oversight and human control of the application.

III. Question 3: Do you know of effective means to address the risks that you identified in your reply to the above questions?

81 The DAV welcomes the work on the fundamental principles identified by the High-Level Expert Group (HLEG) on Artificial Intelligence in its Guidelines on Trustworthy AI. The seven key requirements for ‘Trustworthy AI’ – namely 1) human agency and oversight, 2) technical robustness and safety, 3) privacy and data governance, 4) transparency, 5) diversity and non-discrimination and fairness, 6) societal and environmental well-being and 7) accountability should be placed at the heart of future regulation on AI.

82 Based on these principles, the following means should be considered to effectively address the identified risks in the previous section:

83 First of all, legally binding (i.e. not appealable) decisions by a court and similarly intervention-intensive decisions by state actors should never be based solely on an autonomous decision but should be taken by a human being (1).

84 Secondly, where this is not possible or not strictly necessary, a high degree of transparency which ensures identifiability and contestability of an AI-based decision should be mandatory (2).

85 Thirdly, in order to facilitate access to justice and ensure that individuals affected by a wrong or harmful AI application are compensated for any suffered loss, efficient and comprehensive remedies and a liability regime are needed (3).

86 More specifically, the following means could be adopted:

1. The primacy of human decision

87 Legally binding court or similarly invasive public authority decisions should not be based solely on an automated decision-making system. As outlined in the previous section, the right to be heard by an independent and impartial tribunal is only satisfied if the deciding judge is a human being, not a software. A future EU framework on AI should reaffirm this principle to ensure legal clarity.

88 This principle is also reflected in Art. 22 of the General Data Protection Regulation ("GDPR") which stipulates that a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects with regard to him or her or similarly significantly affects him or her. This principle applies even more so to situations that may lead to a legally binding court ruling.

89 The demand for 'human' decision-making as a basic prerequisite for a functioning judicial system can only be met if there continues to be sufficient and adequately trained human expertise. In other words, the progressive digitalization and automation should not lead to a reduction in personnel. Rather, legal professionals will need additional training and education in the field of technical and digital applications. To this end, EU-wide knowledge-sharing and funding would prove helpful. In addition, special units for AI-related content may be formed.

90 Further, adequate safety measures and 'analogue' fallback plans to ensure the functioning of the entity in case of a system's breakdown are required.

2. Transparency

91 Another crucial element that has been underlined in the Ethical Guidelines of the HLEG is to create transparent systems.

92 To prevent the postulate of transparency from becoming an empty phrase, clear requirements and criteria must be formulated. Subsequently, the practical means to implement them will be outlined.

a) The required degree of transparency

93 Modern machine learning systems create complex models which can make it difficult to identify why and how they generate a particular output. And even systems that utilize algorithms whose underlying operation and logic can be explained (for example, because they follow a decision-tree analysis) may not openly display their reasoning. Finally, if information about a system is provided, end-users will often not be able to comprehend or assess such information because of the quantity of information and complexity of these systems. These factors result in their characterization as 'black boxes'.[26]

94 The opacity of self-learning algorithmic systems not only helps to hide potentially biased or erroneous decisions. It may also hinder access to justice if no usable evidence can be extracted from an individual decision. At the same time, the demand for full disclosure of all technical functions of an algorithm could also prove counterproductive. Similar regulatory approaches, such as the duty to consent to the processing of personal data under the GDPR, have demonstrated the risk of information overload: If individuals are being provided with too much information about a transaction they cannot comprehend, the risk of creating even more opacity arises.

95 Based on the rule of law, the main purpose of transparency is to give individuals the right to understand, assess and challenge a particular decision. In the context of AI used by government action, transparency is also a means to fulfil the legal obligation to state reasons for administrative acts, as laid down in Article 41(2) EChFR.

---

[26] Yeung, Karen, Responsibility and AI, Council of Europe Study, September 2019, available at: <https://rm.coe.int/responsability-and-ai-en/168097d9c5>, p. 21 [accessed on May 12, 2020].

96 In light of these findings, the principle of transparency should satisfy three key criteria:

97 It should ensure

1) identifiability,

2) meaningful contestability and

3) adequate oversight.

(1) Identifiability

98 Each AI-application should be easily and clearly identifiable as such for end-users. Individuals should have a right to know whether they are subject to an autonomous decision-mechanism or not. Operators should further disclose the intended purpose of using an AI-system.

99 Individuals should also be informed in clear and understandable language whether or not the solutions offered by the artificial intelligence tools are binding and if they have alternative options. Furthermore, they need to be informed that they have the right to obtain legal advice and the right to access a court. They must also be clearly informed of any prior processing of a case by artificial intelligence before or during a judicial process and have the right to object.

(2) Contestability

100 To ensure the right to contest a decision, information should be provided about the basic features of the **individual decision** in question, namely:

- The criteria used,
- their weightings and the
- training data of the self-learning algorithm.

(3) Adequate oversight

101 Meaningful oversight means that especially public entities relying on AI-technology should allow independent third parties to conduct independent testing of the technology.

102 For instance, if a court wished to rely on a specific predictive justice tool, it would need to ask its technology provider to make technical capabilities available to enable legitimate, independent and reasonable tests for accuracy and unfair performance differences across distinct subpopulations.

103 In addition, the public technology provider should disclose any complaints or reports of bias regarding the service. It should further be required to publish information regarding the error rate of the system.

104 Furthermore, ongoing monitoring obligations should apply. The operator should also ensure that its technology provider is subject to dynamic operator obligations, which would make him responsible for the results of decisions and the procedural correctness of the system.

b) Means to implement transparency aspects: Regulation by and in design

105 To implement the above-mentioned identified transparency requirements, the approach of 'regulation by and in design' could be followed. The rationale behind 'regulation by design' is that relevant norms are embedded in the technology itself.[27] The concept is inspired by Article 25(1) GDPR which requires controllers by default to process only those data that are strictly relevant for each specific purpose. This idea was further developed and is now recognized under the term of 'ethics by or in design', meaning that also other relevant requirements may be incorporated into the system itself.[28] When incorporating the above-mentioned criteria into the architecture of an AI system by default, transparency of the system would be enhanced as these would be clearly identifiable and traceable in the system.

c) Means to ensure transparency regarding the underlying technology

106 Explaining the technical functioning and logic of applications based on neural networks is subject to high hurdles. Current research focuses especially on tools that aim to make neural systems explainable with the help of decoding algorithms (1). Another option is to use blockchain technology (2).

[27] Buchholtz, Gabriele, Artificial Intelligence and Legal Tech: Challenges to the Rule of Law, in: Wischmeyer, Thomas/Rademacher, Timo (edt) Regulating Artificial Intelligence, Cham: Springer 2019, p. 192.
[28] *Cf.* fn. 23, p. 74.

(1) Explainable AI models

107 Explainable AI (XAI) is a concept based on the idea that algorithms provide explanations of their own decisions.[29] It goes back to the 'Explainable AI' initiative that was launched in 2016 by the US Defense Advanced Research Projects Agency. This initiative of several organizations and companies aims at developing ways to decode deep-learning algorithms.

108 For instance, the 'Quantitative Input Influence'-model, is a system capable of measuring the degree of influence from input data to output.[30] The 'Layer-wise relevance propagation' XAI is a system that allows the thought process of neuronal systems to run backward and, thus, to detect which neurons have caused certain decisions and how these contributed to the result.[31] The 'local interpretable model agnostic explanation' operates as a counterfactual model and identifies on the basis of thousands of tests in each of which minimal variants are changed, which factor was vital for a decision.[32] The 'Generalized Additive Model' finds linear trends in data sets and could potentially also be applied to more complex data sets.[33]

109 In order to develop practical solutions to meet transparency requirements, the DAV invites the Commission to invest more in initiatives and start-ups that create tools to explain AI systems.

---

[29] Nassar, Mohamed/Salah, Khaled/ur Rehman Muhammad Habib/Svetinovic, Davoc Blockchain for explainable and trustworthy artificial intelligence, WIREs Data Mining Knowl. Discov., 10(1), October 17, 2019, available at: <https://doi.org/10.1002/widm.1340>, p.1 [accessed on May 12, 2020].
[30] Datta, Anupam/Sen, Shayak/Zick, Yair, Algorithmic Transparency via Quantitative Input Influence: Theory Experiments with Learning Systems, available at: <https://www.andrew.cmu.edu/user/danupam/datta-sen-zick-oakland16.pdf>, p. 1, [accessed on May 12, 2020].
[31] Montavon, Grégoire/Binder, Alexander/Lapuschkin, Sebastian/Samek, Wojciech/Müller, Klaus-Robert, Layer-Wise Relevance Propagation: An Overview, in: Samek, Wojciech/Montavon, Grégoire/Vedaldi, Andrea/Hansen, Lars Kai/Müller, Klaus-Robert (edt) Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, Lecture Notes in Computer Science, 11700, Cham: Springer, 2019, available at: <https://link.springer.com/chapter/10.1007/978-3-030-28954-6_10> p. 193 [accessed on May 12, 2020].
[32] Barredo Arieta, Alejandro *et al*., Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI, Information Fusion 58, June 2020, available at: <https://doi.org/10.1016/j.inffus.2019.12.012>, p. 94 [accessed on May 12, 2020].
[33] Ibid., p. 91.

(2) Blockchain technology

110 Another potential means to enhance transparency of AI technology is to make use of the so-called blockchain technology. Blockchain technology is a decentralized, distributed ledger that records the provenance of a digital asset. Through the use of blockchain technology, immutable records of all the data, variables, and processes are available. The audit trail could be used as evidence and thus help to challenge a decision in court.

111 Thus, blockchain technology could make a major contribution to creating transparency of AI. So far, however, this is only cautiously proposed as a solution. One reason is that blockchain technology requires high energy input. Yet another problem arises with regard to the GDPR: Due to the decentralized structure and mode of operation of blockchain, it is not compatible with the primacy of the GDPR, according to which each data processing must be able to appoint a responsible data controller. Furthermore, the fact that transactions in the blockchain can hardly be changed and are, therefore, deemed immutable to hacking is difficult to reconcile with the right to be forgotten, codified in Art. 17 of the GDPR. According to a study by the European Parliament[34], however, the identified tensions are primarily a result of a lack of certainty on how specific concepts of the GDPR should be interpreted.

112 Given the outlined legal insecurities of blockchain in relation to the GDPR, the DAV invites the Commission to provide further regulatory guidance to reconcile these conflicting regimes.

3. Liability and Redress Mechanisms

113 One of the core problems of liability in the context of AI is that automation and limited ex-post traceability make it significantly more difficult, if not impossible, to prove causality. The injured party has almost no possibilities to enquire and detect the cause for the defect. Although it is, in principle, possible to record all decision-making processes (so-called “logging”), there are practical capacity problems in view of the large amounts of data. This finding is reinforced by the combination of

[34] European Parliamentary Research Service, Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf>, p. 97 [accessed on May 12, 2020].

AI as software with machines as hardware or the interconnection of several AIs and hardware (“internet of things”, IoT). In addition, a responsible handling of data in accordance with applicable data protection regulations is needed.

114 The high need for adaptation speaks against extending the existing dualism of the liability regimes of fault-based liability (here especially Sec. 823 German Civil Code) and strict liability (here especially Sec. 1 German Product Liability Act) – which has been established in Germany and other Member States – to the field of AI. This applies to the definitions, the burden of proof and the defences. In order to take into account the specificities of AI and to include the foreseeable developments, a new risk-based strict liability regime should be introduced comparable to the model of motor vehicle liability.

a) Definition

115 First of all, we agree with the EU Commission's demand for a clear definition of AI, which, on the one hand, is flexible enough to keep up with the ongoing technological development and, on the other hand, is sufficiently precise in the interest of legal certainty.[35] However, any details should be left to experts with technical and legal expertise.

116 Given the wide range of possible applications, developing a precise definition poses a particular challenge. AI could be used independently as a pure software product, built into (a third-party) hardware, or marketed in connection with services. On the other hand, possible modifications by third parties, for example through software updates or add-ins, must also be taken into account.

117 A rigid definition would not be helpful regarding the ability to react to new technologies, which are subject to constant innovation. To a certain extent, one may rely on case law, but the courts may at the same time be overwhelmed by the complexity of such task.

b) Liable persons

118 A distinction between developers on the one hand and operators on the other hand as addressees of potential liability claims is useful. However, further distinctions will also be necessary.

[35] Cf. definitions in: Zech ZfPW 2019, 198 (199 f.); High Level Expert Group on Artificial Intelligence, A definition of AI: Main capabilities and disciplines, p. 8; Dettling PharmR 2019, p. 634.

(1) Regarding the product supply chain

119 If AI is used as a pure software product and put on the market, liability should be limited to the developer.

120 If a third party modifies, extends or updates the AI by means of software and damages occur as a result of these interventions, the third party who interfered should consequently be held liable. Currently, Article 3 para 1 Product Liability Directive (PLD) provides that in addition to the actual manufacturer, also the producer of any raw material or the manufacturer of a component part may be held liable. According to Article 5 PLD they may be jointly and severally liable. However, it is already difficult to apply the term “supplier” to software modifications. Irrespective of this, joint and several liability appears problematic because in many constellations this will also hold parties liable who had almost no impact and no participation in the causation. The actual investigation of causes is thus often shifted to joint and several compensation proceedings, which seems hardly suitable for this purpose. As a consequence, disputes between joint and several debtors are likely to increase enormously since very often one of the joint and several debtors will not have contributed to the causal link of the damage or will have made only a very small and negligible contribution. Several third-party notices could further increase cost risks for the parties to the proceedings and thus make efficient law enforcement more difficult. The enforceability of claims may be complicated and thus made very difficult by a large number of third-party notices and interveners. All in all, any claim would resemble a "scattershot", because anyone who has even remotely come into contact with the AI causing the damage would qualify as a potential liability addressee. Such an extension of liability to "non-causers" should be avoided.

121 An attempt should be made to retain the basic liability principle of the originating actor, but to create stronger liability priorities. In view of the complexity of the matter and the associated difficulties in proving the facts, it is often almost impossible for the injured party to identify the right addressee for its liability claims in this constellation. Whether the damage was caused by the software modification of the third-party, the original AI software or a faulty interaction between the two

can hardly be proven due to, among other things, the autonomy and self-learning ability of AI and a regularly technically limited logging.

122 However, if the developer releases corresponding interfaces or enables access to the software as a whole or at least in part, the focus of liability should be on him. Liability of third party providers who provide software updates, add-ins or similar for the existing AI software may then be waived. The developer can, at his own discretion, determine or limit external influence. He knows the potential sources of error and has the best possibilities to investigate the cause. In these cases, the injured party would have the advantage of a central point of contact that can be determined with reasonable effort. If the damage was actually caused by the modification of the third-party supplier, the developer who bears the burden of proof could take recourse against the third-party supplier. This would then not be a joint and several compensation, but classic third-party recourse.

123 The same should apply to impacts on the AI software by IoT when the AI communicates with other electronic devices and displays certain behaviour based on the communication. The AI developer deliberately releases such interfaces in order to provide more functions or services to users. The developer can define or limit the influence of the other devices which are to be connected in advance. He also has to observe the market, as in classical product liability. If the injured party were dependent on a determination of the actual damaging party or the damaging interconnected device, the burden to pursue such claims would be enormous. Even if the causal interconnected device could be determined, it would still be questionable whether this device or the AI's reaction was faulty. Therefore, a legal framework should allow for uncomplicated compensation by the AI developer without the need to investigate further actors or contexts. Recourse of the developer against the developer/manufacturer of the respective interconnected device would then follow in a second step.

124 If AI is used in hardware owned by other manufacturers, which itself has faults and can cause damage, the distribution of liability is clearer, since determining the cause of damage would be easier in these cases. This is because, in contrast to software updates or the networking of electronic devices with purely software-based risk potentials, there is an interaction between software and (tangible)

hardware. In this case, it is not a matter of the data-based modification of already existing and complex, because evolving, software, but only of the use of control electronics for an already existing hardware. This constellation is not new (see operating systems for computers, robots etc.) and lacks the non-transparency and complexity characterising the potential danger of AI through autonomy and self-learning ability.

125 It may also be impossible to tell whose AI software is being used in a piece of hardware. In such cases, following the example of the "quasi-manufacturer" in the sense of the Product Liability Directive, it may make sense to hold the person liable who visibly appears externally (with his hardware) as the manufacturer and who needs the software for the functioning of his hardware.

(2) As regards the operators

126 If damage is caused by the use of AI systems, the operators must ensure that the injured party is adequately compensated. In this respect, however, the differentiation between professional and private users of AI, as suggested by the expert group, does not seem convincing because the resulting risks and potential damage do not depend on whether a user uses software professionally or privately.

c) Regulatory nature

127 As proposed in the White paper, the regulatory framework should be both preventive in the sense of reducing the risks before market introduction and facilitating enforcement in the event of damage. This is already common practice in German law as well as in the General Product Safety Directive (Directive 2001/95/EC) and the PLD.

d) Possible regulatory options

The White Paper proposes different regulatory options which will be addressed in the following:

(1) Voluntary Labeling

128 The labelling proposed in the White Paper is useful as a complement to the liability regimes. However, it hardly seems effective on a voluntary basis. Mandatory

labelling for products placed on the EU market along the lines of CE marking would be preferable.

(2) Mandatory risk-based requirements at least for high risk applications

129 A distinction between high and low risk applications for newly established liability regimes, such as strict liability, is in principle appropriate, but it is likely to lead to difficult questions of delimitation. Courts could be overwhelmed with the task, and the outcome would be difficult for market participants to predict.

130 The above proposed risk matrix would be more appropriate (see paragraph 71 et seq.). The area of application and the potential danger should be key factors for classification.

131 In any case, for high-risk AI systems, a harmonised strict liability regime should be established, as is the case for motor vehicle liability. Limiting strict liability, as in the case of car owners or pets, to those AI systems with a high-risk potential will avoid over-regulation and the stifling of innovation. The proposed classification through the cumulative assessment of the area of application as an area of risk on the one hand (e.g. health care, transport, administration, etc.) and the risk potential of the application on the other hand ties in with the right criteria. Exact areas and appropriate limits with regard to the sector and the risk have to be drawn and regularly assessed in an interdisciplinary manner. Similarly, jurisprudence is constantly dealing with the state of the art and is doing a good job with the help of experts. However, this differentiation does not provide legal clarity for the developers and operators of AI. Companies would probably always have to insure AI under the risk of strict liability in order to be on the safe side in view of the wide range of applications. Therefore, strict liability for all areas in which AI is used could in principle also be considered the right regulatory approach.

132 It makes sense to consider mandatory insurance obligation, as already established for other liability regimes. For example, under the harmonised rules on motor vehicle insurance, an insurance obligation is imposed on the owner, which protects the injured party by providing a solvent counterparty (compulsory insurance) to ensure smooth processing, on the one hand, and the injuring party,

who may be exposed to particularly high claims for compensation, on the other. Neither for operators of AI nor for developers of products in general had such an insurance obligation existed at Union level so far. This should be seriously considered for high-risk applications and perhaps also for AI in general.

(3) Safety and liability regimes

133 As already mentioned, adjustments to the established legal and liability systems so far are necessary in order to address the specificities of AI.

134 Two defences arising from the PLD for the developer would have to be modified: the exceptions to the defence currently regulated in Art. 7 b) (no existence at the time when the product was put into circulation) and e) (state of the art defence) of the Product Liability Directive, should be rejected in relation to AI. Given the self-learning features of AI as well as further developments through updates it is of particular importance that the developer may be strictly liable for defects that appear after the AI-product was put on the market. It would be contradictory for an AI developer who is aware of the learning ability of his software and also consciously enables this ability to learn to waive liability for changes made after the software has been put into circulation.

135 In many cases, the developer can eliminate errors which are detected after the AI system has been put into circulation by providing software updates. Therefore, the assumption of a certain degree of contributory negligence on the part of the users is also to be welcomed if they do not carry out (security-relevant) updates within a reasonable period of time.

e) Facilitation of the burden of proof

136 The behaviour of AI is in principle very difficult or even impossible for users to understand. This is not only due to the autonomy and learning ability of such systems. By using complex techniques such as algorithms or artificial neural networks, AI systems are extremely complex even in their "basic configuration". Much remains hidden because valuable trade secrets are involved. If such systems additionally change (possibly even depending on external conditions and other, random parameters) due to their ability to learn and external influences, and thus modify their "basic configuration", this phenomenon is even intensified.

137 These circumstances make it more difficult for the injured party to prove the defect or fault, let alone a causal link. Due to the necessary expertise and analytical capacities, experts would have to be involved, which regularly leads to high costs. Such costs could deter many injured parties from asserting their claims and hinder access to justice.

138 Further problems arise due to the different possible uses of AI: If the AI-system is not marketed exclusively as software; it will regularly be used in hardware from other third party manufacturers, which in turn may have faults and cause damage on top. The identification of the cause of damage caused by AI can also be rendered more difficult by software updates or add-ins from third-party suppliers, similar to apps on smartphones. The same applies to IoT when the AI-driven system communicates with other electronic devices and even accepts commands from them, or at least shows a certain behaviour based on the communication.

139 Injured parties must be granted certain alleviations from the burden of proof with regard to the fault or defect and the causal link. Additionally, users should be granted certain access rights which would have to take effect in advance of any claim to identify the missing information. Ideally, this should only apply to those injured parties who actually face such difficulties.

140 In the case of strict liability of developers and operators of high-risk applications, which is being considered by the EU Commission, it should be sufficient for the injured party to prove that the damage occurred during the operation of the AI or the product or service interconnected with the AI, as it is the case for motor vehicle liability. The injured party should not have to prove fault, defect or causal link. Demonstrating the damage in the case of AI systems, however, should not pose particular difficulties.

141 Outside of high-risk applications, however, the existing principles of liability provisions should apply: Possible difficulties of proof should be countered with the help of so-called "logging" obligations. Developers must be obliged to record and make available the relevant data, i.e. a special form of the obligation to secure findings under product liability law. In the event that the AI-driven system does not, incorrectly or incompletely record or store this data, a reversal of the burden of proof for defect and causation should be applied at the expense of the developer.

However, in view of the on-going development, it might become difficult to store such large amounts of data in the long run.

142 In relation to users, outside high-risk applications, the injured third party should benefit from a facilitation of the burden of proof. The operator of the AI-driven system would then have to rebut his fault. No differentiation between private and professional users of AI should be made in this regard as the circumstances would be comparable.

IV. Question 4: Which single actors or groups of actors are best placed to address the risks that you identify?

143 Three different groups of actors can be identified when it comes to addressing risks in the context of AI-applications.

144 First of all, the legislator – be it on national or EU-level – should ensure that existing regulation applies to AI-systems and that regulatory gaps (such as in the case of liability further outlined in the section above) are closed and that these laws are being enforced efficiently. Lawyers, being the free and independent advisors in all legal matters, and also constituting independent organs of the administration of justice in countries such as Germany, need to play a central role in safeguarding the protection of the rule of law and the defense of fundamental human rights.

145 Secondly, quasi-state actors could be assigned certification and auditing tasks when it comes to particularly high-risk uses of AI. The advantage of quasi-governmental bodies over third parties would be that it would be more difficult for companies to rely on trade secrets or copyrights vis-à-vis them. As a result, the transparency of algorithms used in particularly critical areas would be easier to verify.

146 Thirdly, independent third-party actors could play a significant role when it comes to auditing the requirements for Trustworthy AI and assigning voluntary or compulsory labels in low-risk categories. The requirements and procedures for an AI to be labeled as trustworthy should be defined on EU level and not left to each Member State. Experience with the introduction of a label for compliance with the

requirements of the GDPR has shown that such a label is of little practical use if it is not applied unanimously throughout the EU.[36] It is therefore crucial to create uniform and clear rules on EU level when creating an EU-wide label for 'Trustworthy AI'.

V. Question 5: What situations do you know of where the use of AI applications made the effective compliance with or enforcement of applicable legislation difficult?

147 The enforcement of legislation is particularly difficult in the context of AI-based applications on social media platforms.

148 Although libel, copyright infringements and other typical online infringements are regulated on national or on EU level, many AI-based acts take place in a certain 'grey area' between lawful and unlawful conduct. As a result, monitoring compliance with these laws is particularly difficult. In addition, actors can easily hide their identity behind their applications.

149 Due to the limited regulatory possibilities in this area, it is in particular the task of the courts and lawyers to reconcile the conflicting interests. In the following, two particularly critical AI applications, namely social bots and deep fakes will be outlined. Subsequently, the major difficulties of these tools and potential solutions will be analyzed.

1. Example 1: Social bots

150 One sensitive AI tool in this context, that is neither clearly lawful nor unlawful, is the use of social bots, i.e. accounts entirely controlled by software. These accounts are critical, as they can be used to place advertisements, but also to disseminate information or disinformation. The use of such social bots has played a fundamental role in election campaigns in countries, such as the United States or Brazil, but also many smaller nations. What makes them more risk-inherent than human-controlled accounts is their ability to create the impression that a large number of users share a particular opinion and can, thus, be used as multiplicators

[36] Gasparotti, Alessandro/Harta, Lukas, Europäische Strategie zur Künstlichen Intelligenz, February 11, 2020, available at: <https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepAdhoc_Europaeische_Strategie_zur_kuenstlichen_Intelligenz/cepAdhoc_Europaeische_Strategie_zur_kuenstlichen_Intelligenz.pdf>, p. 5 [accessed on May 12, 2020].

in public opinion shaping.[37] The enforcement of law is further complicated by the fact that users of social bots can often hide their identity behind their tools.

2. Example 2: Deep fakes

151 Another highly critical AI-application on social media is that of so-called 'deep fakes'. Deep fake videos make use of deep learning techniques with the input of large samples of video images to synthesize new visual products. These are products of at least two AI algorithms, a 'generator' and a 'discriminator algorithm' which work together in an 'generative adversarial network'.[38]

152 The dangers of this technology are manifold: deep-faked news reports could target the reputation of individuals, portray false or fabricated events (e.g. a fake terrorist attack) or impact electoral campaigns. In the long run, they may be used as a catalyst to erode trust in political institutions, and to deepen polarization among social groups. Hence, the very nature of deep fakes puts fundamental rights as well as fundamental principles of liberal democracies at risk.[39]

153 These dangers become even more realistic when looking at recent studies, which suggest that people not only overestimate their ability to separate truth from falsehood, but also overestimate political news that are in line with their beliefs and discount news which are contrary to their beliefs.[40]

3. Measures to improve enforcement

a) Regulatory difficulties

154 Regulation in the area of social media is difficult in many ways:

155 Filtering and blocking of content on social media may endanger the users' individual right to access to impart information, which is included in the right to freedom of expression. On the other hand, the providers' right to freedom of expression might be affected as a result of too heavy regulation of social

---

[37] Krönke, Christoph, Social Media and Artificial Intelligence, in: Wischmeyer, Thomas/Rademacher, Timo (edt) Regulating Artificial Intelligence, Cham: Springer 2019, p. 149.
[38] Chivers*, Tom,* What do we do about deepfake videos, The Guardian, June 23, 2019, available at: <https://www.theguardian.com/technology/2019/jun/23/what-do-we-do-about-deepfake-video-ai-facebook> [accessed on May 12, 2020].
[39] Meskys, Edvinas/Liaudanskas, Aidas/Kalpokiene, Julija/Jurcys, Paulius., Regulating deep fakes: legal and ethical considerations, Journal of Intellectual Property Law and Practice 2020, 15 (1), pp. 24, 31.
[40] Ibid.

media.[41]Additionally, practices that are aimed at influencing the political debate might implicate the right to freedom of expression's inherent aim of creating an enabling environment for pluralist public debate.

156 This also raises the question of whether the main responsibility for monitoring compliance should lie with the operators of social platforms or with public prosecutors. Placing all responsibility to remove illegal content on providers bears the risk of handing off law enforcement responsibilities to private companies. The lack of meaningful and effective state oversight could also raise concerns about the rule of law.[42]

157 Furthermore, the algorithms used to detect those illegal acts are not currently able to identify ironic or critical analysis. The filtering of speech to eliminate harmful content through algorithms therefore faces a high risk of over-blocking and removing speech that is not only harmless but might contribute positively to the public debate.[43]

158 From a regulatory side, the DAV invites the Commission to consider the particularities of AI-applications when drafting the new Digital Services Act, which will introduce new liability rules for platform operators on EU level.

b) Possible ways forward

159 To improve the enforcement of existing laws in this area, the following considerations should be taken into account:

160 First of all, it should be recognized that creating new public spheres for public opinion making on social platforms cannot be prohibited per se. In fact, there is no prototype of a democratic public sphere or a fixed model of public communication. With digitization, new forms of communication have emerged and replaced its classical normative concepts.[44] Political activities on social media as such, therefore, obviously do not threaten democracy. However, combined with technology, they cannot only affect opinions, but also the integrity of due process and the rule of law.

---

[41] *Cf.* fn. 26, p. 31.
[42] Ibid.
[43] Ibid.
[44] *Cf.* fn. 37, p. 156.

161 The necessary and critical individual weighing is, therefore, not solved on the regulatory, but on the enforcement level: Here, it is particularly the task of lawyers and courts to reconcile the conflicting interests. Some AI applications, for instance, should not be covered by fundamental rights in the first place. Such an exception could be discussed, for example, with regard to providers who operate with social bots under pseudonyms and hence falsely pretend that the accounts are actually run by (a large number of) human beings. Moreover, users who conduct coordinated (mis)information campaigns on the basis of AI could also fall within this exclusion.[45]

162 In order to facilitate the enforcement of AI-based law infringements on social media, states should be encouraged to create more specialized units in public prosecution offices and courts to combat cybercrime. This could additionally produce guiding case law.

163 From a technological point of view developing tools to better filter out fake-accounts, fake-news and detect social bots should be encouraged on EU level. With regard to deep fakes, for example, neural networks could be used to detect eye blinking in the videos, which is a physiological signal of a synthesized fake video.[46] Further studies cite blockchain as a solution for the creation of tamper-proof content.[47]

164 However, technical solutions can only ever be a part of the problem solution. As the example of deep fakes shows, there will always be new inventions that present new challenges. For this reason, it is all the more important that lawyers and government agencies continue to train and educate their staff to deal with new risks. It also shows that human expertise is particularly important in difficult balancing issues. These cannot and should not be replaced by technology.

[45] *Cf.* fn. 37, p. 154.
[46] Li, Yuezun/Chang, Ming-Ching/Lyu, Siwei, In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking, 2018 IEEE International Workshop on Information Forensics and Security (WIFS), 2018, available at: <https://arxiv.org/pdf/1806.02877.pdf> [accessed on May 12, 2020].
[47] *Cf.* fn. 39, p. 30.

Bibliography:

Algorithm Watch, Automating Society – Taking Stock of Automated Decision-Making in the EU, A Report by AlgorithmWatch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations, 1st edition, January 2019, pp. 100, available at: <https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf> [accessed on May 12, 2020].

Barredo Arieta, Alejandro *et al*., Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI, Information Fusion 58, June 2020, available at: <https://doi.org/10.1016/j.inffus.2019.12.012>, p. 82 [accessed on May 12, 2020].

Buchholtz, Gabriele, Artificial Intelligence and Legal Tech: Challenges to the Rule of Law, in: Wischmeyer, Thomas/Rademacher, Timo (edt) Regulating Artificial Intelligence, Cham: Springer 2019, p. 192.

Chivers, Tom, What do we do about deepfake videos, The Guardian, June 23, 2019, available at: <https://www.theguardian.com/technology/2019/jun/23/what-do-we-do-about-deepfake-video-ai-facebook> [accessed on May 12, 2020].

Cui, Yadong, Artificial Intelligence and Judicial Modernization, Shanghai: Springer 2020, p. 26.

Datta, Anupam/Sen, Shayak/Zick, Yair, Algorithmic Transparency via Quantitative Input Influence: Theory Experiments with Learning Systems, available at: <https://www.andrew.cmu.edu/user/danupam/datta-sen-zick-oakland16.pdf>, p. 1, [accessed on May 12, 2020].

Data Ethics Commission of the Federal Government, Opinion of the Data Ethics Commission, January 22, 2020, available at: <https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.html>, p. 177 [accessed on May 12, 2020].

Djeffal, Christian, Artificial Intelligence and Public Governance Normative Guidelines for Artificial Intelligence in Government and Public Administration, in: Wischmeyer, Thomas/Rademacher, Timo (edt) Regulating Artificial Intelligence, Cham: Springer 2019, p. 281.

Enders, Peter, Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 2018, p. 721.

European Parliamentary Research Service, Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?, available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf>, p. 97 [accessed on May 12, 2020].

Feng, Zhen/Xia, Helen, China: Three Cyberspace Courts now online and open for business, October 16, 2018, available at: <https://www.jdsupra.com/legalnews/three-cyberspace-courts-now-online-and-91459> [accessed on May 12, 2020].

Gasparotti, Alessandro/Harta, Lukas, Europäische Strategie zur Künstlichen Intelligenz – Eine Bewertung des Entwurfs eines Weißbuchs der EU-Kommission zur KI, February 11, 2020, available at: <https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepAdhoc_Europaeische_Strategie_zur_kuenstlichen_Intelligenz/cepAdhoc_Europaeische_Strategie_zur_kuenstlichen_Intelligenz.pdf>, p. 5 [accessed on May 12, 2020].

Harris, Briony, Could an AI ever replace a judge in court?, July 11, 2018, available at: <https://www.worldgovernmentsummit.org/observer/articles/could-an-ai-ever-replace-a-judge-in-court> [accessed on May 12, 2020].

High Level Expert Group on Artificial Intelligence: A definition of AI: Main capabilities and disiplines, available at: < https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651 >

Hill, Caroline, 'Machine beats man' in Casecrunch lawyer challenge, Legal IT Insider, October 30, 2017, available at: <https://legaltechnology.com/machine-beats-man-in-casecrunch-lawyer-challenge/> [accessed on May 12, 2020].

Hillebrand Pohl, Jens, The Right to Be Heard in European Union Law and the International Minimum Standard- Due Process, Transparency and the Rule of Law, June 8, 2018, available at: <https://ssrn.com/abstract=3192858>, p. 3 [accessed on May 12, 2020].

iBorderCtrl, Intelligent Portable Control System, Project Presentation, available at: <https://www.iborderctrl.eu/sites/default/files/publications/iBorderCtrl%20global%20presentation%20v5.pdf> [accessed on May 12, 2020].

Krönke, Christoph, Social Media and Artificial Intelligence, in: Wischmeyer, Thomas/Rademacher, Timo (edt) Regulating Artificial Intelligence, Cham: Springer 2019, p. 149.

Li, Yuezun/Chang, Ming-Ching/Lyu, Siwei, In Ictu Oculi: Exposing AI Created Fake Videos by Detecting Eye Blinking, 2018 IEEE International Workshop on Information Forensics and Security (WIFS), 2018, available at: <https://arxiv.org/pdf/1806.02877.pdf> [accessed on May 12, 2020].

Marr, Bernard, The Future of Lawyers: Legal Tech, AI, Big Data and Online Courts, Forbes, January 17, 2020, available at: <https://www.forbes.com/sites/bernardmarr/2020/01/17/the-future-of-lawyers-legal-tech-ai-big-data-and-online-courts> [accessed on May 12, 2020].

Martini, Mario, Grundlinien Eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse, available at: <https://www.uni-speyer.de/fileadmin/Lehrstuehle/Martini/2019_Gutachten_GrundlageneinesKontrollsystemendgueltig.pdf> [accessed on May 12, 2020].

Matczak, Marcin, 10 Facts on Poland for the Consideration of the European Court of Justice, May 13, 2018, available at: <https://verfassungsblog.de/10-facts-on-poland-for-the-consideration-of-the-european-court-of-justice/>, citing Case of Daktaras v. Lithuania – Application no. 42095/98 [accessed on May 12, 2020].

Meskys, Edvinas/Liaudanskas, Aidas/Kalpokiene, Julija/Jurcys, Paulius., Regulating deep fakes: legal and ethical considerations, Journal of Intellectual Property Law and Practice 2020, 15 (1), p. 24.

Montavon, Grégoire/Binder, Alexander/Lapuschkin, Sebastian/Samek, Wojciech/Müller, Klaus-Robert, Layer-Wise Relevance Propagation: An Overview, in: Samek, Wojciech/Montavon, Grégoire/Vedaldi, Andrea/Hansen, Lars Kai/Müller, Klaus-Robert (edt) Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, Lecture Notes in Computer Science, 11700, Cham: Springer, 2019, p. 193.

Nassar, Mohamed/Salah, Khaled/ur Rehman Muhammad Habib/Svetinovic, Davoc Blockchain for explainable and trustworthy artificial intelligence, WIREs Data Mining Knowl. Discov., 10(1), October 17, 2019, available at: <https://doi.org/10.1002/widm.1340> [accessed on May 12, 2020].

Niller, Eric, Can AI Be a Fair Judge in Court? Estonia Thinks So, WIRED, March 25, 2020, available at: <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so> [accessed on May 12, 2020].

Ronsin, Xavier/Lampos, Vasileios, Appendix I – In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data, in: European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Strasbourg, CEPEJ - Commission Européene pour l'Efficacité de la Justice, 2018, available at:

<https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>, p. 42 [accessed on May 12, 2020].

Yeung, Karen, Responsibility and AI, Council of Europe Study, September 2019, available at: <https://rm.coe.int/responsability-and-ai-en/168097d9c5>, p. 21 [accessed on May 12, 2020].

Zweig, Katharina, Algorithmische Entscheidungen: Transparenz und Kontrolle, January 2019, available at: <https://www.kas.de/documents/252038/4521287/AA338+Algorithmische+Entscheidungen.pdf/533ef913-e567-987d-54c3-1906395cdb81?version=1.0&t=1548228380797>, [accessed on May 12, 2020].

Unknown Author, Mannheim testet verhaltensbasierte Videoüberwachung, Heise Online, December 3, 2018, available at: <https://www.heise.de/newsticker/meldung/Mannheim-testet-verhaltensbasierte-Videoueberwachung-4239279.html> [accessed on 12 May 2020].