4.2 Data Protection and EU-Regulation for Artificial Intelligence

Andrea Ruppert, Domenik H. Wendt

Abstract

The advancing use of modern technology in nursing care, especially the development of technical assistance systems through robotics, digitization and Artificial Intelligence (AI), can open up new opportunities for those affected. At the same time, however, the use of these technologies also carries risks for this group of people, especially for their fundamental right to informational self-determination, due to the extensive processing of personal data. This article describes the risks for data subjects and explains the current legal framework regarding the protection of personal data in the European Union. The authors conclude, that applying data protection and data security to technical assistance systems, robots and AI from the beginning not only leads to legally compliant practices but also strengthens the trust of users and society as a whole in the use of these systems.

The use of AI-based systems raises further (legal) questions that go beyond data protection and data security. The authors first address the various definitions of the term „Artificial Intelligence" in the academic literature. They then describe the European Union's various regulatory approaches to the use of AI starting with the European Commission's "Strategy for Artificial Intelligence" published in 2018, followed by the "AI White Paper" published in 2020 and ending with the European Commission's proposal for a Regulation laying down harmonised Rules on Artificial Intelligence- Artificial Intelligence Act (AIA) published in April 2021. Here, in particular, aspects of „scope", „transparency" and „impact on the healthcare sector" will be examined in more detail and the still necessary need for legal policy discussion will be highlighted.

Keywords: Artificial Intelligence (AI), data protection, data security, right to informational self-determination, EU Strategy for Artificial Intelligence, EU AI White Paper, EU Artificial Intelligence Act (AIA), scope, transparency, impact on the healthcare sector

Data Protection Requirements in the Use of Assistive Systems Involving Artificial Intelligence

Introduction

Constantly increasing life expectancy, demographic change and changing living conditions towards more single households confront modern societies with considerable challenges in the area of nursing care. People want to live self-determined in their own homes and participate in social life, even in old age or with physical limitations. The advancing use of modern technology in nursing care can open up new opportunities here. It provides a significant contribution to improving nursing care by relieving or supporting care workers and relatives and can thus improve the quality of life of all involved (Bemelmans et al., 2012, 114-120). The development of technical assistance systems using robotics, digitalisation and artificial intelligence opens up new potential here. Their use implies the extensive processing of personal data, especially those that require a very high level of protection. Sensors (camera sensors, environment-based sensors and wearable sensors including biosensors) are used to collect and process highly sensitive personal data that require special protection.

Application and Risks of Algorithms (Machine Learning/ AI) in Assistance Systems

Recent developments of assistive systems and support robots increasingly focus on adaptive algorithms that collect information, evaluate it and draw their own conclusions. The advantage is that these systems can be set up very individually to the needs of the user, the disadvantage is that at present it is probably not even clear to the programmers where this will lead (Hoeren & Niehoff, 2018, 50, 58).

By using algorithms (machine learning/AI), the behaviour of users can be predicted. Activity recognition is the core building block in many high-impact applications, ranging from health monitoring to assistive technology and elder-care. The chance to recognise and prevent dangerous activities at an early stage (Kozina et al., 2013, 13-23) is accompanied by the disadvantage that the user is constantly monitored and becomes predictable.

In addition, activity recognition carries the risk that not only the user‘s data is processed, but also data of other people who support the user, such as caregivers, doctors, etc., or people from the private environment, such as friends, relatives, neighbours, etc., which also makes these people data subjects in the sense of data protection.

The use of artificial intelligence (AI) in technical assistance systems also bears risks for the data subjects, as it requires the provision of large amounts of data (big data) (Hoeren & Niehoff, 2018, p. 47).

In order to protect the fundamental right to informational self-determination of those affected, developers and manufacturers, but also users, must observe the requirements of data protection and data security (e.g. transparency, data economy, „real“ freedom of choice). This data can be combined with personal information from other sources - including healthcare providers and pharmaceutical companies. The use of algorithmic classification systems enables profiling and discrimination based on ethnicity, age, gender, medical condition and other information, which can lead to potential harms such as discriminatory profiling, manipulative marketing, and security breaches. This affects not only individuals, but also groups and the society as a whole.

Wearable devices also play an important role in assistance systems. These small computers, which are worn on or in the body, are directly or indirectly connected to the internet, usually via a smartphone. If we look at the area of health apps, the following topics play a role: optimised diagnostics, monitoring of treatment processes, home emergency calls. The data collected by wearable devices are often sensitive, as they allow conclusions to be drawn about the state of health, movement patterns, etc.

Especially in the case of wearable devices, the transfer of sensitive personal data to third countries with inadequate data protection levels cannot be avoided, as cloud computing is usually used.

Acceptance and Data Protection

The acceptance of assisting systems and robotics in private, assistive and care contexts depends to a large extent on users‘ trust in the assisting technology and the protection of their fundamental rights and freedoms.

The data flows resulting from the use of assistance systems and robotics must be protected in terms of data protection and data security, since assistive technologies affect the (constitutionally) protected rights of those involved and enable an unhindered flow of data, e.g. the creation of personality profiles and all-round surveillance. Therefore, it must be clarified which requirements the affected users have for the protection of their private and intimate sphere when it comes to enabling or prolonging a safe and as independent as possible life in their private environment and how these individual requirements can be ensured.

Insufficient data protection and data security can increase the possibilities for data breaches and misuse. Any processing of personal data initially represents an encroachment on the rights and freedoms of the data subjects and must therefore be justified. When developing technical assistance systems using robotics, digitisation and artificial intelligence, a number of legal and ethical aspects (personal rights, data protection and data security) must therefore be taken into account, with opportunities and risks always being weighed up on a case-by-case basis.

The precondition for justifying the processing of sensitive personal data is compliance with the requirements of the General Data Protection Regulation (GDPR), the ePrivacy Directive and the Member State regulations based on them, in Germany the "Bundesdatenschutzgesetz and the sector-specific law. All processing activities must comply with the requirements of the GDPR, as required in a concentrated form by Art. 5 of the GDPR with the principles. In addition, there are in particular the requirements from Art. 25 of the GDPR on data protection through technical design and from Art. 32 of the GDPR regarding the security and resilience (see Gonscherowski, S. et al., 2018, 442) of the processing. Furthermore, a procedure for the regular review of processing activities must be implemented in accordance with Art. 32 (1) (d) of the GDPR. In concrete terms, this means that data protection and IT security management must be implemented, with which the controller implements and enforces protection and control measures.

According to Art. 6 para. 1 GDPR the principle of lawfulness requires the existence of legal grounds for the processing. In the case of sensitive personal data (special categories), processing is generally prohibited under Art. 9 para. 1 GDPR, which includes in particular the health data of persons in need of assistance, unless one of the justification grounds listed in Art. 9(2) GDPR applies. A legal basis must be determined for each processing purpose. The legal basis for the described processing activities in the private, domestic sphere is primarily consent according to Art. 6 para. 1 sentence 1 lit. A, Art. 9 para.2 lit. a GDPR.

However, according to Art. 7 GDPR, a legally valid consent to the processing of personal data must be given voluntarily and be based on sufficient information provided by the data subject. Both requirements pose major hurdles to lawfulness. On the one hand, the functioning of robots and technical assistance systems, especially if they are based on the use of artificial intelligence, are usually very complex and can usually not be explained to laypersons in the necessary appropriate depth in an understandable way. On the other hand, voluntariness is only given if the persons concerned actually have a real choice. However, it is more than questionable whether this voluntariness is still given if consent is a precondition for the use of assistance systems, which is essential for a self-determined, autonomous life and participation in social life, and otherwise no (feasible) alternatives are available, so that one can speak of a „de facto compulsion“ to use. Also, „social pressure“ from supporters from both the caregiving and family sectors, who are relieved by the use of the assistance systems, can question voluntariness.

The self-determination desired by the legislator through the importance of consent thus becomes self-disenfranchisement (Woopen, C., 2015, 4).

It is therefore necessary to apply data protection and data security to assistive systems and robots in the field of health and care from the very beginning, as this will strengthen the trust of the users and the consent necessary for the processing of the required personal data can be given without reservations.

From the perspective of data protection, the main risks for the personal data of the data subjects in the processing of data arise from the operators of the data processing systems. Therefore, the technical and organisational measures implemented there must be suitable to assure the protection of the data with regard to unauthorised processing not covered by the purpose of the processing. These measures must be carefully and comprehensibly documented in a verifiable manner (Hoeren & Niehoff, 2018, 60) so that the necessary transparency is provided and those affected by the data processing can also develop the necessary understanding and trust.

Harmonised EU-Regulation for Artificial Intelligence Ante Portas – Possible Impacts on the Healthcare sector

Introduction

The use of Artificial Intelligence (AI) is becoming real. The European Commission expects AI to improve healthcare, increase the efficiency of farming, contribute to climate change mitigation and enhance security in the European Union (EU) (European Commission, White Paper, 2020, 1). The EU has increased investments for AI-related research and innovation to € 1.5 billion, with the aim of attracting more than € 20 billion of total investments in AI per year over the next decade (European Commission, Communication, 2018, 5 f.).

Despite all the appropriate optimism, the use of AI-based systems also raises different (legal) questions (see Graf von Westphalen, BB, 2020, 1859 - impact on contract law; Graf von Westphalen, VuR, 2020, 248 - impact on product liability law valuations; Günther, InTeR, 2020, 142 - impact on the environment; Härtel, NuR, 2020, 439 - impact on sustainable agriculture; Melzer, InTeR, 2020, 145 - implications for international law; Rodenbeck, StV, 2020, 479 - implications for criminal procedure; Steege, NZV, 2021, 6 - implications for liability in transport and mobility; Wendt/Jung, ZIP, 2020, 2201, 2208 - implications for the application of contract generators; see also Möslein, RDI, 2020, 34 - guidelines for AI): What is AI and how can it be legally subsumed? Which fields are already existing for its application, and which will be added? To what extent do existing regulation take these developments into account? Do existing regulations need to be amended or do completely novel evaluations need to be found? What is the relationship between AI and, for instance, responsibility and liability? What about the protection of the users? Is there a need for European legislation or are national legal developments sufficient and efficient (see Ebers, § 3 Regulation of AI and Robotics in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 2020, § 3 paras 35 ff. and 147 ff)?

In the White Paper „On Artificial Intelligence - A European approach to excellence and trust" (AI White Paper), published on 19 February 2020, the European Commission announced a regulatory framework for AI (European Commission, White Paper, 2020, 13 ff., 16 ff). Thereby, a risk-based regulatory approach is proposed (European Commission, White Paper, 2020, 17). This approach, which is correct in essence, is not without potential for debate. Then, on 21 April 2021, the European Commission published the Proposal for a Regulation Laying down harmonised rules on artificial intelligence (so called Artificial Intelligence Act). Both drafts give good reasons to get an overview of key regulations and identify any impact on the healthcare sector.

Definition for Artificial Intelligence

There are various definitions of the term „AI" in the academic literature (overview in Kaulartz/Braegelmann, Chapter 1 Introduction in: Kaulartz/Braegelmann, Legal Handbook Artificial Intelligence and Machine Learning, 2020, 1, para. 2 ff.; Bues, Artificial Intelligence im Recht in: Hartung/Bues/Halbleib, Legal Tech - Die Digitalisierung des Rechtsmarkts, 2018, para. 1162; furthermore von Bünau, Künstliche Intelligenz im Recht in Breidenbach/Glatz, Rechtshandbuch Legal Tech, 2018, para. 5; critically Hacker, NJW, 2020, 2142, 2142 f., who would like to speak of machine learning techniques). On the one hand, they encounter the question of the meaning of „intelligence" (Armour/Eidenmüller, ZHR (183), 2019, 169, 172; Guggenberger, NVwZ, 2019, 844, 845; Herberger, NJW, 2018, 2825, 2826 f). On the other hand, they are subject to the dynamics of technological progress. Any attempt to define AI is therefore required to describe the boundaries of „not yet" AI and „no more" AI in a carefully and well considered way.

The fact that it is not a simple matter is shown, for example, by the development of the definition used by the European Commission. According to the European Commission, AI initially referred to

> „systems that display intelligent behavior by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" (European Commission, Communication, 2018, 1).

According to this broad understanding, AI-based systems

> „can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)" (European Commission, Communication, 2018, 1).

The High-Level Expert Group on Artificial Intelligence (AI HLEG), set up by the European Commission, developed this definition further and updated it. Accordingly, AI systems are

> „software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions" (AI HLEG, Definition of Artificial Intelligence, 2018, p. 6)

This rather technical and no doubt detailed definition may seem bulky. However, it has the advantage that is does not contain vague legal terms, such as „intelligent behaviour", „some degree of autonomy" or „specific goals". Furthermore, it enables objective links (Wendt/Jung LR, 2021, 34, 37). Admittedly, the term „best action(s) to take" gives interesting room for interpretation.

In the Proposal for a Regulation laying down harmonised Rules on Artificial Intelligence - Artificial Intelligence Act (AIA) one can find the following definition:

> “artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.”

The different definitions show how challenging it is to design a precise legal definition for AI. Linking a definition to an annex risks shifting the challenge rather than solving it.

Nevertheless, it is helpful to distinguish between weak and strong AI. Weak AI refers to systems that are intended to support humans in achieving their goals as intelligently as possible regarding concrete issues (Kaulartz/Braegelmann, Kapitel 1 Einführung in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, 4). Strong AI, on the other hand, is supposed to acquire or surpass the intellectual skills of humans and thus be able to replace human action (Niederée/Neidl, Teil I., § 2 Technische Grundlagen der KI in: Ebers/Heinze/Krügel/Stienrötter, Künstliche Intelligenz und Robotik, 2020, para 2, Rz. 1) Rz. 2; Pils/Rektorschek, Teil 3., § 24 Industrie in: Ebers/Heinze/Krügel/Stienrötter, Künstliche Intelligenz und Robotik, 2020, Rz. 2, m.w.N.). Taking such a differentiating view as a basis, the use of weak AI should, at least in the medium term, primarily be included in the debates on „best action(s) to take“.

AI Strategy and AI White Paper of the European Commission

AI Strategy

The starting point for the current European regulatory proposals is the European Commission’s strategy for AI (AI Strategy), published in April 2018 (European Commission, Communication, COM(2018) 237 final, 3). Following on from this, it presented a coordinated European plan on AI in December 2018, which will run until 2027 (European Commission, Communication, COM(2018) 795 final). Here, the European Commission stated that a sufficiently flexible regulatory framework for AI was needed both to promote innovation and to ensure high levels of protection and safety (European Commission, Communication, COM(2018) 795 final, 7 f. or section 2.6 „Developing ethics guidelines with a global perspective and ensuring an innovation friendly legal framework"). It also announced AI ethics guidelines. These were initially published as a draft by the AI HLEG on 18 December 2018 (see AI HLEG, Draft Ethics Guideline 2018; cf. on this Dettling/Krüger, MMR, 2019, 211) and revised after an open consultation in April 2019 (AI HLEG, Ethics Guidelines, 2019; see Groß, CB, 2020, 155). In addition, the new European Commission President von der Leyen announced in her political guidelines that she would put forward legislation for a coordinated European approach on the human and ethical implications of AI within her first 100 days in office (von der Leyen, Agenda, 2019, 13).

AI White Paper

In the AI White Paper published on 19 February 2020, the European Commission states that, in addition to non-binding guidelines of the AI HLEG, a clear regulatory framework for Europe could build consumer and business confidence in AI and thereby accelerate its uptake (European Commission, White Paper, 2020, 13 ff.). In this sense, the existing EU legislation applicable to AI-based systems should be reviewed for necessary adjustments, such as the EU product safety legislation. In addition, the European Commission believes that a new EU regulatory framework would be needed. A key issue hereby would be the definition of the scope of application by means of a precise and flexible definition of AI.

In order to establish an „effective" and „excessively prescriptive" new EU regulatory framework, the AI White Paper envisages a risk-based regulatory approach. This is also intended to protect small and medium-sized enterprises (SMEs) from disproportionate burdens (European Commission, White Paper, 2020, 17).

This risk-based regulatory approach provides for a categorisation of AI applications. This categorisation shall measure whether the use of an AI application offers a high-risk potential or not. The relevant criteria should be whether the sector and the intended use bear significant risks (in particular from the point of view of safety, consumer rights and fundamental rights).

Specifically, an AI application should fall under the „high-risk" category if it meets both of the following criteria:

- Sector: The AI application is used in a sector in which significant risks are to be expected due to the nature of the typical activities, i.e. the occurrence of risks is generally most likely.
- Use: The AI application is used in the sector in such a many that significant risks are likely to be expected.

According to the European Commission, high-risk sectors are, e.g. healthcare. Of course, not every AI application in this sector is necessarily associated with significant risks. For example, a flaw in an appointment system used in the healthcare sector is not necessarily significantly risky. Therefore, it must also be considered whether risks are associated with the specific use of the AI application. In order to assess the level of risk, the European Commission proposes to consider the impacts on the parties affected. Moreover, it does not exclude that there could also be AI applications that are to be classified as high-risky as such, regardless of the sector concerned.

Furthermore, the European Commission proposes requirements for high-risk AI applications. They could consist of training data, data and record-keeping, information to be provided, robustness and accuracy, and human supervision. In addition, specific requirements are intended for certain AI applications, such as remote biometric identification based on AI (European Commission, White Paper, 2020, 17).

To label AI applications not qualifying as high-risk, the European Commission further proposes a voluntary labelling. Economic operators could use it to indicate that their AI-based products and services meet harmonised EU-wide benchmarks that go beyond the basic legal obligations. This should increase trust and acceptance in AI systems (European Commission, White Paper, 2020, 24).

Proposal for the European "Artificial Intelligence Act"

Overview

On 22 April 2021 the European Commission published the Proposal for a Regulation laying down harmonised Rules on Artificial Intelligence - Artificial Intelligence Act (AIA). This is the first complete legislative proposal to regulate AI within the EU. The importance should therefore not be underestimated. The proposal is already considered to be of global significance because it can be an important orientation for further proposals.

The AIA provides harmonised rules for the development, placing on the market and use of AI systems in the EU. The rules are proportionate to the risks. The AIA includes a risk methodology to classify high-risk AI systems. These are systems that pose significant risks to the health and safety or fundamental rights of individuals. For these AI systems, the AIA regulates horizontal requirements and a conformity assessment procedure.

Scope and Definitions

Art. 1 AIA contains the subject matter of the proposes regulation and fixes the scope. In Art. 2 AIA one can find the definitions that will be used throughout the regulation, for example the definition for AI systems. Aim of this definition is to be as technology-neutral and future-proof as possible. The rules in Artt. 1- 3 AIA are linked to an Annex I (Art. 4 AIA). This Annex I details concepts and techniques for AI development. It can be adapted by the European Commission as new technological developments arise. As noted above, linking scope provisions or essential definitions with an annex risks shifting the challenge rather than solving it.

Art. 5 AIA contains a list of prohibited AI practices. This is part of the risk-based approach. This approach distinguishes between applications of AI that pose unacceptable risks, high risks and low or minimal risk. The list of prohibited practices includes all AI systems that are deemed unacceptable because they violate EU values, such as fundamental rights.

Artt. 6 - 51 AIA contains specific provisions for AI systems that pose a high risk to the health and safety or fundamental rights of natural persons. Those high-risk AI systems are allowed on the EU market if they comply with certain mandatory requirements. Classification as a high-risk AI system is based on the intended purpose of the AI system according to existing EU product safety regulations. As already contemplated in AI White paper, classification as a high-risk AI system depends not only on the function of this system, but also on its specific purpose and application modalities.

Transparency

The AIA proposal claims to meet the demands of the European Council to promote AI on condition that a high level of data protection, digital rights and ethical standards are guaranteed. Art. 5 AIA explicitly prohibits manipulative or exploitative practices with respect to children or disabled persons. With regard to other groups of persons, reference is made to the existing possibilities for protection such as data protection or consumer protection, since these grant a right to appropriate information on the basis of which the data subjects have the possibility to reject practices that enable manipulation or profiling (Art. 13 AIA, Explanatory Memorandum, 5.2.2.). In this respect, the principle of transparency already implemented in the GDPR is continued.

According to Art. 52 AIA, there shall be transparency obligations for systems that are used, for example, to interact with people for the recognition of emotions or their classification into (social) groups on the basis of biometric data. The resulting information obligations are intended to enable data subjects to make informed decisions regarding their use.

The resulting problems with regard to true voluntariness of consent will remain in this respect. It would be important that these regulations are not weakened in the further development process of the regulation, but strengthened overall.

Impact on the Healthcare Sector

In recital 28 of the AIA, the European Commission states that AI systems could have a negative impact on the health and safety of individuals, especially when such systems are used as components of products . Explicitly addressed are increasingly autonomous robots, whether in manufacturing or personal assistance and care. They should be able to operate safely and perform their functions in complex environments. Similarly, diagnostic systems and human decision support systems should be reliable and accurate in the healthcare sector, where risks to life and limb are particularly high.

Assistance systems that use AI carry significant risks for the rights of data subjects, for example due to non-transparent algorithms. The AIA seeks to regulate these through appropriate legislative measures in such a way that the advantage generated by the AI system can be used without entailing excessive risks for the data subjects. This also applies in particular to biometric identification systems or AI decision-making systems used in technical assistance systems in the care or healthcare sector. The AIA aims to strike an appropriate balance here between the interests of users in the protection of their fundamental rights and the security of their data and the interests of industry in the development and introduction of AI.

Even though the legislative process of the AIA will certainly take several more years and the regulations that will ultimately apply cannot yet be predicted with certainty, developers of technical assistance systems with artificial intelligence should already take the requirements of the proposal into account now, as it will certainly lead to a ban on certain AI systems.

Conclusion

The use of AI-based systems raises a number of interesting legal questions. The starting point is the question of a suitable definition of AI. The definition developed by the AI HLEG dispenses with uncertain legal terms such as „intelligent behaviour“, „with some degree of autonomy“ and „specific goals“ and thus enables objective links. However, the term „best action(s) to take“ in particular offers room for interpretation that cannot be easily filled. At least in the medium term, it seems worth considering taking greater account of the common differentiation between so-called strong and weak AI in legal issues as well.

The AI Strategy, initiated by the European Commission, shows a thoroughly optimistic picture of the benefits of AI-based developments. The associated investments are considerable.

The AI White Paper lays a solid foundation for legislative initiatives. The intended risk-based regulatory approach is basically convincing. The classification into criteria provided for this purpose should serve legal certainty. The proposed link to the sector on the one hand and the concrete use on the other hand leads to the expectation of an accurate classification for a large number of AI applications.

The AIA shows good approaches for a necessary regulation of AI. The aspects of „scope“, „transparency“ and „impact on the healthcare sector“ considered here show that there is a need for a legal policy discussion.

References

Armour, J., Eidenmüller H. (2019): Selbstfahrende Kapitalgesellschaften? Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht, ZHR 183, 169 – 189.

Bemelmans, R., Gelderblom, G. J., Jonker, P. and de Witte, L. (2012): Socially Assistive Robots in Elderly Care: A Systematic Review into Effects and Effectiveness. Journal of the American Medical Directors Association 13, 2 (2012), 114 – 120.e1. https://doi.org/10.1016/j.jamda.2010.10.002, zitiert nach Pascher, M.; Baumeister, A.; Klein, B.; Schneegass, S.; Gerken, J. (2019) Little Helper: A multi-robot system in home healthcare environments. In: Proceedings of International workshop on Human-Drone

Interaction a spart oft he Conference on Human Factors in Computing Systems (iHDI´19)

Breidenbach, S., Glatz, F. (2021): Rechtshandbuch Legal Tech, 2. ed.

Dettling, H.-U., Krüger, S. (2019): Erste Schritte im Rechts der Künstlichen Intelligenz – Entwurf der „Ethik-Leitlinien für eine vertrauenswürdige KI. Zeitschrift für IT-Recht und Recht der Digitalisierung MMR, 211 – 217 (2019).

Ebers, M., Heinze, C., Krügel, T., Steinrötter, B. (2020): Rechtshandbuch Künstliche Intelligenz und Robotik.

Gonscherowski, S., Hansen, M. & Rost, M. (2018): Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung. Datenschutz und Datensicherheit DuD 42, 442 – 446 (2018). https://doi.org/10.1007/s11623-018-0976-3

Graf von Westphalen, F. (2020): Definition der Künstlichen Intelligenz in der Kommissionsmitteilung COM (2020) 64 final – Auswirkungen auf das Vertragsrecht. BetriebsBerater BB, 1859 – 1865 (2020)

Graf von Westphalen, F. (2020); Produkthaftungsrechtliche Erwägungen beim Versagen Künstlicher Intelligenz (KI) unter Beachtung der Mitteilung der Kommission COM(2020) 64 final. Verbraucher und Recht VuR, 248 – 256 (2020)

Groß, J. (2020): Braucht Künstliche Intelligenz Ethik? Compliance-Berater CB, 155 – 159 (2020)

Guggenberger, L. (2019): Einsatz künstlicher Intelligenz in der Verwaltung. Neue Zeitschrift für Verwaltungsrecht NVwZ, 844 – 850 (2019)

Günther, M. (2020): Umwelt 4.0 – Künstliche Intelligenz für eine saubere und Gesunde Luft? Zeitschrift für Innovations- und Technikrecht InTeR 2020, 142 – 145 (2020)

Hacker, P. (2020): Europäische und nationale Regulierung von Künstlicher Intelligenz. Neue Juristische Wochenschrift NJW, 2142 – 2147 (2020)

Hartung, M., Bues, M.-M., Halbleib, G. (2018): Legal Tech- Die Digitalisierung des Rechtsmarkts

Härtel, I. (2020), Künstliche Intelligenz in der nachhaltigen Landwirtschaft – Datenrechte und Haftungsregime, Natur und Recht NuR, 439 – 453 (2020)

Herberger, M. (2018): „Künstliche Intelligenz“ und Recht – Ein Orientierungsversuch, Neue Juristischen Wochenschrift NJW, 2825 – 2829 (2018)

Hoeren, T., Niehoff, M. (2018): KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen. RW Rechtswissenschaft, 47-66. https://doi.org/10.5771/1868-8098-2018-1-47

Kaulartz, M./Braegelmann, T. (2020): Rechtshandbuch Artificial Intelligence und Machine Learning, 2020

Kozina, S., Gjoreski, H., Gams, M. and Luˇstrek, M. (2013): Efficient activity recognition and fall detection using accelerometers, in Evaluating AAL Systems Through Competitive Benchmarking, Springer, 13 – 23

Melzer, J. (2020): Auswirkungen von Künstlicher Intelligenz auf Völkerrecht. Zeitschrift für Innovations- und Technikrecht, InTeR, 145 – 150 (2020)

Möslein, F. (2020): Die normative Kraft des Ethischen - Ein Fallbeispiel zur Effektivität von Leitlinien für Künstliche Intelligenz. Recht Digital, RDI, 34 – 41

Rodenbeck, J. (2020), Lügendetektor 2.0- Der Einsatz von Künstlicher Intelligenz zur Aufdeckung bewusst unwahrer Aussagen im Strafverfahren. Strafverteidiger, StV 2020, 479 – 483 (2020)

Steege, H. (2021): Auswirkungen von künstlicher Intelligenz auf die Produzentenhaftung in Verkehr und Mobilität. Neue Zeitschrift für Verkehrsrecht, NZV, 6 – 13 (2021)

Wendt, D., Jung, C. (2020), Rechtsrahmen für Legal Technologie. Zeitschrift für Wirtschaftsrecht ZIP, 2201 – 2210 (2020)

Wendt, D., Jung, C. (2021), Europäischer Rechtsrahmen für Künstliche Intelligenz (Teil I) – Risikobasierte Regulierungsansatz und technologische Anwendungen im Rechtsverkehr. LEGAL REVOLUTIONary, LR, 34 – 41 (2021)

Woopen, C., Die Vermessung des Menschen – Big Data und Gesundheit. Jahrestagung des Deutschen Ethikrats (21. Mai 2015), 4

References (European Union/Politics)

AI HLEG, DRAFT ETHICS GUIDELINES FOR TRUSTWORTHY AI: Working Document for stakeholders' consultation, 18 December 2018
(AI HLEG, Draft Ethics Guidelines, 2018)

AI HLEG, A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines, 18. December 2018
(AI HLEG, Definition of Artificial Intelligence, 2019)

AI HLEG, ETHICS GUIDELINES FOR TRUSTWORTHY AI, 8 April 2019
(AI HLEG, Ethics Guidelines, 2019)

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Artificial Intelligence for Europe, 25.4.2018, COM(2018) 237 final
(European Commission, Communication, COM(2018) 237 final)

European Commission, WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust, 19.2.2020, COM(2020) 65 final
(European Commission, White Paper, 2020)

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, 22 April 2021, COM(2021) 206

von der Leyen, A Union that strives for more: My agenda for Europe: POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024
(von der Leyen, Agenda, 2019)