Trusted Artificial Intelligence: On the Use of Private Data

Norbert Jastroch

Trusted Artificial Intelligence: On the Use of Private Data

Norbert Jastroch
MET Communications, 61352 Bad Homburg, Germany
norbert.jastroch@metcommunications.de

Abstract. Artificial Intelligence has come into focus anew in the context of digitization and global competition. So has the tension between human ethics, regulation, and the potential gains this technology field offers for economic and societal progress. This paper is intended to contribute to the ongoing debate about opportunities and uncertainties in particular with respect to the use of private data in AI. We discuss the status of AI outcomes in terms of their validity, and of AI input as to the quality of data. In a first order approach we distinguish between the commercial, public, industrial, and scientific data spheres of AI systems. We resume the ethical and regulative approaches to the utilization and protection of massive private data for AI. Regarding the currently favoured ways of organizing the collection and protection of data we refer to respective ruling and denominate distributed ledger systems and open data spaces as functional means. We conclude by arguing that governing data privacy and quality by distinguishing different AI data spheres will enable a reasonable balance of these two aspects.

Keywords: Artificial Intelligence, Data Privacy, Data Quality, Ethics, Regulation, Open Data Spaces.

1 Introduction

While the concept of Artificial Intelligence has been introduced into the technological evolution decades ago already, it has gained novel interest by taking up recent developments in the context of the digital revolution. Significant progress in computing power and communication technology, in advanced sensor capabilities, and in large scale data generation and distribution drive research into and the application of systems incorporating hardware, software and data for the purpose of automated information analysis and synthesis. In particular, systems that allow for software controled decision making leading to the automated performance of related action are gaining focus attention. Such systems are currently highly promoted worldwide, and the term Artificial Intelligence has become a widely used label, comprising a variety of concepts like data reasoning, robotics, and machine learning, to name a few. In [5] the AI HLEG provide a comprehensive description and suggest a sound definition of

Artificial Intelligence (AI). For reasons of methodological clarity, and to avoid the vagueness that is often inherent to the talking about Artificial Intelligence, we employ this terminology.

Artificial Intelligence is expected to offer new and powerful economic potential, contribute to scientific progress, and support sustainable societal development. In the wider context of digitization, Körner et al [12] present a discussion of chances and fears that go with the economic and socio-economic consequences as far as these can be foreseen from today's perspective. Körner [13] also takes a look onto societal implications and political challenges, where, on a global scale, various and sometimes conflicting systems of constitutional principles create significant differences in the uptake of AI, hence in potential opportunities and threats related with its application.

Intrinsic to AI is the lack of transparency this technology bears not only for those lacking the required technical expertise, but also for those who make use of it or have to deal with its implications. Embedded algorithmic reasoning can produce unforeseeable results and lead to unexpected action, as could be observed in various examples. In the economic sphere, however, the proprietary character of algorithms is often considered a crucial competitive element, hence the interest in transparency is limited. Trustworthiness of AI applications, nevertheless, is regarded an essential requirement to ensure acceptance of AI systems which, in turn, impacts their successful implementation. The European Commission therefore has put transparency on a prominent place in the list of ethical principles to address in AI [6]. But there are far more ethical reflections needed. With respect to the use of data in AI, Floridi and Taddeo [4] suggest 'data ethics' as a comprehensive approach to understand ethical implications that come with the combination of hardware, software and data, as is the case in applied AI.

The availability of data is fundamental to successful utilization of AI. Data is often called the new resource, the novel raw material of the economy in the digital age. In the industrial field, the use and flow of data are core features of digitized applications. Manufacturing intelligence, under the headline of e.g. Industry 4.0 or Smart Manufacturing, has become subject to research and development programs throughout the world [19], and may to certain extent be subsumed under the concept of artificial intelligence. In a wider context, Wellsandt et al [21] identified characteristics of information and data feedback in product development and product lifecycle management. While the quantity of data to be processed in these industrial applications rises, the quality of data is getting higher attention as a key feature of their relevance. With focus on product lifecycle management, Wuest et al [22] suggested an approach to the analysis of information quality in the context of a specific production process, based upon a framework of fifteen dimensions of information quality.

The prominent role of data and information is valid likewise in the field of public administration, as well as in science. While most of these data originate from the private sphere of individuals here, need is there to reflect upon the use of data and the limitations that must be addressed. It is out of the scope of this paper to present a deep and comprehensive investigation of the related questions for all fields or AI applications. We therefore focus, in the following, on basic reflections, with a look on specific sectors like e. g. health only to exemplify particular consideration.

First question we address, in chapter 2, is the status of the outcome AI systems generate when they use empirical data as their input. In chapter 3 we discuss the utilization of massive data for applied AI for commercial, administrative, industrial, or scientific purposes. An overview of principles intended to govern the use of private data follows in chapter 4. Then we present promising approaches for the collection and protection of private data from a technical perspective in chapter 5, and end up with the formulation of concluding remarks, chapter 6.

2 Pattern Recognition, Data Reasoning and Knowledge Generation

Beyond the question of what intelligence does mean and if it is valid to attribute this concept to an artificial device, there are two aspects that call for clarification of the status of AI systems' output. These are machine learning, and automated decision making and action taking. The AI HLEG [5] provided comprehensive specifications of both these we are using as reference.

Be it robotics, big data applications, or sensor driven actuation, AI systems typically work with empirical or statistical data as their input. These are processed by embedded algorithms to detect patterns of interest (that are also used to advance the experience base of the system) and suggest or initiate a certain decision or action, according to predefined goals. While in human intelligence these mental processes involve evaluative attributes like 'good' or 'right', and include deductive assessments of theoretical nature, these are missing in artificial intelligence systems. Results generated by an AI application are correlation based and have an empirical status. They do not comply with the scientific concept of epistemics. The term machine learning, however, suggests that an AI system generates a kind of knowledge. While, from a functional point of view, it may be reasonable to talk about AI in these terms, one must bear in mind that a specific dimension of knowledge is meant (compare also [9], and for a more detailed discussion with regard to the medical sector, compare [15]). In [10] we have made explicit different dimensions of knowledge and discussed some implications for their externalization and internalization. It is essential, however, to consider the special status of AI generated 'knowledge' if it is to be used for scientific purposes or in scientific theory. AI systems produce probabilistic results. Epistemics calls for cause-effect analyses and deductive syntheses[1].

In pointing out this distinction, attention is drawn to the issue of reliability of applied AI, with regard to both input data and output decision or action. This issue is a principal, not a gradual one. E.g., facial recognition delivers probabilistic identification of a person, with probabilistic matching getting better, the higher the number of

1 As an illustration of this distinction, think of a right-angled triangle. An AI system may well be able to recognize that every triangle it has analyzed where the square over the longest side and the sum of the squares over the two other sides are equal is right angled, and vice versa. And it may reason that this is the case with a new triangle it comes across with. But it will not be able to deduce, formulate and prove that this equivalence is true in general for any triangle - what the ancient hellenic mathematicians successfully did.

measured parameters is – but the matching remains probabilistic. This implies the possibility of false-positive as well as false-negative identification. If such a technique is integrated into an application that enacts a pre-defined action, it bears the principal risk of error. This risk of error is problematic (the more, the higher the impact of the action is), as the question of responsibility is an open issue. Here again, the AI HLEG's Guidelines [6] offer some helpful orientation. What remains, though, is the fundamental dependence of AI systems on the quality not only of their algorithms, but in particular of their data used.

The reflections made in this chapter advise to differentiate the level of data quality that is held sufficient for an AI application in accordance with the status of the application. The following chapter is intended to shed some more light on this.

3 Utilizing Massive Data

At the current stage of development in AI, frequently no real distinction of AI and, say smart IT systems, or digitization, is made. Any attempt to specify distinguishing features must relate to the machine learning aspects of an AI system, which lie basically in the dynamics of the empirical data used, expanded throughout operation by feeding in more input data and by the use of former patterns as the experience base for the generation of improved patterns. In [9] we provided an illustration of the learning process from data to information to knowledge to competence, in a general sense, the principles of which are also applicable to the special case of AI.

Hence there are two aspects of central relevance: the elicitation of new input data and the algorithms for pattern detection and generation. Both aspects contribute to the added value to be realized by an AI application and are fundamental to the innovative potential of AI. In this paper, focus is on the input data aspect, the one affecting individuals and institutions more or less directly and therefore being subject to a wide public debate about chances and risks. We leave the investigation into and discussion of the functional algorithmic aspect to further work.

3.1 Data as Knowledge Objects

Data, understood as the formal representation of quantitative or qualitative features of a something that is knowledgeable, is basically not free of intentionality, nor of context.[2] Referring to an analysis provided in [11], we consider data a knowledge object, as such made of the core content, fixed in its syntax and semantics, and embedded in an environment of aspects useful for abstraction, translation, and interpretation (exhibit 1). Such aspects are *glossary*, providing semantic support by clarifying terms used, *notation*, providing information regarding syntax and structure employed, and

2 A terminological clarification can be drawn from the example of the in-flight collection of weather data by aircraft: *data* measured are e.g. temperature, time, and location; their linking provides *information* regarding the atmospheric state at a specific point in space and time; feeding multiple of such empirical objects into an appropriate 'weather application' delivers *information* about the meteorological processes in the atmosphere we call weather. All this is *knowledgeable*, i.e. can be internalized by one's mind.

purpose and *view,* standing for the observational perspective. They also include reference to specific conceptual domains, like *ontologies*, and to systemic abstractions, like process *models.*

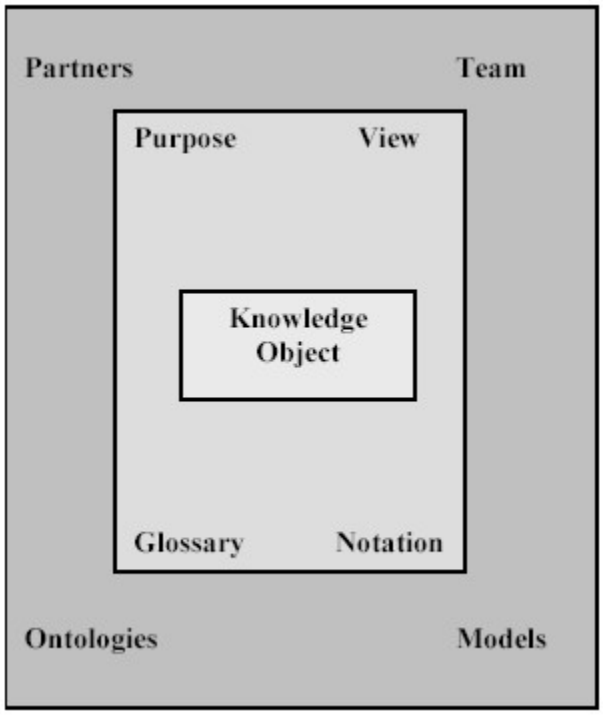

Exhibit 1: Data as contextual knowledge objects (Source: [11])

Meaningful data hence has to be considered bound to such aspects. In fact, e.g. location data is, as to its meaning, tied to the specification – be that explicit, or implicit – of these aspects. That makes what we call Data Spheres. In the example of in-flight weather data collection, location data of the measuring sensor will be GPS coordinates including height. In the context of intelligent manufacturing, location data of a part to be used in the production process will be some warehouse specification. In the case of public traffic management, it will be GPS data of vehicles (eventually enriched by data from the measurement of distance to other vehicles, when we think of assisted driving). For commercial purposes, location data will involve GPS coordinates, or cell identification of a smart phone.

The concept of data spheres described so far is similar to that of data spaces for e.g. certain industries, which are subject to a number of initiatives currently, while it is of lower level of specifity. It is useful, though, as it allows for the investigation and evaluation of data quality and likewise of data privacy interference issues.

3.2 Data Spheres

Data used as input to AI systems originate from different sources and are used within various spheres. For our considerations here, we take four major spheres into view that are predominant in the current discourse on AI: commercial, industrial, public, and scientific (exhibit 2), to be distinguished by the specifics of the aspects denominated in 3.1 above. They may be exemplified as follows:

Commercial: Platform businesses, social media

Industrial: Internet of things, Industry 4.0, robotics

Public: Traffic and mobility, administration and security

Scientific: Health and medicine, field research

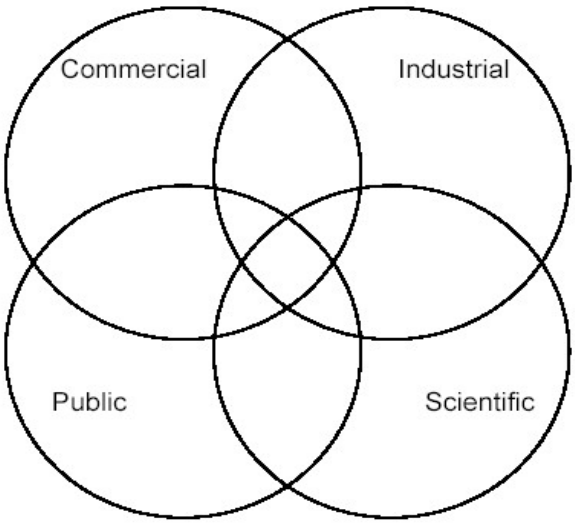

Exhibit 2: Major data spheres relevant to AI applications

These spheres are obviously not mutually exclusive but overlapping. Their distinction enables separate perspectives with regard to the collection and utilization of data in terms of quality and privacy.

3.2.1 Commercial

Main purpose of data utilization here is to influence individual behaviour, in particular buying behaviour. The concept behind is targeted advertising. Massive data collection enables the detection of preference patterns which in turn are used to generate personalized advertisement. Web based platforms for this business model of digital

commerce have two functional elements: Collecting private data of users and addressing individuals by personalized advertisement and product offers. As the correlation of private attributes of users and certain product preferences is stronger, the more information about the user is available, there is the clear interest of platform business operators to dig for as much private user data as possible. Personalization, on the other hand, creates individual information spaces for users, by setting the information focus while excluding other information that is assumed to be of no interest to the user. These functions are basically in-transparent for users.

3.2.2 Industrial

Within the concept of digitization, the relevance of data for the industry, in particular manufacturing, lies in the optimization of processes, where optimization includes both the automization, especially machine-to-machine linking, and flexibilization, in essence on demand production. Control of these processes requires high quality of data in terms of reliability and precision. Sensors must provide data with adequate precision, and the communication with actuators has to be robust and reliable. This calls for high functional quality of the technical devices applied, including software as in AI systems. In the context of connected processes between different sites or enterprises, privacy and sovereignty of data becomes an issue of conflicting interest, as it is a competitive element in general and, in particular, can have significant value as potential input to machine learning in AI applications.

3.2.3 Public

The public sphere, where public administration plays the leading role, comprises the control of traffic on land, air and water, the organization of public services including democratic procedures, and the societal aspects of security and safety. Apparently, constitutional principles and government practices differ to a large extent between nations. So does the availability of private data in established administrative structures and the collection of such data by surveillance of public and private life. AI applications like facial recognition, automated traffic surveillance and control, or personalized political influencing mechanisms can be very powerful means of effective governance. And they are the more powerful in realizing the potentials in these areas, if they are implemented on a massive scale, and intrude the private sphere of citizens deeply. Data privacy then tends to dissolve in favour of data quality.

3.2.4 Scientific

Science, as mentioned in chapter 2 above, is founded in agreed methodological principles that are bound to guarantee validity of insights in a general sense, invariant to specific settings or a select empirical base. Nevertheless, many hypotheses in science are initially generated from empirical data and then made subject to methodological investigation aiming at epistemically valid results. AI can definitely be a worthwhile source for the detection of data patterns that allow for the formulation of research hypotheses. Their relevance must be expected to depend on the quality of input data. Hence the need for high quality of data on the one hand. On the other hand, the worth of input data ideally is independent from its being anonymous or attributed to person-

al or private features. The latter holds true even if data used for scientific purposes in this sense may be most private, personal data, as is the case e.g. in medicine or the health sector. Car et al [2] investigated examples of the use of big data studies to stimulate medical research. They concluded taking a positive position, while remaining concerned about ethical issues like interference with data privacy.

4 Data Privacy, Ethics and Regulation

The utilization of massive data affects both data privacy, the origin of data, and data sovereignty, the control of data. These are subject to a wide discourse addressing the tension between individual rights and economic (or public) interest. Not surprisingly, there is no globally agreed concept of their balancing. Moreover, even the assessment of risks and chances are disputed, although it is clear the potential impact of the novel technology AI will not be constrained regionally but have its effects globally. The lines of conflict appear similar to those showing up in other fields, like genomics and bioengineering, or climate change and action, to name two prominent ones only. The question therefore is how to approach this dilemma adequately.

Europe, more precisely the EU, have chosen to develop their position from start on by taking into consideration ethical principles, societal values, and regulative means. The High Level Expert Group on AI, set in charge by the European Commission, elaborated on Ethical Guidelines for Trustworthy AI and presented their final report early 2019 [6]. Therein four principles are stated which developers, deployers, users, and regulators should follow in order to uphold the purpose of human-centric and trustworthy AI. These are the principles of respect for human autonomy, prevention of harm, fairness, and explicability [6, page 12 ff]. They are intended to build an ethical fundament for AI that is aimed to guarantee this new technological field to be trustworthy. Like the Oviedo Convention for the Protection of Human Rights and Dignity in the Biomedical field, the ethical guidelines for AI are an ambitious attempt to set limits to what shall be done in research (and development) into a technology which is bound to entail transformations of potentially deep impact to human lives and societal constituencies.

While it is far from being likely that these guidelines will become globally accepted easily, they contribute to the debate about ethics and regulation of AI as opposed to innovation and competitiveness. Consensus is that regulation is contrafactual to innovation. The question comes down to how far regulation goes. The central problem, that of the balance between regulation and innovation in AI, appears to be one of different perspectives, the economic versus the societal one. This is similar to a problem discussed in [17] on the subject of organ donation. The issue there in the context of organ allocation for transplantation is that of fundamentally diverging perspectives which make a specific question unresolvable in a general sense. The argument is that instead of trying to force obligatory political decision, it is more promising to organize an institutionalized permanent ethical reflection on the subject under consideration. Taking such an approach and transferring it to the problem of balancing regulation and innovation in the field of AI offers a way how to deal with the fundamental

perspective differences here. Floridi [3] suggests a likewise approach when he distinguishes soft and hard ethics, putting focus on the implications of a soft ethical perspective.

With a view on the current state of AI in general, and of the utilization of private data in particular, one can expect these issues to remain disputed. Nevertheless, need is there to set standards proactively in order to ensure the basic principles of human autonomy and the prevention of harm will be kept (cf. Floridi [3], and the comprehensive discussion by Morley et al regarding the health sector in [16]). Having put in place the General Data Protection Regulation GDPR, Europe took such an important step after a long public debate. As AI technology evolves, adjustments may follow. These should well be addressing various spheres by different levels of regulation, taking into account considerations like those made in chapter 3 above.

5 Organizing the Collection and Protection of Private Data

The relevance of massive data for AI applications is uncontested. E.g. platform businesses realize a major part of their value creation by collecting data from their users and analyzing these with respect to individual preferences. These can be used for commercial purposes like personalized advertising, but also for other ways of influencing individual behaviour or opinion. Facial recognition, another example, produces more reliable results, the larger the quantity of data in the experience base is. The nature of these data is private, their collection and utilization interfere with data privacy. These are examples from the commercial resp. public sphere, where probabilistic results generated by AI algorithms in general are sufficient. Hence these spheres allow for lower data quality without having to accept low validity of the results.

In the industrial or scientific sphere, the need for highly reliable data is much more relevant. This is immediately evident for applications regarding the autonomous car which are frequently subsumed to AI. A number of examples in the recent past have revealed the consequences of deficient input data, which caused fatal dysfunctionalities, affected severely the acceptance of these applications in the public opinion, and had significant impact on the economic assessment of R&D in this sector. Science, as is easy to understand, needs even higher quality of data as useful input e.g. to systems in the medical, pharmaceutical, or, generally, the health sector. For these spheres, in most cases it is feasible to use anonymous input data, what keeps the interference with data privacy on a low level.

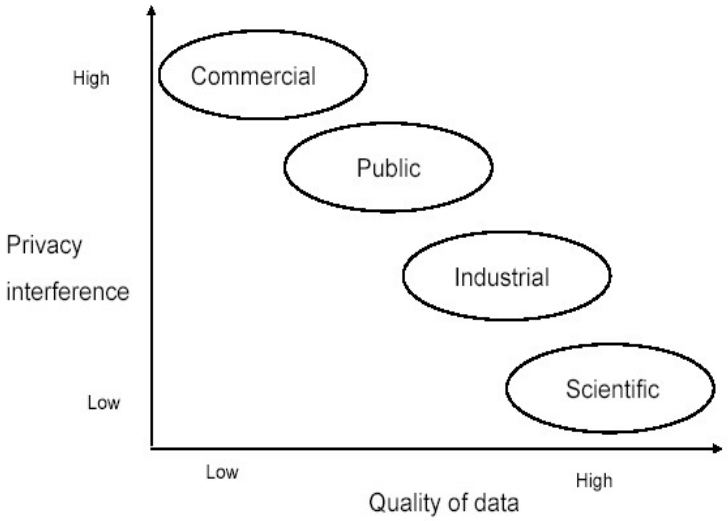

Exhibit 3: Level of data quality and privacy interference in different AI spheres

Exhibit 3 depicts the localization of the data spheres of AI we take into view according to the respective levels of interference with data privacy and the quality of data, as exemplified. Resuming what has been considered in chapters 2, 3 and 4 above allows to suggest a twofold approach to the way the collection and protection of input data for AI can be organized.

The basic principle to guide the privacy of data is human dignity, one of the fundamental rights of humans as laid down in the declaration of human rights, reflected in the German constitution as the right of informational self-control, and on European level in the GDPR. Extended and broadly elaborated, it has been incorporated into the Ethical Guidelines [6], which are the source of the Policy and Investment Recommendations for Trustworthy AI [7]. Beyond the regulative ruling following the GDPR in Europe, and further to encryption methods used to protect data (for a medical sector focused suggestion cf. [20]), for the organization of the collection of data there are two major concepts currently discussed: blockchain based distributed ledger technology, and (industrial) open data spaces.

A blockchain concept for the health sector has been proposed by Koscina et al [14]. Within the architecture they develop, it is the health care institutions that hold blockchain contracts which control shared data and make it traceable. One could consider extending such a concept even to the commercial or public sphere, however, it is far from being realistic this point in time to see private users become blockchain contractors in a distributed data sharing system. The, from a privacy point of view, ideal situation of keeping individuals in full control of their private data under the blockchain concept thus seems out of sight for the time being. Furthermore, even a concept like this has restrictions to data protection, as it is subject to the considerations presented by Hittmeyer et al [8] on the possibility of identity disclosure by powerful analyses of individual attributes from synthetic data.

For the industrial, but also for the scientific sector, the concept of shared (industrial) data spaces (or multi-sided platforms) offers a promising approach that is put into focus by several initiatives in Europe. The idea is to create open data systems that are made accessible for third parties within an alliance for commercial or scientific use. Bohlen et al [1] present a respective position paper of the IDS association, describing their approach to an Open Data Ecosystem where trust and security are realized based upon a certification concept. Otto and Jarke [18] provided a resume of the findings from a case study in the IDS association with regard to the design of a multi-sided platform for data sharing. There are various similar initiatives on European level (European Data Space) or in an industry specific setting, for example for the automotive sector. Initiatives like these are intended to make high quality data available by adhering to the limitations data privacy principles and respective regulation may impose.

6 Conclusion

The need for data privacy is undeniable, as human dignity and individual autonomy are most basic principles of human rights. Individual freedom, furthermore, is an acknowledged source of innovative progress, not only, but also in economic context. With regard to the novel technologies expected to evolve under the label Artificial Intelligence, the utilization of massive data provides a second source of innovation, the value of which becomes higher, the better their quality is. However, privacy and quality of data tend to be in mutual conflict. This calls for prudent balancing of these two aspects of the utilization of massive data.

In order to enable this balancing, we distinguish various data spheres that let show different levels of privacy interference and quality of data. The purpose is to tailor adequate governance of data protection for each of the spheres of commercial, public, industrial, and scientific data utilization. Exhibit 2 illustrates our first order approach to a useful specification of data spheres, while exhibit 3 suggests a reasonable assessment of these spheres according to the level of data privacy interference and data quality.

We have made explicit the fundamental principles of ethics, the regulation as it is in place in Europe or being discussed elsewhere, and currently pursued concepts of data privacy protection. On this background we argue for the governance of protection and usability of private data to be adjusted to different fields of AI application (thus taking up economic and scientific motivation), and to be dynamically adapted as AI research and development progresses.

References

1. Bohlen, V., Bruns, L., Menz, N., Kirstein, F., Schimmler, S.: Open Data Spaces – Towards the IDS Open Data. Fraunhofer Institute FOKUS, https://www.internationaldataspaces.org/wp-content/uploads/2019/07/Open-Data-Spaces-IDSA.pdf (2018), last accessed 2020/02/02
2. Car, J. et al: Beyond the hype of big data and artificial intelligence: building foundations for knowledge and wisdom. BMC Medicine (2019) 17:143. https://doi.org/10.1186/s12916-019-1382-xAuthor, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016).
3. Floridi, L.: Soft ethics**,** the governance of the digital and the General Data Protection Regulation. *Phil. Trans. R. Soc. A* **376**: 20180081. http://dx.doi.org/10.1098/rsta.2018.0081 (2018)
4. Floridi, L., Taddeo, M.: What is data ethics? Phil. Trans. R. Soc. A **374**: 20160360. http://dx.doi.org/10.1098/rsta.2016.0360 (2016)
5. High Level Expert Group on Artificial Intelligence (AI HLEG): A definition of AI: Main capabilities and scientific disciplines. European Commission, Brussels (2018)
6. High Level Expert Group on Artificial Intelligence (AI HLEG): Ethics Guidelines for Trustworthy AI. European Commission, Brussels (2019)
7. High Level Expert Group on Artificial Intelligence (AI HLEG): Policy and Investment Recommendations for Trustworthy AI. European Commission, Brussels (2019)
8. Hittmeyer, M., Mayer, R., Ekelhart, A.: A Baseline for Attributed Disclosure Risk in Synthetic Data. In: Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (CODASPY'20), March 16–18, 2020, New Orleans, LA, USA. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3374664.3375722 (2020)
9. Jastroch, N., Neumann, M.: Innovation im wissensintensiven Umfeld. LNI Vol. 35, pages 351-358 (2003)
10. Jastroch, N.: Wissensmanagement – Darstellung und Transfer von Wissen – Potenziale und Grenzen. GI Lecture Notes in Informatics, Vol. P-28. Bonn 2003 and http://CEUR-WS.org/Vol-85/ (2003)
11. Jastroch, N.: Advancing Adaptivity in Enterprise Collaboration. Journal of Systemics, Cybernetics and Informatics, JSCI, Vol. 7/6, pp. 7-11 (2009)
12. Körner, K., Schattenberg, M., Heymann, E.: Digitale Wirtschaft - Wie künstliche Intelligenz und Robotik unsere Arbeit und unser Leben verändern. DB Research (2018) https://www.dbresearch.de/MAIL/RPS_DE-PROD/PROD0000000000468838.pdf, last accessed 2020/02/02
13. Körner, K.: Digitalpolitik – KI, Big Data und die Zukunft der Demokratie. DB Research (2019) https://www.dbresearch.de/MAIL/RPS_DE-PROD/PROD0000000000499444.pdf, last accessed 2020/02/02
14. Koscina, M., Manset, D., Negri, C., Perez Kempner, O.: Enabling trust in healthcare data exchange with a federated blockchainbased architecture. In IEEE/WIC/ACM International Conference on Web Intelligence (WI '19 Companion), October 14–17, 2019, Thessaloniki, Greece. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3358695.3360897
15. Morley, J., Floridi, L.: An ethically mindful approach to AI for health care. www.thelancet.com Vol 395 January 25, (2020)
16. Morley, J. et al.: The Debate on the Ethics of AI in Health Care: a Reconstruction and Critical Review. https://digitalethicslab.oii.ox.ac.uk/wp-content/uploads/sites/87/2019/11/The-Debate-on-the-EThics-of-AI-in-Health-Care-pre-print-.pdf (2019)

17. Nassehi, A. et al: The Strength of Weak Procedures, Zeitschrift fuer Soziologie 48(3), de Gruyter Oldenbourg (2019), https://doi.org/10.1515/zfsoz-2019-0015
18. Otto, B., Jarke, M.: Designing a multi-sided data platform: findings from the International Data Spaces case. Electronic Markets (2019) 29:561–580, https://doi.org/10.1007/s12525-019-00362-x
19. Thoben, K.-D., Wiesner, S., Wuest, T.: "Industrie 4.0" and Smart Manufacturing. A Review of Research Issues and Application Examples. Int. J. of Automation Technology Vol.11 No.1 (2017)
20. Vitiziu, A. et al.: Privacy-Preserving Artificial Intelligence: Application to Precision Medicine. Conference proceedings of the 41st Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), 6498-6504, DOI: 10.1109/EMBC.2019.8857960 (2019)
21. Wellsandt, S., Thoben, K-D., Klein, P.: Information Feedback in Product Development: Analysing Practical Cases. International Design Conference - DESIGN 2018. https://doi.org/10.21278/idc.2018.0379 (2018)
22. Wuest, T., Wellsandt, S., Thoben K.-D.: Information Quality in PLM: A Production Process Perspective. In: Bouras A., Eynard B., Foufou S., Thoben KD. (eds) Product Lifecycle Management in the Era of Internet of Things. PLM 2015. IFIP Advances in Information and Communication Technology, vol 467. Springer, Cham (2016)