Centre for European Integration Research

Working Paper Series

The need for ethical algorithms:

The European approach to Artificial Intelligence

David Leopoldi-Wieshaupt

Working Paper No. 03/2020

Centre for European Integration Research
Department of Political Science
University of Vienna

Apostelgasse 23
1030 Vienna/Austria

Telefon: +43-1-4277-49456
Fax: +43-1-4277-49497

Email: eif@univie.ac.at
Web: eif.univie.ac.at

Abstract

(Deutsch)

Das vorliegende Forschungsprojekt untersucht den Europäischen Ansatz zu Künstlicher Intelligenz. Mit dem sozialkonstruktivistischen Konzept der ‚*Normative Power Europe*' wurde das Thema auf zwei verschiedenen Abstraktionsniveaus behandelt. Auf einer empirischen Ebene wurden die Vereinigten Staaten, China und die EU in Bezug auf Datenschutzrecht und militärische Anwendungen Künstlicher Intelligenz verglichen; mit dem Ergebnis, dass die EU als schwache normative Kraft klassifiziert wurde. Auf einem höheren Abstraktionsniveau wurde die Charakterisierung der EU als normative Macht damit begründet, dass sie einen menschen-zentrierten Ansatz gewählt hat, vertrauenswürdige Technologie entwickeln will und der Fokus im Diskurs auf Menschenrechten liegt.

(English)

This research project examined the European approach to Artificial Intelligence. With the social constructivist concept of Normative Power Europe, the topic has been discussed on two levels of abstraction. Empirically, the United States, China and the EU have been compared regarding the aspects of data protection regulation and military AI, which resulted in the classification of the EU as Weak-Normative Power. On a more abstract level, the EU's human-centric approach to Artificial Intelligence, the emphasis on developing trustworthy technology and the focus on human rights in the discourse led to the characterisation of the European Union as normative power.

General note: Opinions expressed in this paper are those of the author and not necessarily those of the EIF.

Table of contents

0. Introduction

The current Corona crisis has speeded up digitisation in a not foreseeable way and significantly shortened the time span of the transition to digital devices in various sectors. Artificial Intelligence (AI) has been one of the hottest topics during the last years in the field of digital transformation, which will have a massive influence on our society and economy. The discourse which was started in academic and technology-affine circles, already reached the attention of the public, journalists and policy-makers. In 2017, Russian president Putin said whoever would become the leader in AI '*will become the ruler of the world.*'[1] This statement shows that big nation states like Russia with claims regarding military strength and geopolitics are already on the subject. The United States (US) and China pursue ambitious national initiatives to master the technology, which will be subject to analysis in this paper. The dual-use nature of AI enables applications in commercial and military realms and some even compare it to electricity due to its omni-use potential and capability to disruptively change various different areas.[2] The European Union (EU) takes a different approach to AI. Having in mind the comprehensive challenges in the field of ethics and society with the political will to protect fundamental rights, the need for ethical algorithms has been recognised. The main goal of this research project is to characterise the EU's approach to Artificial Intelligence next to a comparison to the US and China regarding data protection and military AI. For this purpose, the author tries to make Ian Manners'[3] concept of Normative Power Europe (NPE) fruitful for this topic.

In the first part of this paper, the research design will be outlined. In the second part,

the context and especially the impact of AI will be discussed. The third part will compare the US, China and the EU regarding the two categories data protection and military AI, including an assessment and classification of the EU as normative power, weak normative

[1] Gonçalo Carriço, 'The EU and Artificial Intelligence: A Human-Centred Perspective', *European View*, 17.1 (2018), 29–36 (p. 31).

[2] Jeffrey Ding, *Deciphering China's AI Dream* (Governance of AI Program, Future of Humanity Institute, University of Oxford, 2018), p. 11 <https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf> [accessed 25 March 2020].

[3] Ian Manners, 'Normative Power Europe: A Contradiction in Terms?', *JCMS: Journal of Common Market Studies*, 40.2 (2002), 235–58.

power or not-normative power. Building on the results, the fourth part of the paper will focus on the European approach to AI in more detail especially discussing the recent publications of the European Commission (hereinafter also referred to as the Commission, then the European Commission is always meant). Finally, the findings will be summarised and concluding remarks will be given.

I. Research design

A. State-of-the-art literature and research question

Among the huge quantity of academic and non-academic publications on AI in the last years, some of the most relevant for the research and their key findings will be summarised. The Washington D.C.-based think tank Center for Data Innovation published a report called '*Who is winning the AI race: China, the EU or the United States?*' in August 2019.[4] The comparison was made among the six categories talent, research, development, adoption, data and hardware. It resulted in the US leading and China being ahead of the European Union. In numbers, the United States received 44.2 points, followed by China with 32.3 and the EU with 23.5 out of 100.[5] The reasons for the leadership are the American AI start-up ecosystem, their advantage concerning hardware production, and the high-quality of research papers and talent. Chinese companies have more access to data and start-ups receive high amounts of funding; however, the country lags behind concerning AI researchers. The EU has high-class AI talent but is behind in AI adoption, the start-up and economic environment.[6] In addition, the authors see European regulation on data protection critically and argue that it led to an '*artificial scarcity of data*' that makes it more difficult for corporations to use consumer data for business operations.[7]

In December 2019, Stanford University's Human-Centered AI Institute released their '*AI Index 2019 Annual Report*', which aims for a more nuanced approach that

[4] Daniel Castro, Michael McLaughlin, and Eline Chivot, *Who Is Winning the AI Race: China, the EU or the United States?* (Center for Data Innovation, Washington D.C. and Brussels, 2019) <http://www2.datainnovation.org/2019-china-eu-us-ai.pdf> [accessed 5 March 2020].

[5] Castro, McLaughlin, and Chivot, p. 2.

[6] Castro, McLaughlin, and Chivot, p. 2 f.

[7] Castro, McLaughlin, and Chivot, p. 42.

includes more states besides the US, China and the EU.[8] With almost 300 pages, the report is one of the most comprehensive presentations and comparisons regarding Artificial Intelligence on the basis of research and development, conferences, technical performance, economy, education, autonomous systems, public perception, societal considerations and national strategies. China now publishes as many AI journals and conference papers per year as Europe, but the Field-Weighted Citation Impact of US publications is still about 50% higher than China's.[9] With 19.8 billion US-Dollars (USD), the US leads in terms of start-up funding, before China with USD 16.6 billion and Europe with USD 4.6 billion.[10]

A research project from the University of Oxford's Future of Humanity Institute in 2018 compared the US and China, while focusing on the latter.[11] The comparison was conducted on the basis of four factors that are supposed to drive the overall development of AI: hardware, data, research and algorithm development and commercial AI ecosystem. The outcome was an AI Potential Index, where China reached 17 and the US 33 out of 100 points.[12] According to the results, China is leading in the field of data access and is catching-up in semiconductor production and supercomputer facilities. While it is generally assumed that China's approach to AI is defined by its top-down nature and the role of the central government, private companies, academic labs, local governments and bureaucratic agencies are all pursuing their own interests to stake out their claims to China's AI dream.[13]

A report by the European Commission's Joint Research Centre (JRC) presented a European perspective on Artificial Intelligence in which the US and China, among others have been discussed.[14] The United States are leading in the field of corporate and industrial players and dominate the start-up sector with almost half of the total worldwide. In opposition to the above-mentioned findings, the JRC's report states that

[8] Perrault and others.
[9] Perrault and others, p. 4.
[10] Perrault and others, p. 92 f.
[11] Ding.
[12] Ding, p. 29.
[13] Ding, p. 3.
[14] Craglia and others.

the Chinese approach is strongly coordinated, including government policy, industrial applications and research. China's dream and clear objective to become the world leader in AI by 2030 is an ambitious but achievable target, according to the document. Key areas of strength in the EU are the number of AI papers published in top scientific journals as well as the sector for automated and connected vehicles and robotics.[15]

The research interest of this paper is to examine the European approach to Artificial Intelligence. This will be conducted by using two elements of analysis. First, the US, Chinese and European approach to data protection regulation and military AI will be compared. The different approaches of the three systems regarding data protection regulation make more detailed research necessary and interesting. For military AI, very little academic literature that compares all three exists, and this gap is to be addressed. The two categories will allow a detailed comparison of the three regions. Second, the actions outlined in the recent publications of the EU regarding the development of the technology will be examined with the goal of finding out if they can be characterised as norm-guided. In this master's thesis, actions are regarded as norm-guided if they are based on values and principles, with special emphasis on human rights and international law. This view follows Ian Manners concept Normative Power Europe, that will be discussed in more detail in chapter I.C. The Commission's documents, which have been published in February 2020, have not yet been subject to analysis in academic literature and thus will provide new insights. Although the US, China and the EU have been compared on the basis of different variables, this social constructivist approach, which aims at characterising the European approach on AI, is going to provide further understanding of the EU's position on this important matter. The author expects, based on the theoretical concept of Ian Manner, that the EU does act with a certain amount of normative power. The research is guided by the following two questions:

In how far does the concept Normative Power Europe fit the European approach to Artificial Intelligence?
What are the main differences to China and the US regarding data protection and military AI?

[15] Craglia and others, p. 9.

After reviewing the state-of-the art literature, outlining the research interest and presenting the research question, the following paragraph will look into the project's operationalisation.

B. Operationalisation

To operationalise the project, the literature regarding data protection regulation and military AI will be analysed in detail and the results will provide the possibility to classify the European actions as normative, weakly normative or not normative. If the EU acts in a norm-guided way, comprehensive data protection regulation would have to be in place. A data protection regime will be regarded as comprehensive, if three elements are given.

- First, it has to have an omnibus scope on federal level. An omnibus law is characterized by the coverage of '*all personal data processing, whether in the public or private sector. These laws are then bolstered by sectoral laws that single out specific kinds of data processing and increase the specificity of regulatory norms.*'[16]
- Second, credible sanctions have to be provided in order to incentivise compliance with the legal framework.[17]
- Third, enforceability of rights has to be guaranteed by independent courts and strong enforcement mechanisms.[18]

Regarding military AI, the norm-guided course of action of the EU would be confirmed, if the EU is not focusing on military AI, which is fulfilled if two criteria are met.

- First, military AI is not declared a main target in the governmental documents.
- Second, there are no substantial financial resources provided for the development of military AI.

  The evaluation if the resources spent are substantial is quite challenging due to the difficulty to get precise numbers for China. In order to assess the financial resources, the size of research programmes that foster military AI or at least

[16] Paul M. Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law', *Georgetown Law Journal*, 106.1 (2017), 115–79 (p. 128).

[17] Filippo Maria Lancieri, 'Digital Protectionism? Antitrust, Data Protection, and the EU/US Transatlantic Rift', *Journal of Antitrust Enforcement*, 7.1 (2019), 27–53 (p. 32 f).

[18] Paul De Hert and Dr. Vagelis Papakonstantinou, 'The Data Protection Regime in China. In-Depth Analysis', 2015, p. 8 <https://www.ssrn.com/abstract=2773577> [accessed 13 April 2020].

include the possibility to do so are considered and compared to both the overall military expenses and the national GDP.

The three elements regarding data protection regulation and the two criteria for military AI will each be marked with yes or no. If the result is more nuanced, a question mark will be added in the table that provides the summary (see table 2 and table 4, chapter III.C). In the case that the factors data protection regulation and/or military AI can only be partially confirmed, the actions of the EU would be classified as weakly normative. However, if one or both factors cannot be confirmed (and are therefore marked with 'no'), the assessment for the EU's actions would result in the classification of non-normative power. Both conditions are necessary in order to grade the EU as a normative power.

The differences between the EU, China and the US vary specifically, why a scale with three gradings (yes, partially, no) is used to measure and compare the three systems. If only two grades (i.e. yes and no) would be used, the result would be a scheme which is more '*black and white*', where not only important nuances would be lost, but further the classification could become difficult, as the gap between yes and no is quite large. More than three gradings are not useful, as it is not necessary for the illustration of the differences and for reasons of limited resources. Another advantage of this design is the clearness and simple understandability on an abstract level. The categories allow specific comparison and will show differences and similarities. Table 1 gives an overview of all possible results.

Table 1: Overview of operationalisation and all possible results[19]

Comprehensive data protection regulation	Not focusing on military AI	Result
yes	yes	NPE
yes	partially	Weak-NPE
partially	partially	Weak-NPE
partially	yes	Weak-NPE

[19] Table 1: Overview of operationalisation and all possible results, own presentation.

partially	no	Non-NPE
no	partially	Non-NPE
no	yes	Non-NPE
yes	no	Non-NPE
no	no	Non-NPE

The classification to a concept alternative to NPE will not be conducted. The reasons are on the one hand, the limited resources of this academic project and on the other, that the author considers the added value to be low because the selected categories are strongly linked to normative values and a comparison with market power or strategic power would therefore not be possible, at least not in-depth. In the next chapter the theoretical framework will be presented.

C. Theory

The theoretical approach of this research project is twofold. On a more abstract level, the concept of '*Normative Power Europe*' (NPE) will be used to better understand the material (for detailed information on the material see chapter I.D). The concept NPE was developed by Ian Manners building on Francois Duchêne's characterisation of Europe as '*civilian power*' in the 1970s.[20] According to Manners

> *the notion of a normative power Europe is located in a discussion of the 'power over opinion', idée force, or 'ideological power', and the desire to move beyond the debate over state-like features through an understanding of the EU's international identity*.[21]

He argues that the historical prerequisites led to a European normative difference, which developed into a hybridity of supranational and international forms of governance. Certain principles like strong commitment to and protection of fundamental rights were common among the Member States of the EU.[22] While debates about military actions

[20] Manners, p. 235 f.
[21] Manners, p. 239.
[22] Manners, p. 240 f.

tended to divide Europe, the emphasis on human rights and the moral role in world politics provided a ground for coherence.[23] After the Cold War, the fusion of historical context, hybrid polity and legal constitution '*accelerated a commitment to placing universal norms and principles at the centre of its relations with its Member States.*'[24] The difference to pre-existing political actors serves as a predisposition '*to act in a normative way*', which can be seen as the core element of the concept.[25] Manners identifies five core norms as the EU's normative basis, which are peace, liberty, democracy, rule of law and respect for human rights and fundamental freedoms.[26] Scheipers and Sicurelli stress that normative power should be understood '*in terms of being an ideological power, that is, the power to shape the patterns of discourse when it comes to basic principles and values.*'[27] They emphasise that the concept is linked to the emergence or construction of a '*specific European identity*.'[28] According to Diez, the concept of NPE has a '*social constructivist ring to it*'[29] and he argues that the European identity is constructed '*against an image of others in the 'outside world."*[30]

Some scholars criticise the EU for a lack of reflexivity arguing the EU tries to export certain ideal '*EUtopian*' values, which do not represent '*what the EU actually is.*'[31] For assessing the degree of reflexivity, two options are provided by the literature. On the one hand, the '*consistency between the internal and external planes*' could be evaluated. On the other, reflexivity could be interpreted '*in the sense of refraining from* '*utopian normativity.*''[32]

Countering the critique, the authors Scheipers and Sicurelli argue that the measurement between internal and external policies is not clear as there are no objective

[23] Sibylle Scheipers and Daniela Sicurelli, 'Normative Power Europe: A Credible Utopia', *JCMS: Journal of Common Market Studies*, 45.2 (2007), 435–57 (p. 436).
[24] Manners, p. 241.
[25] Manners, p. 242.
[26] Manners, p. 242.
[27] Scheipers and Sicurelli, p. 453.
[28] Scheipers and Sicurelli, p. 453.
[29] Thomas Diez, 'Constructing the Self and Changing Others: Reconsidering `Normative Power Europe'', *Millennium: Journal of International Studies*, 33.3 (2005), 613–36 (p. 616).
[30] Diez, p. 614.
[31] Scheipers and Sicurelli, p. 438.
[32] Scheipers and Sicurelli, p. 438.

criteria for its evaluation. Furthermore, even if the EU may be inconsistent, it does not mean that it is no longer credible. After all, inconsistency is an aspect typical of collective identities. Regarding the argument of utopian normativity, they see successful self-representation necessarily connected with utopian values, which are crucial for attracting others.[33] In sum, they see the aspect of reflexivity '*neither appropriate nor useful*' when it comes to assessing Europe's level of normative power.[34] Two case studies, the institutionalisation of the International Criminal Court (ICC) and the elaboration of the Kyoto Protocol, were conducted by Scheipers and Sicurelli to examine the EU's normative power. The result were four features that characterise the EU's identity. First, the principles the EU tries to institutionalise are universal in reach and validity, for instance human rights or the precautionary principle regarding environmental protection. Second, the EU wants to position itself as pioneer for international challenges such as global warming and human rights, especially in sharp demarcation to the United States. Third, the restriction to diplomatic and non-military actions is advantageous over other approaches, again with respect to the US. Fourth, the European identity strongly favours compliance with international law.[35]

To sum up, the author of this master's thesis understands NPE as actions or statements that are based on values and principles. More specifically, the concept implies a strong commitment to human rights and international law. Importantly, Ian Manners uses the concept to analyse if the EU shapes the patterns of discourse. However, subject to this master's thesis are not debates and discourses, but statements that appear in EU discussion papers with regard to Artificial Intelligence and related laws such as the General Data Protection Regulation (GDPR). The concept seems suitable for the topic AI and the examination of the European approach, because elements concerning human rights, international law and other ethical aspects as discussed in chapter II.B.b. are at stake.

Empirically, the topic will be discussed with a focus on the two factors data protection and military AI. When it comes to maximising the benefits of AI, two of the

[33] Scheipers and Sicurelli, p. 438.
[34] Scheipers and Sicurelli, p. 439.
[35] Scheipers and Sicurelli, p. 453.

most fundamental tensions are on the one hand the protection of data for privacy concerns and on the other the free provision of data for the development of the technology. Data, sometimes referred to as the '*ultimate driver*' of the technology and the protection of the very same is therefore a necessary aspect of any strategy for Artificial Intelligence.[36] While most reports on AI include data as an element of comparison and even assess it as the most important component,[37] much fewer publications focus on data protection. Lancieri (2019)[38] discusses the EU and the US regarding data protection, while Feng (2019)[39] provides deep insights into the Chinese data protection regime. The author will bring together the relevant information concerning data protection in the US, China and the EU and assess if comprehensive data protection regulation is provided.

Military AI, the second category, is less used as a factor for comparing the three players in the scholarly literature. However, most experts affirm the importance of AI on military and warfare, which makes this topic crucial, not only for security reasons but the dual-use technology's omni-use potential makes spill-over to other sectors likely. Scholars and media reports indicate an AI arms race between China and the US.[40] Concerning the EU, some argue that Europeans are putting too little attention to military AI[41] while others emphasise the potential for the EU to become a dominant actor in that field with the largest impediment of the mixed intents of the Member States.[42] As discussed above, both ethical aspects of military AI as well as legal questions concerning international and humanitarian law make this category especially relevant for this research project. The category has been developed by the author on the basis of the literature. Although a comparison on the basis of further factors would be imaginable,

---

[36] Ding, p. 28.

[37] Castro, McLaughlin, and Chivot; Ding; Craglia and others.

[38] Filippo Maria Lancieri, 'Digital Protectionism? Antitrust, Data Protection, and the EU/US Transatlantic Rift', *Journal of Antitrust Enforcement*, 7.1 (2019), 27–53.

[39] Yang Feng, 'The Future of China's Personal Data Protection Law: Challenges and Prospects', *Asia Pacific Law Review*, 27.1 (2019), 62–82.

[40] Ding, p. 31 f.

[41] Ulrike Esther Franke, *Not Smart Enough: The Poverty of European Military Thinking on Artificial Intelligence* (European Council on Foreign Relations, 2019), p. 2 f <https://www.ecfr.eu/page/-/Ulrike_Franke_not_smart_enough_AI.pdf> [accessed 25 March 2020].

[42] Justin Haner and Denise Garcia, 'The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development', *Global Policy*, 10.3 (2019), 331–37 (p. 334 f).

both the limited resources and the fact that data protection and military AI are a perfect fit to the conceptual framework, make a restriction necessary as well as reasonable.

D. Methodology and data

The methodology that is used to conduct the research will be a qualitative content analysis, focusing on official EU documents, journal articles, academic books, reports from think-tanks and to a limited extent newspaper articles. For the US and China, due to limited resources, only secondary sources will be used for analysis choosing the most pertinent literature. Given the focus on the European Union, the attempt is to look into all important publications on the topic especially emphasising the most recent documents, which have been published in February 2020. Both primary and secondary sources will be used for researching the EU. After discussing the research design of the project, the next chapter will look into the context of the topic with special emphasis on the impact of AI on ethics and society.

II. Context

A. General aspects

a. History and definition

The origins of Artificial Intelligence date back to the 1950s, when British computer scientist Alan Turing asked if machines are able to think.[43] Since then, the technology experienced some sort of roller coaster development concerning expectations as well as funding. What started with logic-based systems in the fifties and knowledge-based approaches in the seventies and eighties eventually led to data-driven operations from 2000 onwards. Defining AI is not an easy task, especially due to various differences in publications on the topic. As the main focus of this research project is the European Union's approach to the technology, the definition provided in official documents will be used. In its communication, the European Commission defined AI as

> *systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based*

[43] Carriço, p. 29.

> *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).*[44]

The Commission's white paper further emphasises the fact that the behaviour of systems is both defined and constrained by programmers, who set the goals an algorithm then optimises for. Importantly, the definition in legal frameworks needs to remain flexible for adjustments with technical progress while providing a necessary degree of precision to ensure legal certainty.[45]

Recent breakthroughs in computing processing capabilities and data enabled Machine Learning (ML), which was seen as a paradigmatic shift in information processing. Up to this point, programmers have used computer codes to set the rules for data inputs to get an answer as result. '*In ML, the computer receives input data as well as the answers expected from the data, and the ML agent needs to produce the rules. […] An ML system is trained rather than explicitly programmed.*'[46] The set of rules that has arisen as a result can in turn be used for new data records and the production of original answers. Another new form of information processing is Deep Learning (DL), which is similar to ML, but can process even '*noisier*' data (i.e. data containing irrelevant or meaningless information) by '*increasing significantly the number of neural layers and neurons, and the amount of data used for the training.*'[47]

---

[44] 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, COM 237 Final' (Brussels, 2018), p. 1 <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF> [accessed 25 March 2020].

[45] European Commission, 'White Paper: On Artificial Intelligence - A European Approach to Excellence and Trust COM 65 Final' (Brussels, 2020), p. 16 <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [accessed 25 March 2020].

[46] Massimo Craglia and others, *Artificial Intelligence: A European Perspective* (Joint Research Centre, Luxembourg: Publications Office of the European Union, 2018), p. 20 <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC113826/ai-flagship-report-online.pdf> [accessed 25 March 2020].

[47] Craglia and others, p. 21.

Different forms of AI are distinguished in terms of capabilities. Narrow Artificial Intelligence, for instance ML or DL systems, are able to perform specific tasks they are trained for. The results are algorithms that outperform world-leading human players in games like Go or different computer games. In the case of Artificial General Intelligence, the machine would be as smart as a human being, able to perform intellectual tasks and could solve various problems rather than just specific ones the system was trained to deal with. Artificial Superintelligence would be a machine smarter than the brightest person on earth in every single field. While the first one, Narrow AI is already used in various applications (see chapter I. A. b. for details), both General AI and Superintelligence have only been subject to science fiction films.[48] According to experts in the field, General AI will be out of reach for several decades.[49] Having presented a short history and a working definition of AI, the next section will discuss opportunities and risks of the technology.

b. Opportunities and risks of AI

The fact that AI will have a huge impact on our society and economy harbours both opportunities and risks. A first aspect is connected to self-realisation, meaning the personal self-fulfilment by evolving people's abilities and skills. Smart automation could increase free time, which could be used for intellectual, cultural and social activities. Therefore, similar effects innovations such as washing machines had could be the result. The main problem in this regard is the speed of the change, since the devaluation of skills produces unemployment if retraining measures are not sufficiently provided. In addition, the use of AI in sensitive sectors like health care and aviation creates risks in the case of malfunctioning of the technology or issues connected to cyber-attacks.[50]

Second, human agency could be enhanced and with the support of AI, people could do more, better and faster. That kind of advanced or augmented intelligence could be compared to the effects of engines on society. Importantly, responsibility is crucial in order to ensure the distribution of benefits and advantages, while an insufficient level of responsibility would pose risks. A problem could be the view that AI cannot be

[48] Carriço, p. 30.

[49] Craglia and others, p. 22.

[50] Luciano Floridi and others, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations', *Minds and Machines*, 28.4 (2018), 689–707 (p. 690 ff).

understood by human beings and therefore actions to decipher the black box are omitted. The connection of people's understanding and control of the technology is also shown by the example of algorithms deciding on a person's creditworthiness. It would pose a problem of legitimacy if the decisions could not be understood.[51]

Third, Artificial Intelligence offers numerous opportunities to radically improving or at least changing people's lives such as providing new forms of mobility and logistics or curing and preventing diseases. One danger would be, for example, to delegate important decisions to algorithms which would reduce the possibility to monitor the performance by human beings. It is particularly important to ensure that the ambitious possibilities form a balance with the level of human supervision and control of these developments.[52]

Fourth, AI can be useful to deal with the increased complexity of coordination emerging from international challenges such as climate crisis or nuclear proliferation, ideally with the result of more support for societal cohesion and collaboration. AI systems could be the basis for societal frameworks that try to drastically reduce greenhouse gases. A useful aspect for this is self-nudging, where people design their environment in a way that makes it easier for them to make right or better decisions and eventually reach their long-term goals. However, a possible erosion of human self-determination is problematic if human behaviour is influenced by algorithms too much. Therefore, it is important to promote social cohesion and prevent undermining basic human values such as dignity.[53] After discussing four opportunities and risks of AI for society, the fifth and final aspect concerns the technology's potential for weaponization. The military application of AI is especially emphasised by the US, China and Russia.[54] While ethical and legal aspects of military AI are outlined in chapter I.B.c, the topic will be discussed in more detail in chapter III.B. Having outlined the opportunities and risks of the technology, the next section will discuss the impact of AI.

---

[51] Floridi and others, p. 692 f.
[52] Floridi and others, p. 693.
[53] Floridi and others, p. 693 f.
[54] Carriço, p. 31.

B. Impact of Artificial Intelligence

While AI is going to influence a wide range of sectors, both private and public, with many different potential applications using software for instance for medical diagnosis, hardware such as smart home applications or both in the case of autonomous cars, this thesis focuses on aspects regarding ethics, society and warfare. To begin with, the impact on economy and labour markets will be briefly outlined, before the main aspects will be discussed.

a. On economy and labour markets

In 2017, a PricewaterhouseCoopers (PwC) study found that AI will contribute up to 15.7 trillion USD to the economy until 2030 on a global perspective. This equals a plus similar to the current economic output of India and China together. Productivity gains are expected to be responsible for 6.6 trillion USD and 9.1 trillion USD are foreseen to come from consumption side effects.[55] For the labour market, some studies predict mass unemployment as people are increasingly being replaced by machines and algorithms; however, history suggests that innovation spurts have resulted in an overall increase in jobs as well as incomes.[56] The pace of change and uptake of digitisation is very important as an AI-induced reallocation of workers and skills takes time, and mitigating the negative effects over a longer period becomes more manageable. Developing new algorithms and Machine Learning models needs a vast amount of competence, nevertheless, the high visibility of the topic and the current demand suggests rapid allocation of talents in the field.[57] Due to uncertainties on the job market, monitoring of AI deployment is important to increase the speed of necessary intervention.[58] After outlining the most crucial aspects regarding economy and labour markets, the impact on ethics and society will be discussed in the following paragraphs.

---

[55] PricewaterhouseCoopers, 'Sizing the Prize What's the Real Value of AI for Your Business and How Can You Capitalise', 2017 <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf> [accessed 25 March 2020].

[56] Craglia and others, p. 77.

[57] Craglia and others, p. 72.

[58] Craglia and others, p. 85.

b. On ethics and society

The importance of ethics for Artificial Intelligence has been widely debated in the last years among scholars, journalists, policy-makers and the public. The number of conference papers addressing ethical concerns is still rising.[59] Various guidelines and principles have been developed that should help to ensure that the technology's development is in line with crucial principles of human dignity and well-being.[60] '*Asilomar AI Principles*', which were developed in conjunction of the Asilomar conference in January 2017 in collaboration with the Future of Life Institute, a non-profit research organisation specialising on potential risks of AI, are important to mention among the internationally influential initiatives.[61] Other important documents are the '*Montreal Declaration for Responsible AI*'[62] of the University of Montreal, the '*Global Initiative on Ethics of Autonomous and Intelligent Systems*'[63] by the Institute of Electrical and Electronics Engineers (IEEE), a technical professional organization dedicated to advancing technology for the benefit of humanity and the '*Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*'[64] of the European Commission's European Group on Ethics in Science and New Technologies (EGE). The different frameworks offer insights into the complex ethical debates that have to be addressed with the technology's rise. A common differentiation in academia is to discuss ethical

---

[59] Raymond Perrault and others, *The AI Index 2019 Annual Report* (Human-Centered AI Institute, Stanford University, 2019), p. 44 <https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf> [accessed 25 March 2020].

[60] Floridi and others, p. 689 f.

[61] Future of Life Institute, 'Asilomar AI Principles', 2017 <https://futureoflife.org/ai-principles/?cn-reloaded=1#top> [accessed 2 June 2020].

[62] no author, 'Montreal Declaration for a Responsible Development of Artificial Intelligence' (Montreal: University of Montreal, 2018) <https://5dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf> [accessed 2 June 2020].

[63] The IEEE Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems', 2017 <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v1.pdf> [accessed 6 February 2020].

[64] European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and "Autonomous" Systems' (Brussels: European Commission, 2018) <http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf> [accessed 6 February 2020].

issues on the two dimensions of impact on individual and societal level, which this thesis is going to follow.[65]

i. Challenges on individual level

Ethical approaches, especially in the European context, are often connected to human rights and their codification, for instance in the Universal Declaration of Human Rights and the Charter of Fundamental Rights of the European Union. The right to life, to privacy, freedom of expression, non-discrimination and others provide the debate with a starting point.[66] One of the most important aspects regarding challenges on an individual level is autonomy. It is not only one of the core values of Western ethics, but reflects everyone's capacity of individual choice, rights and freedoms.[67] The degree of autonomy of intelligent systems is simplistically described with three levels. If a human is in control of a machine's actions, the person is '*in the loop*', but operator and machine do not have to be in the same place, because of the possibility of remote control. When a natural person and a machine share the controlling actions, the human is described as being '*on the loop*', while for autonomously acting machines the person is said to be '*out of the loop*'.[68] In digital media communications, it became increasingly difficult to determine whether one is interacting with a bot or a natural person.[69] However, the right to meaningful human interaction is seen as very important and especially regarding care work emphasis is put on emotional and social aspects for psychological well-being.[70]

Identity as the attributes, actions, beliefs and desires a person uses to distinguish herself in socially relevant ways is another aspect deeply affected by Artificial Intelligence when personal information is used for marketing, profiling and other algorithmic

---

[65] Bernd Carsten Stahl, Job Timmermans, and Catherine Flick, 'Ethics of Emerging Information and Communication Technologies: On the Implementation of Responsible Research and Innovation', *Science and Public Policy*, 44.3 (2017), 369–81.

[66] Luciano Floridi, 'Soft Ethics and the Governance of the Digital', *Philosophy & Technology*, 31.1 (2018), 1–8 (p. 4 f).

[67] Craglia and others, p. 56.

[68] Rathenau Instituut, *Human Rights in the Robot Age: Challenges Arising from the Use of Robotics, Artificial Intelligence, and Virtual and Augmented Reality* (The Hague: Council of Europe Report, 2017), p. 16 <https://www.rathenau.nl/sites/default/files/2018-02/Human%20Rights%20in%20the%20Robot%20Age-Rathenau%20Instituut-2017.pdf> [accessed 3 June 2020].

[69] Craglia and others, p. 57.

[70] Rathenau Instituut, p. 44.

applications.[71] New technologies may influence the views of individuals about what it means to be human including conceptions of authenticity and dignity.[72] The first article of the Charter of Fundamental Rights of the European Union states that '*[h]uman dignity is inviolable. It must be respected and protected.*'[73] If emerging technologies interfere with dignity, the most basic human right, it is likely that other rights are massively affected as well. Among them are other basic rights, such as the right to life and the right to the integrity of a person, or the right to respect for private life.[74] These important notions for the protection from harm caused to individuals and vulnerable groups have to be respected during the development of Artificial Intelligence. The increased interactions with machines could lead to the erosion of rights and responsibilities.[75] As smart systems cannot be accorded the moral standing of human beings, it is problematic to let them guide individuals. While the automation of production provides less ethical issues, '*it is not appropriate to manage and decide about humans in the way we manage and decide about objects or data, even if this is technically conceivable.*'[76]

Another crucial challenge on the individual level is related to privacy and data protection, which are protected rights in Article 7 and 8 of the Charter of Fundamental Rights of the European Union.[77] Emerging technologies create new methods of storing, processing and analysing the vast amounts of data produced by personal users that lead to increased privacy issues.[78] Regularly, data is sent to manufacturers of devices like phones or smart meters without knowledge of the process. Applications in the medical sectors are even more sensitive, for example when a diagnosis or treatment is suggested or if insurance or technology firms use data in a not agreed way.[79] Data protection in the US, China and the EU, with special emphasis on the General Data Protection Regulation,

---

[71] Craglia and others, p. 57.

[72] Stahl, Timmermans, and Flick, p. 374.

[73] 'Charter of Fundamental Rights of the European Union', 2012 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN> [accessed 20 April 2020].

[74] Rathenau Instituut, p. 27.

[75] European Data Protection Supervisor (EDPS), *Towards a Digital Ethics* (Brussels, 2018), p. 16 <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> [accessed 3 June 2020].

[76] European Group on Ethics in Science and New Technologies, p. 9 f.

[77] 'Charter of Fundamental Rights of the European Union'.

[78] Stahl, Timmermans, and Flick, p. 373.

[79] Craglia and others, p. 57.

will be discussed in chapter III below. In addition to the challenges on the individual level, the development and emergence of Artificial Intelligence has broader consequences on the societal level as well.

ii. Challenges on societal level

A main aspect discussed in this context is fairness and equity as well as if social inequalities will be increased or decreased by the emergence of Artificial Intelligence. Scholars found that decision-making by AI systems can lead to unfair results, because the use of algorithms could produce discriminatory outcomes for particular groups, for example in criminal justice.[80] The source of discrimination could come both from the quality of the data which is the base for training Machine Learning algorithms as well as biases of the programmers. If the high-quality standards of data cannot be ensured, AI could potentially exacerbate social inequalities present today. A bot programmed by developers of Microsoft caused sensation, as the AI application which has been released on Twitter in 2016 was removed from the platform just a few hours after the launch, because it started to use '*racial slurs, defended white supremacist propaganda, and supported genocide.'*[81] The European Group on Ethics in Science and New Technologies published a statement on AI which provides three arguments for reaching and preserving a high level of fairness and equity with emerging technologies. They argue, that the benefits have to be shared in a fair way, that equal opportunities have to be provided within societies and that governments have to foster equity by active engagement.[82]

Another cluster of topics concerns responsibility, accountability and transparency of AI systems. Accountability and the possibility to explain decisions taken by AI systems are necessary for social acceptance. In addition, explicability is a fundamental prerequisite for the justification of decisions made by algorithms and they could not be considered legitimate if they cannot be explained, especially in crucial aspects of life that

[80] Alexandra Chouldechova, 'Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments', *Big Data*, 5.2 (2017), 153–63.

[81] The Future Society, 'Making the AI Revolution Work for Everyone', 2017, p. 21 f <http://thefuturesociety.org/wp-content/uploads/2019/08/Making-the-AI-Revolution-work-for-everyone.-Report-to-OECD.-MARCH-2017.pdf> [accessed 3 June 2020].

[82] European Group on Ethics in Science and New Technologies, p. 17.

have high influence on individuals in areas like justice, health, employment or credit.[83] With increased complexity, the difficulty to assess the bearer of the responsibility of consequences of AI systems rises and smart applications provide the risk of a responsibility gap that could erode the ultimate accountability.[84] Algorithms are often referred to as black-boxes, which reflects the difficulty to explain its decision-making and provide issues regarding transparency.[85] When automated decision-making is used by authorities for predictive policing or risk assessment, it would be critical if they do not understand the functioning and therefore, transparency is important for accountability as well.[86] The GDPR goes one step further and provides a '*right to information*', which means that meaningful information about the logic behind automated decision-making processes has to be ensured.[87] Intellectual property rights are going to hinder the full disclosure of codes for algorithms, but a potential solution could be the release of certain variables used, including values and deviations as well as the data used for training.[88]

The online presence of internet users and the collection of vast amounts of data is characterised as mass-surveillance by some scholars[89] and the process of comprehensively using information about an individual is referred to as datafication, which is difficult to escape.[90] The interpretation of big data by globally leading digital companies reveals truths about human beings that can be categorised and allow the identification of needs, desires and behavioural aspects.[91] Another form of surveillance is seen in the Quantified Self movement, where people use tracking devices with the possibility of voluntary self-surveillance that provide users with management tools for

---

[83] Mission Villani, 'For a Meaningful Artificial Intelligence: Towards a French and European Strategy', 2018, p. 115 f <https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf> [accessed 3 June 2020].

[84] Stahl, Timmermans, and Flick, p. 375.

[85] Mission Villani, p. 114.

[86] Craglia and others, p. 59.

[87] Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation', *International Data Privacy Law*, 7.4 (2017), 233–42 (p. 1).

[88] Craglia and others, p. 59.

[89] Douwe Korff and others, *Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes* (University of Cambridge Faculty of Law Research Paper No. 16/2017, 2017), p. 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490> [accessed 4 June 2020].

[90] Rathenau Instituut, p. 24.

[91] Annette N Markham, Katrin Tiidenberg, and Andrew Herman, 'Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction', *Social Media + Society*, 4.3 (2018), 205630511878450 (p. 4).

health and other aspects of life.[92] In surveillance debates, some scholars argue for the creation of a new human right which provides people with '*the right to not be measured, analysed or coached.*'[93]

Artificial Intelligence is expected to influence democracy and questions about a collective human identity and the good life are raised. The Cambridge Analytica scandal gave an insight into the possibilities of algorithms to influence elections and the usage for political profiling.[94] AI systems could further increase the undermining of public discourses by massive amounts of false content that cannot easily be identified as such.[95] The use of bots already decreased trust in online environments; however, if this process was accelerated, it could create an advantage for populist politics that can make use of low-trust societies.[96] Moreover, if AI systems solely determine which content is shown via online platforms '*it challenges the freedom to receive and impart information and ideas without interferences*', which is protected by article 10 of the European Convention on Human Rights.[97] Finally, the emerging technologies bring up fundamental questions about a collective human identity and what a '*good life*' would entail. Technology could change the way human beings view themselves and alter the conditions for interaction between people. If society is technologically enhanced, questions about the essence will be raised like what it is to be human.[98] According to the Institute of Electrical and Electronics Engineers' AI principles, human well-being should always be prioritised in the process of the development of emerging technologies.[99] Another dimension that is highly influenced by AI is the use of the technology in warfare, which will be discussed in the following paragraphs.

---

[92] Lucia Vesnic-Alujevic, Melina Breitegger, and Ângela Guimarães Pereira, '"Do-It-Yourself" Healthcare? Quality of Health and Healthcare Through Wearable Sensors', *Science and Engineering Ethics*, 24.3 (2018), 887–904 (p. 887).

[93] Rathenau Instituut, p. 5.

[94] Ivan Manokha, 'Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective', *Theory & Event*, 21.4 (2018), 891–913 (p. 3).

[95] Miles Brundage and others, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Information Society Project, Future of Humanity Institute, 2018), p. 43 <https://arxiv.org/pdf/1802.07228.pdf> [accessed 8 June 2020].

[96] Brundage and others, p. 46.

[97] Rathenau Instituut, p. 37.

[98] Stahl, Timmermans, and Flick, p. 374.

[99] Floridi and others, p. 696.

iii. Challenges regarding warfare

The advances in Machine Learning and Artificial Intelligence are seen to be a turning point in warfare. Enhanced capabilities of intelligent and increasingly autonomous systems provide various legal and ethical challenges.[100] Examples of applications are remotely piloted vehicles (RPVs), mostly called drones or lethal autonomous weapons systems (LAWS). While different military AI applications are discussed in chapter III. B. a), this paragraph focuses on ethical and legal challenges that are raised by the development as well as the use of this technology. To begin with, the four general principles of International Humanitarian Law (IHL), also known as the Law of Armed Conflict (LOAC), will be presented. The first one, distinction, means to distinguish combatants and civilians while employing force. The second, proportionality, states that the military advantage has to be proportional to the loss of civilian life and property. The third, called principle of humanity, states that suffering has to be minimised and unnecessary suffering has to be avoided. Fourth, military necessity has to be given and force can only be applied to legitimate objectives.[101] If AI systems used lethal force without human intervention, so to say autonomously, many scholars would see conflict and inconsistency with the standards of International Humanitarian Law. The arguments behind are the potential incapability of machines to distinguish combatants from civilians and to assess the proportionality of an attack.[102] In the foreseeable future, the possibility of autonomous weapons systems' (AWS) compliance with these rules is doubted. If an AWS is to comply with IHL conditions, the weapon system should be capable of '*respecting the principles of distinction and proportionality at least as well as a competent and conscientious human soldier.*'[103] Other scholars go even further and state that the use of lethal force by machines is incompatible with human rights and consider the

---

[100] Gregory Allen and Taniel Chan, *Artificial Intelligence and National Security* (Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2017), p. 5 <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> [accessed 9 June 2020].

[101] Vivek Sehrawat, 'Legal Status of Drones under LOAC and International Law', *Penn State Journal of Law & International Affairs*, 5.1 (2017), 164–206 (p. 176 ff).

[102] Eleanor Bird and others, 'The Ethics of Artificial Intelligence: Issues and Initiatives' (EPRS, European Parliamentary Research Service, Brussels, 2020), p. 64 f <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf> [accessed 29 May 2020].

[103] Daniele Amoroso and Guglielmo Tamburrini, 'The Ethical and Legal Case Against Autonomy in Weapons Systems', *Global Jurist*, 18.1 (2018), p. 5 f <https://www.degruyter.com/doi/10.1515/gj-2017-0012> [accessed 9 June 2020].

delegation of life or death decisions to be morally wrong.[104] The use of lethal force is so severe that it can only be made by humans as only they can feel the agony.[105]

The aspect of the responsibility of a drone operator for war crimes is seen as the most controversial legal question. International criminal law and LOAC state that military forces are responsible for war crimes they commit during war. For Peter Maurer, president of the International Committee of the Red Cross (ICRC), there is no doubt that drone operators share the same responsibility as other military personnel operating directly on the battlefield. The fact that a person who remotely controls a drone is far away from the battlefield does not affect the accountability codified by IHL. Drone operators and their chain of command have to ensure compliance with the LOAC principles.[106] Other scholars argue that the responsibility for AI-enabled autonomous systems that commit war crimes should '*fall on both the individual who programmed the AI, and the commander or supervisor*'.[107] In an interview, Peter Maurer stated that drones are not expressly prohibited by International Humanitarian Law. However, if equipped with chemical weapons or '*precision-guided Hellfire*' missiles, they would be prohibited by IHL.[108]

As a result of the legal and moral issues, the author of this master's thesis considers the application of AI in the military realm as inconsistent with the basic values implied by Ian Manners' concept normative power. The development of military AI is associated with many uncertainties and absolute prevention of possible abuse is difficult to achieve. After discussing challenges regarding ethics, society and warfare, the next chapter will outline AI initiatives by some selected states.

---

[104] Peter Asaro, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making', *International Review of the Red Cross*, 94.886 (2012), 687–709 (p. 687 f).

[105] Aaron M. Johnson and Sidney Axinn, 'The Morality of Autonomous Robots', *Journal of Military Ethics*, 12.2 (2013), 129–41 (p. 136).

[106] Sehrawat, p. 201 f.

[107] Bird and others, p. 65.

[108] Sehrawat, p. 184 f.

C. National initiatives

A couple of years ago, various states started implementing national initiatives on the development of Artificial Intelligence. The global landscape shows that the US, China and the European Union are leading, while other countries such as Canada, Japan, South Korea, India, Israel and Singapore have considerable development projects running as well.[109] The most relevant for this paper will be outlined in the following paragraphs.

a. 'America first' in AI

The Obama Administration was one of the first to publish a report on the impact of AI in 2016. It included impact assessments, a strategic outlook for research and development (R&D) as well as security considerations.[110] In 2018, The Defense Advanced Research Project Agency (DARPA) of the Department of Defense (DoD) announced its '*AI Next Campaign*' with funding of two billion US-Dollar and the goal of developing the next wave of AI applications.[111] At the beginning of 2019, President Trump signed an executive order launching the initiative on '*Maintaining American Leadership in AI.*'[112] The approach asks for an acceleration of the US leadership stating that the government will play a central role and not only facilitate AI R&D, but also promote trust, train AI talents, take security interests sufficiently into account and foster cooperation with foreign partners and the private sector.[113] In June 2019, the US government launched an update of its strategic plan on AI emphasising the need to focus on eight pillars. These are long-term investments in AI, developing effective methods for human-AI collaboration, understanding and addressing the societal, legal and ethical aspects of AI, ensuring safety and security of AI systems, developing shared public data sets and environments for AI training and testing, measuring AI technology via standards and benchmarks, better

---

[109] Craglia and others, p. 25 ff.

[110] Executive Office of the President, *Preparing for the Future of Artificial Intelligence* (Washington, D.C.: National Science and Technology Council Committee on Technology, 2016) <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf> [accessed 13 August 2020].

[111] Defense Advanced Research Projects Agency (DARPA), 'DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies', 2018 <https://www.darpa.mil/news-events/2018-09-07> [accessed 2 May 2020].

[112] Donald J. Trump, *Executive Order on Maintaining American Leadership in Artificial Intelligence* (Washington, D.C.: The White House, 2019) <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/> [accessed 13 August 2020].

[113] Perrault and others, p. 179.

understanding the needs of the workforce for US AI R&D and fostering public-private partnerships.[114] While Chinese plans for leadership in AI seem partly similar, differences can be ascertained, as the following subchapter shows.

b. Chinese plans for leadership

China's ambitious AI development plan has many similarities with the reports published by the Obama administration. Some observers argue that the Chinese government copied America's plan and wants to dominate the AI sector with even higher efforts.[115] In October 2017, president Xi Jinping mentioned the possibilities of economic growth and increased productivity through AI in the opening speech of the 19th Party Congress of the Communist Party.[116] But China's dream of leading the world in AI technologies is not only an abstract goal, it has been formulated in clear steps with three different stages in the '*Next Generation Artificial Intelligence Development Plan.*'[117] By 2020, China's AI industry will be '*in line*' with the most advanced competitors having a gross output of the core industry with at least USD 22.5 billion and more than USD 150 billion of the related sectors. By 2025, the country seeks to be '*world-leading*' in some fields of AI technology with a core AI industry gross output exceeding USD 60 billion and AI-related industries gross output exceeding USD 750 billion. By 2030, China aims to be the world's '*primary*' AI innovation centre with a core AI industry gross output of more than USD 150 billion and AI-related gross output of more than USD 1.5 trillion.[118]

A few months after the announcement of the initiative in 2017, the Chinese Ministry of Science and Technology (MOST) came up with concrete decisions regarding AI development. Tencent, China's social networking platform comparable to Facebook,

---

[114] Select Committee on Artificial Intelligence, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (Washington, D.C.: National Science and Technology Council Committee on Technology, 2019) <https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf> [accessed 13 August 2020].

[115] Gregory Allen and Elsa B. Kania, 'China Is Using America's Own Plan to Dominate the Future of Artificial Intelligence', *Foreign Policy*, 8 September 2017 <https://foreignpolicy.com/2017/09/08/china-is-using-americas-own-plan-to-dominate-the-future-of-artificial-intelligence/> [accessed 25 March 2020].

[116] Ding, p. 8.

[117] Eurasia Group, *China Embraces AI: A Close Look and A Long View* (New York, 2017), p. 9 <https://www.eurasiagroup.net/files/upload/China_Embraces_AI.pdf> [accessed 13 August 2020].

[118] Ding, p. 10.

was designated to lead the medical AI platform. Baidu, a search engine sometimes called '*Chinese Google*' is responsible for the development of autonomous vehicles. Online retailer and cloud operator Alibaba, which has similarities to Amazon, was determined for smart city innovation and iFlyTek for speech interfaces.[119] This shows how the state interferes and guides the development of the technology. In general, those Chinese ambitious initiatives are seen as a reflexion of the political goal of '*setting the pace*' in AI technology, rather than '*running after.*'[120] In the next paragraph, the European aspects will shortly be outlined.

c. The EU's need to catch up

The emergence of Chinese digital champions that compete with US companies on the global market has increased the pressure on Europe for creating its own AI strategy. Digital champions such as Google, Amazon and Facebook are important players in the field of Artificial Intelligence, as these companies not only invest heavily in the technology, have access to massive amounts of data, the most significant resource for AI, but additionally have the best trained experts working for them.[121] Although the EU is behind the US and China regarding the corporate sector, it plays a significant role concerning Research and Development with about one quarter of AI research players globally.[122] In 2018, the Commission allocated additional funding for AI through the research and innovation framework programme Horizon 2020 of around 1.5 billion Euro by the end of 2020, which was an increase of approximately 70 percent.[123] The plans set in the European Commission's white paper come with the objective to '*attract over €20 billion of total investment in the EU per year in AI over the next decade.*'[124] The European initiatives on AI will be discussed in more detail in chapter IV. In general, the focus of the EU lies on ensuring trustworthy, ethical, human-centric AI that is based on European values and fundamental rights. The next chapter will compare the US, China and the EU regarding data protection regulation and military AI.

---

[119] Eurasia Group, p. 9.
[120] Ding, p. 12.
[121] Eurasia Group, p. 5.
[122] Craglia and others, p. 32.
[123] European Commission, 'Artificial Intelligence for Europe, COM 237 Final', p. 5 f.
[124] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 5.

III. Comparing the US, China and the EU

A. No data, no glory

Data is supposed to be the most important factor for the information economy, sometimes referred to as the '*ultimate driver*' for the development of Artificial Intelligence[125] and is regularly compared to oil, which was the most crucial resource for the industrial economy. Apart from the centrality to the respective field, the analogy is critically reflected by some scholars who argue that the metaphor is misguiding and does not put enough emphasis on the individuals from whom the data is collected, in opposition to oil, which is extracted from natural sources.[126] Looking at the economic characteristics of data shows that it can be depicted by three main aspects namely economies of scale, economies of scope and non-rivalry. The first can be described with the high fixed costs of high-quality data sets for the training of, for instance, Machine Learning algorithms, while the marginal costs of further use could be quite low. The second implies that the analysis of a merged data set delivers greater benefits than a separate evaluation. The third means that an algorithm can be used by more people at the same time, while products and services are often subject to rivalry and therefore can only be used by a single person.[127]

As Artificial Intelligence systems, especially Machine Learning, require huge amounts of data for the training processes, data availability is crucial for the development of the technology.[128] However, the perfect balance between open access to foster innovation and restricting it for privacy protection is one of the main challenges.[129] This issue leads to conflicting strategies and approaches, which are both interesting and important to assess among the three systems. Therefore, this chapter is going to discuss the US, Chinese and European approaches regarding the protection of personal data and regulation for privacy concerns. The United States have a liberal approach, where

---

[125] Ding, p. 28.

[126] Lauren Scholz, 'Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies', *SSRN Electronic Journal*, 2018 <https://www.ssrn.com/abstract=3252543> [accessed 9 April 2020].

[127] Craglia and others, p. 103.

[128] Castro, McLaughlin, and Chivot, p. 36 ff.

[129] Craglia and others, p. 103.

individuals are seen as '*online consumers.*' The US Federal Trade Commission (FTC) ensures that actors have access to the terms of the transaction to make informed decisions, but companies are free to contract data collection, processing, and retention.[130] China's current level of protection is slightly lower than the standards provided by the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe in the early 1980s. However, in 2018, the Standing Committee of the National People's Congress of China updated its legislative agenda, planning to enact a comprehensive data protection law by March 2022. The implementation comes with many obstacles such as counteracting Information and Communications Technology (ICT) development strategies, the existing legal framework and limited voices of scholars, public and ordinary lawmakers.[131] In contrast, for Europeans, data protection is an inalienable right. EU online users are '*data subjects*' whose fundamental rights are protected with strong legal instruments like the General Data Protection Regulation.[132]

Apart from the three systems' own regulatory regimes, there are some noteworthy international data protection alternatives provided by the OECD, the Council of Europe and the Asia-Pacific Economic Cooperation (APEC).[133] In 1980, the OECD, where most of the Member States of the European Union and the United States are involved, published '*Guidelines on the Protection of Transborder Flow of Personal Data.*'[134] The Guidelines, which have been updated in 2013, are foundational for the EU's approach while the US took a different path, a so-called sectoral approach which will be discussed below.[135] The document regards an enforcement mechanism as important, but due to the flexibility in their wording and the fact that it is voluntary, a more global outreach has been achieved.[136] The Council of Europe Data Protection Convention was signed in 1981 with the advantage of openness for ratification to non-European countries as well. It

---

130 Lancieri, p. 31 f.

131 Feng.

132 Lancieri, p. 27 ff.

133 Paul De Hert and Dr. Vagelis Papakonstantinou, 'The Data Protection Regime in China. In-Depth Analysis', 2015, p. 9 <https://www.ssrn.com/abstract=2773577> [accessed 13 April 2020].

134 OECD, 'Guidelines on the Protection of Transborder Flow of Personal Data', 1980 <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [accessed 16 April 2020].

135 W. Gregory Voss and Kimberly A. Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies', *American Business Law Journal*, 56.2 (2019), 287–344 (p. 293 f).

136 De Hert and Papakonstantinou, p. 9.

already included high-level principles, enforcement agencies and application to all data processing, which is the main structure of the EU model until today.[137] The APEC framework is broadly in line with the EU model and provides basic rules for the processing of personal data on a voluntary basis, but has major differences concerning enforcement mechanisms and the protection of individuals in general.[138]

The field of data offers different aspects for a comparison of the three systems. Among the possible elements are the number of mobile payments, which are especially high in China, data created by Internet of Things devices, again with Chinese leadership, electronic health records, genetic data and others.[139] These factors have already been subject to comparison in other AI-reports,[140] while this project mainly focuses on the regulatory framework for data protection in the United States, China and the EU. It is considered the most relevant aspect for the assessment of Europe as a normative power and whether the EU acts in line with its principles. If the EU has a comprehensive data protection regime in effect, this category would be regarded as norm-guided. The chapter will start with the US approach, will be followed by the Chinese perspective and then look into the regulatory framework of the EU.

a. Freedom for data in the US

In 1890, Samuel Warren and Louis Brandeis, both American lawyers, published a journal article called '*The Right to Privacy*'[141] in the Harvard Law Review, which was not only credited with '*legendary status*' by some scholars, but is seen as the pathbreaking force for the development of the '*right to privacy*' in US law.[142] The Constitution of the United States did not mention data privacy, data protection or privacy at all. However, based on the arguments of the two lawyers, the right to privacy, which has been derived from and

[137] De Hert and Papakonstantinou, p. 9.
[138] De Hert and Papakonstantinou, p. 9.
[139] Castro, McLaughlin, and Chivot, p. 36 ff.
[140] Castro, McLaughlin, and Chivot.
[141] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', *Harvard Law Review*, 4.5 (1890), 193–220.
[142] Benjamin E Bratman, 'Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy', *Tennessee Law Review*, 69.3 (2002), 623–51.

implied by the '*right to life*' and common law, has been accepted by US courts later.[143] The legal foundation is a paragraph in the Fourth Amendment, which says '*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.*'[144] This can be seen as the historical start for American privacy leadership, that regards protection against state authorities and privacy in one's home as crucial rights.[145]

The fundamental perspective of American privacy law always imagines '*the home as the primary defense, and the state as the primary enemy*,'[146] and therefore, in the public sector, a certain degree of protection is given.[147] The negative freedom at the core of the concept of privacy reflects the American values of liberty, self-government, self-determination, freedom of expression as well as the marketplace of ideas[148] and shows a different culture of privacy protection than for instance in the European Union.[149] Importantly, the Constitution and the Fourth Amendment did not provide privacy protection among private actors for '*horizontal-to-horizontal*' relations. The legal document did not oblige the government with actively creating the conditions to allow the existence of fundamental rights.[150] A scholar argued that the reason behind was the fear of oppression from state authority and the political will of limiting the government's power.[151] However, the protection of privacy in the US does not stop in the sphere of public-private relationships, as the courts have recognised privacy against private actors, although the Fourth Amendment did not provide enforcement for these circumstances.[152] Another commentator saw the dissent between rulings and interpretations of the Supreme Court and the Congress as well as the limited scope that the Fourth Amendment

---

[143] Warren and Brandeis, p. 193 ff; Alan Charles Raul, Christopher C. Fonzone, and Snezhana Stadnik Tapia, 'Chapter 26: United States', in *The Privacy, Data Protection and Cybersecurity Law Review* (London: Law Business Research Ltd., 2019), p. 399 f.

[144] Voss and Houser, p. 296.

[145] Raul, Fonzone, and Stadnik Tapia, p. 399.

[146] James Q. Whitman, 'The Two Western Cultures of Privacy Dignity Versus Liberty', *The Yale Law Journal*, 113.6 (2004), 1151–1221 (p. 1215).

[147] Schwartz and Peifer, p. 133.

[148] Lancieri, p. 31 f.

[149] Lancieri, p. 30.

[150] Schwartz and Peifer, p. 132 f.

[151] Schwartz and Peifer, p. 133.

[152] Voss and Houser, p. 296.

provided as a reason for the federal government's decision to establish laws that protect special areas of information rather than developing a broader regulatory framework for all kinds of data. This sectoral approach, which will be discussed in more detail below, is still central for today's privacy protection in the US, that relies on a mix of legislation, regulation and self-regulation.[153]

On the contrary, a field that enjoys constitutional protection in the United States is the free flow of data. The principle of free information circulation makes processing of data possible, as long as no law directly prohibits it, which is a fundamental difference to the European approach.[154] In short, there is no omnibus law that protects individual's privacy, which leaves significant aspects of personal information use free from legal limitations.[155] An important aspect is the fact that companies are free to contract around data collection and data in general is seen as an asset which can be freely traded.[156] This reflects the dominance of the marketplace logic in the discourse which aims at protecting consumers and encourages the promotion of competition.[157] The FTC, while having no data protection mandate nor fining authority, is responsible for the regulation of the private information markets and has to ensure that consumers have access to the terms and conditions of their transactions for being able to make informed decisions.[158] This agency tries to prevent unfair or deceptive practices and has stopped companies from '*tricking consumers, overpromising privacy, and engaging in unexpected and unreasonable data practices.*'[159] The two most important aspects in that regard are notice and consent. Statutes in the US require companies to notice individuals about privacy practices, to inform the customer about how organisations plan to use their personal data and the information must be '*clear, conspicuous and accurate.*'[160] For consent, two different types can be distinguished. In the case of opt-in, unless the individual has given the permission, personal data processing cannot take place. Under opt-out, if the individual has not

[153] Voss and Houser, p. 294 ff.
[154] Schwartz and Peifer, p. 135.
[155] Schwartz and Peifer, p. 136 f.
[156] Lancieri, p. 32.
[157] Schwartz and Peifer, p. 136.
[158] Lior Strahilevitz, 'Towards a Positive Theory of Privacy Law', *Harvard Law Review*, 126.7 (2013), 2010–41 (p. 2036); Lancieri, p. 32.
[159] Schwartz and Peifer, pp. 136, 150.
[160] Schwartz and Peifer, p. 148.

objected, the processing can take place.[161] The FTC assumes that the consumer reads the online terms and conditions, which is seen as an '*idealized*' form of consent by some scholars, some even calling it a '*legal fiction*', because '*most consumers do not read privacy policies.*'[162] Another problem is raised by US courts, as some judges see privacy policies as contracts, while others do not find the terms enforceable in contracts.[163]

Moreover, US data processors do not need a legal justification for using, processing or collecting personal data, as the Constitution does not include a respective mandate. In fact, no equivalent to the EU's fundamental right to data protection exists.[164] As long as digital companies follow sectoral and other legal requirements, and disclose their data practices, the actions are in line with the regulations.[165] In opposition to the EU, the strongest constitutional protection is given to data processors, and not to the consumers whose data and personal information are at stake.[166] The upside of this legal framework is a regulatory environment which promotes growth of digital companies.[167] Some scholars argue that a comprehensive federal privacy law would have negative effects on experimentation and innovation, while a sectoral approach is superior in that aspect, because it only regulates a specific area of information use.[168]

In the following paragraphs, the legal framework of the United States will be discussed. Concerning the terms used in the field of privacy protection, the EU is quite concise and mainly uses 'personal data', while the United States have different legal terms. Personal information, and personally identifiable information (PII) are among the ones used with the highest frequency.[169] The legal framework of the US consists of federal and state law. Federal law has three main aspects, the FTC, cybersecurity and data breaches as well as specific regulatory areas. The United States not only lacks an omnibus federal privacy law, but a central data protection authority, too. The FTC with its function

[161] Schwartz and Peifer, p. 152.
[162] Schwartz and Peifer, p. 150.
[163] Schwartz and Peifer, p. 151.
[164] Schwartz and Peifer, p. 137.
[165] Schwartz and Peifer, p. 151.
[166] Schwartz and Peifer, p. 137.
[167] Schwartz and Peifer, p. 137.
[168] Paul M. Schwartz, 'Preemption and Privacy', *The Yale Law Journal*, 118.5 (2009), 902–47.
[169] Voss and Houser, p. 292.

of ensuring consumer privacy is the closest equivalent to such an authority.[170] Cybersecurity has been constituted as a major aspect in the last years, but a general authority for ensuring the protection does not exist, again with the FTC being the closest equivalent. The National Institute of Standards and Technology (NIST) developed a cybersecurity framework, which aims to support companies regarding cybersecurity risks, especially those holding sensitive consumer and business information.[171] In addition, some areas are specifically protected by federal law which are financial information, healthcare information, information about children, electronic communications and records, and credit and consumer reports.[172]

On a state level, the degree of protection among the 50 US states varies significantly. Particular emphasis in state law was put on the requirement of notifications after data protection breaches.[173] Regarding consumer protection, the state attorneys general are in charge of enforcement actions, and have a similar function to the FTC on federal level.[174] The sectoral approach is also implemented at state-level. Legislations encompass biometric information, cyberstalking, data disposal, privacy policies, employer access to employee social media accounts, unsolicited commercial communications and electronic solicitation of children, among others.[175] The state with the most comprehensive data protection legislation is California, where the California Consumer Privacy Act (CCPA), sometimes referred to as '*California's General Data Protection Regulation (GDPR)*' came into effect on 1 January 2020.[176] It will apply to businesses that reach one of the thresholds of: '*(1) annual gross revenue of 25 million US-Dollar, (2) obtains personal information of 50,000 or more California residents, households, or devices annually; or (3) fifty percent or more annual revenue from selling California residents' personal information.*'[177] The bill includes the right for residents of the state to access and delete their personal information and the right to stop businesses from selling

[170] Raul, Fonzone, and Stadnik Tapia, p. 401.
[171] Raul, Fonzone, and Stadnik Tapia, p. 402.
[172] Raul, Fonzone, and Stadnik Tapia, p. 403.
[173] Raul, Fonzone, and Stadnik Tapia, p. 407.
[174] Raul, Fonzone, and Stadnik Tapia, p. 408.
[175] Raul, Fonzone, and Stadnik Tapia, p. 408.
[176] Raul, Fonzone, and Stadnik Tapia, p. 416.
[177] Voss and Houser, p. 307.

their information to third parties.[178] Following the Californian lead, other states started to implement stricter regulations as well.[179]

The United States, once seen as a global leader in privacy protection, was painted in a different light in the last decades. The commitment to technological superiority in the information age led to a more flexible regulatory approach, that benefitted the development of the industry. However, latest incidents with high-profile data breaches in the private and public realm and increasing concerns about disinformation and misuse of data led to a '*crisis of new technology*' or a '*techlash*' which shifted public opinion in the country.[180] In this regard, the latest settlement between Facebook and the FTC is especially noteworthy. On 24 July 2019, the biggest settlement any privacy regulator ever made was sealed. The company agreed to pay five billion US-Dollar in the aftermath of the Cambridge Analytica scandal.[181] In order to drop the charges, the company further agreed on implementing a new governance for privacy and data protection, which should ensure the accountability of the corporation's decisions regarding user privacy.[182] As a result, some even assess a new privacy zeitgeist to emerge in the United States.[183] The following chapter will discuss the Chinese data protection framework.

b. China: Forerunner or laggard?

China has no omnibus privacy and data protection law in place, but industry specific regulations.[184] In general, the comparison of the Chinese legal system with a European or Western-type human rights model is not an easy task. There are big differences in culture and the fact that China is lacking some of the most crucial components for human rights such as independent courts, legal certainty and horizontal application makes it even more difficult.[185] Although a shift in the direction of more individual privacy can be observed

---

178 Raul, Fonzone, and Stadnik Tapia, p. 416.
179 Raul, Fonzone, and Stadnik Tapia, p. 417 f.
180 Raul, Fonzone, and Stadnik Tapia, p. 399 f.
181 Alan Charles Raul, *The Privacy, Data Protection and Cybersecurity Law Review* (London: Law Business Research Ltd., 2019), p. 2.
182 Raul, Fonzone, and Stadnik Tapia, p. 411 f.
183 Raul, Fonzone, and Stadnik Tapia, p. 400.
184 Hongquan Yang, 'Chapter 8: China', in *The Privacy, Data Protection and Cybersecurity Law Review*, 6th edn (London: Law Business Research Ltd., 2019), p. 115; De Hert and Papakonstantinou, p. 1 ff.
185 De Hert and Papakonstantinou, p. 3 f.

in the country, traditional collective values about the concept of society are still very dominant.[186] While US privacy protection laws are generally focused on the public sector and the individual's freedom against state interference, the legislative framework in China provides citizens with some basic protection against private network operators, but has very little regulation regarding the collection of data in the public sector in place.[187] When it comes to setting the priorities, the Chinese system provides constitutional protection for the industrial development of the country, while on the contrary, the right to privacy does not enjoy such backing.[188] The importance of personal data as a commodity for businesses and political organisations created an area of conflict between the robustness of economic growth and the protection of privacy.[189]

The Chinese constitution, which was adopted in 1982 and has been amended five times since then, is in general seen to be unprepared for a comprehensive data protection regime.[190] Important to mention is the fact that the constitution cannot be perceived in the same way as in Western legal systems. For instance, Article 35 states that '*citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession, and of demonstration*.' However, Chinese courts do not conduct enforcements of legal complaints on the basis of violations against the constitution. In addition, there is no procedure to invalidate legal paragraphs or articles if the rights guaranteed by the constitution are not respected.[191] Therefore, China's constitution is in general regarded as '*non-justiciable*'.[192] While the enforcement is questionable, some privacy-related aspects are mentioned in the constitution, for instance Article 38 states that '*the personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false charge or frame-up directed against citizens by any means is prohibited.*'[193] In addition, Article 40 protects '*the freedom and privacy of correspondence.*' However, the

---

[186] Charles Ess, '"Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)', *Ethics and Information Technology*, 7.1 (2005), 1–6 (p. 2).

[187] Feng, p. 68 f.

[188] Feng, p. 64.

[189] Tao Fu, 'China's Personal Information Protection in a Data-Driven Economy: A Privacy Policy Study of Alibaba, Baidu and Tencent', *Global Media and Communication*, 15.2 (2019), 195–213 (p. 196).

[190] Feng, p. 69.

[191] De Hert and Papakonstantinou, p. 14.

[192] Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (United Kingdom: Oxford University Press, 2014), p. 196.

[193] De Hert and Papakonstantinou, p. 14.

very low number of cases regarding the protection of fundamental rights suggests that the constitution alone provides little potential for the derivation of data or privacy protection.[194]

For criminal law, Article 253 (a) provides specific regulation for the sectors of finance, telecommunications, transportation, education and medical treatment.[195] If individuals or organisations sell or illegally provide personal information, the threat of punishment makes imprisonment of up to three years and/or monetary fines possible.[196] While the threshold for criminalising the abuse of data is quite low in China, in reality, the rate of conviction is pretty low and the vast majority is able to escape from criminal punishment because enforcement agencies' lack of resources.[197] Regarding civil law, the 1986 General Principles of Civil Law (GPCL), the country's civil code, provide a '*right of reputation.*'[198] Until the promulgation of the GPCL in 2017, no independent right to privacy was formulated in the legal document.[199] However, the Supreme People's Court's interpretations already suggested the protection of privacy, because the disclosure of personal information was seen as an interference to the right to reputation and personality.[200] In the field of civil law, one finds a right to privacy in the Tort Liability Law since its recognition in 2009, which now enjoys protection to the same extent as reputation.[201] After the GPCL's latest update in 2017, Article 111 of this law claims to protect citizens' personal information, which can be seen as an extension of the scope of protection regarding data privacy.[202] Although the right to privacy is increasingly respected, the legal developments are not mirrored in the numbers of judicial cases, as the laws are mainly underused. Reasons for that can be the still dominant traditional collectivist values, which lead to the hesitation of courts to offer protection for the infringement of privacy.[203]

---

[194] De Hert and Papakonstantinou, p. 14.
[195] De Hert and Papakonstantinou, p. 14 f.
[196] Fu, p. 201.
[197] Feng, p. 71 f.
[198] De Hert and Papakonstantinou, p. 15.
[199] Feng, p. 69; De Hert and Papakonstantinou, p. 15.
[200] Greenleaf, p. 200.
[201] Feng, p. 69.
[202] Feng, p. 69.
[203] Feng, p. 70 f.

Apart from the general legal framework in China, one of the most significant developments regarding data protection over the last years was probably the promulgation of the Cybersecurity Law (CSL) in 2016.[204] While personal information protection is an aspect of the CSL, the main focus lies on cybersecurity (i.e. the protection of internet-connected systems such as hardware, software and data from cyber-threats), network operation as well as network information security[205] and the law is based on the claim that China wants to increase cyberspace sovereignty and security.[206] The provisions of the law include protection rules that can be organised around general requirements for network operators, such as notice and consent, purpose limitation, data quality, transparency, security, correction, data localisation, and accountability.[207] These propositions led to uncertainty regarding foreign companies' operation in the country.[208] Some internet firms even withdrew their cloud services from China or switched to Chinese suppliers and a chilling effect can be seen.[209] As the main target of this legislation is cybersecurity and only a small part concerns data protection, it is difficult to consider it '*China's first data protection law.*'[210] However, both scope and comprehensiveness suggest that it can be seen as a milestone for the development of a data protection regime. An area of conflict that has to be addressed is the problem of public security as a threat to an individual's privacy. While cyber- and national security are reasonable claims, the negative effect on online anonymity and privacy have to be considered.[211] Looking into the specific Articles of the law will give more insight. Regarding personal information protection, the CSL only comes with general obligations for data collectors such as stated in Article 41: '*[n]etwork operators shall abide by the 'lawful, justifiable and necessary' principles to collect and use personal information*.'[212] Article 43 states that '*[e]ach individual is entitled to require a network operator to delete his or her personal information*

[204] Feng, p. 72.
[205] Yang, p. 133.
[206] Feng, p. 72.
[207] Feng, p. 72.
[208] Max Parasol, 'The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams', *Computer Law & Security Review*, 34.1 (2018), 67–98.
[209] Jyh-An Lee, 'Hacking into China's Cybersecurity Law', *Wake Forest Law Review*, 53.1 (2018), 49 (p. 80).
[210] Feng, p. 72.
[211] Feng, p. 74.
[212] Yang, p. 119.

if he or she founds that collection and use of such information by such operator violate the laws, […].'[213] The CSL added new or more explicit requirements concerning data correction rights and deletion, but typical elements found in other jurisdictions such as explicit user access rights, requirements for data quality and special provisions for sensitive data as well as a determined government authority for data protection are still missing.[214]

China's last two decades of data protection development have been guided by a sectoral approach, where both legally binding rules such as the CSL have been implemented, but also regulations, ministerial rules and non-binding guidelines and standards have been published.[215] In 2013, the non-binding '*Information Security Technology Guidelines for Personal Information Protection on Public and Commercial Service Information Systems*' for the protection of privacy and data came into effect and represents the first national standard regarding the topic.[216] The guidelines announced eight principles, which are clear purpose, least sufficient use, open notification, individual consent, quality guarantee, security guarantee, honest implementation and clear responsibilities, which have close similarities to the CSL.[217] In 2018, a new national standard, called '*Information Security Techniques – Personal Information Security Specification*' came into effect.[218] Similar to the guidelines published in 2013, the standard lacks the force of law, however, the latter one has less limitations and is proposed to cover both public and private organisations.[219] In contrast to the two non-binding documents, another binding ministerial provision came into effect in 2013 and was published by the Ministry of Industry and Information Technology (MIIT).[220] A study found that the Chinese internet giants Alibaba, Tencent and Baidu are generally compliant with the Provisions developed by the MIIT, and while they offer very little about choice, the

[213] Yang, p. 122.
[214] Graham Greenleaf and Scott Livingston, 'China's Personal Information Standard: The Long March to a Privacy Law', *150 Privacy Laws & Business International Report 25-28*, 2017, p. 1.
[215] Feng, p. 73.
[216] Fu, p. 201.
[217] Fu, p. 201.
[218] Greenleaf and Livingston, p. 1.
[219] Greenleaf and Livingston, p. 2.
[220] Fu, p. 201.

disclosure concerning what information is collected and used was adequate.[221] The companies did not limit their collection in order to give value to the user, but rather used a '*providing-a-better-service-or-product rationale […] for making money.*'[222]

A main obstacle regarding most of the legal provisions is their ineffectiveness. In 2017, a report by the Standing Committee of the National People's Congress (NPCSC) concluded that '*the work of personal information protection encounters was severely difficult.*'[223] At the core of the problem lies the lack of a unified supervisory authority that controls and enforces the compliance with legal provisions. At the time, the responsibilities are divided among diverse government agencies, and they cannot pay adequate attention to data protection, as their main focus lies on different duties. For instance, the People's Bank of China is the responsible authority for the enforcement of data protection in the financial realm.[224] The country has neither a supervising state authority as seen in the EU, nor an US-style Federal Trade Commission with concentrated authority.[225] As a result, different government agencies try to increase compliance with other means. In 2018, the MIIT required the three Chinese internet companies Baidu, Alibaba and Toutiao to revise their practice and '*protect the users' right to know and right to choose.*'[226] In 2019, the China Consumer Association (CAC) published a report about the collection of personal information and privacy policies of 100 apps for the purpose of consumer information.[227] The Ministry of Public Security (MPS) launched a campaign for the clearance and punishment of illegal activities on the internet.[228] Campaign-style enforcement is typical for the Chinese system and is usually adopted when regular measures fail.[229] Another '*Special Crackdown Campaign*' was released in January 2019 by

[221] Fu, p. 206 f.
[222] Fu, p. 207.
[223] Feng, p. 74.
[224] Feng, p. 75.
[225] De Hert and Papakonstantinou, p. 22.
[226] Yang, p. 116.
[227] Yang, p. 116.
[228] Yang, p. 131.
[229] Nicole Ning Liu and others, 'Campaign-Style Enforcement and Regulatory Compliance', *Public Administration Review*, 75.1 (2015), 85–95.

the CAC and many other government organisations joined. The result was public exposure and the order to rectify illegal practices regarding personal data collection.[230]

In sum, China is at least 30 years behind in the field of privacy protection.[231] It's current degree of protection is slightly lower than the OECD and Council of Europe standards *'of the early 1980s and much lower than the 'European standards' of the mid-1990s.'*[232] However, 20 years ago, for many Chinese citizens the right to privacy was only a vague and '*strange*' concept, with difficulties to distinguish '*shameful secret (yinsi) and privacy (yinsi)*', which only have different tones in their pronunciation.[233] Although accompanied by a high degree of uncertainty, the Standing Committee of the National People's Congress of China updated its legislative agenda in 2018 with the prospect of the enactment of a comprehensive data protection law in March 2022.[234] The biggest obstacles remain the focus on state and industry-driven development, which are probably going to shape future data protection frameworks.[235]

c. The EU and the gold standard of data protection

The European Union's data protection regulatory framework is, in opposition to the two systems discussed above, of omnibus nature.[236] An omnibus law is characterised by the coverage of the processing of both public and private sector data, no matter which economic field is touched, and no areas are left unregulated.[237] In general, Europeans consider data protection an inalienable right and personal privacy is more comprehensively protected, which reflects for instance German and French cultures.[238] The starting point of this development occurred before World War II, when different national governments in Europe equipped their constitutions with the rights of personality and dignity. The post-war constitutions of Italy and Germany, which drew their lessons about the importance of human dignity after their devastating experiences

230 Yang, p. 116.
231 Fu, p. 197.
232 Feng, p. 73.
233 Guobin Zhu, 'The Right to Privacy: An Emerging Right in Chinese Law', *Statute Law Review*, 18.3 (1997), p. 208.
234 Feng, p. 62.
235 Feng, p. 64.
236 Voss and Houser, p. 324.
237 Schwartz and Peifer, p. 128 f.
238 Lancieri, p. 27 ff.

of the war are particularly to mention.[239] Moreover, Europe recognised the necessity of supranational legal systems for fundamental rights. Today, protection of these rights is provided by the European Court of Justice, an official EU institution, and the European Court of Human Rights, an international court.[240]

The legal basis of the protection is multi-layered. The European Convention of Human Rights, an international treaty that was signed in Rome in 1950, is one of the core pillars.[241] In Article 8, the '*Right to respect for private and family life*' is provided.[242] The Treaty on the Functioning of the European Union (TFEU), one of the foundational documents of the EU, states in Article 16 (1) that: '*[e]veryone has the right to the protection of personal data concerning them.*'[243] The Charter of Fundamental Rights, a primary constitutional text of the EU, which came into effect in 2009 with the Treaty of Lisbon, serves as the second core pillar within European law.[244] Its Article 7 '*Respect for private and family life*' states that '*[e]veryone has the right to respect for his or her private and family life, home and communications.*' Article 8 '*Protection of personal data*' states in paragraph one that: '*[e]veryone has the right to the protection of personal data concerning him or her.*'[245] In sum, there are different sources for fundamental rights in Europe and the protection is guaranteed by constitutional courts.[246] These legal provisions show the strong constitutional anchor of European data protection law.[247] The inalienability of these fundamental rights is argued on the grounds of human dignity.[248]

---

[239] Schwartz and Peifer, p. 123.

[240] Schwartz and Peifer, p. 123 f.

[241] Council of Europe, 'European Convention on Human Rights', 1950 <https://www.echr.coe.int/Documents/Convention_ENG.pdf> [accessed 21 April 2020]; Schwartz and Peifer, p. 123.

[242] Council of Europe.

[243] 'Treaty of the Functioning of the European Union (TFEU)', 2012 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN> [accessed 20 April 2020].

[244] Schwartz and Peifer, p. 123.

[245] 'Charter of Fundamental Rights of the European Union'.

[246] Federico Fabbrini, *Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspective*, Oxford Studies in European Law, First edition (Oxford, United Kingdom: Oxford University Press, 2014), p. 26.

[247] Schwartz and Peifer, p. 127.

[248] Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, First edition (Oxford, United Kingdom: Oxford University Press, 2015), p. 241.

The constitutional obligations to protect the individual's privacy mandates the enactment of regulations, directives or other statutory laws that limit and regulate the processing and use of data.[249] In general, the processing of personal data requires a legal basis, which is expressed in Article 8 (2) of the Charter of the European Union, that permits processing only for specified purposes and with the consent of the data subject or a direct permission by law.[250] While the US or China use restrictions for specific categories of information with their sectoral approaches, in the EU there is one general definition for personal data, which is protected by law.[251] The Directive 95/46/EC[252] which came into effect in 1995, provided a legal definition of the term '*personal data*', that was further interpreted by case law.[253] Article 2 (a) states that:

> *'personal data' shall mean any information relating to an identified or identifiable natural person (' data subject'); an identifiable person is one who can be identified , directly or indirectly , in particular by reference to an identification number or to one or more factors specific to his physical , physiological , mental, economic, cultural or social identity;*[254]

Directives are not directly binding in Member States, but require national governments to enact respective laws, often with room for adaptation to their own legal systems. The harmonising effect comes with minimum requirements that all countries have to fulfil.[255] The definition is very close to both the wording of the OECD Guidelines from 1980 and the Council of Europe Data Protection Convention, which was signed in 1981.[256] The focus of this definition is the identification of a data subject, for instance by an identification number. However, an exemption is provided as well, because '*the*

---

[249] Schwartz and Peifer, p. 127.

[250] 'Charter of Fundamental Rights of the European Union'; Schwartz and Peifer, p. 127.

[251] Voss and Houser, p. 313.

[252] European Parliament and Council of the European Union, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (Brussels, 1995) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en> [accessed 20 April 2020].

[253] Voss and Houser, p. 292.

[254] European Parliament and Council of the European Union, 'Directive 95/46/EC'.

[255] Schwartz and Peifer, p. 129.

[256] Voss and Houser, p. 314.

principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.'[257] The directive has been replaced by the Regulation 2016/679[258], the so-called General Data Protection Regulation (GDPR), which came into effect on May 25, 2018. The definition for personal data in Article 4 (2) is quite similar to the one from 1995, but includes location data, online and genetic means of identification. The standards created by a regulation are directly enforceable and the decision to use this legal instrument instead of a directive is due to the dissatisfaction with the different EU Member States' privacy protection implementations, according to some scholars.[259] Additionally, for mapping the GDPR's entire scope, the definition of processing is necessary. Article 4 (2) defines processing as

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*[260]

When an individual processes personal data and the action is of purely personal nature or is part of the household activity, the regulation does not apply.[261] It applies if the processor or controller has an establishment in the EU, or if the processor or controller uses personal data in relation to the offering of goods and services in the EU, or if behaviour of individuals in the EU is monitored and their activities take place within the Union.[262] A controller is any natural or legal person that determines the purpose and means of the data process, while a processor is the subject which carries out the process

---

[257] European Parliament and Council of the European Union, 'Directive 95/46/EC' Recital clause (26).

[258] European Parliament and Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' (Brussels, 2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> [accessed 20 April 2020].

[259] Schwartz and Peifer, p. 128.

[260] European Parliament and Council of the European Union, 'Directive 95/46/EC (General Data Protection Regulation)' Article 4 (2).

[261] William RM Long and others, 'Chapter 2: EU Overview', in *The Privacy, Data Protection and Cybersecurity Law Review*, 6th edn (London: Law Business Research Ltd., 2019), p. 6.

[262] Long and others, p. 6.

for the controller.[263] Under the GDPR, controllers and processors are subject to certain obligations. They have to comply with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation and storage limitation, accuracy, confidentiality and accountability. Technical and organisational measures have to be undertaken, in order to ensure data protection by design and by default. Moreover, under certain circumstances, a data protection officer (DPO) has to be appointed for the supervision of internal processes and to ensure the compliance.[264] The European Court of Justice (ECJ) uses a wide interpretation of the term personal data. According to the ECJ's rulings, records of working time, the mentioning of a foot injury as well as Internet Protocol (IP) addresses count as personal.[265]

An important aspect of the European data protection regime are the specific rights of data subjects. While many rights, such as the right to access the personal data being processed, rectify inaccurate data, restrict data processing, object to the processing of personal data, the right not to be subject to a decision that produces legal effects based solely on automated processing including profiling and transparency were already included in the 1995 directive, two new rights have been established with the GDPR. These are the right to be forgotten and the right to data portability.[266] Moreover, the protection is controlled by data supervisory authorities, which operate on a national level for the enforcement of the obligations.[267] High administrative penalties of up to 20 million Euro or four per cent of annual turnover act as harsh sanctions.[268] In sum, the protection of the individual is directly provided by binding European law. Specific legal definitions and enforcement agencies ensure legal certainty for the data subject. The application of the data protection regime is triggered by the processing of personal data, and even in the absence of sensitive data or harm to monetary or property interest, the protection of fundamental rights is guaranteed.[269]

---

[263] Long and others, p. 2.
[264] Long and others, p. 7 ff.
[265] Voss and Houser, p. 315 ff.
[266] Voss and Houser, p. 328; Long and others, p. 19 ff.
[267] Long and others, p. 25.
[268] Long and others, p. 27.
[269] Voss and Houser, p. 292; Schwartz and Peifer, p. 129.

While high data protection security is guaranteed on paper, there are still problems with the GDPR in practice. Data protection activists like Max Schrems criticise it as dysfunctional, as the national data protection authorities (DPA) do not work together efficiently. For instance, the Irish data authority has not yet imposed a single private sector penalty, with over 7,000 complaints pending.[270] As most tech companies have their headquarters in Ireland, the distribution of the workload is particularly concentrated in Dublin. John Naughton, professor of the public understanding of technology at the Open University in the United Kingdom, wrote in the British newspaper '*The Guardian*' that national authorities are overwhelmed and lack sufficient resources. Therefore, the GDPR remains a powerful regulation with, until now, quite serious enforcement problems.[271] Having comprehensively discussed the US, Chinese and European approaches to data protection, the following chapter will look into the topic of military AI.

B. Military AI

a. Introduction

Military researchers, experts and scholars observe increased usage of AI in military and defence technology and see major implications for security. The assessments range from changes in the '*nature of war*' and alterations in '*the psychological essence of strategic affairs*' to less radical views that discuss innovation and application in technological realms.[272] Unmanned aerial vehicles (UAVs) and remotely piloted vehicles, mostly referred to as drones, are already used on the battlefield. However, experts see armed drones only as forerunners and propose the possibility of lethal autonomous weapons systems that require the use of Artificial Intelligence in the next step of development. Such devices, often called killer robots, would be able to select targets without further human intervention.[273] The systems could be designed to act autonomously with AI as crucial component of the decision-making process.[274] In addition, the use and supervision

---

[270] ORF.at, 'Schrems: EU-Datenschutzrecht "Nur Auf Dem Papier"', *Www.Orf.At* (Vienna, 25 May 2020) <https://orf.at/stories/3167007/> [accessed 16 September 2020].

[271] John Naughton, 'Data Protection Laws Are Great. Shame They Are Not Being Enforced.', *The Guardian* (London, 2 May 2020) <https://www.theguardian.com/commentisfree/2020/may/02/data-protection-laws-are-great-shame-they-are-not-being-enforced> [accessed 16 September 2020].

[272] Franke, p. 5.

[273] Aiden Warren and Alek Hillas, 'Lethal Autonomous Weapons Systems: Adapting to the Future of Unmanned Warfare and Unaccountable Robots', *Yale Journal of International Affairs*, 12.1 (2017), p. 72.

[274] Franke, p. 5.

of humans in various hardware products such as tanks, planes or ships could be reduced.[275] Opposition comes from civil society through organisations such as the International Committee for Robot Arms Control (ICRAC) or the Campaign to Stop Killer Robots. There, Austria is the only European country that signed the ban of autonomous weapons systems. China is a signatory too, but only wants to ban the use, not the development and production.[276] Germany, France and other countries suggest using the United Nation's mechanism of the Convention on Certain Weapons (CCW)[277] to develop a code of conduct for autonomous weapons systems development in harmony with international law.[278]

Although LAWS received by far the highest amount of public interest, there are other types of defence and military applications for AI. In general, AI is seen to be an enabler, not a weapon itself. Similar to electricity, the technology is not designed for a single purpose, but for general-purpose. Its applications are very broad, fit to various other inventions and some even called it the '*ultimate enabler.*'[279] In the field of intelligence and surveillance, one of the core capabilities of AI, which is processing and analysing huge amounts of data, becomes an advantage. Programmes used to diagnose skin cancer or other diseases via image recognition, can be used for the identification or categorisation of photos and videos collected by sensors and drones.[280] Another aspect where effects are foreseeable is logistics. Via predictive maintenance, the exchange of repair parts can be improved, as the use and functioning of systems are closely monitored and timing for repair and replacement can be forecasted.[281] Another area of application of the technology is swarming, a complex task that combines the actions of various

---

[275] Michael C. Horowitz, 'Artificial Intelligence, International Competition, and the Balance of Power', *Texas National Security Review*, 1.3 (2018), p. 41.

[276] Campaign to Stop Killer Robots, *Country Views on Killer Robots*, 2018 <https://www.stopkillerrobots.org/wp-content/uploads/2019/10/KRC_CountryViews_25Oct2019rev.pdf> [accessed 30 April 2020].

[277] Convention on Certain Weapons (CCW) Group of Government Experts, *Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (Geneva: United Nations Office at Geneva, 2018) <https://www.unog.ch/80256EDD006B8954/(httpAssets)/20092911F6495FA7C125830E003F9A5B/$file/CCW_GGE.1_2018_3_final.pdf> [accessed 30 April 2020].

[278] Haner and Garcia, p. 335.

[279] Horowitz, p. 41.

[280] Horowitz, p. 41.

[281] Franke, p. 7.

systems and actors like drones or unmanned vehicles and tanks. The actions of such systems on the battlefield are characterised by coordinated behaviour and a '*unified whole that is greater than the sum of the individuals.*'[282] The main advantage is increased action speed and scale that allows reaction due to shifting of situations in a faster way than humans ever could.[283]

The new capabilities come along with increased concerns and dangers. As mentioned above, LAWS and other autonomous systems in warfare pose various legal and ethical threats. Ethicists and other experts argue that such machines are unable to grasp the uniqueness and value of human life. Therefore, their use would violate the principles of humanity and basic rules of civilisation.[284] Additionally, lethal AWS could potentially empower authoritarian rulers or undermine peace and democracy.[285] International norms and international law that strictly regulate the use of force have already started to erode due to semi-autonomous weapons – a process that could be pushed further.[286] Another crucial problem is the potential bias implemented in algorithms that could result in massive errors in the systems. Up to 85 percent of AI projects are currently predicted to have such failures that result from biased data for the training process or flaws introduced by the programmers themselves.[287] Apart from the technical aspects, the political sphere provides issues, too. Some scholars argue that programmes for AI-enabled military technology could spark an arms race.[288] This narrative is supported by various newspaper headlines.[289] Others critically reflect the

---

[282] Paul Scharre, 'How Swarming Will Change Warfare', *Bulletin of the Atomic Scientists*, 74.6 (2018), 385–89 (p. 385 f).

[283] Scharre, 'How Swarming Will Change Warfare', p. 387.

[284] Franke, p. 9; Frank Sauer, *Artificial Intelligence in the Armed Forces: On the Need for Regulation Regarding Autonomy in Weapon Systems* (Federal Academy for Security Policy, 2018), p. 3 <https://www.baks.bund.de/sites/baks010/files/working_paper_2018_26.pdf> [accessed 30 April 2020].

[285] Haner and Garcia, p. 331.

[286] Ingvild Bode and Hendrik Huelss, 'Autonomous Weapons Systems and Changing Norms in International Relations', *Review of International Studies*, 44.3 (2018), 393–413 (pp. 398, 411); Haner and Garcia, p. 332.

[287] Haner and Garcia, p. 332.

[288] Franke, p. 9 f; Ding, p. 31 f.

[289] The Economist, 'The Algorithm Kingdom - China May Match or Beat America in AI | Business', *The Economist*, 15 July 2017 <https://www.economist.com/business/2017/07/15/china-may-match-or-beat-america-in-ai> [accessed 9 March 2020]; John Markoff and Matthew Rosenberg, 'China Gains on the U.S. in the Artificial Intelligence Arms Race', *The New York Times*, 4 February 2017

construction of an arms race and see the perception of a competition as a threat itself. The desire to win or to be the first to deploy the systems could potentially lead to neglected or lowered safety measures. Thus, security aspects should remain a central factor in AI design, the rhetoric should become more objective and opportunities for cooperation should be aimed for, because '*[a] race to the bottom on AI safety is a race no one would win.*'[290]

In Military AI, two different aspects have to be differentiated. On the one hand, dual-use technology, i.e. technology which can be used both for military and civil components. On the other, military exclusive AI, which is only used in the military sector. Dual-use AI is mainly developed in the commercial sector, however, the partnering of Google and the US Department of Defense for the development of algorithms to analyse drone footage (discussed in more detail below), perfectly illustrates the transferability of commercial know-how for military purposes. Given the massive economic interest in AI, some scholars argue that the bottleneck of talent and researchers is holding back military development.[291] An example for successful transfer of dual-use technology into the civil sphere is the DoD's Defense Advanced Research Projects Agency, which will be discussed in more detail below. China has not only set-up a similar research agency to the US' DARPA,[292] but moreover concentrates high investments around military & AI development, with a specific focus on civil-military fusion.[293] In contrast, the EU's lack of a centralised budget and common defence policy limits its scope of actions.[294] France and Germany's different approaches to military AI, which will be discussed in subchapter d,

<https://cn.nytimes.com/world/20170204/artificial-intelligence-china-united-states/en-us/> [accessed 9 March 2020].

290 Paul Scharre, 'Killer Apps: The Real Dangers of an AI Arms Race', *Foreign Affairs*, 98.3 (2019), 135–44 (p. 135 f).

291 Horowitz, p. 50.

292 Minnie Chan, 'Chinese Military Sets up Hi-Tech Weapons Research Agency Modelled on US Body', *South China Morning Post*, 25 July 2017 <https://www.scmp.com/print/news/china/diplomacy-defence/article/2104070/chinese-military-sets-hi-tech-weapons-research-agency> [accessed 9 March 2020].

293 Elsa B. Kania, 'Chinese Military Innovation in the AI Revolution', *The RUSI Journal*, 164.5–6 (2019), 26–34.

294 Patricia Nouveau, 'Can Regulation Foster EU Entry to the Digital Race or Is It a Poor Substitute for a Truly EU-Driven Industrial Policy?' (presented at the Workshop on Economic Regulations in a Digital World, Toronto, Canada, 2019), p. 13 f <https://www.researchgate.net/publication/335602941_CAN_REGULATION_FOSTER_EU_ENTRY_TO_THE_DIGITAL_RACE_OR_IS_IT_A_POOR_SUBSTITUTE_FOR_A_TRULY_EU-DRIVEN_INDUSTRIAL_POLICY> [accessed 26 June 2020].

make concentrating European efforts a challenge. Nevertheless, the European Commission proposed the creation of a European Defence Fund (EDF) in 2017.[295] In this section, the US, China and the EU are compared concerning their approaches to military AI. In the first section, the US and its military AI applications as well as governmental initiatives will be discussed. In the second part, the Chinese approach to military AI and the Communist Party's strategies to catch-up will be outlined. The third section focuses on the European approach to military AI.

b. Military AI in the US

The US has been leading in military spending for decades and has a budget greater than China, Russia, South Korea, and all 27 EU Member States and the United Kingdom combined.[296] It is common knowledge that its army is the most advanced in the world. A crucial component of the American leadership is the DoD's DARPA, which was founded in 1958. The research and development organisation focusing on strategically important technologies acts as a risk-taker and supports innovation. The agency is characterised by its slim structure, where independent programme managers support innovative high-risk projects that have the potential to revolutionise the world. While most missions fail or only provide limited results, the ones that succeed create ground-breaking improvements.[297] Although the focus lies on military applications, some game-changing innovations have been transferred into the civil sphere. The results were, among others, the development of the internet and the global positioning system (GPS), which not only aided the country's defence effectiveness, but further supported economic growth.[298] A crucial aspect is that public funding of dual-use technology allows a bypassing of World Trade Organization (WTO) rules in the name of national security.[299] Obviously, DARPA plays an important role in the country's military AI development. In September 2018, the agency started its '*AI Next Campaign*' with a multi-year investment initiative of more than two billion US-Dollar. DARPA director Steven Walker aims at '*transforming computers from specialized tools to partners in problem-solving*' and would like to explore how

[295] Franke, p. 19.
[296] Haner and Garcia, p. 332.
[297] Mahmut Durmaz, 'Defense Technology Development: Does Every Country Need an Organization like DARPA?', *Innovation*, 18.1 (2016), 2–12 (p. 3).
[298] Durmaz, p. 2 f.
[299] Nouveau, p. 13 f.

'*machines can acquire human-like communication and reasoning capabilities.*'[300] Among the key areas are the automation of critical processes in the DoD, reducing inefficiency concerning power and data performance, increasing robustness and security of AI systems and developing more complex algorithms.[301]

In addition, there are other governmental initiatives and policies regarding military AI development. The White House published a memorandum for the heads of executive departments and agencies in 2018, stating that investment in Artificial Intelligence, autonomous systems and other technologies is necessary for maintaining US military superiority.[302] The National Defense Strategy 2018 regards AI as one of the most important technologies for the future of warfare. The authors of the document argue that the crucial part is not to be the first to develop the technology, but to be the first to integrate it better and adapt it to the new possibilities of combat. As part of implementing the strategy, various sections of the DoD made AI and Machine Learning a priority.[303] The US are developing different kinds of AI applications for military usage. According to a study on autonomy by the Defense Science Board (DSB), a federal advisory group of the DoD, there are two different kinds of intelligent systems: autonomy at rest and autonomy in motion. '*In broad terms, systems incorporating autonomy at rest operate virtually, in software, and include planning and expert advisory systems, whereas systems incorporating autonomy in motion have a presence in the physical world and include robotics and autonomous vehicles.*'[304]

One of the most important applications of AI lies in the field of situational awareness and Intelligence, Surveillance and Reconnaissance (ISR). Various sensors on

---

[300] Defense Advanced Research Projects Agency (DARPA).

[301] Satoru Mori, 'US Defense Innovation and Artificial Intelligence', *Asia-Pacific Review*, 25.2 (2018), 16–44 (p. 26).

[302] Executive Office of the President, 'Memorandum for the Heads of Executive Departments and Agencies', 2018 <https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf> [accessed 2 May 2020].

[303] US Department of Defense, 'Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge', 2018 <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf> [accessed 2 May 2020]; Mori, p. 25.

[304] Defense Science Board, 'Summer Study on Autonomy', 2016, p. 5 <https://www.hsdl.org/?view&did=794641> [accessed 5 May 2020].

ISR platforms and communication systems record huge amounts of data, but the capacity of humans to analyse and process the collected files into intelligence remains limited. Thus, the expectations for AI to support the identification of potential threats and opportunities are quite high.[305] To address the problem, the Pentagon launched 'Project Maven' in 2017, which received high amounts of public interest.[306] The mission was to develop an algorithm that automates the analysing process of drone footage by Machine Learning techniques.[307] At first, Google partnered up with the US Department of Defense, but internal objections resulted in the contract not being renewed. Thousands of employees signed an open letter refusing to be involved in the business of war as the technology to be developed could be used for more precise drones strikes.[308] Some scholars concluded that there might be a divide between the Silicon Valley and Washington over the military use of AI after this incident.[309] Other projects for data processing with AI application are carried out by the Central Intelligence Agency (CIA) and the Intelligence Advanced Research Project Agency (IARPA). These are intended to predict future events like civil unrest or terrorist attacks and should accomplish image recognition tasks.[310] In the field of analysing and processing of large amounts of data, the expectations are high that people are going to be replaced by AI systems. Improvements in the area of identifying opportunities, detecting threats and increasing decision-making speed through heightened situational awareness are crucial components for military forces.[311]

Regarding cyber defence, AI is seen to play an important role as the complexity of advanced systems poses various security threats. Two agencies of the US DoD, the National Security Agency (NSA) and DARPA are currently supporting the development of technology that is capable of detecting software flaws, scanning incoming traffic for vulnerabilities and determining the locations of computer hosts that sent malware. In

---

[305] Mori, p. 27 f.
[306] Franke, p. 6.
[307] Horowitz, p. 41.
[308] Penny Crofts and Honni Van Rijswijk, 'Negotiating "Evil": Google, Project Maven and the Corporate Form', *Law, Technology and Humans*, 2.1 (2020), p. 1 f.
[309] Scharre, 'Killer Apps: The Real Dangers of an AI Arms Race', p. 140.
[310] Mori, p. 28.
[311] Mori, p. 28 f.

order to cope with increased sophistication of cyber-attacks, both building resilience and robustness are crucial for the defensive systems. In the realm of logistics, the DoD is partnering with AI companies to develop and test predictive maintenance applications for their armoured troop carriers. The US Air Force experiments with Microsoft's Machine Learning systems to analyse aggregated data of planes and bombers for predictive maintenance. For advances in command and control, the US Air Force is developing systems with Lockheed Martin and others to significantly shorten the time window from the appearance of data to the final decision. While current developments aim at supporting human decision, future defence applications could provide assistance for highly complex situations and link operational planning and tactical execution.[312]

Another promising field for AI application are autonomous unmanned systems and swarm techniques and tactics. The DoD's Strategic Capabilities Office (SCO) has been developing micro drones that operate autonomously. The US Army supposes operations of autonomous ground vehicles to be in field by 2028 and started testing autonomous unmanned boats as well. DARPA is making progress in projects for Offensive Swarm-Enabled Tactics (OFFSET) where '*it seeks to create highly capable, heterogenous swarm systems comprising of up to 250 collaborating autonomous swarm elements […].*'[313] The US military is currently taking a step-by-step approach, to reduce the need for humans in controlling robotic and other unmanned vehicles. The DoD issued a directive where it stated that appropriate levels of human judgement and oversight are crucial for the use of force, and especially lethal force involving AWS.[314] Nevertheless, the US is still the world leader regarding the development of lethal autonomous weapons systems. Semi-autonomous weapons are allowed to engage targets that have been selected by humans and fully autonomous weapons are permitted to do so when senior level DoD approval is provided.[315] The US army already owns more than 20,000 autonomous vehicles and is highly investing in the development of more advanced technology. From 2019 to 2021 alone, 17 billion US-Dollar are going to be spent on drones, as well as other unmanned

[312] Mori, p. 31 f.

[313] Mori, p. 33.

[314] Mori, p. 33 f; Department of Defense, 'Dircetive: Autonomy in Weapons Systems', 2012 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf> [accessed 5 May 2020].

[315] Haner and Garcia, p. 332.

ground, sea, and aerial systems.[316] In the following paragraphs the Chinese approach will be discussed.

c. China

The People's Republic of China (PRC) aims for national rejuvenation, wants to restore the country's great-power status and pursue the 'Chinese dream'. When Xi Jinping came to office in 2012, he pushed for military reforms, not only to strengthen the Chinese Communist Party's (CCP) authority over the People's Liberation Army (PLA), but for the purpose of restructuring and increasing military capabilities.[317] By mid-century, the Chinese president, who also leads the Central Military Commission (CMC), the PLA's highest decision-making body, wants to achieve a transformation into a '*world-class force.*'[318] Artificial Intelligence plays an important role for the fulfilment of this target until 2049. The PRC's National AI Development Plan calls for a '*historic opportunity*' and regards AI a leapfrog development, that is supposed to help the country to catch-up with the world's best military forces. The modernisation of the army is a top priority and cutting-edge technology will help to pursue the goals.[319] The CCP's 13th Five Year Plan 2016-2020 already includes funding for military AI applications.[320] In 2017, Xi Jinping called for the acceleration of '*military intelligentisation*' because it is a necessary means to achieve the goals.[321] The PLA anticipates a shift from '*informatized*' warfare to '*intelligentized*' warfare and regards AI as an integral part of this development. The urgent goal is advancing military innovation and closing the military gap with the United States. China's AI development plan outlines various kinds of AI application for military purpose

316 Haner and Garcia, p. 333; Dan Gettinger, 'Summary of Drone Spending in the FY 2019 Defense Budget Request' (Center for the Study of the Drone at Bard College, 2018) <https://dronecenter.bard.edu/files/2018/04/CSD-Drone-Spending-FY19-Web-1.pdf> [accessed 6 May 2020].

317 Bates Gill and Adam Ni, 'China's Sweeping Military Reforms: Implications for Australia', *Security Challenges*, 15.1 (2019), 33–46 (p. 33 f).

318 Lindsay Maizland, *China's Modernizing Military* (Council on Foreign Relations, 2020), p. 2 f <https://www.cfr.org/backgrounder/chinas-modernizing-military> [accessed 7 May 2020].

319 Gregory Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Center for a New American Security, Washington DC, 2019), p. 8 <https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041> [accessed 7 May 2020].

320 Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Center for a New American Security, Washington DC, 2017), p. 12 <https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805> [accessed 7 May 2020].

321 Kania, 'Chinese Military Innovation in the AI Revolution', p. 27.

such as command decision-making, military deduction, defence equipment, among others.[322] Chinese military academics highlighted '*human-machine hybrid intelligence*' that are crucial for '*human-machine cooperative warfare' and assess* '*a shift from network-centric warfare to algorithm-centric warfare.*' [323]

Another important aspect is the fact that PLA researchers closely analysed projects from the US DARPA and tried to learn from the American success. For instance, Deep Green, an initiative for the development of systems which are capable of supporting the decision-making processes of Army commanders, was launched in 2007 and has been subject to analysis.[324] China created its own '*Chinese DARPA*' in 2017, to steer innovation and fuse civil-military research and development.[325] The goals are the pre-emption of technological surprises crucial for the country's national security and the incubation of breakthrough innovation.[326] '*Civil-military fusion*' became a national strategy to '*leverage synergies between defence, academia, and commercial enterprises, from joint research to improved acquisition.*'[327] As part of the implementation, a High-End Laboratory for Military Artificial Intelligence has been created at Tsinghua University, sometimes referred to as '*China's MIT.*' In Tianjin, one of the largest centres for the development of dual-use technology, a new AI Military-Civil Fusion Innovation Center has been built. Another innovation hub for leveraging commercial technologies for defence applications was launched in Shenzhen, a Chinese tech megacity. These developments suggest a shift towards faster defence innovation, also using the advantages of commercial developments and increasingly adapting to US approaches.[328]

---

[322] Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, p. 12 f.

[323] Kania, 'Chinese Military Innovation in the AI Revolution', p. 28 f.

[324] You Wang and Dingding Chen, 'Rising Sino-U.S. Competition in Artificial Intelligence', *China Quarterly of International Strategic Studies*, 04.2 (2018), 241–58 (p. 244 f); Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, p. 15.

[325] Chan.

[326] Trigkas Vasilis, 'China Has Its DARPA, but Does It Have the Right People?', *The Diplomat*, 9 August 2017 <https://thediplomat.com/2017/08/china-has-its-darpa-but-does-it-have-the-right-people/> [accessed 7 March 2020].

[327] Kania, 'Chinese Military Innovation in the AI Revolution', p. 32.

[328] Kania, 'Chinese Military Innovation in the AI Revolution', p. 32 f.

Looking at the PLA's military AI applications and experimentation projects provides further information about developments in this field. While some appear to be in line with other militaries' efforts, there are some priorities especially focused on by the PLA such as early warning systems, military intelligence, information operations (e.g. cyber defence, electronic warfare and psychological operations), support to command decision-making and advanced weapons systems.[329] Space corporations launched AI-satellites for the processing of sensor data and imagery. The Strategic Support Force is researching and developing capabilities for cyber defence with AI application. The PLA Navy started projects for anti-submarine warfare with experimentation of neural networks for acoustic signal processing that should enhance detection capabilities. Further, the deployment of unmanned surface vessels and autonomous underwater vehicles has been started. Autonomous unmanned ground vehicles seem to be a priority for the PLA, because they increased experimenting with the technology and have annual competitions for self-driving, unmanned vehicles.[330] The Air Force launched a campaign for the development of swarms of drones and already tested swarming technology with more than a thousand remotely piloted vehicles. Regarding autonomous weapons systems, China has plans for production and is likely to have less resistance than other countries, because of high approval rates to AI technology in its population.[331] With improved Automatic Target Recognition (ATR) capabilities, smart weapons are becoming more common and new opportunities for future cruise missiles with high levels of autonomy become more likely.[332] While experimenting with and application of AI technologies in the military realm, PLA scholars started to raise ethical and legal questions including calls for international rules and arms control.[333] The next paragraphs will focus on the European aspects.

d. Europe's divide

In contrast to the US and China, the European Union has no centralised defence budget and common defence policy.[334] In general, European defence policy has been

[329] Kania, 'Chinese Military Innovation in the AI Revolution', p. 32.
[330] Kania, 'Chinese Military Innovation in the AI Revolution', p. 31 f.
[331] Haner and Garcia, p. 333.
[332] Kania, 'Chinese Military Innovation in the AI Revolution', p. 32.
[333] Kania, 'Chinese Military Innovation in the AI Revolution', p. 30.
[334] Nouveau, p. 13.

characterised by intergovernmental dynamics and the supranational features were rather limited. Due to the increased uncertainty and conflicts in the EU's neighbourhood as well as new security threats, the Commission and its then-president Jean-Claude Juncker identified defence policy as a priority area in 2016.[335] In 2017 the European Commission launched a proposal for a European Defence Fund, which shows a shift towards '*more EU*' in that realm.[336] The Preparatory Action on Defence Research (PADR), the first element to increase the spending on such research, was equipped with 90 million Euro. The second component, the EU Defence Industrial Development Programme (EDIDP) came with a budget of 500 million Euro and the next Multiannual Financial Framework programme 2021-2027 includes 4.1 billion Euro for such research and 8.9 billion Euro on development. The reasons for Brussel's increased involvement are both Brexit and doubts about the US commitment to the North Atlantic Treaty Organization (NATO).[337] To meet the military alliance's defence spending goal of two percent, EU members of NATO would have to '*invest an additional €90 billion (about $100 billion) annually, which would be a 45 percent increase compared to their 2017 spending.*'[338]

Some argue that the Commission's increased engagement in the area of defence can be described as a '*paradigm shift.*'[339] The European legal foundations do not provide a mandate for the European Commission to engage in military and defence policy, however, the basis for the activities related to the EDF are Article 173 and 182 of the Treaty on the Functioning of the EU that allows actions in the field of industrial innovation and competition.[340] The Commission's document for the launch of the EDF mentions AI as potential field of innovation for future defence technology and is supposed

---

[335] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Launching the European Defence Fund, COM 295 Final' (Brussels, 2017), p. 2 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0295&from=EN> [accessed 12 May 2020].

[336] Pierre Haroche, 'Supranationalism Strikes Back: A Neofunctionalist Account of the European Defence Fund', *Journal of European Public Policy*, 2019, 1–20 (p. 1 f); Sophia Besch, 'The European Commission in EU Defense Industrial Policy' (Carnegie Europe, 2019), p. 1 <https://carnegieeurope.eu/2019/10/22/european-commission-in-eu-defense-industrial-policy-pub-80102> [accessed 12 May 2020].

[337] Bruno Oliveira Martins and Christian Küsters, 'Hidden Security: EU Public Research Funds and the Development of European Drones: Hidden Security: EU Public Research Funds and the Development of European Drones', *JCMS: Journal of Common Market Studies*, 57.2 (2019), 278–97 (p. 17).

[338] Besch, p. 2.

[339] Haroche, p. 1.

[340] Besch, p. 4.

to support industry in the development phase.[341] Regarding military AI, the Commission's white paper on Artificial Intelligence launched in February 2020 states that it '*does not address the development and use of AI for military purposes.*'[342]

The knowledge about the impacts of AI made calls for European disruptive innovation in the digital realm louder. Some scholars argue that the EU needs to learn from the success of the US DARPA in order to foster innovation and therefore, a more mission-oriented approach is necessary to decrease the '*sprinkling effect*' and concentrate money for research and development on fewer projects with higher impact.[343] A similar bilateral initiative launched by France and Germany is called the Joint European Disruptive Initiative (JEDI), which calls itself the European DARPA. When it comes to the agency's agility and setting of targets in the direction of fostering high-risk breakthrough innovation and securing technological leadership, it is quite similar to its US model. Although '*DARPA inspired us in terms of methodology, JEDI's customer is not the Department of Defense, and is not targeting military applications.*' Therefore, the focus of JEDI lies on the development of civil technology.[344] Moreover, the EDF reserved eight percent of its funding for high-risk technologies and disruptive defence innovation in order to address the problem.[345] In contrast to JEDI, the EDF provides funding for dual-use technology and thus for technology that could be used for defence applications.[346]

While spending for dual-use technology is widely accepted, EU institutions are quite reluctant with the notion of military AI applications, as seen in the Commission's white paper. In some European Member States, the situation is different. The French national AI strategy intensively discusses geopolitical aspects of AI and regards the military applications of the technology as an important element – more than any other

---

341 European Commission, 'Launching the European Defence Fund COM 295 Final', p. 9.

342 European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 1.

343 Nouveau, p. 14 f.

344 André Loesekrug-Pietri, 'JEDI: Joint European Disruptive Initiative', 2018 <https://www.bundestag.de/resource/blob/556394/ff7f0a1f37e430410961b15ceb58e2b4/3--jedi-en-fr-data.pdf> [accessed 12 May 2020]; Daniela Vincenti, 'Return to the JEDI: European Disruptive Technology Initiative Ready to Launch', *Euractiv*, 16 March 2018 <https://www.euractiv.com/section/economy-jobs/news/return-of-the-jedi-european-disruptive-technology-initiative-ready-to-launch/> [accessed 12 May 2020].

345 Franke, p. 13.

346 Besch, p. 2.

European country. In addition, France was the first EU Member State to launch a strategy specifically for the purpose of military AI development.[347] Germany approaches the topic differently and is in general more cautious regarding military AI applications. The country's national strategic document does not discuss geopolitical, military and security aspects. The biggest country in the EU rather focuses on arms control of autonomous weapons systems and regulations for the use of AI in warfare.[348] When it comes to the development of military systems with AI applications, armed drones are the main component in Europe. Although Great Britain is no longer a member of the EU, it should be mentioned that it is the only country in Europe that already used armed drones, specifically in Iraq and Syria.[349] Germany signed a contract to lease Israeli drones that could be armed in the future[350] and France armed its surveillance drones.[351] Therefore, armed unmanned vehicles are already present in Europe.[352]

Some AI-enabled military projects are currently under development. The Dassault nEUROn, according to the Global Security Initiative's autonomy database the most autonomous system of more than 250 analysed, is an unmanned combat air vehicle, which is mainly developed by France, but with involvement of Greece, Italy, Spain, Sweden and Switzerland. Another highly innovative project at an early stage of development is the Airbus and Dassault Future Combat Air System (FCAS), which is developed by France, Germany and Spain. It is expected to be capable of '*teaming between a manned fighter and swarms of autonomous drones.*'[353] Importantly, both are multi-national military projects that did not involve money from EU research funds. However, a relevant part of the more than 200 drone-development projects in Europe received funding under the Research and Development framework programmes of the EU, like the

---

[347] Franke, p. 13.

[348] Franke, p. 14 f.

[349] Martins and Küsters, p. 7.

[350] Ari Rabinovitch, 'Israel Aerospace Signs $600 Million Drone Deal with Airbus for Germany', *Reuters*, 14 June 2018 <https://www.reuters.com/article/uk-il-aerospace-ind-airbus-nl-germany/israel-aerospace-signs-600-million-drone-deal-with-airbus-for-germany-idUSKBN1JA0N3> [accessed 13 May 2020].

[351] no author, 'Florence Parly, Minister of the Armed Forces, Hails Success of the Firing Trials to Arm Drones', *Www.Defense-Aerospace.Com*, 2019 <https://www.defense-aerospace.com/article-view/release/208407/france-arms-reaper-drones-with-gbu_12-laser_guided-bombs.html> [accessed 13 May 2020].

[352] Martins and Küsters, p. 7.

[353] Franke, p. 18.

currently running Horizon 2020 (H2020).[354] The eligibility criteria of these public research funds stipulate that the funded projects '*must not be defence-related, but may have a dual-use nature.*'[355] Via hybrid public-private partnerships, dual-use technology such as drones was developed and funded by the framework programmes, which '*overrode the official EU rule preventing the framework programmes to fund defence research.*'[356] With the EDF as the successor to H2020, the European Union, for the first time in its history, is directly using public funds for military technology research & development.[357] The fund that is endowed with 13 billion Euro '*prohibits the development of lethal autonomous weapons and weapons systems declared illegal by international law (e.g., land mines and nuclear, chemical, and biological weapons) […].*'[358] While the limits are clearly defined, the EU's paradigm shift regarding R&D for defence technology cannot be denied. After the detailed depiction of the US, Chinese and EU approaches to data protection and military AI, the next step will be to assess the differences and to classify the three systems regarding the two before mentioned factors.

C. Categorising the results

a. Data protection

The United States, once a global leader in the field of privacy protection, can no longer be classified as such. While the free flow of data enjoys protection at constitutional level, no omnibus federal law ensures the safeguard of every individual's personal data. Looking at the historical developments in that legal field reveals that the main purpose of privacy regulation was protection against the state. However, today's processors of personal data are mainly private companies, free to contract collection and processing of data without the need for legal justification. The marketplace logic that dominates the discourse, where data is rather seen as an asset which can be freely traded, shows the high priority that lies on economic growth. This environment of open access to data is seen as fruitful for AI development by some scholars and the sectoral approach that only provides

354 Martins and Küsters, p. 1.
355 Martins and Küsters, p. 8.
356 Martins and Küsters, p. 2.
357 Bruno Oliveira Martins and Raluca Csernatoni, *The European Defence Fund: Key Issues and Controversies* (Peace Research Institute Oslo (PRIO), Oslo, 2019), p. 1 <https://www.ies.be/files/PRIO_Policy_Brief_3-2019.pdf> [accessed 12 May 2020].
358 Martins and Csernatoni, p. 4.

protection for specified areas makes it easier for companies to use information on an individual for business purposes.[359] Some analysts argue, a comprehensive federal data protection law would have negative effects on innovation. The downside of the business-friendly environment is the lack of omnibus privacy protection, with the potential exception of California. The Federal Trade Commission and the state attorneys general are in charge of enforcement actions but focus on consumer protection and do not have a mandate for data protection. However, at least to a certain degree, the privacy of consumers is protected. The five billion US-Dollar settlement between Facebook and the FTC in the aftermath of the Cambridge Analytica scandal shows that misconduct is sanctioned. Although the sanctions regarding data protection in the US are way less credible than the European Union's, a shift in the direction of increased safeguard for privacy can be assessed.

To sum up, the United States have no federal omnibus data protection regulation. The privacy of consumers is protected to a certain degree, but the enforcement mechanisms cannot be assessed as strong, because the FTC rather than independent courts or specific data protection authorities is responsible for enforcement. There has been an important case with severe sanctions, however, the level of credibility is not as high as in the EU. Therefore, in the category of comprehensive data-protection regulation, the United States will be marked with '*partially.*'

In China, a shift towards more individual privacy has been observed in the last decades. In contrast to the US, where most privacy laws focus on negative freedom against governmental authority, the Chinese system offers very little regulation for the public sector. The country does not have an omnibus federal data protection law. Similar to the US, sectoral laws provide a certain degree of protection, however, the ineffectiveness of the judicial system is a core obstacle for enforcement. In general, China's constitution is seen to be unprepared for a comprehensive data protection law. Specific provisions in criminal law, tort law or cybersecurity law fail to provide protection given the problems regarding enforceability, which is also reflected by the low number

[359] Eline Chivot and Daniel Castro, *The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy* (Center for Data Innovation, Washington D.C. and Brussels, 2019), p. 5 <http://www2.datainnovation.org/2019-reform-the-gdpr-ai-a4.pdf> [accessed 20 April 2020].

of respective cases. An important aspect that is missing for a comprehensive data protection regulation are credible sanctions. While announcements from the Standing Committee of the National People's Congress of China allow a positive outlook, the current level of protection is lower than the OECD and Council of Europe standards of the early 1980s. As China does not have an omnibus federal data protection law, credible sanctions or effective enforcement mechanisms, the table will be marked with '*no.*'

The European Union's data protection framework is of omnibus nature, which means that both public and private sector data are covered. Privacy and data protection are seen as inalienable rights with a strong constitutional anchor in the European legal framework and specific provisions in primary EU law. The protection of fundamental rights is guaranteed by constitutional courts. Instead of approaching the issue with sector specific regulation as seen in the US and China, a general definition for personal data ensures that no areas are left unregulated. The interpretations of the European Court of Justice for the term are broad, showing the comprehensive extent of protection. Specific rights for data subjects have been implemented with a directive in 1995, which were expanded with the EU's General Data Protection Regulation in 2018. The GDPR and its effects on the development of AI are controversially discussed in academia. Some scholars argue it should be reformed, because it is a barrier to successful AI development. According to them, the restrictions regarding data collection and use as well as the limitations for automated decision-making lead to an '*artificial scarcity of data*' that will negatively affect the competitiveness of the EU.[360] On the contrary, a study of the European Parliamentary Research Service found that the GDPR should not be regarded as an obstacle for successful AI development arguing for possible interpretations and applications of the regulation that allow using AI in a beneficial way.[361] As difficult as the predictions for the GDPR's effects on AI may be, an aspect that is quite clear is the impact

[360] Chivot and Castro, p. 6 f.

[361] Giovanni Sartor and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (EPRS, European Parliamentary Research Service, Brussels, 2020), p. 79 f <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [accessed 17 September 2020].

on data protection. What some commentators call the gold standard of privacy protection has been an important milestone in the field.[362]

To sum up, the European Union provides an omnibus data protection regulation on '*federal*' level that covers all personal data processing. The credibility of sanctions and high administrative fines are given. The enforceability of rights is guaranteed by independent courts accompanied by legal certainty and strong enforcement mechanisms. Therefore, the EU has to be marked with 'yes' concerning comprehensive data protection regulation. Table 2 below provides a summary of the three main aspects that have been considered for categorising the US, China and the EU regarding data protection regulation.

Table 2: Results of the three aspects for the category data protection regulation[363]

	US	China	EU
Federal level omnibus scope?	No	No	Yes
Credible sanctions?	Yes?	No?	Yes
Enforceability?	Yes?	No?	Yes

Table 3 below shows the summary of results of the three political entities' stance regarding the overall category of comprehensive data protection regulation as specified in chapter I. B.

[362] Giovanni Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard', *International Data Privacy Law*, 6.2 (2016), 77–78.

[363] Table 2: Results of the three aspects for the category data protection regulation, own presentation. Question marks are used to show that the specific element cannot be clearly assessed with yes or no and a certain degree of nuance is present.

Table 3: Comprehensive data protection regulation (summary of results)[364]

Comprehensive data-protection regulation	yes	partially	no
US		X	
China			X
EU	X		

In the next paragraph, the aspect of military AI will be assessed.

b. Military AI

The United States regards Artificial Intelligence as crucial part for maintaining its military superiority. DARPA's multi-year '*AI Next Campaign*' that was funded with two billion USD, the Memorandum of the White House on military AI investments and other governmental initiatives show the massive amount of funding provided to ensure disruptive innovation in the field. The US is the world leader in military spending with 3,3 percent of the country's gross domestic product (GDP).[365] Attempts to recruit digital giants like Google and their talented AI researchers for the development of algorithms for military purposes reveals the controversy of the topic, as the employees protested against the cooperation. The country has projects to apply AI in various sectors such as situational awareness, cyber defence, logistics, command and control and others. A crucial component are aspirations to increase the support regarding human decision making as well as the ambitious plans for testing and deploying autonomous unmanned vehicles and other systems. Moreover, the United States are the world leader regarding the development of lethal autonomous weapons systems.

To sum up, official governmental documents show that military Artificial Intelligence is declared a national priority for the US. The country has a GDP of 21,37

[364] Table 3: Comprehensive data protection regulation (summary of results), own presentation.

[365] European Commission, 'The European Defence Fund: Stepping up the EU's Role as a Security and Defence Provider', 2019, p. 2 <https://ec.europa.eu/docsroom/documents/34509/attachments/1/translations/en/renditions/native> [accessed 22 September 2020].

trillion USD.[366] Spending 3,3 percent of the GDP on military technology, the US provides more than 700 billion USD for this sector. Compared to the two billion USD of DARPA's '*AI Next Campaign*' shows that the US is spending approximately 0,3 percent of the total military expenditures on military AI. Therefore, the criterion of substantial resources is fulfilled, and the section will be marked with '*no.*'

Since 2012, when Xi Jinping became Chinese president, reforms in the military sector were conducted to increase its capabilities with the goal of transforming the army into a world class force until mid-century. China regards AI as very important, because it sees the disruptive technology as a leapfrog development and historic opportunity to catch-up with other countries' military power. The country copied US approaches in some aspect and created its own DARPA. Additionally, China is strongly focusing civil military fusion and set up numerous research centres and laboratories to foster the development of dual-use technology.

Pinpointing Chinese military AI expenditure provides difficult; however, scholars estimate that China spent between 300 million and 2.7 billion USD on military AI R&D in 2018.[367] The country's general military spending is estimated with 1,9 percent of the GDP which therefore ranks second place globally after the US.[368] Various applications are under development and sometimes already in use, such as AI satellites, cyber defence technology and neutral networks to enhance detection capabilities. Autonomous unmanned vehicles are seen as a primary target and therefore, testing and experimentation are accelerated by annual competitions. Fast progress is also achieved regarding drone and swarm technology development.

---

366 The World Bank, 'GDP (Current US$): World Bank National Accounts Data, and OECD National Accounts Data Files' <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD> [accessed 23 September 2020].

367 Acharya Ashwin and Arnold Zachary, *Chinese Public AI R&D Spending: Provisional Findings* (Washington, D.C.: Center for Security and Emerging Technology, 2019), p. 13 <https://cset.georgetown.edu/wp-content/uploads/Chinese-Public-AI-RD-Spending-Provisional-Findings-2.pdf> [accessed 22 September 2020].

368 Anthony H. Cordesman and Joseph Kendall, *Estimates of Chinese Military Spending* (Washington, D.C.: Center for Strategic and International Studies, 2016), p. 11 <https://www.jstor.org/stable/pdf/resrep23365.pdf?refreqid=excelsior%3A854028fc75d715dd87c8e999ad0c7541> [accessed 22 September 2020].

In sum, China has declared military AI a national priority, which is reflected in the PRC's National AI Development Plan that regards AI a historic opportunity to become a military leader. The country has a GDP of 14,34 trillion USD.[369] Spending 1,9 percent of the GDP on military purposes, China funds this sector with more than 270 billion USD. The specific numbers for public spending on military AI R&D are difficult to assess, but scholarly estimates range between 300 million and 2.7 billion USD for 2018. Comparing the median of this number, which is 1.5 billion USD, with the general military expenditures shows that China is spending approximately 0,55 percent of the total military expenditures on military AI. Therefore, the criterion of substantial resources is fulfilled, and the section will be marked with '*no.*'

In the European Union, the situation is more ambiguous. In general, the European Commission has no mandate for military and defence policy. The expenditures on defence are 1,34 percent of GDP.[370] Bilateral disruptive research initiatives in Europe like JEDI, which calls itself '*European DARPA*', do not target military applications, but focus on civil technology development. The Commission's white paper on Artificial Intelligence particularly states that the development of military AI is not addressed. However, the increased uncertainty in the region combined with Brexit and less US commitment to NATO resulted in launching a European Defence Fund in 2016 by the Juncker Commission. This has been assessed as '*paradigm shift*' in the direction of '*more EU*' in that field. However, different not to say opposite approaches regarding military AI by France and Germany provide a challenge for finding a common European position. France considers military AI particularly important, while Germany is more cautious and focuses on arms control and regulations for AI in warfare. Various multi-national military projects with AI applications in Europe do not involve funding by EU research programmes. Nevertheless, the versatility of dual-use technology allows a certain leeway for interpretation. While eligibility criteria of public research funds state that projects must not be defence-related, funding for dual-use technology is permitted. Via hybrid public-private partnerships the development of drones has been funded through EU framework programmes. The latest development with the EDF goes one step further and

[369] The World Bank.
[370] European Commission, p. 2.

allows, for the first time in the European Union's history, direct public funds of around two billion Euro per year, for military technology R&D.[371] The limits are the provisions of international law with special emphasis on the prohibition of lethal autonomous weapons systems.

To sum up, the position of the EU regarding military AI is quite nuanced. The white paper of the European Commission particularly opposes the development of military AI, which means it is not declared a main target. The countries of the EU combined have a GDP of 15,59 trillion USD.[372] 1,34 percent of the GDP is spent on general military expenditures, which equals more than 200 billion USD. Comparing what the EU (as a region, i.e. not the EU as an institution) spends on military purposes with the two billion USD, which the EDF provides for military R&D per year, shows that the EU as a region invests one percent of the total military expenditures on military R&D. Although the EDF is, in contrast to US and Chinese R&D programmes, not directly focused on military AI, it provides significant resources for military technology not excluding the development of military AI. Therefore, the criterion of substantial financial resources is given to some degree. As a result, military AI is certainly not declared a main focus of the EU. However, there are some initiatives and public funding for the development of dual-use technology that lead to the conclusion that the EU provides significant resources for military AI. Therefore, the assessment will result with '*partially.*' Table 4 below shows the results of the two aspects that have been considered for the category military AI.

---

371 Bruno Oliveira Martins and Raluca Csernatoni, *The European Defence Fund: Key Issues and Controversies* (Peace Research Institute Oslo (PRIO), Oslo, 2019), p. 2 <https://www.ies.be/files/PRIO_Policy_Brief_3-2019.pdf> [accessed 12 May 2020].

372 The World Bank.

Table 4: Results of the two aspects for the category military AI[373]

	US	China	EU
military AI not declared a main target?	No	No	Yes
No '*substantial financial resources*'	No	No	No?

Table 5 provides a summary of the results regarding the classification of the three political entities in the field of military AI.

Table 5: Military AI (summary of results)[374]

Not focusing on military AI	yes	partially	no
US			X
China			X
EU		X	

The European Union's norm-guided course of action was fully confirmed in the field of comprehensive data protection regulation, but only partially regarding not focusing military AI. Therefore, the EU will be classified as Weak-Normative Power, which will be discussed in more detail later. After categorising the results regarding the two factors, the following chapter will focus on the European approach to AI. At first, the EU's instruments and activities will be discussed, before the EU's attempt to create AI with European values will be looked into.

[373] Table 4: Results of the two aspects for the category military AI, own presentation. Question marks are used to show that the specific element cannot be clearly assessed with yes or no and a certain degree of nuance is present.

[374] Table 5: Military AI (summary of results), own presentation.

IV. The European approach to AI

A. EU instruments and activities

In 2015, the European Union has been working on initiatives crucial for the development of Artificial Intelligence for the first time, but without yet focusing on the technology explicitly. One example is the Digital Single Market Strategy which has been launched in May 2015 by the Commission.[375] Although not mentioning Artificial Intelligence directly, the pillars of the strategy contribute to a favourable environment of AI innovation. Decreasing the fragmentation of the European digital market and improving the free flow of data are desirable features for the development of AI. By enhancing the access to digital goods, establishing conditions for digital networks to flourish and maximising the digital growth potential, the European Commission was already unleashing crucial elements and cornerstones for AI.[376]

In 2016, the European Cloud initiative to improve the data infrastructure, was launched. Again, while neither naming the effects on AI nor the technology itself, it can be seen as an important step in creating the necessary environment. Part of the strategy is the European Open Science Cloud that should allow the scientific community to '*store, share and re-use their data across disciplines and borders.*'[377] Scientific data funded by the Horizon 2020 Research and Development Framework Programme is supposed to be open by default, to increase the efficiency and data reusability. In general, these actions are meant to strengthen data-driven innovation in Europe and increase the competitiveness on a global scale.[378] In addition, the European External Action Service (EEAS) developed a global strategy in 2016, where global rules on Artificial Intelligence have been identified as crucial in the field of Foreign and Security Policy.[379]

---

[375] Carriço, p. 32.

[376] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic Committee and the Committee of the Regions; on the Mid-Term Review on the Implementation of the Digital Single Market Strategy, COM 228 Final' (Brussels, 2017), p. 3 f <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-228-F1-EN-MAIN-PART-1.PDF> [accessed 25 March 2020].

[377] European Commission - Press Release, 'European Cloud Initiative to Give Europe a Global Lead in the Data-Driven Economy' (Brussels, 2016) <https://ec.europa.eu/digital-single-market/en/news/european-cloud-initiative-give-europe-global-lead-data-driven-economy> [accessed 14 May 2020].

[378] European Commission - Press Release.

[379] European External Action Service (EEAS), 'Shared Vision, Common Action A Stronger Europe' (Publications Office of the European Union, Brussels, 2016), p. 43

a. From declaration to coordination

In 2017, the number of EU initiatives increased and their content became more concrete in relation to Artificial Intelligence. In January, the European Parliament's Committee on Legal Affairs published a report with recommendations to the Commission on Civil Law Rules on Robotics.[380] Although the document is of non-binding nature, it contains various interesting aspects, such as general principles concerning the development of AI for civil use. Special emphasis is put on ethical principles which are crucial for updating the legal framework, where compliance with fundamental rights must be ensured.[381] The report suggests founding a European agency for robotics and Artificial Intelligence that bundles technical, ethical and regulatory expertise needed to develop cross-border rules and enhance cooperation between EU institutions and Member States.[382] Moreover, autonomous means of transport such as autonomous vehicles and drones are discussed regarding safety and liability issues among others.[383]

In May 2017, the European Commission's Mid-term review for the Digital Single Market was published. It argues for capacity building in the field of AI and highlights the potential for economic and productivity growth.[384] In the same month, the European Economic and Social Committee (EESC), a consultative body of the European Union representing various interest groups, like employers, employees, the so-called '*social partners*', issued an opinion on consequences of AI on various fields in society and economy. The EESC calls for a '*human-in-command approach*', which ensures that '*people retain control over these machines at all times.*'[385] In addition to general explanations on

<http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf> [accessed 25 March 2020].

380 European Parliament, 'REPORT with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))' (Brussels, 2017) <https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf> [accessed 14 May 2020].

381 European Parliament, p. 8 ff.

382 European Parliament, p. 10.

383 European Parliament, p. 12 f.

384 European Commission, 'Mid-Term Review on the Implementation of the Digital Single Market Strategy, COM 228 Final', p. 21 f.

385 European Economic and Social Committee, 'Opinion of the European Economic and Social Committee on "Artificial Intelligence — The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society", C 288/1' (Official Journal of the European Union, Brussels), p. 3 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016IE5369&from=EN> [accessed 14 May 2020].

the opportunities and risks of AI, aspects of privacy, standards and regulation, influences on working life, education, inclusiveness and democracy were also discussed.

In October 2017, the European Council recognised '*a sense of urgency to address emerging trends*' such as Artificial Intelligence and invited the Commission to develop a European approach to AI by early 2018 that ensures data protection, digital rights as well as ethical standards.[386] In November and December, meetings by the Council of the EU on topics such as the future of work, digital development and cybersecurity put emphasis on Artificial Intelligence, which shows the increased attention the technology receives.[387] Commissioner for Research, Science and Innovation, Carlos Moedas, set up a group of experts on Artificial Intelligence in order to address ethical concerns with the goal of delivering a report in early 2018.[388]

In April 2018, the Member States signed a declaration of cooperation on Artificial Intelligence.[389] The signatories agreed to cooperate on boosting Europe's technology and industrial capacity on AI, addressing socio-economic challenges and ensuring an adequate legal and ethical framework building on EU fundamental rights and values. In particular, the agreement consists of various declarations of intent such as to work towards a comprehensive and integrated European approach to AI, to put humans at the centre of the development, deployment and decision-making of AI, ensure sustainability and trustworthiness of AI-based solutions, exchange best practices, cooperate on reinforcing AI research centres and supporting their pan-European dimension as well as

386 European Council, 'European Council Meeting (19 October 2017) - Conclusions, EUCO 14/17' (Brussels, 2017), p. 7 <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf> [accessed 14 May 2020].

387 Council of the EU, 'Council Conclusions on the Future of Work Making It E-Easy, 15506/17' (Brussels, 2017) <http://data.consilium.europa.eu/doc/document/ST-15506-2017-INIT/en/pdf> [accessed 25 March 2020]; Council of the EU, 'Council Conclusions on the Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence Building Strong Cybersecurity for the EU, 14435/17' (Brussels, 2017) <https://www.consilium.europa.eu/media/31666/st14435en17.pdf> [accessed 25 March 2020]; Council of the EU, 'Digital for Development (D4D) - Council Conclusions, 14542/17' (Brussels, 2017) <http://data.consilium.europa.eu/doc/document/ST-14542-2017-INIT/en/pdf> [accessed 25 March 2020].

388 Carriço, p. 32.

389 EU Member States, 'Declaration - Cooperation on AI' (Brussels, 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50951> [accessed 25 March 2020].

encouraging discussions with stakeholders on AI and support the development of a broad and diverse community of stakeholders in a European AI alliance.[390]

Two weeks later, the Commission published the first comprehensive Communication on Artificial Intelligence. Setting out a European initiative on AI, the document outlines three pillars: boosting the EU's technological and industrial capacity and AI uptake, preparing for socio-economic changes and ensuring an appropriate ethical and legal framework.[391] The first pillar consists of various actions, such as increased investments to strengthen fundamental research. The Commission allocated additional funding for AI through the research and innovation framework programme Horizon 2020 to around 1.5 billion Euro by the end of 2020, which was an increase of approximately 70 percent.[392] In addition, research excellence centres across Europe, digital innovation hubs and infrastructure for testing and experimentation should support the development of the technology. Joint efforts by both public and private sectors are needed and special emphasis is put on small and medium enterprises that should be encouraged to test AI.[393] Moreover, the significance of data has been identified and both private and public data sharing will be encouraged, while ensuring the protection of personal information.[394] The second component addresses societal changes regarding labour markets, transformation of jobs and new (re-)training schemes to ensure the skills mismatch in the EU can be mitigated.[395] The third pillar regards trust and accountability as crucial aspects that have to be ensured by appropriate legal and ethical frameworks with special emphasis to fundamental rights and values.[396]

Building on the Commission's Communication in April 2018, with endorsement of the European Council in its meeting in June[397], the European Commission published the

---

390 EU Member States.
391 European Commission, 'Artificial Intelligence for Europe, COM 237 Final'.
392 European Commission, 'Artificial Intelligence for Europe, COM 237 Final', p. 5 f.
393 European Commission, 'Artificial Intelligence for Europe, COM 237 Final', p. 7 f.
394 European Commission, 'Artificial Intelligence for Europe, COM 237 Final', p. 10.
395 European Commission, 'Artificial Intelligence for Europe, COM 237 Final', p. 11 ff.
396 European Commission, 'Artificial Intelligence for Europe, COM 237 Final', p. 13 ff.
397 European Council, 'European Council Meeting (28 June 2018) - Conclusions, EUCO 9/18' (Brussels, 2018), p. 9 <https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf> [accessed 25 May 2020].

'*Coordinated Plan on AI*' in December 2018.[398] The initiative should maximise the impact of investments at EU and national levels, encourage synergies and cooperation across the EU, exchange best practices and collectively define the way forward as well as identify and consolidate common actions. At the core, the document regards a human-centric approach to AI as crucial and encourages the use of the technology to help solving the most difficult challenges in the world.[399] The plan should provide a strategic framework for national AI strategies and invites the Member States to develop national AI initiatives by mid-2019.[400] In the economic sector, public-private partnerships should be fostered, financing for start-ups and innovative small and medium sized companies increased and excellence in trustworthy AI technologies should be strengthened by tighter networks of European research centres and cross-border testing facilities.[401] Society should be prepared by the adaptation of learning and training programmes and foreign talent attraction should be incentivised.[402] For high competitiveness, the availability of a data ecosystem is crucial, which should be achieved by building up common European data spaces.[403] For the provision of ethics guidelines with a global perspective and an innovation-friendly legal framework, the Commission set up an independent High-Level Expert Group (HLEG) on AI.[404] Regarding security and AI, the document puts emphasis on cybersecurity issues and the importance of human control concerning decision-making in weapons systems.[405] According to some analysts, the impact of the coordination has been undermined due to the fact that some countries already published their national initiatives and for the EU to play the role of a coordinator in AI, Member States need not only to accept the EU's value in this, but further have to view the cooperation as beneficial for their AI efforts.[406]

---

[398] 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: Coordinated Plan on Artificial Intelligence, COM 795 Final' (Brussels, 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56018> [accessed 25 March 2020].

[399] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 1 f.

[400] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 2.

[401] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 3 f.

[402] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 5.

[403] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 6 f.

[404] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 7 f.

[405] European Commission, 'Coordinated Plan on Artificial Intelligence, COM 795 Final', p. 8.

[406] Ulrike Esther Franke and Paola Sartori, *Machine Politics: Europe and the AI Revolution* (European Council on Foreign Relations, 2019), p. 9 <https://www.ecfr.eu/page/-/machine_politics_europe_and_the_ai_revolution.pdf> [accessed 20 May 2020].

In February 2019, the Council of the EU strongly welcomed the Commission's coordinated plan on AI and recalled the main objectives of '*AI Made in Europe*' in the Council conclusions.[407] In April, two reports by the High-Level Expert Group on AI have been published. The first discusses the technology's main capabilities and offers a definition of AI systems. The second provides ethical guidelines for trustworthy AI. In order for AI systems to be trustworthy, they have to be lawful, ethical and robust.[408] Lawful Artificial Intelligence has to comply with EU primary law such as the Charter of Fundamental Rights, secondary law, the United Nations Human Rights treaties and the Council of Europe conventions such as the European Convention on Human Rights. While law does not only provide negative obligations that prohibit certain actions, importantly, it also enables other actions regarding the freedom to conduct business and the freedom of the arts and sciences as well as in the field of data protection and non-discrimination. Although the legal aspects are mentioned briefly, the guidelines rather focus on elements concerning ethical and robust AI.[409]

According to the report, trustworthy AI has to be grounded in fundamental rights. Although fundamental rights are legally enforceable rights, they provide certain values connected to human dignity and respect, which has been used by the High-Level Expert Group to derive five basic principles. These are respect for human dignity, freedom of the individual, respect for democracy, justice and the rule of law, equality, non-discrimination and solidarity as well as citizen's rights. These basic principles were used to develop four ethical principles in the context of AI systems. They are the principle of respect for human autonomy, the principle of prevention of harm, the principle of fairness and the principle of explicability.[410] In order to achieve trustworthy AI, the principles have to be translated into concrete requirements. The HLEG identified the following seven of them: Human agency and oversight, technical robustness and safety,

---

[407] Council of the EU, 'Artificial Intelligence: Conclusions on the Coordinated Plan on Artificial Intelligence, 6177/19' (Brussels, 2019), p. 2 <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf> [accessed 14 May 2020].

[408] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (Brussels: European Commission, 2019), p. 2 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> [accessed 25 March 2020].

[409] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 6.

[410] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 9 ff.

privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental wellbeing and accountability.[411] Another part of the report discusses potential methods of assessing trustworthy AI and offers a pilot version of a '*Trustworthy AI assessment list.*'[412] The last part provides examples of opportunities and risks raised by Artificial Intelligence.[413]

In addition to the two reports of the High-Level Experts Group on AI, the Commission published a communication called '*Building Trust in Human-Centric Artificial Intelligence*' in April 2019 as well. The title shows the special emphasis that was put on the human-centric approach, which calls for AI to be in the service of humanity and the common good and has the goal of improving human welfare.[414] The document is closely related to the HLEG's report and the Commission welcomes the developed principles and guidelines and considers the work useful for its policy-making process. In order to bring the Union's approach to the global stage and build a consensus on human-centric AI, the European Commission calls for strengthening the cooperation with like-minded partners and for engagement in international discussions and initiatives.[415]

In June 2019, the third report of the HLEG on AI regarding policy and investment was released. 33 recommendations focusing on the four main areas humans and society at large, the private sector, the public sector and research and academia should support the beneficial impacts by developing trustworthy AI. Additionally, the main enablers to achieve this goal, which are data and infrastructure, skills and education, governance and regulatory framework as well as funding and investment are discussed.[416] In the same month, the European Council identified four main objectives for the new strategic agenda

---

411 High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 14.

412 High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 24 ff.

413 High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 32 ff.

414 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence, COM 168 Final' (Brussels, 2019), p. 1 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58496> [accessed 25 March 2020].

415 European Commission, 'Building Trust in Human-Centric Artificial Intelligence, COM 168 Final', p. 8.

416 High-Level Expert Group on AI, 'Policy and Investment Recommendations for Trustworthy AI' (Brussels: European Commission, 2019), p. 6 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343> [accessed 25 March 2020].

2019-2024 with '*developing a strong and vibrant economic base*' as one of them.[417] In order to achieve this, the European Council suggests focusing on Artificial Intelligence as a key feature of digital transformation.[418] The institutional cycle of the Juncker Commission ended in November 2019.

b. New Commission, new strategy

The new Commission, chaired by Ursula Von der Leyen, took office in December 2019. In February 2020, the European Commission started to outline its digital strategy with publishing four documents of which one specifically concerns the topic Artificial Intelligence and the three others are closely linked. In its communication '*Shaping Europe's digital future*' the Commission discusses goals and visions and identified three key objectives.[419] The first is to develop technology that works for people, where one of the key actions is the European Commission's White Paper on AI, which will be looked into below. In addition, investments in connectivity (5G and 6G) as well as building and deploying '*cutting-edge*' joint digital capacities are among the plans.[420] The second is providing a fair and competitive economy, which implies ensuring a level playing field for big and small businesses. The Commission's data strategy for Europe, which will be discussed below, and evaluations and reviews of the legislative frameworks for competition are among the key actions.[421] The third is to maintain and achieve an open, democratic and sustainable society.[422] Regarding the international dimension, the document announces a Global Digital Cooperation Strategy to be delivered in 2021.[423]

In the same month, the Commisison published its strategy for data and outlined its vision for a European single market for data with the goal of increasing the EU's share

---

[417] European Council, 'European Council Meeting (20 June 2019) - Conclusions EUCO 9/19' (Brussels, 2019), p. 6 <https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf> [accessed 26 May 2020].

[418] European Council, 'European Council Meeting (20 June 2019) - Conclusions EUCO 9/19', p. 8.

[419] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's Digital Future, COM 67 Final' (Brussels, 2020) <https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf> [accessed 14 May 2020].

[420] European Commission, 'Shaping Europe's Digital Future, COM 67 Final', p. 3 ff.

[421] European Commission, 'Shaping Europe's Digital Future, COM 67 Final', p. 7 ff.

[422] European Commission, 'Shaping Europe's Digital Future, COM 67 Final', p. 10 f.

[423] European Commission, 'Shaping Europe's Digital Future, COM 67 Final', p. 13 f.

of global data economy.[424] Different problems have been identified concerning availability of data, imbalances in market power, data interoperability and quality, data governance, data infrastructures and technologies, empowering individuals to exercise their rights, skills and data literacy and cybersecurity.[425] The European Commission's strategy to address the issues consists of the following four pillars: a cross-sectoral governance framework for data access and use, investments in data and strengthening Europe's capabilities and infrastructures, empowering individuals, investing in skills and small and medium enterprises (SMEs), common European data spaces in strategic sectors and domains of public interest.[426]

Still in February 2020, the European Commission published its report on safety and liability implications of AI, Internet of Things and robotics.[427] It argues that the existing legal framework protects consumers, creates trust in technologies and allows businesses to operate under high levels of legal certainty. However, new technologies like Artificial Intelligence are transforming the characteristics of many products and services. Regarding safety, the Commission calls for security-by-design mechanisms that ensure the high standards for products. Various challenges for the product safety framework occur regarding connectivity, autonomy, mental health risks, data dependency, opacity, complexity of products and systems, software and complex value chains.[428] Liability law provides protection for citizens while creating an innovation-friendly environment for entrepreneurs; however, the changing elements of new technologies could lower their effectiveness. One of the core challenges is the problem to trace back damage to human behaviour, when higher levels of autonomy are implemented. Important for operators is

---

[424] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM 66 Final' (Brussels, 2020), p. 4 <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> [accessed 14 May 2020].

[425] European Commission, 'A European Strategy for Data, COM 66 Final', p. 6 ff.

[426] European Commission, 'A European Strategy for Data, COM 66 Final', p. 12 ff.

[427] European Commission, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, COM 64 Final' (Brussels, 2020) <https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf> [accessed 14 May 2020].

[428] European Commission, 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, COM 64 Final', p. 5 ff.

to have clear legal fault-liability frameworks in order to know which criteria have to be met. Crucial for victims of accidents is that they do not face lower levels of protection. A suggestion for a solution is to implement a risk-based approach where applications with higher risk face increased safety requirements.[429]

The most important document on AI is the Commission's white paper that outlines the '*European approach to excellence and trust*' and aims for the promotion of the new technology's uptake, addressing its risks and clearly rejects the development and use of military AI.[430] The '*ecosystem of excellence*' should be achieved by multiple actions in the fields of cooperation with Member States, research and innovation, skills, a focus on SMEs, public and private sector partnerships and improved infrastructure.[431] The '*ecosystem of trust*' includes an adjusted regulatory and legislative framework that addresses the risks for fundamental rights, privacy, safety and other areas.[432] The concepts of the document will be discussed in more detail in the following chapter.

In March 2020, the European Parliamentary Research Service of the European Parliament published a comprehensive document on ethical and moral questions associated with the deployment of Artificial Intelligence.[433] The impact of the technology on society, economy, environment and human psychology and trust is outlined. In addition, initiatives in the field of AI ethics are described before discussing different national and international strategies for the technology. In the next chapter, the Commission's strategic documents on AI published in 2020 will be analysed and the main concepts will be discussed more closely.

[429] European Commission, 'Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, COM 64 Final', p. 12 ff.
[430] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final'.
[431] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 5 ff.
[432] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 9 ff.
[433] Bird and others.

B. The attempt to AI with European values

a. Putting the human at the centre

The European Commission strongly encourages focusing on a human-centric approach to Artificial Intelligence.[434] It was first mentioned in the Commission's communication '*Building Trust in Human-Centric Artificial Intelligence*' in 2018, when the strategic focus on putting people and their needs at the centre of the development was outlined, with trust as a prerequisite and the ultimate goal of increasing human well-being.[435] In the European Commission's strategy for data, the first element of the vision states that the '*human being is and should remain at the centre.*'[436] Moreover, the communication on the digital future of Europe considers to development of technology that works for people as one of the three key objectives.[437] The High-Level Expert Group on AI offers a definition on human-centric Artificial Intelligence, stating that this approach focuses on ensuring human values are central for the development, deployment or usage of AI systems. Special emphasis is put on the compliance with human rights as well as the inalienable moral status of human beings with respect for every individual's dignity. The definition also includes respecting the natural environment and other creatures present in human ecosystems also emphasising the limitations of the planet and the need to ensure the well-being of future generations.[438] In addition, the Commission wants to continue its efforts to bring the Union's approach to the global stage, cooperate with like-minded partners, play an active role in international discussions and build a consensus on human-centric AI.

This focus could arguably be seen as a result of the ethical considerations of the EU regarding AI and the dominance of human rights aspects in the discourse. One of the most crucial ethical challenges on individual level is autonomy, which is connected to the problem of at some point being '*out of the loop*' if AI systems become more advanced. Other applications, for instance the deployment of robots for care-work could lead to a denial of use, when people refuse to accept these developments. The European

---

[434] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 3.
[435] European Commission, 'Building Trust in Human-Centric Artificial Intelligence, COM 168 Final', p. 1 f.
[436] European Commission, 'A European Strategy for Data, COM 66 Final', p. 4.
[437] European Commission, 'Shaping Europe's Digital Future, COM 67 Final', p. 2.
[438] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 37.

Commission's human-centric approach that puts particular emphasis on the respect of human dignity covers both above mentioned aspects. That is, the final control of algorithms as well as the use in different sensitive areas as the concept is interpreted broadly. These controversially discussed applications could also be the reason why the recent publications have placed a strong focus on building trust in the new technologies.

b. Trustworthy technology

One of the main building blocks of the European Commission's white paper on Artificial Intelligence is the creation of a regulatory framework that enables an '*ecosystem of trust*' and supports the development of European AI that is grounded in values and fundamental rights. This is important as citizens are facing an information asymmetry when dealing with algorithmic decision-making while at the same time companies need legal certainty in order for being able to calculate their business activities. If people's worries regarding malicious effects of AI are not accordingly addressed, the uptake of the technology will be slowed.[439] The High-Level Expert Group describes trustworthy AI with three aspects. It must be lawful (i.e. complying with all applicable laws and regulations), ethical (i.e. ensuring adherence to ethical principles and values) and robust (i.e. both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm).[440]

The foundations of trustworthy AI are fundamental rights, which are enshrined in the EU Treaties, the EU Charter and international human rights law. Further, four ethical principles must be respected in order to ensure that AI systems are developed, deployed and used in a trustworthy manner. These are the respect for human autonomy, the prevention of harm, fairness and explicability.[441] An ecosystem of trust can only be created, when specific requirements are complied with. These were developed by the HLEG on AI and later welcomed in a communication by the Commission.[442] Among the identified key requirements are human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and

[439] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 9.
[440] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 5.
[441] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI', p. 9 ff.
[442] European Commission, 'Building Trust in Human-Centric Artificial Intelligence, COM 168 Final'.

fairness, societal and environmental wellbeing, and accountability.[443] Current EU legislation on fundamental rights, consumer protection or product safety and liability provides a regulatory framework for developers and deployers of AI applications. However, characteristics of AI systems such as opacity ('*black box-effect*'), complexity, unpredictability and partially autonomous behaviour make compliance and enforcement of regulations increasingly difficult.[444]

According to the European Commission's White Paper on AI, the regulatory framework of trustworthy AI should focus on minimising the occurrence of harm. This could be either material damage, regarding health and safety of human beings as well as property, or immaterial harm, for instance concerning privacy, dignity, discrimination or limitations to the right of freedom of expression. The most crucial risks connected to the uptake of AI concern the application of regulations which are supposed to protect basic human rights. The increased capabilities of tracking and analysing human behaviour create higher perils for potential breaches of privacy protection acts.[445] Another potential risk has been found by researchers regarding the use of AI algorithms for predictive performance, for instance on criminal recidivism. The result was evidenced discrimination by Machine Learning models that '*tend to discriminate against male defendants, foreigners, or people of specific national groups.*'[446] Therefore, the usage of similar models which display gender or ethnic bias for decision-making would pose a problem of fairness. Another study found that algorithms for facial analysis discriminate on the basis of gender and ethnic group. In the sample, darker-skinned females were the most misclassified group, while lighter-skinned males had significantly lower error rates.[447] A report by the Council of Europe found that algorithms have an impact on a number of human rights such as fair trial, privacy and data protection, freedom of expression, freedom of assembly and association, effective remedy, prohibition of

[443] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 9.

[444] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 10.

[445] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 10 f.

[446] Songül Tolan and others, 'Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia', in *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law - ICAIL '19* (presented at the the Seventeenth International Conference, Montreal, QC, Canada: ACM Press, 2019), pp. 83–92 <http://dl.acm.org/citation.cfm?doid=3322640.3326705> [accessed 4 August 2020].

[447] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, 81.no issue (2018).

discrimination, social rights and access to public services, the right to free elections and others.[448] The European Commission's white paper puts emphasis on these scholarly findings and states that '*[t]he use of AI can affect the values on which the EU is founded and lead to breaches of fundamental rights.*'[449]

Another aspect which entails risks is connected to safety and a functioning liability regime. If AI systems are embedded in products and services, new perils may occur. The classic example would be the autonomous driving car that has an accident with material damage and injuries of human beings as a result of flaws in the technology. Possible reasons could be issues in the design of the algorithms or connected to availability and quality of training data. '*While some of these risks are not limited to products and services that rely on AI, the use of AI may increase or aggravate the risks.*'[450] Insofar safety regulations are not clearly defined, legal uncertainties for companies arise in addition to risks for people. These uncertainties could lead to an overall decrease in the level of security and affect the competitiveness of European companies as well. When security risks materialise, the lack of clear legal provisions and the above-mentioned characteristics of AI systems pose a problem because of the difficulty to trace back potentially problematic decision-making processes. This in turn could result in damaged individuals having difficult access to compensation for their suffered harm. The EU product liability directive stipulates that '*a manufacturer is liable for damage caused by a defective product.*'[451] If a self-driving car were to cause damage, it could be difficult to prove a defect in the product and the connection to the damage caused. Additionally, the applicability of the directive is still associated with uncertainty, especially for cases where damage results from weaknesses in cybersecurity. The result of this gap between AI systems and traditional technologies regarding security and liability, could lead to injured individuals having problems getting compensation because the evidence needed is difficult to provide.[452] After discussing some problems connected to establishing

---

[448] Committee of Experts on Internet Intermediaries, *Algorithms and Human Rights: Study on the Human Rights Dimension of Automated Data Processing Techniques and Possible Regulatory Implications* (Strasbourg: Council of Europe, 2018) <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> [accessed 4 August 2020].

[449] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 11.

[450] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 12.

[451] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 13.

[452] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 13.

trustworthy technology, potential legal adjustments to address specific risks and situations will be outlined in the next paragraphs.

c. Potential legal adjustments

Regarding the protection of fundamental and consumer rights, various EU legislations ensure legal safety. For instance, the Race Equality Directive, the Directives on equal treatment between men and women in relation to employment and access to goods and services, the Directive on equal treatment in employment and occupation, different consumer protection rules, but also the GDPR for privacy and data protection, as well as sectoral laws as the Data Protection Law Enforcement Directive. For safety and liability, various European regulations provide protection which are '*potentially applicable to a number of emerging AI applications.*'[453] In principle, EU regulations remain valid for AI applications. However, legal adjustments may have to be implemented to ensure enforcement and cover emerging technology's new risks.

The European Commission's white paper on AI outlines specific situations and risks where the legislative framework could need some improvements. The first one concerns effective application and enforcement of existing EU and national legislation. Typical AI characteristics such as opaqueness lead to issues of transparency, which makes the identification of unlawful activities or violation of legal provisions more difficult. To counteract this trend, measures to adapt and clarify existing standards, for example in the area of liability law, are necessary. Second, existing EU legislation and its scope of application have to be adapted in a suitable way. The current EU product safety regulations link liability norms to the placing of commodities on the market. While software that is part of a final product is bound to the product safety standards, the coverage of stand-alone software is still an open question, apart from specific sectors that have explicit rules. In general, the existing EU safety norms apply '*to products and not to services, and therefore in principle not to services based on AI technology either (e.g. health services, financial services, transport services).*'[454]

[453] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 13.
[454] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 14.

Third, the fact that AI systems are sometimes subject to change during their lifecycles provides new risks which did not exist when a certain product was launched. This modification takes place, for instance, in applications that require ongoing software updates or are based on Machine Learning. With regard to security risks, the current legal situation primarily considers risks that already existed when the product was launched. Therefore, risks that occur during the lifetime of a product are not adequately covered by the current legislation. Fourth, the allocation of responsibilities between economic operators in the supply chain has to be clarified in order to reduce uncertainty. In principle, the producer of a product who placed it on the market is liable for the functioning of all components including AI systems. For the case that an algorithmic application is added later by a party that is not the producer, the current legal framework does not provide a clear solution. Finally, the concept of safety itself could be subject to change. The characteristics of AI could lead to the occurrence of new risks which are not covered by the current legislation. For instance, cyber threats, personal security risks connected to smart home applications, risks that occur when connectivity is lost or unstable and others. Such risks could already exist during the launch of a product or only arise later due to self-learning applications or alterations such as software updates. The Commission is of the opinion that these five situations require improvements in the legislative framework. An important aspect for immediate common European action is to avoid national legislation that would risk fragmentation of the EU's single market.[455] After discussing some legal challenges regarding improvements in the EU's legislative framework, the next paragraphs will look into the Commission's suggestion of a risk-based approach which should ensure the appropriateness of regulatory intervention.

d. Risk-based approach

Besides the existing legal framework, which provides strict regulation in the fields of consumer protection, fundamental rights and other specific areas (e.g. healthcare), the Commission suggests adding a new regulatory framework in order to ensure the creation of technology that people can trust. To achieve a balance between the protection of important legal assets as well as a moderate regulation that does not overwhelm small and medium-sized companies, a risk-based approach is aimed for. For determining which

[455] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 14 f.

applications are assessed high-risk, the European Commission's proposal suggests looking at the stakes involved and '*considering whether both the sector and the intended use involve significant risks, in particular from the viewpoint of protection and safety, consumer rights and fundamental rights.*'[456]

The first criterion deals with the sector in which an application is located. The typical characteristics of the activities in this area are to be analysed and it is to be determined whether significant risks can be expected. The goal is to identify areas where risks are likely to occur. The list of sectors should be exhaustive and specific, but the selection needs to be reviewed from time to time. The second criterion is met if the application is ,*used in such a manner that significant risks are likely to arise.*'[457] The intention of this provision is the fact that not all possible uses within a sector involve significant risks. The health sector will certainly be an affected sector, but not all activities within the area involve special risks, for instance administrative matters. Legislative intervention in these areas is probably not justifiable. For determining the level of risk, the impact on the parties concerned could potentially be used as a reference point. Exemplary, this would include applications that have legal effects on the rights of natural or legal persons or that bear the risk of death, injury, or material or immaterial damage. If both cumulative criteria are met, the AI application would be classified as high-risk. A clear framework for action prevents legal uncertainty, which is an important aspect. There could be exceptions in certain areas due to special risks, where AI systems are always subject to strict requirements (see more details below). An example could be recruiting and human resource management, where important legal interests such as employment equality have to be complied with and would therefore be considered high-risk.[458]

Important for the risk-based approach are the types of requirements, which provide the mandatory legal framework for AI deployers and developers. The European Commission's white paper on AI suggests six requirements for high-risk AI systems, that should support and defend European values and rules. The first one concerns the data for

[456] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 17.
[457] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 17.
[458] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 17 f.

training the algorithms, which is a basic requirement for the emergence of AI. To begin with, reasonable assurances should ensure that the use of the services or products is in line with EU standards and that safety regulations are observed. In addition, measures are to be taken to prevent discrimination through AI systems. One way to do this would be to use data sets that are sufficiently representative and depict a broad spectrum of relevant factors in the area of gender, ethnicity, and others. Moreover, privacy and personal data must be secured when using products and services with AI technology with special emphasis to the GDPR's legal framework.[459]

Second, records and data sets of the programming of algorithms for high-risk AI applications have to be kept. Thus, despite the complexity and opacity of the technology, compliance with rules can be ensured and the decision-making processes can be tracked if problems occur. The regulations could stipulate that records of data sets, which are crucial for the training of AI systems, must be kept. This could concern records of the main characteristics and the selection of the data and, in special cases, the data sets themselves. In addition, it would be conceivable that programming and training methods must be documented and specifically explained how the occurrence of prejudices and other prohibited discrimination is prevented. Importantly, the records would only have to be kept for a limited time period.

Third, the provision of adequate information has to be ensured as transparency is crucial for the promotion of responsible and trustworthy AI. The capabilities but also limitations of algorithms should be communicated openly as well as the intended purpose and the expected degree of accuracy, which are important aspects for all stakeholders. If it is not clear that some kind of interaction is carried out with the help of AI technology, citizens have to be informed about it. The information should necessarily be presented in a simple manner and as objectively and concisely as possible.[460]

Fourth, the robustness and accuracy of high-risk AI systems has to be ensured. Potential risks have to be considered in the development process, which in general has to be reflected by high degrees of responsibility and ex-ante precautionary measures. The

[459] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 18 f.
[460] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 19 f.

functioning must be in a reliable way and potential risks have to be minimised. Aspects that need special emphasis for the development of requirements are the guarantee of robustness and accuracy during life cycles of products and services, or at least the degree of accuracy has to be communicated in a correct way. In addition, results have to be reproducible and safety mechanisms for the occurrence of errors must be included. With the implementation of precautionary measures, data manipulation or external interference that affects the functionality are to be prevented.[461]

Fifth, measures have to be taken for human oversight which should ensure that a human being's autonomy is not undermined. Especially high-risk AI systems need human oversight, as the outcome regularly has serious consequences for the stakeholders involved, nevertheless, the degree of supervision could vary among different types of cases. One element to determine the extent of oversight, could be the intended use and the effects for citizens, whereby the GDPR security regulations must be complied with. A prerequisite could be that results of an algorithmic application only take effect when a natural person confirms the outcome. For example, in the case of rejection of social benefits, where a single decision of an AI system would probably be difficult in the light of human rights, however, if human oversight is ensured, the appropriateness could rather be argued. Another way could be to ensure the intervention of natural persons after the decision becomes effective. This should probably be the case with less serious decisions than the above, for instance an application for a credit card. In addition, certain specific applications could need the possibility of real time human intervention during a system's performance. For example, if a person recognises that an autonomous car is not operating safely, a stop button could be necessary to pause the activity in a secure way.[462]

Finally, the use of AI systems for facial recognition that involves collecting biometric data to enable remote identification, is already subject to strict EU regulations and poses risks for human rights. European data protection law regards the possibility of using biometric data for identification processes to be permissible only under certain conditions. The processing must have a high degree of public interest, take place in

[461] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 20 f.
[462] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 21.

compliance with national and European legal provisions, follow the principle of proportionality and guarantee an adequate level of security. In sum, '*AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards.*'[463] After presenting human centric-AI, possibilities for trustworthy technology, potential legal adjustments and the suggestion of a risk-based approach, the following chapter will provide an analysis of the European approach to AI and discuss it in the light of the Normative Power Europe approach.

C. Analysis

In the light of the concept of Normative Power Europe, actions are based on values and principles with a strong commitment to human rights and international law. The above-discussed human-centric approach to AI provides an example of the European way to cover the topic. The strong focus on the human being and its individual inalienable moral status connected to various fundamental rights can be seen as the basic perspective that guides the design of the suggested regulatory framework. At the core lies the recognition that AI affects fundamental values of human life in a substantial way. One of them, autonomy, is not only among the core values of western ethics, but reflects everyone's capacity of individual choice, rights and freedoms. The problem of potential autonomy of systems with the possibility of natural persons becoming '*out of the loop*' is supposed to be addressed by ensuring accurate levels of human oversight for high-risk AI applications. For instance, in cases that have significant legal effects such as a rejection of social benefits, supervision or a second review by a human being seems to be necessary. Other examples concern the interaction of bots and humans. In the case of communication with algorithms instead of natural persons, transparency and information are crucial. When it comes to care for the elderly, special attention must be paid to emotional and social needs of clients, where the human-centric approach to AI tries to include their demands in a pronounced way.

Another category central to the European Union's approach to Artificial Intelligence is trust. According to the European Commission's white paper, European AI that is based on fundamental rights and values should be created. To ensure sufficient

[463] European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 22.

levels of trust, European AI has to be lawful, ethical and robust. The Commission recognised that characteristics like opacity, complexity and unpredictability provide problems connected to the compliance with fundamental rights and the enforcement of provisions which are designed to protect these norms, for instance the GDPR's right to information. In order to address the issue, the suggestion to regulate high-risk AI applications would for example require communicating openly about systems capabilities and limitations. In addition, the level of accuracy would have to be disclosed resulting in higher levels of transparency. The increased possibilities for tracking and analysing human behaviour create higher risks of violation of privacy and data protection laws. As both are protected by fundamental rights in the EU, compliance with and, if necessary, adjustment of the legislative framework have to be ensured.

An aspect of AI application that rather concerns the societal level is the matter of discrimination by algorithms. The EU is aware of the problem connected to predictive performance for criminal recidivism, facial analysis and others; compliance with the high requirements in the area of fairness and equality must be ensured, though. In order to address the issue, the European attempt suggests certain measures to be taken to prevent discrimination.

The Commission's suggestion for a regulatory framework provides that high-risk applications would need special requirements for the data necessary to train the algorithms. These could be obligations for determined levels of representativeness of data sets which depict a broad spectrum of relevant factors in the area of gender, ethnicity, and others. Moreover, various human rights are affected by AI systems, which requires close review that compliance is guaranteed, and citizens are able to trust the technology.

The European Commission suggests the creation of a regulatory framework for high-risk AI applications, in addition to existing regulations. At the current stage, the documents published by the Commission, specifically the white paper on AI, are program documents only that have not yet been put into law. If these were implemented as proposed, the requirements would not only almost certainly be the most comprehensive regulations in the field of AI, but especially compared to China and the US, the extent of distinction would be very large. Given the dominance of human rights in the European

discourse and the specific European identity focused on the compliance with fundamental rights, what Ian Manners calls Normative Power Europe can be witnessed in the area studied here during the phase covered, i.e. largely policy proposals by the Commission.

Considering the future of AI, an important aspect are the decision-making modalities of the EU in connection with the proposals on Artificial Intelligence. The Treaty on the Functioning of the EU, last revised under the Lisbon Treaty, offers no specific references to digital policies.[464] Looking at the case of the Digital Single Market (DSM) shows that its legislation is '*framed within the internal market policy,*'[465] As for internal market policy, the European Union and the Member States have shared competences, the competences in the field of digital policy are shared, too.[466] The European Council, responsible for defining overall digital policy goals, '*represents national interests, which are usually tied to the allocation of funds.*'[467] The requirement of unanimity in the European Council is a challenge to bridge the digital investment gap for AI, because an agreement of all Member States is necessary.[468] Particularly relevant in the legislative process is the decision-making modality of the Council of the European Union as the main legislative body. As stated above, digital policies are applied within the frame of internal market policy. Therefore, the '*voting mechanism is most often that of qualified majority.*'[469] Qualified majority voting (QMV) is defined as *'(1) the votes of fifty-five percent of the Member States, (2) representing at least fifteen states, and (3) representing sixty-five percent of the EU population*.'[470] Particularly important is the fact, that approval requirements are also high for QMV and the risk of blockades as well as

[464] Mirela Mărcuț, *Crystalizing the EU Digital Policy: An Exploration into the Digital Single Market* (Switzerland, Cham: Springer International Publishing, 2017), p. 127.
[465] Mărcuț, p. 136.
[466] Mărcuț, p. 136 f.
[467] Mărcuț, p. 139.
[468] Laura Kayali, Melissa Heikkilä, and Janosch Delcker, 'Europe's Digital Vision, Explained: The EU Is Rolling out Strategic Plans on Data, Artificial Intelligence and Platform Regulation.', *Politico EU*, 19 February 2020 <https://www.politico.eu/article/europes-digital-vision-explained/> [accessed 17 September 2020].
[469] Mărcuț, p. 140.
[470] Stephen C. Sieberson, 'Inching toward EU Supranationalism - Qualified Majority Voting and Unanimity under the Treaty of Lisbon', *Virginia Journal of International Law*, 50.4 (2010), 919–95 (p. 939).

'*lowest-common-denominator*' solutions is significant.[471] Therefore, it is vital that the Commission documents cannot be equated with adopted EU policies. However, Margrethe Vestager, EU Commissioner responsible for digital affairs, announced in a press conference in February 2020 that hard law on AI has to be expected and follow-up on the white paper should be expected in the last quarter of the year.[472]

Scheipers and Sicurelli state that normative force should be understood as power to shape and influence the discourse regarding values and basic principles. A formulated goal of the European Union is to '*exercise global leadership in building alliances around shared values and promoting the ethical use of AI.*'[473] The EU was not only closely involved in the development of the OECD's ethical guidelines, but the Commission's High-Level Expert Group on AI integrated various non-EU organisations as well as a number of governmental observers into the process of developing its ethical principles. The European Commission wants to actively increase its international influence and export its principles globally.[474] Although the EU's influence on the discourse was not subject of this master's thesis, the global ambitions definitely show the Commission's will to shape the discourse.

Looking at the results of the examination of the EU's normative power in the two cases of the elaboration of the Kyoto Protocol and the institutionalisation of the International Criminal Court shows great similarities to the European approach to Artificial Intelligence. First, the affected principles the EU tries to implement in its regulatory framework are universal in reach as human and fundamental rights concern every human being. Second, the EU aims at cooperating with like-minded partners and consensus-building on human-centric AI trying to become a pioneer in ethical applications of the technology. Similar to Kyoto and the ICC, sharp demarcations to the United States can be seen as discussed in chapter III. In addition, while the People's Republic of China was not subject to analysis regarding Kyoto and the ICC, comparable

---

471 Gerda Falkner, 'Introduction: The EU's Decision Traps and Their Exits: A Concept for Comparative Analysis', in *The EU's Decision Traps: Comparing Policies* (Oxford, United Kingdom: Oxford University Press, 2011), pp. 1–17 (p. 3).

472 Kayali, Heikkilä, and Delcker.

473 European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 8.

474 European Commission, 'White Paper: On Artificial Intelligence, COM 65 Final', p. 8 f.

distinction has to be made between the EU and China regarding AI. Third, the restriction to diplomatic and non-military actions can be argued, as the European Commission's white paper opposes the development of military AI. Again, the US and China take a different path with strong commitment to both dual-use technology and military applications of AI. Finally, the European identity as specified by Ian Manners strongly favours compliance with international law and human rights. While the EU is criticised in relation to human rights in the area of migration, the European Commission's current program documents regarding Artificial Intelligence allow a positive outlook. The Commission's focus on conformity with the norms of international humanitarian law, as seen in the EDF's prohibition to fund defence related projects illegal by international law, further reflects this aspect. In sum, the concept of Normative Power Europe is fruitful to characterise the European approach to Artificial Intelligence, because the strong commitment to and protection of fundamental rights is present in the program documents in a pronounced form. Having discussed the European approach to Artificial Intelligence in detail, now the results will be summarised, the research questions answered, and some concluding remarks will be given.

V. Concluding remarks

There are fundamental differences between the United States, China and the European Union regarding data protection regulation. The US does not provide for everyone's privacy via an omnibus legislation, while in contrast, the free flow of data enjoys protection at constitutional level. The privacy of consumers is protected to a certain degree, but the enforcement mechanisms cannot be assessed as strong, because the FTC rather than independent courts is responsible for enforcement. In the US, privacy laws focus on negative freedom against governmental authority, while the Chinese system, in contrast, offers very little regulation for the public sector. China's constitution is seen as unprepared for a comprehensive data protection regime and its judicial system is ineffective when it comes to the enforcement of rights. Announcements from the Standing Committee of the National People's Congress of China allow a positive outlook. However, the current level of protection is lower than the OECD and Council of Europe standards of the early 1980s. The European Union's data protection framework is of omnibus nature and has a strong constitutional anchor. Fundamental rights are protected by

constitutional courts and the GDPR is referred to as the gold standard in the field. In the European Union, a comprehensive level of protection is given, accompanied by legal certainty, strong enforcement mechanisms, high administrative fines and enforceability. The data protection regulation in the US was assessed as partially comprehensive, while the Chinese data protection regime was evaluated as not comprehensive.
In the EU, comprehensive data protection regulation was ascertained. Nonetheless, there is also criticism due to problems with the implementation of the GDPR. National data protection authorities do not work together efficiently and some of them seem to be overwhelmed and lack sufficient resources.

For the US, Artificial Intelligence is a crucial part for maintaining its military superiority. The achievement of the goal is supported by massive amounts of government funding. Not only does the country have various running projects to apply AI systems for military applications but it is even the world leader regarding the development of lethal autonomous weapons systems, too. China aims at developing its army into a world-class force until mid-century. The current situation is seen as a historic opportunity to catch-up with other countries' military power. To reach its ambitious targets, China created its own DARPA, increased its spending in the sector and declared military AI a national priority. In Europe, the situation is ambiguous. The '*European DARPA*' only focuses on civil technology, the European Commission is without mandate for military and defence policy and the Commission's white paper opposes AI for military purposes. However, the launch of the European Defence Fund is described as a '*paradigm shift*' in this field, because direct public funding for military technology research and development is accepted for the first time in EU history. While China and the US clearly have a strong focus on the development of military AI, the position of the EU is rather nuanced, more cautious and does only partially focus on military AI. The actions of the EU regarding comprehensive data protection regulation were classified as norm-guided but concerning military AI only partially norm-guided. Therefore, empirically, the EU can be classified as Weak Normative Power. Especially when compared to the US and China, the results have shown that the EU clearly stands out from the other two and takes a different path.

Table 6: Overview of results[475]

Comprehensive data protection regulation		United States	China	European Union
	yes			X
	partially	X		
	no		X	
Not focusing on military AI				
	yes			
	partially			X
	no	X	X	

On a more abstract level, the concept Normative Power Europe is useful to describe the EU's actions in the field of Artificial Intelligence. There are various problems and challenges connected to the uptake of the technology. Increased capabilities for tracking and analysing of human behaviour leads to new perils for personal privacy. Applications in the field of predictive performance, criminal recidivism and facial analysis pose risks for fairness as gender, ethnic or other biases by algorithms could lead to discrimination and undermining of fundamental rights. Opaqueness and transparency issues create problems for the possibility of tracing back problematic decision-making processes which are vital to ensure compensation of damaged individuals. All these legal assets need to be protected, while striking a balance for not overwhelming SMEs is crucial, too. To address the problems, fundamental rights and human dignity served as the basis for the development of ethical principles for AI. The European discourse is highly dominated by human rights aspects and the building of a human-centric approach to the technology. This focus on the individual and its moral status guided the Commission's proposal for a regulatory framework for Artificial Intelligence. Trustworthy technology, which is lawful, ethical and robust, should prevent discrimination. The involvement in the development of the OECD guidelines for ethical AI and the European ambitions to increase international influence and export its

[475] Table 6: Overview of results, own presentation.

principles globally show the EU's will to actively participate in the discourse when it comes to basic values. While debates about military actions still tend to divide Europe, the emphasis on human rights and the moral role in world politics provides ground for coherence, as has already been argued by Ian Manners. Therefore, his concept of Normative Power Europe can be considered to be fruitful to characterise the European approach to AI.

This work, with its social constructivist approach, reveals the possibility of more precisely classifying the activities of the EU in the field of Artificial Intelligence in the broader context of digitisation. As soon as more detailed information on the implementation becomes known, it could be further investigated to what extent the regulatory options that have been presented in the European Commission's recent publications are actually reflected in the legislative framework.

VI. Bibliography

Allen, Gregory, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Center for a New American Security, Washington DC, 2019) <https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041> [accessed 7 May 2020]

Allen, Gregory, and Taniel Chan, *Artificial Intelligence and National Security* (Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2017) <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> [accessed 9 June 2020]

Allen, Gregory, and Elsa B. Kania, 'China Is Using America's Own Plan to Dominate the Future of Artificial Intelligence', *Foreign Policy*, 8 September 2017 <https://foreignpolicy.com/2017/09/08/china-is-using-americas-own-plan-to-dominate-the-future-of-artificial-intelligence/> [accessed 25 March 2020]

Amoroso, Daniele, and Guglielmo Tamburrini, 'The Ethical and Legal Case Against Autonomy in Weapons Systems', *Global Jurist*, 18.1 (2018) <https://www.degruyter.com/doi/10.1515/gj-2017-0012> [accessed 9 June 2020]

Asaro, Peter, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making', *International Review of the Red Cross*, 94.886 (2012), 687–709

Ashwin, Acharya and Arnold Zachary, Chinese Public AI R&D Spending: Provisional Findings (Washington, D.C.: Center for Security and Emerging Technology, 2019), <https://cset.georgetown.edu/wp-content/uploads/Chinese-Public-AI-RD-Spending- Provisional-Findings-2.pdf> [accessed 22 September 2020].

Besch, Sophia, 'The European Commission in EU Defense Industrial Policy' (Carnegie Europe, 2019) <https://carnegieeurope.eu/2019/10/22/european-commission-in-eu-defense-industrial-policy-pub-80102> [accessed 12 May 2020]

Bird, Eleanor, Jasmin Fox-Skelly, Nicola Jenner, Ruth Larbey, Emma Weitkamp, and Alan Winfield, 'The Ethics of Artificial Intelligence: Issues and Initiatives' (EPRS, European Parliamentary Research Service, Brussels, 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf> [accessed 29 May 2020]

Bode, Ingvild, and Hendrik Huelss, 'Autonomous Weapons Systems and Changing Norms in International Relations', *Review of International Studies*, 44.3 (2018), 393–413

Bratman, Benjamin E, 'Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy', *Tennessee Law Review*, 69.3 (2002), 623–51

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, and Peter Eckersley, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Information Society Project, Future of Humanity Institute, 2018) <https://arxiv.org/pdf/1802.07228.pdf> [accessed 8 June 2020]

Buolamwini, Joy, and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, 81.no issue (2018)

Buttarelli, Giovanni, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard', *International Data Privacy Law*, 6.2 (2016), 77–78

Campaign to Stop Killer Robots, *Country Views on Killer Robots*, 2018 <https://www.stopkillerrobots.org/wp-content/uploads/2019/10/KRC_CountryViews_25Oct2019rev.pdf> [accessed 30 April 2020]

Carriço, Gonçalo, 'The EU and Artificial Intelligence: A Human-Centred Perspective', *European View*, 17.1 (2018), 29–36

Castro, Daniel, Michael McLaughlin, and Eline Chivot, *Who Is Winning the AI Race: China, the EU or the United States?* (Center for Data Innovation, Washington D.C. and Brussels, 2019) <http://www2.datainnovation.org/2019-china-eu-us-ai.pdf> [accessed 5 March 2020]

Chan, Minnie, 'Chinese Military Sets up Hi-Tech Weapons Research Agency Modelled on US Body', *South China Morning Post*, 25 July 2017 <https://www.scmp.com/print/news/china/diplomacy-defence/article/2104070/chinese-military-sets-hi-tech-weapons-research-agency> [accessed 9 March 2020]

'Charter of Fundamental Rights of the European Union', 2012 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN> [accessed 20 April 2020]

Chivot, Eline, and Daniel Castro, *The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy* (Center for Data Innovation, Washington D.C. and Brussels, 2019) <http://www2.datainnovation.org/2019-reform-the-gdpr-ai-a4.pdf> [accessed 20 April 2020]

Chouldechova, Alexandra, 'Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments', *Big Data*, 5.2 (2017), 153–63

Committee of Experts on Internet Intermediaries, *Algorithms and Human Rights: Study on the Human Rights Dimension of Automated Data Processing Techniques and Possible Regulatory Implications* (Strasbourg: Council of Europe, 2018)

<https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5> [accessed 4 August 2020]

Convention on Certain Weapons (CCW) Group of Government Experts, *Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (Geneva: United Nations Office at Geneva, 2018) <https://www.unog.ch/80256EDD006B8954/(httpAssets)/20092911F6495FA7C125830E003F9A5B/$file/CCW_GGE.1_2018_3_final.pdf> [accessed 30 April 2020]

Cordesman, Anthony H. and Joseph Kendall, Estimates of Chinese Military Spending (Washington, D.C.: Center for Strategic and International Studies, 2016), <https://www.jstor.org/stable/pdf/resrep23365.pdf?refreqid=excelsior%3A854028fc75d715dd87c8e999ad0c7541> [accessed 22 September 2020].

Council of Europe, 'European Convention on Human Rights', 1950 <https://www.echr.coe.int/Documents/Convention_ENG.pdf> [accessed 21 April 2020]

Council of the EU, 'Artificial Intelligence: Conclusions on the Coordinated Plan on Artificial Intelligence, 6177/19' (Brussels, 2019) <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf> [accessed 14 May 2020]

———, 'Council Conclusions on the Future of Work Making It E-Easy, 15506/17' (Brussels, 2017) <http://data.consilium.europa.eu/doc/document/ST-15506-2017-INIT/en/pdf> [accessed 25 March 2020]

———, 'Council Conclusions on the Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence Building Strong Cybersecurity for the EU, 14435/17' (Brussels, 2017) <https://www.consilium.europa.eu/media/31666/st14435en17.pdf> [accessed 25 March 2020]

———, 'Digital for Development (D4D) - Council Conclusions, 14542/17' (Brussels, 2017) <http://data.consilium.europa.eu/doc/document/ST-14542-2017-INIT/en/pdf> [accessed 25 March 2020]

Craglia, Massimo, Alessandro Annoni, Peter Benczur, Paolo Bertoldi, Blagoj Delioetrev, Giuditta De Prato, and others, *Artificial Intelligence: A European Perspective* (Joint Research Centre, Luxembourg: Publications Office of the European Union, 2018) <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC113826/ai-flagship-report-online.pdf> [accessed 25 March 2020]

Crofts, Penny, and Honni Van Rijswijk, 'Negotiating "Evil": Google, Project Maven and the Corporate Form', *Law, Technology and Humans*, 2.1 (2020)

De Hert, Paul, and Dr. Vagelis Papakonstantinou, 'The Data Protection Regime in China. In-Depth Analysis', 2015 <https://www.ssrn.com/abstract=2773577> [accessed 13 April 2020]

Defense Advanced Research Projects Agency (DARPA), 'DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies', 2018 <https://www.darpa.mil/news-events/2018-09-07> [accessed 2 May 2020]

Defense Science Board, 'Summer Study on Autonomy', 2016 <https://www.hsdl.org/?view&did=794641> [accessed 5 May 2020]

Department of Defense, 'Dircetive: Autonomy in Weapons Systems', 2012 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf> [accessed 5 May 2020]

Diez, Thomas, 'Constructing the Self and Changing Others: Reconsidering `Normative Power Europe'', *Millennium: Journal of International Studies*, 33.3 (2005), 613–36

Ding, Jeffrey, *Deciphering China's AI Dream* (Governance of AI Program, Future of Humanity Institute, University of Oxford, 2018) <https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf> [accessed 25 March 2020]

Donald J. Trump, *Executive Order on Maintaining American Leadership in Artificial Intelligence* (Washington, D.C.: The White House, 2019) <https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/> [accessed 13 August 2020]

Durmaz, Mahmut, 'Defense Technology Development: Does Every Country Need an Organization like DARPA?', *Innovation*, 18.1 (2016), 2–12

Ess, Charles, '"Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)', *Ethics and Information Technology*, 7.1 (2005), 1–6

EU Member States, 'Declaration - Cooperation on AI' (Brussels, 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50951> [accessed 25 March 2020]

Eurasia Group, *China Embraces AI: A Close Look and A Long View* (New York, 2017) <https://www.eurasiagroup.net/files/upload/China_Embraces_AI.pdf> [accessed 13 August 2020]

European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM 66 Final' (Brussels, 2020) <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf> [accessed 14 May 2020]

———, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the Safety and Liability

Implications of Artificial Intelligence, the Internet of Things and Robotics, COM 64 Final' (Brussels, 2020) <https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf> [accessed 14 May 2020]

———, 'White Paper: On Artificial Intelligence - A European Approach to Excellence and Trust COM 65 Final' (Brussels, 2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> [accessed 25 March 2020]

———, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's Digital Future, COM 67 Final' (Brussels, 2020) <https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf> [accessed 14 May 2020]

———, 'The European Defence Fund: Stepping up the EU's Role as a Security and Defence Provider', 2019, <https://ec.europa.eu/docsroom/documents/34509/attachments/1/translations/en/renditions/native> [accessed 22 September 2020].

———, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence, COM 168 Final' (Brussels, 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58496> [accessed 25 March 2020]

———, '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, COM 237 Final' (Brussels, 2018) <https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF> [accessed 25 March 2020]

———, '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: Coordinated Plan on Artificial Intelligence, COM 795 Final' (Brussels, 2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56018> [accessed 25 March 2020]

———, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Launching the European Defence Fund, COM 295 Final' (Brussels, 2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0295&from=EN> [accessed 12 May 2020]

———, 'Communication from the Commission to the European Parliament, the Council, the European Economic Committee and the Committee of the Regions; on the Mid-Term Review on the Implementation of the Digital Single Market Strategy,

COM 228 Final' (Brussels, 2017) <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-228-F1-EN-MAIN-PART-1.PDF> [accessed 25 March 2020]

European Commission - Press Release, 'European Cloud Initiative to Give Europe a Global Lead in the Data-Driven Economy' (Brussels, 2016) <https://ec.europa.eu/digital-single-market/en/news/european-cloud-initiative-give-europe-global-lead-data-driven-economy> [accessed 14 May 2020]

European Council, 'European Council Meeting (20 June 2019) - Conclusions EUCO 9/19' (Brussels, 2019) <https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf> [accessed 26 May 2020]

———, 'European Council Meeting (28 June 2018) - Conclusions, EUCO 9/18' (Brussels, 2018) <https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf> [accessed 25 May 2020]

———, 'European Council Meeting (19 October 2017) - Conclusions, EUCO 14/17' (Brussels, 2017) <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf> [accessed 14 May 2020]

European Data Protection Supervisor (EDPS), *Towards a Digital Ethics* (Brussels, 2018) <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf> [accessed 3 June 2020]

European Economic and Social Committee, 'Opinion of the European Economic and Social Committee on "Artificial Intelligence — The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society", C 288/1' (Official Journal of the European Union, Brussels) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016IE5369&from=EN> [accessed 14 May 2020]

European External Action Service (EEAS), 'Shared Vision, Common Action A Stronger Europe' (Publications Office of the European Union, Brussels, 2016) <http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf> [accessed 25 March 2020]

European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and "Autonomous" Systems' (Brussels: European Commission, 2018) <http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf> [accessed 6 February 2020]

European Parliament, 'REPORT with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))' (Brussels, 2017) <https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf> [accessed 14 May 2020]

European Parliament and Council of the European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' (Brussels, 2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> [accessed 20 April 2020]

———, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (Brussels, 1995) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en> [accessed 20 April 2020]

Executive Office of the President, 'Memorandum for the Heads of Executive Departments and Agencies', 2018 <https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf> [accessed 2 May 2020]

———, *Preparing for the Future of Artificial Intelligence* (Washington, D.C.: National Science and Technology Council Committee on Technology, 2016) <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf> [accessed 13 August 2020]

Fabbrini, Federico, *Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspective*, Oxford Studies in European Law, First edition (Oxford, United Kingdom: Oxford University Press, 2014)

Falkner, Gerda 'Introduction: The EU's Decision Traps and Their Exits: A Concept for Comparative Analysis', in The EU's Decision Traps: Comparing Policies (Oxford, United Kingdom: Oxford University Press, 2011), pp. 1–17

Feng, Yang, 'The Future of China's Personal Data Protection Law: Challenges and Prospects', *Asia Pacific Law Review*, 27.1 (2019), 62–82

Floridi, Luciano, 'Soft Ethics and the Governance of the Digital', *Philosophy & Technology*, 31.1 (2018), 1–8

Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, and others, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations', *Minds and Machines*, 28.4 (2018), 689–707

Franke, Ulrike Esther, *Not Smart Enough: The Poverty of European Military Thinking on Artificial Intelligence* (European Council on Foreign Relations, 2019) <https://www.ecfr.eu/page/-/Ulrike_Franke_not_smart_enough_AI.pdf> [accessed 25 March 2020]

Franke, Ulrike Esther, and Paola Sartori, *Machine Politics: Europe and the AI Revolution* (European Council on Foreign Relations, 2019) <https://www.ecfr.eu/page/-/machine_politics_europe_and_the_ai_revolution.pdf> [accessed 20 May 2020]

Fu, Tao, 'China's Personal Information Protection in a Data-Driven Economy: A Privacy Policy Study of Alibaba, Baidu and Tencent', *Global Media and Communication*, 15.2 (2019), 195–213

Future of Life Institute, 'Asilomar AI Principles', 2017 <https://futureoflife.org/ai-principles/?cn-reloaded=1#top> [accessed 2 June 2020]

Gettinger, Dan, 'Summary of Drone Spending in the FY 2019 Defense Budget Request' (Center for the Study of the Drone at Bard College, 2018) <https://dronecenter.bard.edu/files/2018/04/CSD-Drone-Spending-FY19-Web-1.pdf> [accessed 6 May 2020]

Gill, Bates, and Adam Ni, 'China's Sweeping Military Reforms: Implications for Australia', *Security Challenges*, 15.1 (2019), 33–46

Greenleaf, Graham, and Scott Livingston, 'China's Personal Information Standard: The Long March to a Privacy Law', *150 Privacy Laws & Business International Report 25-28*, 2017

Greenleaf, Graham, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (United Kingdom: Oxford University Press, 2014)

Haner, Justin, and Denise Garcia, 'The Artificial Intelligence Arms Race: Trends and World Leaders in Autonomous Weapons Development', *Global Policy*, 10.3 (2019), 331–37

Haroche, Pierre, 'Supranationalism Strikes Back: A Neofunctionalist Account of the European Defence Fund', *Journal of European Public Policy*, 2019, 1–20

High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (Brussels: European Commission, 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419> [accessed 25 March 2020]

———, 'Policy and Investment Recommendations for Trustworthy AI' (Brussels: European Commission, 2019) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343> [accessed 25 March 2020]

Horowitz, Michael C., 'Artificial Intelligence, International Competition, and the Balance of Power', *Texas National Security Review*, 1.3 (2018)

Johnson, Aaron M., and Sidney Axinn, 'The Morality of Autonomous Robots', *Journal of Military Ethics*, 12.2 (2013), 129–41

Kania, Elsa B., 'Chinese Military Innovation in the AI Revolution', *The RUSI Journal*, 164.5–6 (2019), 26–34

———, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Center for a New American Security, Washington DC, 2017) <https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805> [accessed 7 May 2020]

Kayali, Laura, Melissa Heikkilä, and Janosch Delcker, 'Europe's Digital Vision, Explained: The EU Is Rolling out Strategic Plans on Data, Artificial Intelligence and Platform Regulation.', Politico EU, 19 February 2020 <https://www.politico.eu/article/europes- digital-vision-explained/> [accessed 17 September 2020]

Korff, Douwe, Ben Wagner, Julia Powles, Renata Avila, and Ulf Buermeyer, *Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes* (University of Cambridge Faculty of Law Research Paper No. 16/2017, 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490> [accessed 4 June 2020]

Lancieri, Filippo Maria, 'Digital Protectionism? Antitrust, Data Protection, and the EU/US Transatlantic Rift', *Journal of Antitrust Enforcement*, 7.1 (2019), 27–53

Lee, Jyh-An, 'Hacking into China's Cybersecurity Law', *Wake Forest Law Review*, 53.1 (2018), 49

Lee, Kyu Yub, Moon hee Cho, Jungu Kang, and Minji Kang, 'Welfare Effects of the EU GDPR and Data Localization Measures', *KIEP Research Paper, World Economy Brief 19-07*, 9.7 (2019) <https://www.ssrn.com/abstract=3407208> [accessed 24 August 2020]

Liu, Nicole Ning, Carlos Wing-Hung Lo, Xueyong Zhan, and Wei Wang, 'Campaign-Style Enforcement and Regulatory Compliance', *Public Administration Review*, 75.1 (2015), 85–95

Loesekrug-Pietri, André, 'JEDI: Joint European Disruptive Initiative', 2018 <https://www.bundestag.de/resource/blob/556394/ff7f0a1f37e430410961b15ceb58e2b4/3--jedi-en-fr-data.pdf> [accessed 12 May 2020]

Long, William RM, Geraldine Scali, Francesca Blythe, and Alan Charles Raul, 'Chapter 2: EU Overview', in *The Privacy, Data Protection and Cybersecurity Law Review*, 6th edn (London: Law Business Research Ltd., 2019)

Lynskey, Orla, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, First edition (Oxford, United Kingdom: Oxford University Press, 2015)

Maizland, Lindsay, *China's Modernizing Military* (Council on Foreign Relations, 2020) <https://www.cfr.org/backgrounder/chinas-modernizing-military> [accessed 7 May 2020]

Manners, Ian, 'Normative Power Europe: A Contradiction in Terms?', *JCMS: Journal of Common Market Studies*, 40.2 (2002), 235–58

Manokha, Ivan, 'Surveillance: The DNA of Platform Capital—The Case of Cambridge Analytica Put into Perspective', *Theory & Event*, 21.4 (2018), 891–913

Mărcuț, Mirela *Crystalizing the EU Digital Policy: An Exploration into the Digital Single Market* (Switzerland, Cham: Springer International Publishing, 2017)

Markham, Annette N, Katrin Tiidenberg, and Andrew Herman, 'Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction', *Social Media + Society*, 4.3 (2018), 205630511878450

Markoff, John, and Matthew Rosenberg, 'China Gains on the U.S. in the Artificial Intelligence Arms Race', *The New York Times*, 4 February 2017 <https://cn.nytimes.com/world/20170204/artificial-intelligence-china-united-states/en-us/> [accessed 9 March 2020]

Martins, Bruno Oliveira, and Raluca Csernatoni, *The European Defence Fund: Key Issues and Controversies* (Peace Research Institute Oslo (PRIO), Oslo, 2019) <https://www.ies.be/files/PRIO_Policy_Brief_3-2019.pdf> [accessed 12 May 2020]

Martins, Bruno Oliveira, and Christian Küsters, 'Hidden Security: EU Public Research Funds and the Development of European Drones: Hidden Security: EU Public Research Funds and the Development of European Drones', *JCMS: Journal of Common Market Studies*, 57.2 (2019), 278–97

Mission Villani, 'For a Meaningful Artificial Intelligence: Towards a French and European Strategy', 2018 <https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf> [accessed 3 June 2020]

Mori, Satoru, 'US Defense Innovation and Artificial Intelligence', *Asia-Pacific Review*, 25.2 (2018), 16–44

Naughton, John 'Data Protection Laws Are Great. Shame They Are Not Being Enforced.', *The Guardian* (London, 2 May 2020) <https://www.theguardian.com/commentisfree/2020/may/02/data-protection-laws- are-great-shame-they-are-not-being-enforced> [accessed 16 September 2020]

no author, 'Florence Parly, Minister of the Armed Forces, Hails Success of the Firing Trials to Arm Drones', *Www.Defense-Aerospace.Com*, 2019 <https://www.defense-aerospace.com/article-view/release/208407/france-arms-reaper-drones-with-gbu_12-laser_guided-bombs.html> [accessed 13 May 2020]

———, 'Montreal Declaration for a Responsible Development of Artificial Intelligence' (Montreal: University of Montreal, 2018) <https://5dcfa4bd-f73a-4de5-94d8-

c010ee777609.filesusr.com/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf> [accessed 2 June 2020]

Nouveau, Patricia, 'Can Regulation Foster EU Entry to the Digital Race or Is It a Poor Substitute for a Truly EU-Driven Industrial Policy?' (presented at the Workshop on Economic Regulations in a Digital World, Toronto, Canada, 2019) <https://www.researchgate.net/publication/335602941_CAN_REGULATION_FOSTER_EU_ENTRY_TO_THE_DIGITAL_RACE_OR_IS_IT_A_POOR_SUBSTITUTE_FOR_A_TRULY_EU-DRIVEN_INDUSTRIAL_POLICY> [accessed 26 June 2020]

OECD, 'Guidelines on the Protection of Transborder Flow of Personal Data', 1980 <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [accessed 16 April 2020]

ORF.at, 'Schrems: EU-Datenschutzrecht "Nur Auf Dem Papier"', *www.orf.at* (Vienna, 25 May 2020) <https://orf.at/stories/3167007/> [accessed 16 September 2020].

Parasol, Max, 'The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams', *Computer Law & Security Review*, 34.1 (2018), 67–98

Perrault, Raymond, Yoav Shoham, Erik Brynjolfsson, Jack Clark, John Etchemendy, Barbara Grosz, and others, *The AI Index 2019 Annual Report* (Human-Centered AI Institute, Stanford University, 2019) <https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf> [accessed 25 March 2020]

PricewaterhouseCoopers, 'Sizing the Prize What's the Real Value of AI for Your Business and How Can You Capitalise', 2017 <https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf> [accessed 25 March 2020]

Rabinovitch, Ari, 'Israel Aerospace Signs $600 Million Drone Deal with Airbus for Germany', *Reuters*, 14 June 2018 <https://www.reuters.com/article/uk-il-aerospace-ind-airbus-nl-germany/israel-aerospace-signs-600-million-drone-deal-with-airbus-for-germany-idUSKBN1JA0N3> [accessed 13 May 2020]

Rathenau Instituut, *Human Rights in the Robot Age: Challenges Arising from the Use of Robotics, Artificial Intelligence, and Virtual and Augmented Reality* (The Hague: Council of Europe Report, 2017) <https://www.rathenau.nl/sites/default/files/2018-02/Human%20Rights%20in%20the%20Robot%20Age-Rathenau%20Instituut-2017.pdf> [accessed 3 June 2020]

Raul, Alan Charles, *The Privacy, Data Protection and Cybersecurity Law Review* (London: Law Business Research Ltd., 2019)

Raul, Alan Charles, Christopher C. Fonzone, and Snezhana Stadnik Tapia, 'Chapter 26: United States', in *The Privacy, Data Protection and Cybersecurity Law Review* (London: Law Business Research Ltd., 2019)

Sartor, Giovanni and Francesca Lagioia, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (EPRS, European Parliamentary Research Service, Brussels, 2020), p. 79 f <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [accessed 17 September 2020]

Sauer, Frank, *Artificial Intelligence in the Armed Forces: On the Need for Regulation Regarding Autonomy in Weapon Systems* (Federal Academy for Security Policy, 2018) <https://www.baks.bund.de/sites/baks010/files/working_paper_2018_26.pdf> [accessed 30 April 2020]

Scharre, Paul, 'Killer Apps: The Real Dangers of an AI Arms Race', *Foreign Affairs*, 98.3 (2019), 135–44

———, 'How Swarming Will Change Warfare', *Bulletin of the Atomic Scientists*, 74.6 (2018), 385–89

Scheipers, Sibylle, and Daniela Sicurelli, 'Normative Power Europe: A Credible Utopia', *JCMS: Journal of Common Market Studies*, 45.2 (2007), 435–57

Scholz, Lauren, 'Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies', *SSRN Electronic Journal*, 2018 <https://www.ssrn.com/abstract=3252543> [accessed 9 April 2020]

Schwartz, Paul M., 'Preemption and Privacy', *The Yale Law Journal*, 118.5 (2009), 902–47

Schwartz, Paul M., and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law', *Georgetown Law Journal*, 106.1 (2017), 115–79

Sehrawat, Vivek, 'Legal Status of Drones under LOAC and International Law', *Penn State Journal of Law & International Affairs*, 5.1 (2017), 164–206

Selbst, Andrew D, and Julia Powles, 'Meaningful Information and the Right to Explanation', *International Data Privacy Law*, 7.4 (2017), 233–42

Select Committee on Artificial Intelligence, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (Washington, D.C.: National Science and Technology Council Committee on Technology, 2019) <https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf> [accessed 13 August 2020]

Sieberson, Stephen C. 'Inching toward EU Supranationalism - Qualified Majority Voting and Unanimity under the Treaty of Lisbon', *Virginia Journal of International Law*, 50.4 (2010), 919–95

Stahl, Bernd Carsten, Job Timmermans, and Catherine Flick, 'Ethics of Emerging Information and Communication Technologies: On the Implementation of

Responsible Research and Innovation', *Science and Public Policy*, 44.3 (2017), 369–81

Strahilevitz, Lior, 'Towards a Positive Theory of Privacy Law', *Harvard Law Review*, 126.7 (2013), 2010–41

The Economist, 'The Algorithm Kingdom - China May Match or Beat America in AI | Business', *The Economist*, 15 July 2017 <https://www.economist.com/business/2017/07/15/china-may-match-or-beat-america-in-ai> [accessed 9 March 2020]

The Future Society, 'Making the AI Revolution Work for Everyone', 2017 <http://thefuturesociety.org/wp-content/uploads/2019/08/Making-the-AI-Revolution-work-for-everyone.-Report-to-OECD.-MARCH-2017.pdf> [accessed 3 June 2020]

The IEEE Initiative on Ethics of Autonomous and Intelligent Systems, 'Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems', 2017 <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v1.pdf> [accessed 6 February 2020]

The World Bank, 'GDP (Current US$): World Bank National Accounts Data, and OECD National Accounts Data Files' <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD> [accessed 23 September 2020].

Tolan, Songül, Marius Miron, Emilia Gómez, and Carlos Castillo, 'Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia', in *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law - ICAIL '19* (presented at the the Seventeenth International Conference, Montreal, QC, Canada: ACM Press, 2019), pp. 83–92 <http://dl.acm.org/citation.cfm?doid=3322640.3326705> [accessed 4 August 2020]

'Treaty of the Functioning of the European Union (TFEU)', 2012 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN> [accessed 20 April 2020]

US Department of Defense, 'Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge', 2018 <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf> [accessed 2 May 2020]

Vasilis, Trigkas, 'China Has Its DARPA, but Does It Have the Right People?', *The Diplomat*, 9 August 2017 <https://thediplomat.com/2017/08/china-has-its-darpa-but-does-it-have-the-right-people/> [accessed 7 March 2020]

Vesnic-Alujevic, Lucia, Melina Breitegger, and Ângela Guimarães Pereira, '"Do-It-Yourself" Healthcare? Quality of Health and Healthcare Through Wearable Sensors', *Science and Engineering Ethics*, 24.3 (2018), 887–904

Vincenti, Daniela, 'Return to the JEDI: European Disruptive Technology Initiative Ready to Launch', *Euractiv*, 16 March 2018 <https://www.euractiv.com/section/economy-jobs/news/return-of-the-jedi-european-disruptive-technology-initiative-ready-to-launch/> [accessed 12 May 2020]

Voss, W. Gregory, and Kimberly A. Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies', *American Business Law Journal*, 56.2 (2019), 287–344

Wang, You, and Dingding Chen, 'Rising Sino-U.S. Competition in Artificial Intelligence', *China Quarterly of International Strategic Studies*, 04.2 (2018), 241–58

Warren, Aiden, and Alek Hillas, 'Lethal Autonomous Weapons Systems: Adapting to the Future of Unmanned Warfare and Unaccountable Robots', *Yale Journal of International Affairs*, 12.1 (2017)

Warren, Samuel D., and Louis D. Brandeis, 'The Right to Privacy', *Harvard Law Review*, 4.5 (1890), 193–220

Whitman, James Q., 'The Two Western Cultures of Privacy Dignity Versus Liberty', *The Yale Law Journal*, 113.6 (2004), 1151–1221

Yang, Hongquan, 'Chapter 8: China', in *The Privacy, Data Protection and Cybersecurity Law Review*, 6th edn (London: Law Business Research Ltd., 2019)

Zhu, Guobin, 'The Right to Privacy: An Emerging Right in Chinese Law', *Statute Law Review*, 18.3 (1997)

VII. Index of abbreviations

AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
ATR	Automatic Target Recognition
AWS	Autonomous weapons systems
CAC	China Consumer Association
CCP	Chinese Communist Party
CCPA	California Consumer Privacy Act
CCW	Convention on Certain Weapons
CIA	Central Intelligence Agency
CMC	Central Military Commission
CSL	Cybersecurity Law
DARPA	Defense Advanced Research Project Agency
DL	Deep Learning
DoD	Department of Defense
DPA	Data protection authority
DPO	Data protection officer
DSB	Defence Science Board
DSM	Digital Single Market
ECJ	European Court of Justice
EDF	European Defence Fund
EDIDP	EU Defence Industrial Development Programme
EEAS	European External Action Service
EESC	European Economic and Social Committee
EU	European Union
EGE	European Group on Ethics and New Technologies
FCAS	Future Combat Air System
FTC	Federal Trade Commission
GDP	Gross domestic product
GDPR	General Data Protection Regulation
GPCL	General Principles of Civil Law
GPS	Global Positioning System
H2020	Horizon 2020
HLEG	High-Level Expert Group
IARPA	Intelligence Advanced Research Project Agency
ICC	International Criminal Court
ICRAC	International Committee for Robot Arms Control
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IHL	International Humanitarian Law
IP	Internet Protocol
ISR	Intelligence, Surveillance and Reconnaissance
JEDI	Joint European Disruptive Initiative
JRC	Joint Research Centre
LAWS	Lethal autonomous weapons systems

LOAC	Law of Armed Conflict
MIIT	Ministry of Industry and Information Technology
ML	Machine Learning
MOST	Ministry of Science and Technology
MPS	Ministry of Public Security
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NPCSC	National People's Congress Standing Committee
NPE	Normative Power Europe
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OFFSET	Offensive Swarm-Enabled Tactics
PADR	Preparatory Action on Defence Research
PII	Personally identifiable information
PLA	People's Liberation Army
PRC	People's Republic of China
PwC	PricewaterhouseCoopers
QMV	Qualified majority voting
R&D	Research and Development
RPVs	Remotely piloted vehicles
SCO	Strategic Capabilities Office
SME	Small and Medium Enterprises
TFEU	Treaty on the Functioning of the EU
UAV	Unmanned aerial vehicles
US	United States
USD	US-Dollar
WTO	World Trade Organization